## 2.1 Congruence and Congruence Classes

Is it possible to write 1,000,003 as a sum of two perfect squares?

It would be possible, but unpleasant, to solve this problem by brute force: check the equation $1000003 = x^2 + y^2$ for $x = 0, 1, 2, \ldots, 1000$ and see whether we get an integer value for $y$. However, this problem is very easy to solve if you know the right trick.

It can be easily checked that if you divide a perfect square by 4, the remainder is always 0 or 1. (Make sure you can prove this!) Therefore, if you divide $x^2 + y^2$ by 4, the remainder must be 0, 1, or 2. Since dividing 1,000,003 by 4 leaves a remainder of 3, we know that 1,000,003 cannot be a sum of two squares.

In short, we prove that the equation $1000003 = x^2 + y^2$ cannot have any solutions by proving an even stronger statement; not only are the left-hand side and right-hand side never equal, they can't even have the same remainder when divided by 4. This trick of classifying integers by their remainder upon division by $m$ is so useful that it has its own terminology and notation.

**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 $m \mid (a - b)$. If $a$ is not congruent to $b$, we write $a \not\equiv b \pmod{m}$. The number $m$ is called the *modulus*.

**Example.** We have $5 \equiv -13 \pmod{6}$ and $5 \not\equiv -13 \pmod{7}$.

One of the main reasons that congruences work so well is that we can still do arithmetic with them:

**Theorem.** *If* $a \equiv b \pmod{m}$ *and* $c \equiv d \pmod{m}$, *then:*

*(a)* $a + c \equiv b + d \pmod{m}$;

*(b)* $a - c \equiv b - d \pmod{m}$;

*(c)* $ac \equiv bd \pmod{m}$.

*Proof.* By definition, $m \mid (a - b)$ and $m \mid (c - d)$. Therefore $m$ divides

$$(a - b) + (c - d) = (a + c) - (b + d),$$

so $a + c \equiv b + d \pmod{m}$. This proves (a). Similarly, $m$ divides

$$(a - b)c + b(c - d) = ac - bd,$$

so $ac \equiv bd \pmod{m}$. This proves (c).

We could easily prove (b) in the same way, but in order to demonstrate a different proof technique, we instead note that it is a direct consequence of (a) and (c). Part (c) shows that $-c = (-1)c \equiv (-1)d = -d \pmod{m}$. Thus, by (a),

$$a - c = a + (-c) \equiv b + (-d) = b - d \pmod{m}.$$

□

## Equivalence relations

Another nice feature of congruence is that "congruence modulo $m$" is an equivalence relation. Essentially, this means that congruence acts much like equality.[1]

**Definition.** We say that a binary relation[2] $\sim$ on a set $S$ is an *equivalence relation* if it is reflexive, symmetric, and transitive. That is, for all $a, b, c \in S$,

- $a \sim a$. (Reflexivity)
- If $a \sim b$, then $b \sim a$. (Symmetry)
- If $a \sim b$ and $b \sim c$, then $a \sim c$. (Transitivity)

**Example.** Equality is the classic example of an equivalence relation. Another example is the relation "is similar to" on the set of all triangles.

**Theorem.** *For any positive integer $m$, "congruence modulo $m$" is an equivalence relation.*

*Proof.* Let $a, b, c \in \mathbb{Z}$.

Clearly $m \mid 0 = (a - a)$, so $a \equiv a \pmod{m}$. This proves reflexivity.

If $a \equiv b \pmod{m}$, then $m \mid (a - b)$, so $m \mid (b - a) = -(a - b)$. Therefore $b \equiv a \pmod{m}$, which proves symmetry.

If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $m \mid (a - b)$ and $m \mid (b - c)$. Therefore

$$m \mid ((a - b) + (b - c)) = (a - c),$$

so $a \equiv c \pmod{m}$. This proves transitivity. □

**Definition.** Given an equivalence relation $\sim$ on a set $S$ and an $s \in S$, the equivalence class of $s$ is

$$[s] = \{t \in S \mid t \sim s\}.$$

In other words, $[s]$ is the set of everything equivalent to $s$.

[1] See Appendix D of the textbook for more information about equivalence relations. Strictly speaking, you don't need to know what an equivalence relation is for this course, but it seems odd to prove that congruence has all the important properties of an equivalence relation without telling you the name for what we're proving.

[2] "Binary" here means that it relates two elements of $S$ at a time.

When the equivalence relation in question is congruence modulo $m$, this becomes:

$$[a] = \{b \in \mathbb{Z} \mid b \equiv a \pmod{m}\}.$$

In this case, we refer to the equivalence class as the *congruence class of $a$ modulo $m$*.

**Example.** The equivalence class of 3 modulo 7 is

$$[3] = \{3 + 7k \mid k \in \mathbb{Z}\} = \{\ldots, -11, -4, 3, 10, 17, \ldots\}.$$

**Note.** The meaning of $[a]$ depends on the choice of $m$. If we are working modulo 7, then $[3]$ is as illustrated above. If we are working modulo 9, then

$$[3] = \{\ldots, -15, -6, 3, 12, 21, \ldots\}.$$

Usually it will be clear what modulus is in use. If not, we can specify it with a subscript, e.g., $[3]_7$ or $[3]_9$.

**Theorem.** *Let $\sim$ be an equivalence relation on a set $S$. If $s, t \in S$, then $s \sim t$ if and only if $[s] = [t]$.*

*Proof.* First suppose $s \sim t$. We prove that $[s] \subseteq [t]$. If $x \in [s]$, then $x \sim s$; by transitivity, $x \sim t$, so $x \in [t]$. Therefore $[s] \subseteq [t]$. By symmetry, the same argument shows that $[t] \subseteq [s]$, so $[s] = [t]$.

Conversely, suppose $[s] = [t]$. By reflexivity, $s \in [s]$, so $s \in [t]$. Therefore $s \sim t$, as we wanted to show. □

**Corollary.** *Let $\sim$ be an equivalence relation on a set $S$. Then two equivalence classes are either disjoint or identical.*

*Proof.* Let $s$ and $t$ be two elements of $S$; assume that $[s]$ and $[t]$ are not disjont. Then there exists some $x \in S$ such that $x \in [s]$ and $x \in [t]$. By the previous theorem, $[s] = [x] = [t]$. □

## Integers modulo $m$

Applying the previous results to congruence modulo $m$, we have:

**Corollary.** *If $a, c \in \mathbb{Z}$, then $a \equiv c \pmod{m}$ if and only if $[a] = [c]$.*

**Corollary.** *Two congruence classes modulo $m$ are either disjoint or identical.*

The previous two corollaries are simply general statements about equivalence classes; we could say the same about any equivalence relation. We are now prepared to give a more specific classification of the congruence classes modulo $m$.

**Theorem.** *Let $m$ be a positive integer.*

1. *If $a \in \mathbb{Z}$ and $r$ is the remainder when $a$ is divided by $m$, then $[a] = [r]$.*
2. *There are exactly $m$ distinct congruence classes modulo $m$, namely $[0], [1], \ldots, [m-1]$.*

*Proof.* 1. By the definition of division, $a = mq + r$ for some $q \in \mathbb{Z}$. Therefore $m \mid mq = (a - r)$, so $a \equiv r \pmod{m}$. As we have seen, this implies $[a] = [r]$.

2. Part (a) shows that every integer is in one of the congruence classes $[0], [1], \ldots, [m-1]$, since its remainder must be one of $0, 1, \ldots, m-1$. It remains only to check that these congruence classes are distinct.

   Suppose that $[a] = [c]$ for some $a, c$ satisfying $0 \leq a, c \leq m-1$. Then $m \mid (a - c)$. But the inequality ensures that $-m < a - c < m$, so this is only possible if $a - c = 0$. That is, if $[a] = [c]$ for $a$ and $c$ among $0, \ldots, m-1$, then $a = c$. This proves that $[0], [1], \ldots, [m-1]$ are distinct.

□

**Definition.** The set of all congruence classes modulo $m$ is denoted $\mathbb{Z}/m\mathbb{Z}$. (This set is sometimes denoted $\mathbb{Z}_m$ instead; the textbook uses this convention. However, this notation has a major drawback: there is a different mathematical object that is also commonly denoted by $\mathbb{Z}_m$. For that reason, I prefer $\mathbb{Z}/m\mathbb{Z}$.)

The previous theorem shows that the set $\mathbb{Z}/m\mathbb{Z}$ has exactly $m$ elements. For example, $\mathbb{Z}/4\mathbb{Z}$ consists of [0], [1], [2], and [3].