Chapter 2, Congruence in \( \mathbb{Z} \) and modular arithmetic.

This leads us to an understanding of the kernels and images of functions between rings (ideals, quotient rings, ring homomorphisms). It will also give us more examples of rings to think about.

**Definition.** An **equivalence relation** is a binary relation which is reflexive, symmetric and transitive.

Note that an equivalence relation on a set \( S \) partitions the set into subsets; these are called the **equivalence classes**. The application of this to congruence of integers is Theorem 2.3. (See Appendix D.)

Examples: =, congruence and similarity of triangles, congruence and similarity of matrices and our real interest:

**Definition, p. 24.** Let \( a, b, n \in \mathbb{Z} \) with \( n > 0 \). We say \( a \) is **congruent** to \( b \) **modulo** \( n \) (written \( a \equiv b \pmod{n} \)) if \( n \) divides \( b - a \).

**Theorem 2.1.** Congruence of integers is an equivalence relation.

**Definition, p. 26.** The equivalence class of an integer \( a \) under the relation of congruence modulo \( n \) is called the **congruence class of \( a \) modulo \( n \)** and denoted by \( [a] \).

**Example.** \([a] = \{ b \in \mathbb{Z} | b \equiv a \pmod{n} \} = \{ a + kn | k \in \mathbb{Z} \}\)

Modulo 2, there are two classes: \([0]\), the set of even numbers and \([1]\), the set of odd numbers.

**Corollary 2.5.** Fix \( n > 1 \).

(1) If \( r \) is the remainder when \( a \) is divided by \( n \), then \([a] = [r]\)

(2) There are \( n \) distinct congruence classes, \([0],[1],\ldots,[n-1]\).

**Proof.** (1) If \( a = qn + r \), then \( n \) divides \( a - r \), so \( a \equiv r \pmod{n} \).

(2) \( 0,1,\ldots,n-1 \) are the only possible remainders. Show that the \( n \) given classes are all distinct. \( \square \)

**Definition, p. 28.** The set of congruence classes modulo \( n \) is denoted by \( \mathbb{Z}_n \).
Theorem 2.2. If \( a \equiv b \pmod{n} \) and \( c \equiv d \pmod{n} \), then

1. \( a + c \equiv b + d \pmod{n} \)
2. \( ac \equiv bd \pmod{n} \)

Proof. Use the definition of congruence. \( \square \)

Theorem 2.6. If \([a] = [b]\) and \([c] = [d]\) in \( \mathbb{Z}_n \), then \([a + c] = [b + d]\) and \([ac] = [bd]\).

Proof. This is a translation of Theorem 2.2 to new notation. \( \square \)

This says that the set of equivalence classes, \( \mathbb{Z}_n \), can have addition and multiplication defined by:

\[
[a] \oplus [c] = [a + c] \quad \text{and} \quad [a] \odot [c] = [ac]
\]

Theorem 2.6 says these operations are “well-defined”; that is, it does not matter which representative we pick from the congruence class to do our addition or multiplication with. We use \( \oplus \) and \( \odot \) only temporarily to emphasize that they are not the same operations that we have in \( \mathbb{Z} \). In fact, we will usually write \( a \) rather than \([a]\) as long as it is clear that we are talking about an element of \( \mathbb{Z}_n \) rather than an element of \( \mathbb{Z} \).

Do an example of arithmetic in \( \mathbb{Z}_3 \). We don’t have to think about the fact that we are working with remainders after division by 3.

Example. \( \mathbb{Z}_3 = \{[0], [1], [-1]\} \). Discuss arithmetic in \( \mathbb{Z}_3 \), solving equations such as \( x^2 \equiv 1 \pmod{3} \), \( x^2 \equiv -1 \pmod{3} \), \( x^2 \equiv -1 \pmod{5} \).

All the usual rules for arithmetic (distributive, commutative laws, etc.) are inherited from the integers: this is the content of Theorem 2.7, page 34.

Some new things happen:

Example. \( 2 \cdot 3 = 0 \) in \( \mathbb{Z}_6 \), but \( 2 \neq 0 \) and \( 3 \neq 0 \).
\( x^2 = -1 \) has a solution in \( \mathbb{Z}_5 \), but not in \( \mathbb{Z}_3 \).
Adding 1 to itself \( n \) times gives 0 in \( \mathbb{Z}_n \).
If \( a \neq 0 \) in \( \mathbb{Z}_5 \), then \( a \) has a multiplicative inverse. Check.
Every \( a \neq 0 \) of \( \mathbb{Z}_5 \) satisfies \( a^4 = 1 \).
In \( \mathbb{Z}_5 \), \((a + b)^5 = a + b \). Compute.

Good things happened in \( \mathbb{Z}_n \) when \( n = 5 \), but bad things happened when \( n = 6 \). What is different? Section 2.3 concentrates on \( \mathbb{Z}_p \) when \( p \) is a prime.
**Theorem 2.8.** Let \( p > 1 \) be an integer. The following are equivalent:

1. \( p \) is a prime.
2. For any \( a \neq 0 \) in \( \mathbb{Z}_p \), the equation \( ax = 1 \) has a solution in \( \mathbb{Z}_p \). (That is, \( a \) has a multiplicative inverse.)
3. Whenever \( ab = 0 \) in \( \mathbb{Z}_p \), then \( a = 0 \) or \( b = 0 \). (That is, \( \mathbb{Z}_p \) has no zero divisors (see p. 62).)

**Proof.** (1) \( \implies \) (2) (When possible, we use the properties of \( \mathbb{Z}_p \) for our proofs, but in this case we don’t yet know enough. We must translate back to congruence and divisibility.) So we assume \( a \in \mathbb{Z} \), \( a \not\equiv 0 \pmod{p} \). So \( \gcd(a, p) = 1 \) (otherwise, it would be \( p \) since \( p \) is prime). By Theorem 1.3, we can write \( 1 = au + pv \) for some integers \( u, v \). Therefore \( au \equiv 1 \pmod{p} \), or equivalently, \( [a][u] = [1] \) in \( \mathbb{Z}_p \).

(2) \( \implies \) (3) If \( a = 0 \), we are done. If \( a \not\equiv 0 \), multiply \( ab = 0 \) by \( u \in \mathbb{Z}_p \), where \( au = 1 \). this gives \( b = 0 \) in \( \mathbb{Z}_p \).

(3) \( \implies \) (1) Assume \( p \) is not prime, say \( p = mn \) for two integers \( 1 < m, n < p \). Then \( [m] \neq [0] \) and \( [n] \neq [0] \) by Corollary 2.5, but \( [m][n] = [p] = [0] \) contradicting (3). ☐

**Corollary 2.9.** Let \( p \) be a positive prime, \( a, b \in \mathbb{Z}_p \) and \( a \not\equiv 0 \). The equation \( ax = b \) has a unique solution in \( \mathbb{Z}_p \).

**Proof.** (Same as for invertible matrices in Math 311.) Use Theorem 2.8 (2) to find a solution \( ub \). If \( ar = b \) also, then \( a(r - ub) = b - b = 0 \), so \( r - ub = ua(r - ub) = u \cdot 0 = 0 \) and we see that \( ub \) is the only solution. ☐

What happens if \( p \) is not prime?

**Corollary 2.10.** Let \( a, b, n \in \mathbb{Z} \) with \( n > 1 \) and \( \gcd(a, n) = 1 \). Then the equation \( [a]x = [b] \) has a unique solution in \( \mathbb{Z}_n \). (Taking \( b = 1 \), this says \( [a] \) has a multiplicative inverse.)

**Proof.** First assume \( b = 1 \) and copy the proof of Theorem 2.8: Since \( \gcd(a, n) = 1 \), by Theorem 1.3, we can write \( 1 = au + nv \) for some integers \( u, v \). Therefore \( au \equiv 1 \pmod{n} \), or equivalently, \( [a][u] = [1] \) in \( \mathbb{Z}_n \). Now copy the proof of Corollary 2.9 to get a unique solution to \( [a]x = [b] \). ☐

Note that the Euclidean algorithm can be used to find \( u, v \) with \( 1 = au + nv \), so we have an algorithmic method of solution to linear equations in \( \mathbb{Z}_n \) if the leading coefficient is invertible. Otherwise, there may be no solutions or many solutions.

**Example.** \( 2x = 1 \) has no solution in \( \mathbb{Z}_4 \) since multiplying by 2 gives \( 0 = 2 \). \( 2x = 2 \) has solutions \( x = 1, 3 \) in \( \mathbb{Z}_4 \) since \( 2 = -2 \). This can be generalized as in the next theorem. It is a standard result in number theory, but not of particular interest to us.
**Theorem 2.11.** Let $a, b, n \in \mathbb{Z}$ with $n > 1$ and let $d = \gcd(a, n)$. Then

1. $[a]x = [b]$ has a solution in $\mathbb{Z}_n$ iff $d|b$.
2. If $d|b$, the equation $[a]x = [b]$ has $d$ distinct solutions.

*Partial proof.* The proof is outlined in the exercises, numbers 8–10, page 40. We will see where the different solutions come from. If there is any solution $[r]$, so that $ar - b = nq$, then $d|a$ and $d|n$, so $d$ divides $b = ar - nq$. Thus we can write $au + nv = d$ by Theorem 1.3, $a = da_1$, $b = db_1$, $n = dn_1$. Check that $ub_1 + kn_1$ gives a solution for $k = 0, \ldots, d-1$:

$$a(ub_1 + kn_1) = da_1(ub_1 + kn_1) = b(a_1u) + n(a_1k) \equiv ba_1u$$

$$= b(1 - n_1v) = b - b_1vn \equiv b \pmod{n}$$

What we have not shown is that these solutions are all different and include all possible solutions. □