7. Modular arithmetic

In this section we introduce modular arithmetic, which might also be called clock arithmetic. If we use a twelve hour clock then 14:00 is the same as 2, and so on.

Definition 7.1. *Let a and b be two integers and let m be a natural number. We say that a is **congruent** to b **modulo** m, denoted $a \equiv b \mod m$, if $a - b$ is divisible by m.*

For example, $a = 10$ and $b = 16$ are congruent modulo 3 as $16 - 10 = 6 = 3 \cdot 2$.

Note that if a is an integer then a, $a+m$, $a+2m$, $\dots a-m$, $a-2m$, $\dots$, are all congruent to a modulo m and the set of all integers congruent to a modulo m is

$$[a] = \{\, a + km \,|\, k \in \mathbb{Z} \,\}.$$

It is convenient to introduce a little bit of abstraction:

Definition 7.2. *Let X be a set. An **equivalence relation** $\sim$ is a relation on X, which is*

reflexive: *For every $x \in X$, $x \sim x$.*
symmetric: *For every x and $y \in X$, if $x \sim y$ then $y \sim x$.*
transitive: *For every x and y and $z \in X$, if $x \sim y$ and $y \sim z$ then $x \sim z$.*

Lemma 7.3. *Let $\sim$ be the relation on $\mathbb{Z}$*

$$a \sim b \qquad \textit{if and only if} \qquad a \equiv b \mod m.$$

Then $\sim$ is an equivalence relation.

Proof. There are three things to check.

First we check reflexivity. Suppose that $a \in \mathbb{Z}$ is an integer. Then $a - a = 0$ is divisible by m. But then $a \sim a$ by definition of $\sim$ and $\sim$ is reflexive.

Now we check symmetry. Suppose that a and b are integers and that $a \sim b$. Then $a - b$ is divisible by m. Thus there is an integer k such that $a - b = mk$. In this case

$$\begin{aligned} b - a &= -(a - b) \\ &= -mk \\ &= m(-k). \end{aligned}$$

But then by definition $b \sim a$. Thus $\sim$ is symmetric.

Finally we check transitivity. Suppose that $a \sim b$ and $b \sim c$. Then $a - b$ is divisible by m and $b - c$ is divisible by m. Thus there are integers p and q such that $a - b = mp$ and $b - c = mq$. On the other hand

$$\begin{aligned} a - c &= (a - b) + (b - c) \\ &= mp + mq \\ &= m(p + q). \end{aligned}$$

Thus $a - c$ is divisible by m and so $a \sim c$. Thus $\sim$ is transitive.

As $\sim$ is reflexive, symmetric and transitive, it is an equivalence relation. □

On the other hand if we are given an equivalence relation, the natural thing to do is to look at its equivalence classes.

Definition 7.4. *Let $\sim$ be an equivalence relation on a set X. Let $a \in X$ be an element of X. The **equivalence class** of a is*

$$[a] = \{\, b \in X \,|\, b \sim a \,\}.$$

We have already seen that the equivalence classes of the equivalence relation given above are

$$[a] = \{\, a + km \,|\, k \in \mathbb{Z} \,\}.$$

In general we denote the set of all equivalence classes by $\mathbb{Z}_m$.

Definition 7.5. *Let X be a set. A **partition** P of X is a collection of non-empty subsets A_i, $i \in I$, such that*

(1) The A_i cover X, that is

$$\bigcup_{i \in I} A_i = X.$$

(2) The A_i are pairwise disjoint, that is, if $i \neq j$ then

$$A_i \cap A_j = \emptyset.$$

$m = 2$ then the equivalence relation above divides the integers into two parts, the evens and the odds.

Lemma 7.6. *Given an equivalence relation $\sim$ on X there is a unique partition of X. The elements of the partition are the equivalence classes of $\sim$ and vice-versa. That is, given a partition P of X we may construct an equivalence relation $\sim$ on X such that the partition associated to $\sim$ is precisely P.*

Concisely, the data of an equivalence relation is the same as the data of a partition.

Note that clock arithmetic makes sense. If it is 9 o'clock and you want to meet someone six hour later, you are going to meet them at 3 o'clock.

Lemma 7.7. *Fix a natural number m.*

If a and b are congruent modulo m and c and d are congruent modulo m then

$$a + c \equiv b + d \mod m \qquad \textit{and} \qquad a \cdot c \equiv b \cdot d \mod m.$$

Proof. By assumption there are integers p and q such that $a - b = mp$ and $c - d = mq$. It follows that $a = b + mp$ and $c = d + mq$. In this case

$$\begin{aligned} a + c &= (b + mp) + (d + mq) \\ &= b + d + mp + mq \\ &= (b + d) + m(p + q). \end{aligned}$$

Thus $(a + c) \equiv (b + d) \mod m$. Similarly

$$\begin{aligned} a \cdot c &= (b + mp) \cdot (d + mq) \\ &= bd + bmq + mpd + mpmq \\ &= bd + m(bq + pd + mpq). \end{aligned}$$

Thus $(a \cdot c) \equiv (b \cdot d) \mod m$. □

(7.7) looks innocuous but it is actually remarkably useful. It says we can add and multiply equivalence classes together and get well-defined answers:

$$[a] + [c] = [a + c] \qquad \text{and} \qquad [a] \cdot [c] = [ac].$$

To add together two equivalence classes, pick elements of each and add those together to get another equivalence class. To multiply together two equivalence classes, pick elements of each and multiply those together to get another equivalence class.

One easy example is as follows. If $m = 2$ then the equivalence classes are odd and even. even plus even is even, odd plus odd is even and odd plus even is odd. Similarly, even times even is even, odd times odd is odd and odd times even is odd.

It is important to realise that defining a function simply by picking representatives usually does not work. For example, imagine assigning a month of the year to a letter of the alphabet as follows. Define an equivalence relation on the set of undergraduates by declaring two undergraduates to be equivalent if they have the same first initial.

The equivalence classes are the set of all first initials, that is, the alphabet. Define a function from the equivalence classes to the months of the year, by picking an undergraduate with that first initial and taking the month of their birth. It is clear this function is not going to be well-defined. There will be plenty of people in the equivalence class J and it is inconceivable they were all born the same month.

Theorem 7.8. *Fix a natural number $m > 1$.*

The equivalence classes $\mathbb{Z}_m$ is a ring, with addition and multiplication defined above.

Proof. All of the axioms for a ring follow automatically, once we know we have a well-defined addition and multiplication. [0] plays the role of zero, [1] plays the role of one, $[0] \neq [1]$ as $m > 1$, $-[a] = [-a]$ and it is easy to check all of the axioms. □

When $m = 2$, the evens are zero and the odds are one. This actually forces the rules for addition and multiplication.

Let us look at a simple example. Suppose we take $m = 6$. It is not hard to see that

$$[0], \quad [1], \quad [2], \quad [3], \quad [4], \quad \text{and} \quad [5],$$

exhaust all equivalence classes. We have the following addition and multiplication tables

+	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[2]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[3]

×	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[0]	[2]	[4]	[0]	[2]	[4]
[3]	[0]	[3]	[0]	[3]	[0]	[3]
[4]	[0]	[4]	[2]	[0]	[4]	[2]
[5]	[0]	[5]	[4]	[3]	[2]	[1].

Note that even though we have a ring, we don't have an integral domain. For example,

$$\begin{aligned} [2] \cdot [3] &= [2 \cdot 3] \\ &= [6] \\ &= [0]. \end{aligned}$$

Thus there are two non-zero elements of $\mathbb{Z}_6$, [2] and [3], whose product is zero.

Definition 7.9. *Let $\phi \colon R \longrightarrow S$ be a function between two rings. We say that ϕ is a ring homomorphism if ϕ all of the ring operations,*

$$\phi(a + b) = \phi(a) + \phi(b) \qquad \phi(a \cdot b) = \phi(a) \cdot \phi(b) \qquad \text{and} \qquad \phi(1) = 1.$$

Using (7.9) we can summarise everything we have done in this lecture by saying that the function

$$\phi\colon \mathbb{Z} \longrightarrow \mathbb{Z}_m \qquad \text{given by} \qquad \phi(a) = [a],$$

is a ring homomorphism.

Let us finish by giving some applications of modular arithmetic. We already mentioned that Fermat proved (observed?) that any natural number is the sum of four squares. He also proved that if a prime is congruent to 1 modulo 4, so that it is of the form $4k + 1$, then it is the sum of two squares.

Let's show the reverse direction, for any odd prime. The trick is to compute the possible congruence classes of squares. Suppose that a is an integer. We can write $a = 4k + r$, where $r = 0$, 1, 2 or 3. Then

$$\begin{aligned} a^2 &= (4k + r)^2 \\ &= 16k^2 + 8kr + r^2 \\ &\equiv r^2 \mod 8. \end{aligned}$$

Thus a^2 is congruent to r^2. But

$$0^2 = 0 \qquad 1^2 = 1 \qquad 2^2 = 4 \equiv 0 \mod 4 \qquad \text{and} \qquad 3^2 = 9 \equiv 1 \mod 4.$$

Thus we only get 0 or 1. In the language of equivalence classes,

$$\begin{aligned} [a]^2 &= [a^2] \\ &= [r^2], \end{aligned}$$

and $[r^2] = [0]$ or $[1]$. Thus if p is a prime and $p = a^2 + b^2$ then

$$[p] = [a^2] + [b^2],$$

so that

$$\begin{aligned} [p] &= [0] + [0] = [0] \\ [p] &= [0] + [1] = [1] \\ [p] &= [1] + [0] = [1] \\ [p] &= [1] + [1] = [2], \end{aligned}$$

that is, $[p] = [0]$, $p = [1]$ or $p = [2]$. As p is odd, we must have $[p] = [1]$, so that $p = 4k + 1$, for some integer k.

Theorem 7.10. *Let $m > 1$ be an integer. Let $f(x_1, x_2, \dots, x_n)$ be a polynomial in the variables $x_1, x_2, \dots, x_n$ with integer coefficients. If $a_1, a_2, \dots, a_n$ and $b_1, b_2, \dots, b_n$ are two sequences of integers and $a_j \equiv b_j \mod m$ then $f(a_1, a_2, \dots, a_n) \equiv f(b_1, b_2, \dots, b_n) \mod m$.*

We skip the proof of (7.10). We give a proof in the homework for one variable and the general case proceeds by induction on n. The key point is to realise that any polynomial is built up by repeated addition and multiplication, so the result follows from the fact that equivalence modulo m respects addition and multiplication.

We will need two results.

Theorem 7.11. *Let k be a non-zero integer.*

If $(k, m) = d$ and $ka \equiv kb \mod m$ then $a \equiv b \mod (m/d)$.

Proof. Suppose first that $d = 1$. We may find integers λ and μ such that

$$1 = \lambda k + \mu m.$$

If we multiply both sides by $a - b$ we get

$$a - b = \lambda k(a - b) + \mu m.$$

By assumption m divides $k(a - b)$ and so m divides $a - b$. But then $a \equiv b \mod m$.

In general, note that $(k/d, m/d) = 1$. As m divides $k(a-b)$ it follows that m/d divides $(k/d)(a - b)$. Thus $(k/d)a \equiv (k/d)b \mod m/d$ and by what we already proved we conclude that $a \equiv b \mod (m/d)$. □

Theorem 7.12. *Let $m > 1$ be an integer.*

(1) If m is composite then $\mathbb{Z}_m$ is not an integral domain.

(2) If p is prime then $\mathbb{Z}_p$ is a field.

In particular $\mathbb{Z}_m$ is an integral domain if and only if m is prime.

Proof. Suppose that m is composite. Then $m = ab$, for integers $a > 1$ and $b > 1$. In particular $a < m$ and $b < m$.

In this case

$$\begin{aligned} [a] \cdot [b] &= [a \cdot b] \\ &= [m] \\ &= [0] \\ &= 0. \end{aligned}$$

As $[a] \neq 0$ and $[b] \neq 0$, this shows that $\mathbb{Z}_m$ is not an integral domain. This is (1).

Now suppose that p is a prime. We have to show that every non-zero element of $\mathbb{Z}_p$ is a unit, that is, every element has a multiplicative inverse. The non-zero elements of $\mathbb{Z}$ are represented by integers a that are not multiples of p. As p is a prime number, it follows that $(a, p) = 1$. But then we may find integers λ and μ such that

$$1 = \lambda a + \mu p.$$

It follows that

$$\begin{aligned} 1 &= [1] \\ &= [\lambda a + \mu p] \\ &= [\lambda][a] + [\mu][p] \\ &= [\lambda][a]. \end{aligned}$$

Thus $[\lambda]$ is the inverse of $[a]$. It follows that every non-zero element of $\mathbb{Z}_p$ is a unit. □