Congruence

When we consider the classes of even and odd integers, we are doing modular 
arithmetic. An integer is even if and only if after dividing it by 2 the remainder 
is 0, whereas an integer is odd if and only if after dividing it by 2 the remainder 
is 1. We say that two integers are congruent modulo 2 if either they are both 
even or they are both odd.

More generally:

**Definition 19.1.1.** Let $m$ be a positive integer. Two integers $a$ and $b$ are 
 **congruent modulo** $m$ if and only if their difference $a - b$ is divisible by $m$.

**Notation:** We often write this as $m | (a - b)$ and often use the fact that this 
means that there exists $q \in \mathbb{Z}$ such that

$$a - b = mq.$$ 

One writes

$$a \equiv b \mod m$$

for $a$ and $b$ being congruent modulo $m$.

**Examples:**

(1) 

17 and 5 are congruent modulo 3

since $17 - 5 = 12$ is divisible by 3. We write this as

$$17 \equiv 5 \mod 3.$$ 

(2) As above, two integers $a$ and $b$ are congruent modulo 2 if and only if 
either

$a$ and $b$ are both even or $a$ and $b$ are both odd.

For example the two odd integers 23 and 7 are congruent modulo 2 since 
$23 - 7 = 16$ is divisible by 2.

**Equivalence Relation Properties of Congruence Modulo $m$:**

**(1) Reflexive.** Any integer $a$ is congruent to itself modulo $m$:

$$a \equiv a \mod m$$

since $a - a = 0$ is of course divisible by $m$: $0 = m \cdot 0$.

**(2) Symmetric.** If $a$ is congruent to $b$ modulo $m$, then $b$ is congruent to 
a modulo $m$, i.e.,

$$a \equiv b \mod m \text{ implies } b \equiv a \mod m.$$ 

Indeed, $m | (a - b)$ implies $m | (b - a)$. (Check that if $m$ divides an integer, then 
m divides its negative.)
(3) **Transitive.** If \(a\) is congruent to \(b\) modulo \(m\) and if \(b\) is congruent to \(c\) modulo \(m\), then \(a\) is congruent to \(c\) modulo \(m\), i.e.,

\[ a \equiv b \mod m \quad \text{and} \quad b \equiv c \mod m \quad \text{implies} \quad a \equiv c \mod m. \]

Indeed, \(m | (a - b)\) and \(m | (b - c)\) implies \(m | ((a - b) + (b - c))\), i.e., \(m | (a - c)\).

(We used that if \(m\) divides two integers, then \(m\) divides their sum.)

**Examples:**

1. Reflexive: \(87 \equiv 87 \mod 18\).
2. Symmetric: \(6 \equiv 32 \mod 13\) implies \(32 \equiv 6 \mod 13\).
3. Transitive: \(6 \equiv 32 \mod 13\) and \(32 \equiv 45 \mod 13\) implies \(6 \equiv 45 \mod 13\).

**Exercise 1.** Using what you did in Homework #7, show that:

(a) If \(a \in \mathbb{Z}\), then \(a^2 \equiv 0 \mod 4\) or \(a^2 \equiv 1 \mod 4\).
(b) If \(a \in \mathbb{Z}\), then \(a^2 \equiv 0 \mod 3\) or \(a^2 \equiv 1 \mod 3\).
(c) Find out what \(a^2 \mod 5\) can be. Hint: look at the solution to Exercise 15.2 on p. 330.

**Addition and multiplication and modulus:**

**Proposition 19.1.3:** If \(a_1 \equiv a_2 \mod m\) and \(b_1 \equiv b_2 \mod m\), then

(i) \(a_1 + a_2 \equiv b_1 + b_2 \mod m\),

(ii) \(a_1 - a_2 \equiv b_1 - b_2 \mod m\),

(iii) \(a_1 a_2 \equiv b_1 b_2 \mod m\).

Note that:

Even + Even = Even,

Odd + Odd = Even,

Even + Odd = Even,

Odd + Even = Even.

That is, an even integer plus an even integer is always an even integer, etc.

We can write this in a ‘addition table’:

<table>
<thead>
<tr>
<th>+</th>
<th>Even</th>
<th>Odd</th>
</tr>
</thead>
<tbody>
<tr>
<td>Even</td>
<td>Even</td>
<td>Odd</td>
</tr>
<tr>
<td>Odd</td>
<td>Odd</td>
<td>Even</td>
</tr>
</tbody>
</table>

We also have a ‘multiplication table’:

<table>
<thead>
<tr>
<th>(\times)</th>
<th>Even</th>
<th>Odd</th>
</tr>
</thead>
<tbody>
<tr>
<td>Even</td>
<td>Even</td>
<td>Even</td>
</tr>
<tr>
<td>Odd</td>
<td>Even</td>
<td>Odd</td>
</tr>
</tbody>
</table>

What we have observed above, in a different language, is the following.

**Exercise 2.** Show that if \(a_1\) and \(a_2\) are congruent modulo 2 and \(b_1\) and \(b_2\) are congruent modulo 2, then \(a_1 + b_1\) and \(a_2 + b_2\) are congruent modulo 2. What does this have to do with the addition table above?
Congruence and remainders.

Recall that the Division Theorem says that given \( m \in \mathbb{Z}^+ \) and \( a \in \mathbb{Z} \), there exist unique integers \( q \) and \( r \) such that

\[
a = mq + r, \quad 0 \leq r \leq m - 1. \tag{1}
\]

That is, we can divide \( a \) by \( m \) to get a remainder \( r \). Let

\[ R_m = \{0, 1, 2, \ldots, m - 1\} \]

be the set of remainders (modulo \( m \)).

**Example:** (a) The set of remainders modulo 4 is

\[ R_4 = \{0, 1, 2, 3\}. \]

A square number always has a remainder of either 0 or 1 modulo 4. (See earlier exercise.)

(b) The set of remainders modulo 10 is

\[ R_4 = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}. \]

For any integer \( x \), we have \( x \equiv y \mod 10 \), where \( y \) is the last digit of \( x \). For example,

\[ 193, 654, 932, 648, 297 \equiv 7 \mod 10. \]

Notice what the possible last digits of square numbers are.

Equation (1) implies

\[ a - r = mq. \]

So, by definition,

\[ a \equiv r \mod m. \]

We have shown that:

*For any \( m \in \mathbb{Z}^+ \) and \( a \in \mathbb{Z} \) there exists a unique integer \( r \in R_m \) such that \( a \equiv r \mod m \).*

**Exercise 3.** Prove that two integers are congruent modulo \( m \) if and only if they have the same remainder after being divided by \( m \).

**Example.** Congruence modulo 3 divides the integers into 3 classes:

- integers congruent to 0,
- integers congruent to 1,
- integers congruent to 2.

We can think of congruence as assigning colors to integers. Two integers having the same color does not mean they are equal. But we think of two integers having the same color as saying that they are equivalent in a sense. Each positive integer \( m \) gives a unique sense in which integers are equivalent.
Congruence modulo 3 assigns three possible colors to numbers. Say the integers congruent to 0 are red, the integers congruent to 1 are white, and the integers congruent to 2 are blue.

**Exercise 4.** Show that adding a red integer to an integer does not change the color of that integer. Show that the sum of a white integer and a blue integer must be a red integer.

The exercise tells us:

*The color of* $a + b$ *depends only on the color of* $a$ *and the color of* $b$.

Another way of saying this is:

*If* $a_1$ *and* $a_2$ *have the same color and if* $b_1$ *and* $b_2$ *have the same color, then* $a_1 + b_1$ *and* $a_2 + b_2$ *have the same color.*

In other words:

*If* $a_1 \equiv a_2 \mod 3$ *and* $b_1 \equiv b_2 \mod 3$, *then* $a_1 + b_1 \equiv a_2 + b_2 \mod 3$. 
