Chapter 4

Modular arithmetic

4.1 The modular ring

Definition 4.1. *Suppose $n \in \mathbb{N}$ and $x, y \in \mathbb{Z}$. Then we say that x, y* are equivalent modulo n, *and we write*

$$x \equiv y \bmod n$$

if

$$n \mid x - y.$$

It is evident that equivalence modulo n is an equivalence relation, dividing $\mathbb{Z}$ into equivalence or *residue* classes.

Definition 4.2. *We denote the set of residue classes* mod n *by $\mathbb{Z}/(n)$.*

Evidently there are just n classes modulo n if $n \geq 1$;

$$\#(\mathbb{Z}/(n)) = n.$$

We denote the class containing $a \in \mathbb{Z}$ by $\bar{a}$, or just by a if this causes no ambiguity.

Proposition 4.1. *If*

$$x \equiv x', \ y \equiv y'$$

then

$$x + y \equiv x' + y', \ xy \equiv x'y'.$$

Thus we can add and multiply the residue classes mod$d$.

Corollary 4.1. *If $n > 0$, $\mathbb{Z}/(n)$ is a finite commutative ring (with 1).*

Example: Suppose $n = 6$. Then addition in $\mathbb{Z}/(6)$ is given by

+	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	4

while multiplication is given by

$\times$	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

4.2 The prime fields

Theorem 4.1. *The ring $\mathbb{Z}/(n)$ is a field if and only if n is prime.*

Proof. Recall that an *integral domain* is a commutative ring A with 1 having no zero divisors, ie

$$xy = 0 \implies x = 0 \text{ or } y = 0.$$

In particular, a field is an integral domain in which every non-zero element has a multiplicative inverse.

The result follows from the following two lemmas.

Lemma 4.1. *$\mathbb{Z}/(n)$ is an integral domain if and only if n is prime.*

Proof. Suppose n is not prime, say

$$n = rs,$$

where $1 < r, s < n$. Then

$$\bar{r}\,\bar{s} = \bar{n} = 0.$$

So $\mathbb{Z}/(n)$ is not an integral domain.

Conversely, suppose n is prime; and suppose

$$\bar{r}\,\bar{s} = \overline{rs} = 0.$$

Then

$$n \mid rs \implies n \mid r \text{ or } n \mid s \implies \bar{r} = 0 \text{ or } \bar{s} = 0.$$

□

Lemma 4.2. *A finite integral domain A is a field.*

Proof. Suppose $a \in A$, $a \neq 0$. Consider the map

$$x \mapsto ax : A \to A.$$

This map is injective; for

$$ax = ay \implies a(x - y) = 0 \implies x - y = 0 \implies x = y.$$

But an injective map

$$f : X \to X$$

from a *finite* set X to itself is necessarily surjective.

In particular there is an element $x \in A$ such that

$$ax = 1,$$

ie a has an inverse. Thus A is a field. □

□

4.3 The additive group

If we 'forget' multiplication in a ring A we obtain an additive group, which we normally denote by the same symbol A. (In the language of category theory we have a 'forgetful functor' from the category of rings to the category of abelian groups.)

Proposition 4.2. *The additive group $\mathbb{Z}/(n)$ is a cyclic group of order n.*

This is obvious; the group is generated by the element $1 \bmod n$.

Proposition 4.3. *The element $a \bmod n$ is a generator of $\mathbb{Z}/(n)$ if and only if*

$$\gcd(a, n) = 1.$$

Proof. Let

$$d = \gcd(a, n).$$

If $d > 1$ then 1 is not a multiple of $a \bmod n$, since

$$1 \equiv ra \bmod n \implies 1 = ra + sn \implies d \mid 1.$$

Conversely, if $d = 1$ then we can find $r, s \in \mathbb{Z}$ such that

$$ra + sn = 1;$$

so

$$ra \equiv 1 \bmod n,$$

Thus 1 is a multiple of $a \bmod n$, and so therefore is every element of $\mathbb{Z}/(n)$. □

Note that there is only one cyclic group of order n, up to isomorphism. So any statement about the additive groups $\mathbb{Z}/(n)$ is a statement about finite cyclic groups, and vice versa. In particular, the result above is equivalent to the statement that if G is a cyclic group of order n generated by g then g^r is also a generator of G if and only if $\gcd(r, n) = 1$.

Recall that a cyclic group G of order n has just one subgroup of each order $m \mid n$ allowed by Lagrange's Theorem, and this subgroup is cyclic. In the language of modular arithmetic this becomes:

Proposition 4.4. *The additive group $\mathbb{Z}/(n)$ had just one subgroup of each order $m \mid n$. If $n = mr$ this is the subgroup*

$$\langle r \rangle = \{0, r, 2r, \dots, (m-1)r\}.$$

4.4 The multiplicative group

If A is a ring (with 1, but not necessarily commutative) then the *invertible elements* form a group; for if a, b are invertible, say

$$ar = ra = 1, \; bs = sb = 1,$$

then

$$(ab)(rs) = (rs)(ab) = 1,$$

and so ab is invertible.

We denote this group by $A^\times$.

Proposition 4.5. *The element $a \in \mathbb{Z}/(n)$ is invertible if and only if*

$$\gcd(a, n) = 1.$$

Proof. If a is invertible mod$n$, say

$$ab \equiv 1 \bmod n,$$

then

$$ab = 1 + tn,$$

and it follows that

$$\gcd(a, n) = 1.$$

Conversely, if this is so then

$$ax + ny = 1,$$

and it follows that x is the inverse of a mod n. □

We see that the invertible elements in $\mathbb{Z}/(n)$ are precisely those elements that generate the additive group $\mathbb{Z}/(n)$.

Definition 4.3. *We denote the group of invertible elements in $\mathbb{Z}/(n)$ by $(\mathbb{Z}/n)^\times$. We call this group the* multiplicative group mod n*.*

Thus $(\mathbb{Z}/n)^\times$ consists of the residue classes mod n coprime to n, ie all of whose elements are coprime to n.

Definition 4.4. *If $n \in \mathbb{N}$, we denote by $\phi(n)$ the number of integers r such that*

$$0 \le r < n \text{ and } \gcd(r, n) = 1.$$

This function is called *Euler's totient function.* As we shall see, it plays a very important role in elementary number theory.

Example:

$$\begin{aligned}
\phi(0) &= 0, \\
\phi(1) &= 1, \\
\phi(2) &= 1, \\
\phi(3) &= 2, \\
\phi(4) &= 2, \\
\phi(5) &= 4, \\
\phi(6) &= 2.
\end{aligned}$$

It is evident that if p is prime then

$$\phi(p) = p - 1,$$

since every number in $[0, p)$ except 0 is coprime to p.

Proposition 4.6. *The order of the multiplicative group $(\mathbb{Z}/n)^\times$ is $\phi(n)$*

This follows from the fact that each class can be represented by a remainder $r \in [0, n)$.

Example: Suppose $n = 10$. Then the multiplication table for the group $(\mathbb{Z}/10)^\times$ is

	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

We see that this is a cyclic group of order 4, generated by 3:

$$(\mathbb{Z}/10)^\times = C_4.$$

Suppose $\gcd(a, n) = 1$. To find the inverse x of a mod n we have in effect to solve the equation

$$ax + ny = 1.$$

As we have seen, the standard way to solve this is to use the Euclidean Algorithm, in effect to determine $\gcd(a, n)$.

Example: Let us determine the inverse of 17 mod 23. Applying the Euclidean Algorithm,

$$\begin{aligned} 23 &= 17 + 6, \\ 17 &= 3 \cdot 6 - 1. \end{aligned}$$

Thus

$$\begin{aligned} 1 &= 3 \cdot 6 - 17 \\ &= 3(23 - 17) - 17 \\ &= 3 \cdot 23 - 4 \cdot 17. \end{aligned}$$

Hence

$$17^{-1} = -4 = 19 \bmod 23.$$

Note that having found the inverse of a we can easily solve the congruence

$$ax = b \bmod n$$

In effect

$$x = a^{-1}b.$$

For example, the solution of

$$17x = 9 \bmod 23$$

is

$$x = 17^{-1}9 = -4 \cdot 9 = -36 \equiv -13 \equiv 10 \bmod 23.$$

4.5 Homomorphisms

Suppose $m \mid n$. Then each remainder mod n defines a remainder mod m.

For example, if $m = 3,\ n = 6$ then

$$\begin{aligned} 0 \bmod 6 &\mapsto 0 \bmod 3, \\ 1 \bmod 6 &\mapsto 1 \bmod 3, \\ 2 \bmod 6 &\mapsto 2 \bmod 3, \\ 3 \bmod 6 &\mapsto 0 \bmod 3, \\ 4 \bmod 6 &\mapsto 1 \bmod 3, \\ 5 \bmod 6 &\mapsto 2 \bmod 3. \end{aligned}$$

Proposition 4.7. *If $m \mid n$ the map*

$$r \quad \bmod n \mapsto r \quad \bmod n$$

is a ring-homomorphism

$$\mathbb{Z}/(n) \to \mathbb{Z}/(m).$$

4.6 Finite fields

We have seen that $\mathbb{Z}/(p)$ is a field if p is prime.

Finite fields are important because linear algebra extends to vector spaces over any field; and vector spaces over finite fields are central to coding theory and cryptography, as well as other branches of pure mathematics.

Definition 4.5. *The* characteristic *of a ring A is the least positive integer n such that*

$$\overbrace{1 + 1 + \cdots + 1}^{n\ 1\text{'s}} = 0.$$

If there is no such n then A is said to be of characteristic 0.

Thus the characteristic of A, if finite, is the order of 1 in the additive group A.

Evidently $\mathbb{Z},\ \mathbb{Q},\ \mathbb{R},\ \mathbb{C}$ are all of characteristic 0.

Proposition 4.8. *The ring $\mathbb{Z}/(n)$ is of characteristic n.*

Proposition 4.9. *The characteristic of a finite field is a prime.*

Proof. Let us write

$$n \cdot 1 \text{ for } \overbrace{1 + 1 + \cdots + 1}^{n\ 1\text{'s}}.$$

Suppose the order n is composite, say $n = rs$. By the distributive law,

$$n \cdot 1 = (r \cdot 1)(s \cdot 1).$$

There are no divisors of zero in a field; hence

$$r \cdot 1 = 0 \text{ of } s \cdot 1 = 0,$$

contradicting the minimality of n. □

The proof shows in fact that the characteristic of any field is either a prime or 0.

Proposition 4.10. *Suppose F is a finite field of characteristic p. Then F contains a subfield isomorphic to $\mathbb{Z}/(p)$.*

Proof. Consider the additive subgroup generated by 1:

$$\langle 1 \rangle = \{0, 1, 2 \cdot 1, \ldots, (p-1) \cdot 1\}.$$

It is readily verified that this set is closed under addition and multiplication; and the map

$$r \bmod p \mapsto r \cdot 1 : \mathbb{Z}/(p) \to \langle 1 \rangle$$

is an isomorphism. □

This field is called the *prime subfield* of F.

Corollary 4.2. *There is just one field containing p elements, up to isomorphism, namely $\mathbb{Z}/(p)$.*

Theorem 4.2. *A finite field F of characteristic p contains p^n elements for some $n \geq 1$*

Proof. We can consider F as a vector space over its prime subfield P. Suppose this vector space is of dimension n. Let $e_1, \ldots, e_n$ be a basis for the space. Then each element of F is uniquely expressible in the form

$$a_1 e_1 + \cdots + a_n e_n,$$

where $a_1, \ldots, a_n \in P$. There are just p choices for each a_i. Hence the total number of choices, ie the number of elements in F, is p^n. □

Theorem 4.3. *There is just one field F containing $q = p^n$ elements for each $n \geq 1$, up to isomorphism.*

Thus there are fields containing 2,3,4 and 5 elements, but not field containing 6 elements.

We are not going to prove this theorem until later.

Definition 4.6. *We denote the field containing $q = p^n$ elements by $\mathbb{F}_q$.*

The finite fields are often called *Galois fields*, after Evariste Galois who discovered them.