

CM10196
Topic 5: Groups, Rings and Fields
A brief introduction to algebra

Guy McCusker

1W2.1

Data plus operations

In programming, and in mathematics, we are often interested in manipulating certain kinds of data in certain kinds of ways.

That means we are working with

- ▶ a collection of *data values*: that is to say, some kind of set
- ▶ a collection of *operations* on that set: ways of manipulating the data.

Usually, the operations we are using have particular properties that we exploit; for instance, if we put an element onto the front of a list, and then look at the front element of the list, we expect to get back the element we just put there. So we can add to our situation

- ▶ a collection of *equations* which describe how the operations work.

Example: lists

A data structure for "lists of numbers" might look as follows:

- ▶ the data we work with are the numbers (e.g. integers) and the lists
 - ▶ the operations we have are:
 - ▶ create an empty list
 - ▶ put an element onto a list
 - ▶ retrieve the first element of a list (the *head*)
 - ▶ retrieve the rest of the elements of the list (another list, called the *tail*)
 - ▶ the equations say things like
 - ▶ if we put n onto a list, the head of the resulting list is equal to n
 - ▶ if we put n onto a list l , the tail of the resulting list is equal to l
- and so on.

Algebra

The field of mathematics known as *algebra* studies exactly this kind of situation.

The basic plan of action in algebra is

- ▶ observe that certain collections of operations and equations are of interest in more than one setting
- ▶ define an abstract structure, called an *algebra*, which makes the operations and equations precise
- ▶ study the properties of these algebras at a general level
- ▶ apply the general properties to particular instances of the structure to find out useful facts.

We've already done this once, with *boolean algebras* in Topic 1.

Operations

What do we mean by *operations* on a set?

In this course, we will only study three kinds of operation:

- ▶ binary operations
- ▶ unary operations
- ▶ nullary operations

Binary operations

A binary operation takes two elements of the set and operates on them to give a third element.

Example

- ▶ addition is a binary operation on the integers
- ▶ conjunction and disjunction are binary operations on the truth values
- ▶ union and intersection are binary operations on $\mathcal{P}(A)$ for any set A
- ▶ subtraction of one number from another is a binary operation on the integers, but not on the natural numbers because for example $3 - 5$ does not give a natural number.

Unary operations

A unary operation takes a single element of a set and operates on it to give a new element.

Example

- ▶ The successor (add one) function is a unary operation on the natural numbers and on the integers
- ▶ Multiplication by -1 is a unary operation on the integers.
- ▶ Negation is a unary operation on the truth values.

Nullary operations

A nullary operation takes *no* elements of a sets as input, and gives an element as output.

That is, a nullary operation is just an element of a set, sometimes called a *constant*. When defining an algebra, the constants pick out particular elements that are of interest.

Example

- ▶ The constant values `true` and `false` are nullary operations on the set of truth values.
- ▶ Any natural number could be a constant in the set of natural numbers, but one of particular interest if we're doing addition is zero, because it's a *unit* for addition.

You shouldn't have too much trouble imagining that there are other kinds of operation: ternary ones (three inputs), infinitary ones (infinite number of inputs) and so on.

Operations are functions

When we describe a set with a binary operation on it, we'll have to give two pieces of data:

- ▶ the set itself; this will be some set A
- ▶ the operation; this will be a function $f : A \times A \rightarrow A$.

For instance, the set \mathbb{N} of natural numbers together with the addition function $+: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ is a "set with a binary operation".

If we wanted to specify a unary operation, we'd have to give a function $g : \mathbb{N} \rightarrow \mathbb{N}$.

To specify a nullary operation (a constant), we just give an element $n \in \mathbb{N}$.

Monoids

Let's define an algebra!

Definition

A *monoid* is given by

- ▶ a set A
- ▶ a binary operation on A , usually written as a dot (e.g. $a \cdot b$ denotes the result of applying the operation to elements a and b) or as concatenation ab
- ▶ a constant i.e. an element of A , usually called e , and referred to as the *unit* or *identity* of the monoid.

such that the following equations hold for all $a, b, c \in A$:

associativity $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

unit $a \cdot e = a$ and $e \cdot a = a$

Examples of monoids

- ▶ The natural numbers with the operation of addition and the constant 0 form a monoid; this works on the integers too.
- ▶ The natural numbers with the operation of multiplication and the constant 1 form a monoid; this works on the integers too.
- ▶ The truth values, with the operation of conjunction and the constant value `true` form a monoid.
- ▶ The truth values, with the operation of disjunction and the constant value `false` form a monoid.
- ▶ The collection of *finite lists of numbers*, with the operation of *concatenation* and the constant value *the empty list*, forms a monoid.

What about implication?

Can we make a monoid out of the implication operation?

The answer is no, because it is not associative:

$$\begin{aligned}(\text{false} \rightarrow \text{false}) \rightarrow \text{false} &= \text{false} \\ \text{false} \rightarrow (\text{false} \rightarrow \text{false}) &= \text{true}\end{aligned}$$

On the other hand, the operation of logical equivalence, \equiv , is associative, and `true` is a good unit for it, so we can make a monoid out of that.

Integers mod k

Arithmetic modulo k , for some nonzero natural number k , gives us a large and important class of monoids.

The underlying set we will work with is called $\mathbb{Z}/k\mathbb{Z}$ (for slightly complex reasons); all we need to know is that

$$\mathbb{Z}/k\mathbb{Z} = \{0, 1, 2, \dots, k-1\}.$$

We can then define *addition mod k* :

$a +_k b$ = the unique $c \in \mathbb{Z}/k\mathbb{Z}$ such that $a + b = nk + c$ for some integer n

and similarly *multiplication mod k* :

$a \times_k b$ = the unique $c \in \mathbb{Z}/k\mathbb{Z}$ such that $a \times b = nk + c$ for some integer n

Two monoids on the same set

This gives us two monoids on the same set:

- ▶ $\mathbb{Z}/k\mathbb{Z}$ with the operation of addition mod k , and the constant 0, is a monoid
- ▶ $\mathbb{Z}/k\mathbb{Z}$ with the operation of multiplication mod k and the constant 1 is a monoid.

Exercise

Suppose we consider the same set but without the element 0, and the operation of multiplication mod k . Is the operation well-defined on this smaller set? What if k is a prime?

The question is asking if, given a and b in $\mathbb{Z}/k\mathbb{Z} \setminus \{0\}$, the number $a \times_k b$ is still in the set.

Functions on a set

Let A be any set, and consider the set A^A , that is, the set of all functions from A to A .

Given f and $g : A \rightarrow A$, we can form a new function $g \circ f : A \rightarrow A$.

We know that

$$h \circ (g \circ f) = (h \circ g) \circ f$$

and also that, if we write id for the identity function on A ,

$$\text{id} \circ f = f \circ \text{id} = f.$$

All this says that

the set of functions from A to itself, with function composition as the binary operation and id as the constant, form a monoid.

Identities are unique

Let's prove a fact about monoids *in the abstract*, i.e. without talking about a particular monoid.

Theorem

In any monoid, there is exactly one identity element, i.e. exactly one element e such that $e \cdot a = a = a \cdot e$ for all a .

Proof We know from the definition of a monoid that there is at least one identity element, so we have to show that there cannot be more.

Suppose e_1 and e_2 both have the required property. Then

$$e_1 = e_1 \cdot e_2 = e_2$$

using the unit equation for e_2 to get the first equality, and the unit equation for e_1 to get the second. \square

The monoid of functions

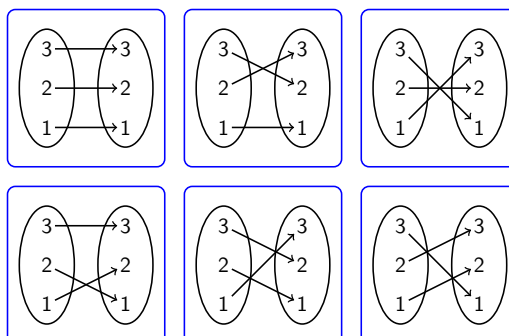
We can find *submonoids* of the monoid A^A :

- ▶ since the identity is 1-1, and composing two 1-1 functions gives another 1-1 function, the set of 1-1 functions forms a monoid with the same operation (composition) and the same unit (the identity function).
- ▶ similarly, all the onto functions form a monoid
- ▶ combining the above observations we can see that the bijective functions form a monoid too.

This last monoid, which we will call S_A , plays a very important role in mathematics. It is called the *symmetric monoid* on the set A .

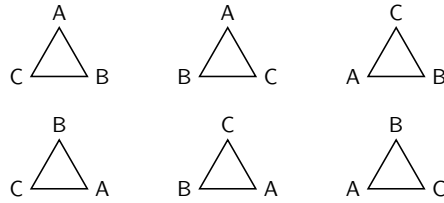
Symmetric monoid on $\{1, 2, 3\}$

Here are all six of the bijections from the set $\{1, 2, 3\}$ to itself.



Symmetries of a triangle

These six maps correspond to the six ways of drawing a triangle with corners labelled A, B and C:



Notice that each layout of the triangle can be obtained by rotating and reflecting the original one.

Inverses

The symmetries of a triangle (or any set) have a special property: each such map has an *inverse*, that is to say, another map you can compose it with to end up with the identity.

Monoids where every element has an inverse are the subject of a large and important area of algebra called *group theory*.

To make the idea of “monoid with inverses” precise, we’ll define a new kind of algebraic structure, called a group.

Groups

Definition

A *group* is given by

- ▶ a set A
- ▶ a binary operation on A (written with a dot or with concatenation, as before)
- ▶ a nullary operation (constant) called the unit or identity and written e
- ▶ a unary operation called *inverse*; the inverse of an element a is written a^{-1}

such that the following equations hold for all $a, b, c \in A$:

associativity $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

unit $a \cdot e = a$ and $e \cdot a = a$

inverse $a \cdot a^{-1} = e = a^{-1} \cdot a$.

Examples of groups

- ▶ The integers with addition as the operation, 0 as the unit, and $-n$ as the inverse of n , form a group.
- ▶ The non-zero rational numbers with multiplication as the operation, 1 as the unit, and $1/x$ as the inverse of x , form a group.
- ▶ The bijective functions from a set A to itself, with composition as the operation, the identity function as unit, and the inverse of a function as inverse, form a group S_A .

Non-examples of groups!

Some non-examples:

- ▶ The natural numbers with addition as the operation do not form a group because there's no inverse for any $n > 0$.
- ▶ The integers with multiplication do not form a group because no number other than 1 has an inverse.
- ▶ The rationals with multiplication do not form a group because 0 has no inverse.
- ▶ The 1-1 functions on a set do not form a group because a function which is not bijective does not have an inverse.

Inverses are unique

We already know (from the fact about monoids) that a group has exactly one identity element.

We can also show that every element has exactly one inverse:

Theorem

In any group, each element a has exactly one inverse, i.e. there is exactly one element b such that $a \cdot b = e = b \cdot a$.

Proof We know that a has at least one inverse because a^{-1} must exist by definition of a group. So we just show that there cannot be two inverses.

Suppose b_1 and b_2 are both inverses of a . Then

$$b_1 = b_1 \cdot e = b_1 \cdot (a \cdot b_2) = (b_1 \cdot a) \cdot b_2 = e \cdot b_2 = b_2.$$

□

Note that we used the property of associativity, as well as the fact that b_1 and b_2 are inverses of a and that e is a unit. All the group axioms are at

Facts about inverses

Knowing that inverses are unique lets us demonstrate a few simple facts which hold in every group.

Theorem

For any element a of a group. $(a^{-1})^{-1} = a$.

Proof Since inverses are unique, we just have to show that a is an inverse of a^{-1} . But this just means that

$$aa^{-1} = e = a^{-1}a$$

which is true because a^{-1} is the inverse of a . \square

Exercise

Show that, for any elements a and b of a group,

$$(ab)^{-1} = b^{-1}a^{-1}.$$

Cancellation laws

Theorem

In any group, for any a , b and c ,

- ▶ if $a \cdot b = a \cdot c$ then $b = c$
- ▶ if $b \cdot a = c \cdot a$ then $b = c$.

Exercise

Prove this. It's easy. Remember inverses exist.

The group $(\mathbb{Z}/n\mathbb{Z})^+$

For any natural number n , the set

$$\{0, 1, 2, \dots, n-1\}$$

can be given the structure of a group:

- ▶ the operation is addition modulo n
- ▶ the unit is 0
- ▶ the inverse of a is $n - a$.

The notation $(\mathbb{Z}/n\mathbb{Z})^+$ is used to denote this group.

The group $(\mathbb{Z}/p\mathbb{Z})^*$

Let p be any prime. We can turn the set

$$\{1, 2, \dots, p-1\}$$

into a group under the operation of multiplication mod p :

- ▶ 1 is the identity element
- ▶ it turns out that for any a in the set there is some b such that $a \times_p b = 1$, so inverses exist.

The notation $(\mathbb{Z}/p\mathbb{Z})^*$ is used for this group.

Let's check that inverses exist for the case $p = 5$:

- ▶ the inverse of 1 is 1: $1 \times 1 = 1$
- ▶ the inverse of 2 is 3: $2 \times 3 = 6 = 1 \pmod{5}$
- ▶ the inverse of 3 is 2: $3 \times 2 = 6 = 1 \pmod{5}$
- ▶ the inverse of 4 is 4: $4 \times 4 = 16 = 1 \pmod{5}$

Multiplication tables

Sometimes, for small groups, it can help to write out a *multiplication table*, showing how the binary operation of the group works.

For $(\mathbb{Z}/5\mathbb{Z})^*$, the multiplication table looks like this.

\cdot	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Cyclic groups

In this group, the element 3 is called a *generator*: if we look at the sequence

$$3, \quad 3 \cdot 3, \quad 3 \cdot 3 \cdot 3, \quad \dots$$

we reach every element of the group: the sequence is the same as

$$3, 4, 2, 1, 3, 4, 2, 1, \dots$$

Because multiplying by 3 takes us round and round this loop, hitting all the elements as we go, the group is called *cyclic*.

Exercise

Check that 2 is also a generator for the group. What about 1 and 4?

Order of a group and an element

The number of elements in a finite group is called its *order*. So the group we just saw is called the *cyclic group of order four*.

Given any element a of a group, we can look at the elements

$$a, a \cdot a, a \cdot a \cdot a, \dots$$

These are referred to as

$$a, a^2, a^3, \dots$$

We also define $a^0 = e$, the identity element.

The *order* of element a is the smallest $n > 1$ such that $a^n = e$.

Order of an element

Theorem

In a finite group, every element has a finite order.

Proof Write down the sequence of elements

$$a, a^2, a^3, a^4, \dots$$

This is an infinite sequence of elements of the group, but the group is finite so at some point we must find two elements the same. That is, there must be some m and n (with $m < n$, say) such that

$$a^m = a^n.$$

But this means $a^m = a^m \cdot a^{n-m}$. If we now multiply both sides by $(a^m)^{-1}$, we get

$$e = (a^m)^{-1} \cdot a^m = (a^m)^{-1} \cdot a^m \cdot a^{n-m} = e \cdot a^{n-m} = a^{n-m}$$

so the order of a is at most $n - m$. □

Cyclic groups again

A finite group of order n is a *cyclic group* if it has a generator.

A generator is just an element of order n , i.e. an element a such that

$$a, a^2, a^3, \dots, a^{n-1}$$

are all different, but

$$a^n = e,$$

which of course means that any a^k with $k \geq n$ is equal to one of

$$e, a, a^2, a^3, \dots, a^{n-1}.$$

The group $(\mathbb{Z}/n\mathbb{Z})^+$ again

For any n , the group $(\mathbb{Z}/n\mathbb{Z})^+$ is a cyclic group of order n .

The element 1 is always a generator: because the operation is addition (mod n), we have

$$\begin{aligned}1^1 &= 1 \\1^2 &= 2 \\&\vdots \\1^k &= k \\&\vdots \\1^{n-1} &= n-1 \\1^n &= 0\end{aligned}$$

Logarithms

In the real numbers, any positive number x has a *logarithm* base 2, which is to say a number y such that

$$2^y = x.$$

In any cyclic group with generator g , every element a can be written as g^n for some n . By analogy with the above, we refer to this n (actually, we use the smallest such n) as the *logarithm base g of a* .

The difficulty of computing the logarithm of a number in $(\mathbb{Z}/p\mathbb{Z})^*$ is the key to the cryptographic methods that make secure internet transactions possible.

If you're interested, research the *Diffie-Hellman algorithm* (easy exercise in using Google.)

Groups of symmetries

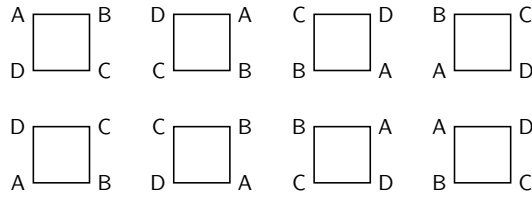
Another important collection of examples of groups are the *symmetries* on regular polygons. That is, for a given regular polygon, like an equilateral triangle or a square, pentagon etc., consider all the ways of *rotating* and *reflecting* it.

We've already seen this group (as a monoid) in the case of a triangle. In that case, every permutation of the set $\{1, 2, 3\}$ gave us an element of the group.

In general, for an n -sided polygon, the group of symmetries has $2n$ elements, while the group of all permutations of $\{1, 2, 3, \dots, n\}$ has $n!$ elements, so they're not the same.

Symmetries of the square

Below are the eight elements of the group of symmetries of a square.

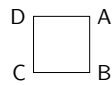


Symmetries and permutations

The symmetries of the square correspond to bijections on $\{A, B, C, D\}$ in an obvious way.

For each picture, construct a map which takes A to the element in the top-left, B to the top-right, C to the bottom-right and D to the bottom-left.

So for instance,



corresponds to the map

$$\begin{aligned} A &\mapsto D \\ B &\mapsto A \\ C &\mapsto B \\ D &\mapsto C \end{aligned}$$

Subgroups

If we have a group, sometimes we can find a subset of its elements which also forms a group, with the same operation, unit and inverse as the original group.

For instance, consider the set of permutations (bijective functions) on the three-element set $\{A, B, C\}$.

There are 6 of them, corresponding to the symmetries of the triangle we drew before.

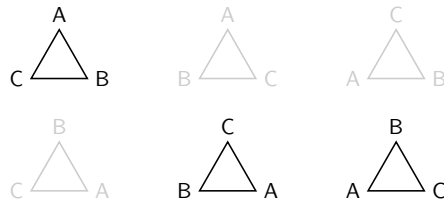
Three of these correspond to *rotations*, without any reflection. Since rotating and then rotating again gives another rotation, these three elements are *closed under composition*.

Thus these three themselves form a group.

(It's a cyclic group, again: rotating once is a generator, so we have the cyclic group of order three.)

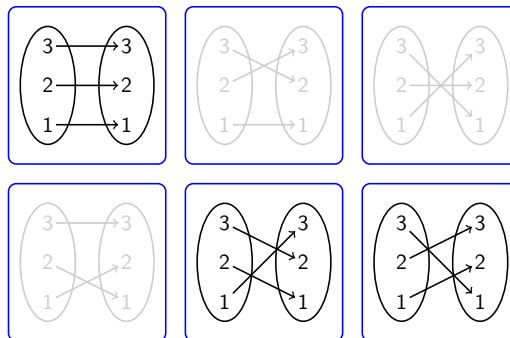
Rotations of the triangle

Here are all the symmetries of the triangle, with the ones that are not rotations drawn in grey.



Rotational permutations

Here are all six of the bijections from the set $\{1, 2, 3\}$ to itself, with the ones that are not rotations greyed out. Notice the way these bijections correspond to the symmetries of the triangle on the previous slide.



Abelian groups

A group is called *Abelian* if its binary operation is commutative: that is, if

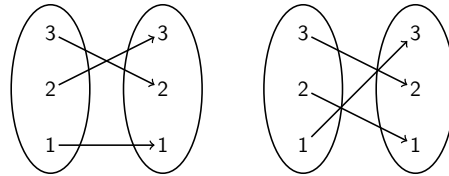
$$ab = ba$$

for all a and b in the group.

All the groups we've seen that are based on addition or multiplication of numbers are Abelian, because addition and multiplication are themselves commutative.

A non-Abelian group

The group of permutations on $\{1, 2, 3\}$ is not Abelian: consider composing the two maps



Composing one way round, 1 is sent to 1 and then to 3; composing the other way around, 1 is sent to 3 and then to 2. So the two compositions do not give the same map.

Rotations are Abelian

On the other hand, if we restrict to the rotations we get another Abelian group.

In fact, any cyclic group is Abelian: since every element can be written as g^n where g is the generator, we always have

$$g^n \cdot g^m = g^{n+m} = g^{m+n} = g^m \cdot g^n.$$

Rings

Notice that lots of our examples of groups seemed to be generalizations of ideas from arithmetic: multiplication or addition played a key role, for example.

In arithmetic, though, we are interested in *both* multiplication and addition at the same time (and more besides). That is to say, we care about more than one binary operation.

To talk about these things in general, we introduce the structure of a *ring*.

Rings

Definition

A *ring* is given by

- ▶ a set A
- ▶ a binary operation called *multiplication* on A , written \times
- ▶ a binary operation called *addition* on A , written $+$

such that

- ▶ there is an element 0 , and a unary operation taking each element a to $-a$, which make the set A with operation $+$ into an Abelian group.
- ▶ there is an element 1 which makes the set A with operation \times into a monoid
- ▶ multiplication distributes over addition:

$$a \times (b + c) = (a \times b) + (a \times c)$$

$$(a + b) \times c = (a \times c) + (b \times c)$$

Warning

What we've defined is sometimes called a *ring with 1* or *unitary ring*: sometimes rings are not required to have the unit for the multiplication operation.

Examples

- ▶ The integers with the usual operations of addition and multiplication of course form a ring.
- ▶ The rationals and the reals are rings with the usual operations.
- ▶ The set $\mathbb{Z}/n\mathbb{Z}$ is a ring, with the operations of addition mod n and multiplication mod n . Note that in this case $-a$ is the number $n - a$.

Some simple facts

Theorem

In any ring, for any a and b :

- ▶ $0 \times a = 0 = a \times 0$
- ▶ $(-a) \times b = a \times (-b) = -(a \times b)$

Proof For the first one, we calculate

$$0 + (0 \times a) = 0 \times a = (0 + 0) \times a = (0 \times a) + (0 \times a)$$

and then use the cancellation property of the group to deduce that $0 = 0 \times a$.

For the second one, we show that $(-a) \times b$ is an inverse of $a \times b$ with respect to $+$:

$$(a \times b) + (-a \times b) = (a + -a) \times b = 0 \times b = 0$$

and then use the fact that inverses are unique to deduce the equation we need. \square

Fields

Rings talk about addition and multiplication, but not division. We can request further structure to arrive at a *field*.

Definition

A *field* is a ring such that

- ▶ $0 \neq 1$
- ▶ multiplication is commutative
- ▶ for every $a \neq 0$, there exists a^{-1} such that $a \times a^{-1} = a^{-1} \times a = 1$.

To put it another way, the non-zero elements of the ring form an Abelian group.

Examples

- ▶ The integers do not form a field because division is not possible
- ▶ The rationals and the reals do form fields
- ▶ The rings $\mathbb{Z}/p\mathbb{Z}$ where p is prime are fields.
- ▶ If n is not prime, $\mathbb{Z}/n\mathbb{Z}$ is not a field, because multiplicative inverses do not exist.

No zero divisors

Theorem

In any field, if $a \times b = 0$ then at least one of a and b is zero.

Proof Suppose $a \times b = 0$. If $a = 0$, we're done. If $a \neq 0$, then a^{-1} exists, and we have

$$b = 1 \times b = (a^{-1} \times a) \times b = a^{-1} \times (a \times b) = a^{-1} \times 0 = 0.$$

□

This says that 0 has no interesting divisors; it is therefore said that a field has *no zero divisors*.

That's why $\mathbb{Z}/n\mathbb{Z}$ is not a field if n is not prime: if we have $a \times b = n$ where a and b are not zero or one, then $a \times_n b = 0$, so the structure cannot be a field.

And on into algebra...

The topic of algebra concerns the study of these kinds of structure in great depth. There are many amazing things that can be constructed and proved using the kinds of ideas we've seen here.

We have barely scratched the surface.

The most important ideas are here, though: the idea that we can *abstractly* capture the kinds of operations and equations we make use of, and reason about these structures at a *general level*.

Appendix 1: proving that $(\mathbb{Z}/p\mathbb{Z})^*$ is a group

We need to show that for every element a there is some b such that

$$a \times_p b = 1$$

i.e. that $ab = np + 1$ for some integer n .

To do this, we use a very interesting lemma:

Lemma

Let a and b be integers, and let c be the least positive integer of the form $ax + by$, where x and y are integers. Then c is the greatest common divisor of a and b .

Once we've got this lemma, the fact we need follows immediately: since the gcd of a and p is 1, we get

$$1 = ax + py$$

for some x and y , and then $a \times_p x = 1$.

Proving the lemma

We first show that the number c divides both a and b .

We know there is some m with $0 \leq m < c$ such that $a = nc + m$. But then

$$\begin{aligned}m &= a - nc \\ &= a - nax - nby \\ &= a(1 - nx) + b(-ny)\end{aligned}$$

Since c is the smallest integer of this form, and since $m < c$, we must have $m = 0$ i.e. c divides a . Similarly we show c divides b .

Proving the lemma

Finally we show that any number that divides both a and b divides c . This is easy.

Suppose n divides a and b . Then n divides ax and also by , so it divides $ax + by$, for any x and y . Hence n divides c .

So c is a divisor of both a and b , and any other common divisor divides c . Thus c is the greatest common divisor of a and b .

