2. The Euclidean algorithm and modular arithmetic

We will be interested in properties of the integers, $\mathbb{Z}$. Recall that $a \in \mathbb{Z}$ is a divisor of $b \in \mathbb{Z}$ if there exists $c \in \mathbb{Z}$ such that $b = ac$.

Lemma 2.1: For $a, b \in \mathbb{Z}$ with $b \neq 0$, there exist unique $q, r \in \mathbb{Z}$ such that

$$a = bq + r$$

with $0 \leq r < |b|$.

Proof: Consider $S = \{nb : n \in \mathbb{Z}\}$. Some of the elements in S are greater than a, and some are less than a. Let qb be the greatest element of S such that $qb \leq a$. Then by definition $qb + |b| > a$ and so $0 \leq a - qb < |b|$. Set $r = a - qb$. The uniqueness of q (and hence of r) is clear. □

Definition 2.2: For $b \in \mathbb{N}$ we write $r = a \mod b$ to mean than $a = bq + r$ for some $q \in \mathbb{Z}$ with $0 \leq r < b$. By Lemma 2.1, such an r always exists. More generally we write

$$x \equiv y \mod b$$

to mean that $x - y = bq$ for some $q \in \mathbb{Z}$. Note that $x \equiv y \mod b$ implies that $x \mod b = y \mod b$.

Note that if $r = 0$ then b is a divisor of a.

Given $a, b \in \mathbb{Z}$ non-zero we can consider the set of all positive integers that divide *both* a and b. There are only finitely many such integers (as they are all between 0 and a), and hence there must be a largest one.

Definition 2.3: Given $a, b \in \mathbb{Z}$ non-zero, their greatest common divisor, denoted GCD(a, b), or just (a, b), is the largest positive integer dividing a and b. If $(a, b) = 1$ we say that a and b are coprime.

We can find (a, b) efficiently using the Euclidean Algorithm.

Theorem 2.4: (The Euclidean Algorithm)
Given $a, b \in \mathbb{N}$ non-zero, with $b < a$, we set $r_{-1} = a$ and $r_0 = b$. Let

$$r_1 = r_{-1} \mod r_0$$

and continue recursively setting

$$r_i = r_{i-2} \mod r_{i-1}$$

(so that $r_{i-2} = r_{i-1}q_i + r_i$ for some $q_i \in \mathbb{Z}$) until get $r_{n+1} = 0$. Then $r_n = (a, b)$.

Proof: First notice that $r_1 > r_2 > \ldots \geq 0$, and so eventually there is an n such that $r_{n+1} = 0$.

Now suppose that x divides r_i *and* r_{i+1}. Then

$$r_i = r_{i+1}q_{i+2} + r_{i+2} \tag{1}$$

implies that x divides r_{i+2}. Next suppose that x divides r_{i+1} *and* r_{i+2}. Then again by (1) we see that x divides r_i. We have shown that the common divisors of r_i and r_{i+1} are the same as the common divisors of r_{i+1} and r_{i+2}.

Thus

$$(a, b) = (r_{-1}, r_0) = (r_0, r_1) = \cdots = (r_{n-1}, r_n).$$

But r_{n-1} is a multiple of r_n (as $r_{n+1} = 0$) and so

$$(r_{n-1}, r_n) = r_n$$

as required. □

Example 2.5: (i) Take $a = 72$ and $b = 30$. Set $r_{-1} = 72$ and $r_0 = 30$. Then

$$\begin{array}{lll} r_1 = 72 \mod 30 & & 72 = 2 \times 30 + 12 \\ \quad = 12 & & q_1 = 2 \\ r_2 = 30 \mod 12 & & 30 = 2 \times 12 + 6 \\ \quad = 6 & & q_2 = 2 \\ r_3 = 12 \mod 6 & & 12 = 2 \times 6 + 0 \\ \quad = 0 & & q_3 = 2 \end{array}$$

So $n = 2$ and $(72, 30) = r_2 = 6$.

(ii) Take $a = 176$ and $b = 52$. Set $r_{-1} = 176$ and $r_0 = 52$. Then

$$\begin{array}{lll} r_1 = 176 \mod 52 & & 176 = 3 \times 52 + 20 \\ \quad = 20 & & q_1 = 3 \\ r_2 = 52 \mod 20 & & 52 = 2 \times 20 + 12 \\ \quad = 12 & & q_2 = 2 \\ r_3 = 20 \mod 12 & & 20 = 1 \times 12 + 8 \\ \quad = 8 & & q_3 = 1 \\ r_4 = 12 \mod 8 & & 12 = 1 \times 8 + 4 \\ \quad = 4 & & q_4 = 1 \\ r_5 = 8 \mod 4 & & 8 = 2 \times 4 + 0 \\ \quad = 0 & & q_5 = 2 \end{array}$$

So $n = 4$ and $(176, 52) = r_4 = 4$.

Given $a, b \in \mathbb{N}$ with $b < a$ we have defined sequences r_i and q_i, with $r_{-1} = a$, $r_0 = b$, and $r_{i-2} = r_{i-1}q_i + r_i$ for $1 \leq i \leq n$. We have seen that $(a, b) = r_n$.

The following pairs of sequences will also be very useful.

Let $x_0 = 1$, $x_1 = 0$ and for $1 \leq i \leq n$

$$x_{i+1} = q_i x_i + x_{i-1}.$$

Let $y_0 = 0$, $y_1 = 1$ and for $1 \leq i \leq n$

$$y_{i+1} = q_i y_i + y_{i-1}.$$

Proposition 2.6: For $0 \leq i \leq n+1$ we have

$$r_{i-1} = (-1)^i x_i a + (-1)^{i+1} y_i b.$$

Proof: We will proceed by induction on i. First note that

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

and

$$r_0 = b = (-1)^1 \times 0 \times a + (-1)^2 \times 1 \times b$$

as required.

Now suppose that the result is true for r_{i-1} and r_{i-2}. We want that it is also true for r_i. By definition

$$\begin{aligned} r_i &= r_{i-2} - r_{i-1} q_i \\ &= (-1)^{i-1} x_{i-1} a + (-1)^i y_{i-1} b - ((-1)^i x_i a + (-1)^{i+1} y_i b) q_i \\ &= ((-1)^{i-1} x_{i-1} - (-1)^i x_i q_i) a + ((-1)^i y_{i-1} - (-1)^{i+1} y_i q_i) b \\ &= (-1)^{i-1} (x_{i-1} + x_i q_i) a + (-1)^i (y_{i-1} + y_i q_i) b \\ &= (-1)^{i-1} x_{i+1} a + (-1)^i y_{i+1} b \\ &= (-1)^{i+1} x_{i+1} a + (-1)^{i+2} y_{i+1} b \end{aligned}$$

as required. The result follows by induction. □

The importance of this result is the following corollary.

Corollary 2.7: (Bezout's identity)
Let $a, b \in \mathbb{N}$. Then there exists $u, v \in \mathbb{Z}$ such that

$$(a, b) = ua + vb.$$

Proof: We have

$$(a, b) = r_n = (-1)^{n+1} x_{n+1} a + (-1)^{n+2} y_{n+1} b$$

and hence can take $u = (-1)^{n+1} x_{n+1}$ and $v = (-1)^{n+2} y_{n+1}$. □

Notice that Corollary 2.7 not only shows that u, v exist, but also gives a procedure for calculating them (using x_i and y_i). Calculating the x_i and y_i as well as the r_i and q_i is known as the extended Euclidean algorithm.

Notice also that for any $u, v \in \mathbb{Z}$ non-zero, $ua + vb$ must be a multiple of (a, b), and so Bezout's identity gives the smallest positive integer x such that

$$x = au + vb$$

with $u, v \in \mathbb{Z}$.

Corollary 2.8: $a, b \in \mathbb{N}$ are coprime if and only if there exist $u, v \in \mathbb{Z}$ with

$$1 = ua + vb.$$

Example 2.9: We return to Example 2.5 for the Euclidean algorithm.
(i) Take $a = 72$ and $b = 30$. We saw that $(a, b) = 6$ and $n = 2$ with $q_1 = q_2 = q_3 = 2$.
Set $x_0 = 1$ and $x_1 = 0$. Then

$$\begin{aligned} x_2 &= q_1 x_1 + x_0 = 2 \times 0 + 1 = 1 \\ x_3 &= q_2 x_2 + x_1 = 2 \times 1 + 0 = 2 \end{aligned}$$

Set $y_0 = 0$ and $y_1 = 1$. Then

$$\begin{aligned} y_2 &= q_1 y_1 + y_0 = 2 \times 1 + 0 = 2 \\ y_3 &= q_2 y_2 + y_1 = 2 \times 2 + 1 = 5 \end{aligned}$$

So $u = (-1)^3 x_3 = -2$ and $v = (-1)^4 y_3 = 5$. Indeed

$$-2 \times 72 + 5 \times 30 = -144 + 150 = 6 = (a, b).$$

(ii) Take $a = 176$ and $b = 52$. We saw that $(a, b) = 4$ and $n = 4$ with $q_1 = 3$, $q_2 = 2$, $q_3 = q_4 = 1$.
Set $x_0 = 1$ and $x_1 = 0$. Then

$$\begin{aligned} x_2 &= q_1 x_1 + x_0 = 3 \times 0 + 1 = 1 \\ x_3 &= q_2 x_2 + x_1 = 2 \times 1 + 0 = 2 \\ x_4 &= q_3 x_3 + x_2 = 1 \times 2 + 1 = 3 \\ x_5 &= q_4 x_4 + x_3 = 1 \times 3 + 2 = 5 \end{aligned}$$

Set $y_0 = 0$ and $y_1 = 1$. Then

$$\begin{aligned} y_2 &= q_1 y_1 + y_0 = 3 \times 1 + 0 = 3 \\ y_3 &= q_2 y_2 + y_1 = 2 \times 3 + 1 = 7 \\ y_4 &= q_3 y_3 + y_2 = 1 \times 7 + 3 = 10 \\ y_5 &= q_4 y_4 + y_3 = 1 \times 10 + 7 = 17 \end{aligned}$$

So $u = (-1)^5 x_5 = -5$ and $v = (-1)^6 y_5 = 17$. Indeed

$$-5 \times 176 + 17 \times 52 = -880 + 884 = 4 = (a, b).$$

Consider the days of the week. These repeat cyclically, and after 7 days we return to where we started (and similarly with the hours of the day). Often we do only care which day of the week it is and not which week — for example Ciphers and Number Theory is on Mondays.

In a similar way it will be useful to consider the integers modulo n, rather than the integers themselves. We will now show how to define a modular version of arithmetic.

Fix $n \in \mathbb{N}$ and set $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$. Given $z \in \mathbb{Z}$ there exists (by Lemma 2.1) a unique $\overline{z} \in \mathbb{Z}_n$ such that $\overline{z} = z \mod n$. We would like to define addition, subtraction, multiplication, and (if possible) division in $\mathbb{Z}_n$.

Definition 2.10: Given $x, y \in \mathbb{Z}_n$ we define $x \oplus y$, $x \ominus y$, and $x \otimes y$ in $\mathbb{Z}_n$ by

$$\begin{aligned} x \oplus y &= \overline{x + y} \\ x \ominus y &= \overline{x - y} \\ x \otimes y &= \overline{xy}. \end{aligned}$$

Example 2.11: If $x = 5$, $y = 7$, and $n = 9$ then

$$\begin{aligned} x \oplus y &= \overline{5+7} = \overline{12} = 3 \\ x \ominus y &= \overline{5-7} = \overline{-2} = 7 \\ x \otimes y &= \overline{5 \times 7} = \overline{35} = 8. \end{aligned}$$

Lemma 2.12: If $x, y \in \mathbb{Z}$ with $\overline{x} = x \mod n$ and $\overline{y} = y \mod n$ then

$$\begin{array}{rcl} x + y \mod n & = & \overline{x} \oplus \overline{y} \\ x - y \mod n & = & \overline{x} \ominus \overline{y} \\ x \times y \mod n & = & \overline{x} \otimes \overline{y} \end{array}$$

Proof: Let $x = \overline{x} + pn$ and $y = \overline{y} + qn$ for some $p, q \in \mathbb{Z}$. Then

$$\begin{array}{rcl} x + y & = & \overline{x} + \overline{y} + pn + qn \\ & = & \overline{x} + \overline{y} + (p + q)n \\ & \equiv & \overline{x} + \overline{y} \mod n \quad = \quad \overline{x} \oplus \overline{y}. \end{array}$$

A similar argument holds for $x - y$. For $x \times y$ we have

$$\begin{array}{rcl} x \times y & = & (\overline{x} + pn)(\overline{y} + qn) \\ & = & \overline{x} \times \overline{y} + n(p\overline{y} + q\overline{x} + pqn) \\ & \equiv & \overline{x} \times \overline{y} \mod n \quad = \quad \overline{x} \otimes \overline{y}. \end{array}$$

□

Example 2.13: Let $x = 8$, $y = 9$, and $n = 5$. Then

$$x = 3 \mod 5 \qquad y = 4 \mod 5$$

and

$$xy \mod 5 = 72 \mod 5 = 2$$

while

$$\overline{x} \otimes \overline{y} = 3 \times 4 \mod 5 = 12 \mod 5 = 2.$$

Thus

$$xy \mod 5 = \overline{x} \otimes \overline{y}.$$

From now on we will just use the ordinary $+, -, \times$ symbols instead of $\oplus, \ominus, \otimes$, as Lemma 2.12 says that these are the same operations mod n.

Lemma 2.14: If $a \equiv b \mod n$ and $c \equiv d \mod n$ then

$$ac \equiv bd \mod n.$$

Proof: By assumption we have $\overline{a} = \overline{b}$ and $\overline{c} = \overline{d}$. Now the result follows from Lemma 2.12. □

Example 2.15: Find the remainder when 2^{101} is divided by 7.
We have

$$2^{101} = (2^3)^{33} \times 2^2$$

and

$$2^3 = 8 \equiv 1 \mod 7.$$

Therefore

$$2^{101} \equiv 8^{33} \times 4 \equiv 1^{33} \times 4 \equiv 1 \times 4 \equiv 4 \mod 7$$

and so the remainder is 4.

This example begins to illustrate the usefulness of modular arithmetic.

We would line to be able to divide as well as multiply. But there is a problem.

What does $z = x/y$ mean? It means that $z = xy^{-1}$ where y^{-1} is a number such that $y^{-1}y = 1$.

So can we find a number $y^{-1} \in \mathbb{Z}_n$ for each $y \in \mathbb{Z}_n$ such that

$$y^{-1}y = 1 \mod n?$$

(Of course, we cannot expect to do this for $y = 0$.)

Also, such an element y^{-1} had better be unique!

Example 2.16: Suppose that $n = 6$ and $y = 2$.
If y^{-1} exists then $y^{-1} \in \{0, 1, 2, 3, 4, 5\}$ with

$$yy^{-1} = 2y^{-1} \equiv 1 \mod 6.$$

We have

$$\begin{array}{rcl} 0 \times 2 & = & 0 \quad \equiv \quad 0 \mod 6 \\ 1 \times 2 & = & 2 \quad \equiv \quad 2 \mod 6 \\ 2 \times 2 & = & 4 \quad \equiv \quad 4 \mod 6 \\ 3 \times 2 & = & 6 \quad \equiv \quad 0 \mod 6 \\ 4 \times 2 & = & 8 \quad \equiv \quad 2 \mod 6 \\ 5 \times 2 & = & 10 \quad \equiv \quad 4 \mod 6 \end{array}$$

and so there is *no* inverse to 2 in $\mathbb{Z}_6$.

We had similar problems when we first defined division in $\mathbb{Z}$. In that case we added extra numbers to form $\mathbb{Q}$. In this case we will leave $\mathbb{Z}_n$ unchanged but instead put restrictions on n to prevent such bad examples.

Before working out what restrictions we need on n to have a well-defined inverse to $y \mod n$, we need the following consequence of Bezout's identity.

Lemma 2.17: Suppose that $a, b \in \mathbb{N}$ with $(a, b) = 1$, and that a divides bn. Then a divides n.

Proof: By assumption we have $bn = am$ for some $m \in \mathbb{Z}$. Bezout's identity (2.7) implies that there exist $u, v \in \mathbb{Z}$ such that

$$1 = (a, b) = ua + vb.$$

So

$$\begin{array}{rcl} n & = & uan + vbn \\ & = & uan + vam \\ & = & a(un + vm). \end{array}$$

Clearly $un + vm \in \mathbb{Z}$ and so a divides n. □

Theorem 2.18: The equation $xy \equiv 1 \mod n$ has a solution if and only if $(y, n) = 1$. If there is a solution then it is unique modulo n.

Proof: Let $g = (y, n)$ and suppose that $xy \equiv 1 \mod n$. Then g divides $xy - 1$ as $xy - 1$ is divisible by n and g divides n. But g divides xy as g divides y, and so g divides 1. Hence $g = 1$. Thus $xy \equiv 1 \mod n$ implies that $g = 1$.

Now suppose that $g = 1$. By Bezout's identity there exist $u, v \in \mathbb{Z}$ such that $1 = uy + vn$, and hence $1 \equiv uy \mod n$. So $x = u$ is a solution to the given equation.

Finally, suppose that x_1 and x_2 are two solutions to the given equation. Then

$$x_1 y \equiv 1 \equiv x_2 y \mod n$$

and so $(x_1 - x_2)y$ is divisible by n. But $(y, n) = 1$ implies (by Lemma 2.17) that $x_1 - x_2$ is divisible by n; that is $x_1 \equiv x_2 \mod n$. □

By the last result, if $(y, n) = 1$ then we can define y^{-1} to be the unique element of $\mathbb{Z}_n$ such that $y^{-1}y \equiv 1 \mod n$.

Obviously this is not possible when $y = 0$, but we would like this to be the only impossible case.

Corollary 2.19: There are inverses to all non-zero elements of $\mathbb{Z}_n$ if and only if n is prime.

Proof: If n is prime then $(y, n) = 1$ for all non-zero $y \in \mathbb{Z}_n$, and so y^{-1} exists by Theorem 2.18.

If $n = ab$ with $1 < a, b < n$ then $(a, n) = a > 1$ and so a^{-1} does not exist in $\mathbb{Z}_n$ by Theorem 2.18. □

Thus when n is prime we can define division in $\mathbb{Z}_n$ by setting $x/y = xy^{-1}$.

It is easy to check that $\mathbb{Z}_p$ with p prime satisfies all the usual properties for $+, -, \times, /$ that we expect, eg

$$(x+y)+z = x+(y+z) \quad \text{and} \quad x(y+z) = xy+xz.$$

Sets with these nice properties are called fields; other examples include $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, but *not* $\mathbb{N}$ or $\mathbb{Z}$. [We wont give the precise definition here.]

So now we have a *finite* set in which we can add, subtract, multiply, and divide.

Example 2.20: (i) Let $n = 5$. Here is the multiplication table for $\mathbb{Z}_5$.

$\times$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

From this we see that

$$1^{-1} = 1 \quad 2^{-1} = 3 \quad 3^{-1} = 2 \quad 4^{-1} = 4.$$

Thus, for example, in $\mathbb{Z}_5$ we have

$$\begin{array}{rclclcl} 2/4 & = & 2 \times 4^{-1} & = & 2 \times 4 & = & 3 \\ 3/2 & = & 3 \times 2^{-1} & = & 3 \times 3 & = & 4. \end{array}$$

(ii) Let $n = 4$. Here is the multiplication table for $\mathbb{Z}_4$.

$\times$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Thus the element 2^{-1} does not exist in $\mathbb{Z}_4$ (as Theorem 2.18 predicts, since $(2,4) \neq 1$). But we can define $1^{-1} = 1$ and $3^{-1} = 3$ in $\mathbb{Z}_4$.