# Congruences

## 1 The congruence relation

The notion of congruence modulo $m$ was invented by Karl Friedrich Gauss, and does much to simplify arguments about divisibility.

**Definition.** Let $a, b, m \in \mathbb{Z}$, with $m > 0$. We say that $a$ **is congruent to** $b$ **modulo** $m$, written

$$a \equiv b \pmod{m},$$

if $m \mid (a - b)$. We call $m$ a **modulus** in this situation.If $m \nmid (a - b)$ we say that $a$ **is incongruent to** $b$ **modulo** $m$, written

$$a \not\equiv b \pmod{m}.$$

**Example.**

- $m = 11$. We have $-1 \equiv 10 \pmod{11}$, since $11 \mid (-1 - 10) = -11$. We have $108 \not\equiv 7 \pmod{11}$ since $11 \nmid (108 - 7) = 101$.
- $m = 2$. When do we have $a \equiv b \pmod{2}$? We must have $2 \mid (a - b)$.In other words, $a - b$ must be even. This is true iff $a$ and $b$ have the same *parity*: i.e., iff both are even or both are odd.
- $m = 1$. Show that for any $a$ and $b$ we have $a \equiv b \pmod{1}$.
- When do we have $a \equiv 0 \pmod{m}$? This is true iff $m \mid (a - 0)$ iff $m \mid a$. Thus the connection with divisibility: $m \mid a$ iff $a \equiv 0 \pmod{m}$.

Congruence is meant to simplify discussions of divisibility, and yet in our examples we had to use divisibility to prove congruences. The following theorem corrects this.

**Theorem.** *Let $a, b, m \in \mathbb{Z}$ with $m > 0$. Then $a \equiv b \pmod{m}$ if and only if there is a $k \in \mathbb{Z}$ such that $b = a + km$.*

*Proof.* We have $a \equiv b \pmod{m}$ if and only if $m \mid (a - b)$. By definition this is true iff there is a $k$ such that $a - b = km$, which is true iff $a = b + km$ for some $k$. □

The previous theorem makes it an easy to task, given say an integer $a$ and a modulus $m$, to list all integers congruent to $a$ modulo $m$. Just take the set $\{a + km : k \in \mathbb{Z}\}$.

**Example.** Take $m = 3$.

- The set of all integers congruent to 0 modulo 3 is $\{0 + k3 : k \in \mathbb{Z}\} = \{\dots, -6, -3, 0, 3, 6, 9, \dots\}$.
- The set of all integers congruent to 1 modulo 3 is $\{1 + k3 : k \in \mathbb{Z}\} = \{\dots, -5, -2, 1, 4, 7, 10, \dots\}$.
- The set of all integers congruent to 2 modulo 3 is $\{2 + k3 : k \in \mathbb{Z}\} = \{\dots, -4, -1, 2, 5, 7, 12, \dots\}$.

## 2 Congruence classes

Congruence modulo $m$ defines a binary relation on $\mathbb{Z}$. One property that makes this such a useful relation is that it is an equivalence relation!

**Theorem.** *Let $m \in \mathbb{Z}^+$ and consider the relation $R_m$ defined by*

$$a \, R_m \, b \text{ if and only if } a \equiv b \pmod{m}.$$

*Then $R_m$ is an equivalence relation.*

*(i)* $R_m$ *is reflexive: for all* $a \in \mathbb{Z}$ *we have* $a \equiv a \pmod{m}$.

*(ii)* $R_m$ *is symmetric: if* $a \equiv b \pmod{m}$*, then* $b \equiv a \pmod{m}$.

*(iii)* $R_m$ *is transitive: if* $a \equiv b \pmod{m}$ *and* $b \equiv c \pmod{m}$*, then* $a \equiv c \pmod{m}$

*Proof.* (i) Since $m \mid (a - a) = 0$, we have $a \equiv a \pmod{m}$.

(ii) If $m \mid (a - b)$, then $m \mid (-1)(a - b) = (b - a)$. Thus $a \equiv b \pmod{m}$ implies $b \equiv a \pmod{m}$.

(iii) Suppose $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$. Then by the previous theorem we can write $b = a + km$ for some $k$ and $c = b + k'm$ for some $k'$. But then $c = b + k'm = a + km + k'm = a + (k + k')m$, and thus $a \equiv c \pmod{m}$.

□

Since $R_m$ is an equivalence relation, we can speak of its corresponding equivalence classes. These are called *congruence classes*.

**Definition.** Let $m$ be a modulus. Given an integer $a$, its **congruence class modulo** $m$ is the set

$$[a]_m := \{x \in \mathbb{Z} \colon a \equiv x \pmod{m}\} = \{a + km \colon k \in \mathbb{Z}\}.$$

**Example.** Let $m = 3$. Then $[0]_3 = \{\dots, -3, 0, 3 \dots\}$, $[1]_3 = \{\dots, -2, 1, 4 \dots\}$, $[2]_3 = \{\dots, -1, 2, 5 \dots\}$.

Why not consider $[3]_3$ in the last example? Because

$$[3]_3 = \{\dots, -3, 0, 3, 6, \dots\} = [0]_3.$$

Similarly $[4]_3 = [1]_3$ and $[5]_3 = [2]_3$.

**Comment.**

- We see that congruence classes have many different "names": $[1]_3 = [4]_3 = [-2]_3$. In fact we can show that for any element $a \in [1]_3$, we have $[1]_3 = [a]_3$.
- Apparently the three congruence classes $[0]_3, [1]_3$, and $[2]_3$ are in fact *all* of the congruence classes modulo $m$.

The following theorem confirms and expands upon these observations.

**Theorem** (Congruence Theorem)**.** *Let* $m$ *be a modulus. Then:*

*(i)* $[a]_m = [b]_m$ *if and only if* $a \equiv b \pmod{m}$.

*(ii) the collection of congruence classes* $[a]_m$ *form a partition of* $\mathbb{Z}$*: i.e., distinct congruence classes are disjoint, and every element of* $\mathbb{Z}$ *is contained in (exactly) one of the congruence classes.*

*(iii) In fact there are exactly* $m$ *congruence classes, namely* $[0]_m, [1]_m, \dots, [m-1]_m$*. Thus for each* $x \in \mathbb{Z}$*, we have* $x \in [i]_m$ *for exactly one* $i$ *with* $0 \le i \le m - 1$.

*Proof.*

(i)-(ii) The first two statements are true of *any* equivalence relation, so we get them for free! For example, the first follows from the fact that if $R$ is an equivalence relation, then $[x]_R = [y]_R$ if and only if $xRy$.

(iii) We need to show that $[i]_m \neq [j]_m$ for any $i \neq j$ with $i, j \in \{0, 1, \dots, m-1\}$, and that for any $a \in \mathbb{Z}$ we have $[a]_m = [i]_m$ for some $i \in \{0, 1, \dots, m-1\}$.

We can prove both in one fell swoop by showing that for all $a \in \mathbb{Z}$ there is *exactly* one $i \in \{0, 1, 2, \dots, m-1\}$ such that $[a]_m = [i]_m$.(Think about this.)To do this, apply the division algorithm! This says there is one *and only one* $r \in \{0, 1, \dots, m-1\}$ such that $a = qm + r$ for some $q$. Then $a \equiv r \pmod{m}$. By (i), this means that $[a]_m = [r]_m$, so we can choose $i = r$. This choice is unique thanks to the uniqueness claim in the division algorithm.

□

The results of the Congruence Theorem (CT) give rise to some definitions.

**Definition.** Let $m$ be a modulus. We saw that for any $a \in \mathbb{Z}$ there is a unique $r \in \{0, 1, \ldots, m-1\}$ such that $a \equiv r \pmod{m}$ (or equivalently, $[a]_m = [r]_m$). We call $r$ the *least nonnegative residue* of $a$ and write $a$ **mod** $m = r$. (Note the bold print!)

**Comment.** Be careful not to confuse our two notions. To say that $a \equiv b \pmod{m}$ is to assert a certain *relation* holds between $a$ and $b$, whereas $a$ **mod** $m$ is an honest to goodness number. In fact, the least nonnegative residue allows us to define a *function*

$$\_ \textbf{ mod } m \colon \mathbb{Z} \longrightarrow \{0, 1, \ldots, m-1\},$$

sending an integer $a \in \mathbb{Z}$ to $a$ **mod** $m \in \{0, 1, \ldots, m-1\}$.

**Example.** Take $m = 5$. We have $23$ **mod** $5 = 3$, since $23 \equiv 3 \pmod{5}$. Similarly, we have $-97$ **mod** $5 = 3$, since $-97 \equiv 3 \pmod{5}$. This shows that in general the function $f(x) = x$ **mod** $m$ is not injective!

In fact we have the following description of the *fibers* of $f(x) = x$ **mod** $m$.

**Corollary.** *Let $m$ be a modulus. Then $a$* **mod** *$m = b$* **mod** *$m$ if and only if $a \equiv b \pmod{m}$. In other words, given $r \in \{0, 1, \ldots, m-1\}$ the set of $x \in \mathbb{Z}$ such that $f(x) = x$* **mod** *$m = r$ is the congruence class $[r]_m$.*

**Definition.** Let $m$ be a modulus. A set of $m$ integers $\{r_1, r_2, \ldots, r_m\}$ whose congruence classes $[r_1]_m, \ldots, [r_m]_m$ exhaust all possible congruence classes is called a **complete system of residues modulo** $m$.

**Example.** Let $m = 3$ Then $\{0, 1, 2\}$ is a complete system of residues modulo 3, but so is $\{-3, 4, 5\}$ and $\{33, -29, 8\}$.

**Theorem.** *Let $m$ be a modulus, and let $r_1, r_2, \ldots r_m$ be integers. The following statements are equivalent.*

*(i) The $r_i$'s comprise a complete system of residues modulo $m$.*

*(ii) For all $a \in \mathbb{Z}$ there is a* unique *$r_i$ such that $a \equiv r_i \pmod{m}$.*

*(iii) The $r_i$'s are pairwise incongruent; i.e., if $i \neq j$, then $r_i \not\equiv r_j \pmod{m}$.*