Notes on the Equivalence Relation, Congruence modulo 3 ($\equiv_{\text{mod 3}}$)

It is proved below that $\equiv_{\text{mod 3}}$ is an equivalence relation (i.e., it is reflexive, symmetric, and transitive), and a similar proof shows that, for any modulus $n > 0$, $\equiv_{\text{mod n}}$ is an equivalence relation, also.

Definition: Define the relation “Congruence modulo 3” on the set of integers $\mathbb{Z}$ as follows:

For all $a, b \in \mathbb{Z}$, $a \equiv_{\text{mod 3}} b$ if and only if $3 \mid (a - b)$

[Equivalently: $a \equiv b \pmod{n}$ if and only if $3 \mid (a - b)$].

Similarly, let $n$ be any positive integer, $n > 0$. Define “Congruence modulo $n$” as follows:

For all $a, b \in \mathbb{Z}$, $a \equiv_{\text{mod n}} b$ if and only if $n \mid (a - b)$. ($n$ is called the “modulus”.)

The Traditional Notation: "$a \equiv_{\text{mod n}} b$" is usually expressed as: "$a \equiv b \pmod{n}$".

(Mod 3) examples: (Here, $n = 3$)

\[
22 \equiv_{\text{mod 3}} 16 \text{ since } 3 \mid (22 - 16). \quad \text{Equivalently, } 22 \equiv 16 \pmod{3}.
\]

\[
17 \equiv_{\text{mod 3}} 2 \text{ since } 3 \mid (17 - 2). \quad \text{Equivalently, } 17 \equiv 2 \pmod{3}.
\]

\[
21 \equiv_{\text{mod 3}} 0 \text{ since } 3 \mid (21 - 0). \quad \text{Equivalently, } 21 \equiv 0 \pmod{3}.
\]

In fact, for all $a \in \mathbb{Z}$, $3a \equiv_{\text{mod 3}} 0$ since $3 \mid (3a - 0)$.

Thus, all multiples of 3 are (mod 3) congruent to 0.

Note: $22 = 1 + 21$, so $22$ = “1 + (multiple of 3)” and

\[
16 = 1 + 15, \text{ so } 16 = \text{ “1 + (multiple of 3)” , and } 22 \equiv_{\text{mod 3}} 16.
\]

This is no coincidence. Any “1 + (multiple of 3)” $\equiv_{\text{mod 3}}$ Any other “1 + (multiple of 3)”.

Thus, for any integers $k$ and $\ell$, $1 + 3k \equiv_{\text{mod 3}} 1 + 3\ell$ since $(1 + 3k) - (1 + 3\ell) = 3(k - \ell)$ and $3 \mid 3(k - \ell)$.

Similarly, $2 + 3k \equiv_{\text{mod 3}} 2 + 3\ell$ and $0 + 3k \equiv_{\text{mod 3}} 0 + 3\ell$. 
Similarly, when any modulus \( n > 0 \) is used: Say \( n = 8 \) and we are considering the relation \( \equiv (\mod 8) \):

\[
57 = 1 + 8 \times 7 \quad \text{and} \quad 25 = 1 + 8 \times 3 \quad \text{and} \quad (57 - 25) = 32, \quad \text{so} \quad 8 \mid (57 - 25), \quad \text{so,}
\]

by definition of \( \equiv (\mod 8) \), \( 57 \equiv (\mod 8) 25 \), or in traditional notation, \( 57 \equiv 25 \mod 8 \).

So, \( 22 \equiv 16 \mod 3 \iff 3 \mid (22 - 16) = 6 \quad \text{(Both are of the form } 1 + \text{“multiple of } 3\text{”)} \)

And, \( 17 \equiv 2 \mod 3 \iff 3 \mid (17 - 2) = 15 \quad \text{(Both of the form are } 2 + \text{“multiple of } 3\text{”)} \)

And, \( 29 \equiv 15 \mod 7 \iff 7 \mid (29 - 15) = 14. \quad \text{(Both of the form are } 1 + \text{“multiple of } 7\text{”)} \)

Equivalently, \( 29 \equiv \mod 7 15 \).

What follows is a proof that the relation \( \equiv (\mod 3) \) is an Equivalence Relation.

That is, in the following proof, it is proved that

the relation \( \equiv (\mod 3) \) is Reflexive, Symmetric, and Transitive.

RULE: In all proofs involving relations, as for instance, "relation R", whenever the definition of relation R is applied, the justification “ by definition of R ” must be included.

Note how in the proofs below, whenever the definition of the relation " \( \equiv (\mod 3) \) " is applied, the justification “ by definition of ’ \( \equiv (\mod 3) \)' ,” is included.

Theorem (From Example 8.2.4):

\( \equiv (\mod 3) \) is an Equivalence Relation.

Proof: [ NTS “ \( \equiv (\mod 3) \) ” is reflexive, symmetric and transitive. ]

[ We prove that “ \( \equiv (\mod 3) \) ” is Reflexive. ]

Let \( x \in \mathbb{Z} \) be given. [ NTS that \( x \equiv (\mod 3) x \) ]

\[ x - x = 0 \quad \text{and} \quad 0 = 3 \times 0 \quad \therefore (x - x) = 3 \times 0 \quad \therefore 3 \mid (x - x). \]

\[ \therefore x \equiv (\mod 3) x, \quad \text{by definition of} \quad \equiv (\mod 3). \]

\[ \therefore " \equiv (\mod 3) " \quad \text{is reflexive, by direct proof}. \]

[ End of the "reflexivity" proof ]
We prove that \( \equiv_{(\text{mod } 3)} \) is Symmetric.

Let \( x \in \mathbb{Z} \) and \( y \in \mathbb{Z} \) be given.

Suppose \( x \equiv_{(\text{mod } 3)} y \). [NTS that \( y \equiv_{(\text{mod } 3)} x \).]

Then, \( 3 \mid (x - y) \), by definition of \( \equiv_{(\text{mod } 3)} \).

\[
\therefore (x - y) = 3k \text{ for some integer } k. \therefore (y - x) = 3(-k). \therefore 3 \mid (y - x).
\]

\[
\therefore y \equiv_{(\text{mod } 3)} x, \text{ by definition of } \equiv_{(\text{mod } 3)}.
\]

\[
\therefore \quad \equiv_{(\text{mod } 3)} \text{ is symmetric, by direct proof.}
\]

[End of the "symmetry" proof]

We prove that \( \equiv_{(\text{mod } 3)} \) is Transitive.

Let \( x, y, z \in \mathbb{Z} \) be given.

Suppose \( x \equiv_{(\text{mod } 3)} y \) and \( y \equiv_{(\text{mod } 3)} z \). [NTS that \( x \equiv_{(\text{mod } 3)} z \).]

Then, by definition of \( \equiv_{(\text{mod } 3)} \), \( 3 \mid (x - y) \) and \( 3 \mid (y - z) \).

\[
\therefore (x - y) = 3k \text{ and } (y - z) = 3\ell \text{ for some integers } k \text{ and } \ell.
\]

\[
\therefore x = y + 3k \text{ and } z = y - 3\ell, \text{ by Rules of Algebra.}
\]

\[
\therefore x - z = (y + 3k) - (y - 3\ell), \text{ by substitution.}
\]

\[
\therefore x - z = 3k + 3\ell = 3(k + \ell) \text{ and } (k + \ell) \text{ is an integer.} \therefore 3 \mid (x - z).
\]

\[
\therefore x \equiv_{(\text{mod } 3)} z, \text{ by definition of } \equiv_{(\text{mod } 3)}.
\]

\[
\therefore \quad \text{For all } x, y, z \in \mathbb{Z}, \text{ if } x \equiv_{(\text{mod } 3)} y \text{ and } y \equiv_{(\text{mod } 3)} z, \text{ then } x \equiv_{(\text{mod } 3)} z, \text{ by direct proof.}
\]

\[
\therefore \quad \equiv_{(\text{mod } 3)} \text{ is transitive, by direct proof.}
\]

[End of the "transitivity" proof]

\[
\therefore \quad \equiv_{(\text{mod } 3)} \text{ is reflexive, symmetric, and transitive.}
\]

\[
\therefore \quad \equiv_{(\text{mod } 3)} \text{ is an Equivalence Relation.}
\]

\[
Q \quad E \quad D
\]

Similarly, for any \( n \in \mathbb{Z} \) such that \( n > 0 \), \( \equiv_{(\text{mod } n)} \) is an Equivalence Relation.
COMMENTS REGARDING THE "by Direct Proof" JUSTIFICATION USED ABOVE

Note 1: In the part of the proof above that proves that relation \( R \) is reflexive, the conclusion that relation \( R \) has been proved to be reflexive is justified using the phrase "by Direct Proof," that is, the conclusion is:

"\( \therefore \equiv_{(mod\ 3)}' \) is reflexive, by direct proof."

This wording is a shortened form of the full statement of the conclusion, namely:

"\( \therefore \) For all \( x \in \mathbb{Z} \), \( x \equiv_{(mod\ 3)} x \), by direct proof.
\[ \therefore \equiv_{(mod\ 3)}' \) is reflexive, by definition of 'reflexive'."

Note 2: In the part of the proof above that proves that relation \( R \) is symmetric, the conclusion that relation \( R \) has been proved to be symmetric is justified using the phrase "by Direct Proof," that is, the conclusion is:

"\( \therefore \equiv_{(mod\ 3)}' \) is symmetric, by direct proof."

This wording is a shortened form of the full statement of the conclusion, namely:

"\( \therefore \) For all \( x, y \in \mathbb{Z} \), if \( x \equiv_{(mod\ 3)} y \), then \( y \equiv_{(mod\ 3)} x \), by direct proof.
\[ \therefore \equiv_{(mod\ 3)}' \) is symmetric, by definition of 'symmetric'."

Note 3: In the part of the proof above that proves that relation \( R \) is transitive, the conclusion that relation \( R \) has been proved to be transitive is justified using the phrase "by Direct Proof," that is, the conclusion is:

"\( \therefore \equiv_{(mod\ 3)}' \) is transitive, by direct proof."

This wording is a shortened form of the full statement of the conclusion, namely:

"\( \therefore \) For all \( x, y, z \in \mathbb{Z} \), if \( x \equiv_{(mod\ 3)} y \) and \( y \equiv_{(mod\ 3)} z \),
then \( x \equiv_{(mod\ 3)} z \), by direct proof.
\[ \therefore \equiv_{(mod\ 3)}' \) is transitive, by definition of 'transitive'."

The same wording of these conclusions can be used when any other relation \( R \) is being proved to be reflexive, symmetric, or transitive.
Definition:  For an Equivalence Relation \( R \) on a set \( A \), and for any element \( a \in A \), the “Equivalence Class of \( a \)” or just the “Class of \( a \)”, denoted \( [a] \), is the set \( [a] = \{ x \in A \mid x \, R \, a \} \).

Any element \( b \) in \( A \) such that \( b \, R \, a \) will also be an element in \( [a] \), and both \( a \) and \( b \) will be called *representatives* of the class \( [a] \), because, in that case, \( [b] = [a] \) as sets.

One obvious representative of \( [a] \) = the "Class of \( a \)" is the element \( a \), but every other element of \( [a] \) is also a representative of that same equivalence class.

A (Mod 3) Example:  What is the “Class of 2” ?  What is \( [2] \) ?

Consider the equivalence relation “ \( \equiv_{(\text{mod } 3)} \) ” with underlying set \( A = \mathbb{Z} \). Let \( a = 2 \).

Then, the “Class of 2” is denoted \( [2] \) and \( [2] = \{ n \in \mathbb{Z} \mid n \, \equiv_{(\text{mod } 3)} \, 2 \} \).

Let \( k \) be any integer and consider \( t = 3k + 2 \).  [ We show that \( (3k + 2) \in [2] \). ]

Then, \( (t - 2) = 3k \), and so, \( 3 \mid (t - 2) \).  \( \therefore \) \( t \equiv_{(\text{mod } 3)} 2 \), by definition of “ \( \equiv_{(\text{mod } 3)} \) ”.

\( \therefore \) \( t \in [2] \).  \( \therefore (3k + 2) \in [2] \).  \( \therefore \) For all \( k \in \mathbb{Z} \), \( (3k + 2) \in [2] \), by direct proof.

\( \therefore \) \( \{ t \in \mathbb{Z} \mid t = 3k + 2 \text{ for some integer } k \} \subseteq [2] \). (***)

Now, suppose that \( s \) is any integer such that \( s \in [2] \). Then, \( s \equiv_{(\text{mod } 3)} 2 \), by definition of "[2]".

\( \therefore 3 \mid (s - 2) \), by definition of " \( \equiv_{(\text{mod } 3)} \) ".

\( \therefore s - 2 = 3\ell \) for some integer \( \ell \).  \( \therefore s = 3\ell + 2 \).

\( \therefore s \in \{ t \in \mathbb{Z} \mid t = 3k + 2 \text{ for some integer } k \} \).

\( \therefore [2] \subseteq \{ t \in \mathbb{Z} \mid t = 3k + 2 \text{ for some integer } k \} \), by direct proof.

Combining this with (***) above, we have proved that

\[
[2] = \{ t \in \mathbb{Z} \mid t = 3k + 2 \text{ for some integer } k \}.
\]

\( \therefore [2] = \{ \ldots, -7, -4, -1, +2, +5, +8, \ldots \} \)

These correspond to \( k \) values:

\( \ldots, -3, -2, -1, 0, +1, +2, \ldots \)

Note that:

(1) each integer in the class \( [2] \) is exactly three less than the next higher integer in the same (mod 3) class and

(2) each integer in the class \( [2] \) is exactly three more than the nearest lower integer in the same (mod 3) class.
For the “(mod 3) congruence” equivalence relation, there are three (3) distinct equivalence classes: [0], [1], [2].

They are precisely:

\[
[0] = \{ t \in \mathbb{Z} \mid t = 3k + 0 \text{ for some integer } k \} = \{ ..., -6, -3, 0, +3, +6, +9, ... \}
\]

\[
[1] = \{ t \in \mathbb{Z} \mid t = 3k + 1 \text{ for some integer } k \} = \{ ..., -5, -2, +1, +4, +7, +10, ... \}
\]

\[
[2] = \{ t \in \mathbb{Z} \mid t = 3k + 2 \text{ for some integer } k \} = \{ ..., -4, -1, +2, +5, +8, +11, ... \}
\]

For the class of \([2]\), the integer 2 is a representative of \([2]\) because \(2 \in [2]\).

But, 5 and 8 are also elements of \([2]\), so both of the integers 5 and 8 are also representatives of the class of 2, since \([2] = [5] = [8]\) as sets.

Thus, –3, 0 and 9 are representatives of \([0]\) (because \([-3] = [0] = [9]\) as sets.)

And, –5, 1 and 13 are representatives of \([1]\) (because \([-5] = [1] = [13]\) as sets.)

A PREVIEW of Theorem (NIB) 4:

For any integer \(a\) and, for any positive integer \(n > 0,\)

\[ a \equiv (a \mod n) \pmod{n} \]

[Equivalently: \(a \equiv (a \mod n) \pmod{n}\).

For Example: \(17 \equiv (17 \mod 3) = 2\) and \(17 \equiv (\mod 3) 2\).

That is, for the integer \(a = 17\) and for the positive integer \(n = 3, \ a \equiv (a \mod n) \pmod{n}\).

Using the Traditional Notation, this principle is almost unintelligible: \(a \equiv (a \mod n) \pmod{n} \).

Note: For “\(\equiv (\mod 3)\)”, there are only three (3) equivalence classes: \([0]\), \([1]\) and \([2]\).

Similarly: For “\(\equiv (\mod 2)\)”, there are 2 equivalence classes: \([0]\) and \([1]\).

For “\(\equiv (\mod 4)\)”, there are 4 equivalence classes: \([0]\), \([1]\), \([2]\) and \([3]\).

For “\(\equiv (\mod 5)\)”, there are 5 equivalence classes: \([0]\), \([1]\), \([2]\), \([3]\) and \([4]\).

For “\(\equiv (\mod n)\)”, there are \(n\) equivalence classes: \([0]\), \([1]\), \([2]\), ..., \([n-2]\), \([n-1]\), for all \(n \in \mathbb{Z}^+\).