Part V. Chapter 19. Congruence of integers

Even and odd integers, revisited

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. Let $R_2 = \{0, 1\}$ be the set of remainders modulo 2.

Note that:

- Even + Even = Even,
- Odd + Odd = Even,
- Even + Odd = Odd,
- Odd + Even = Odd.

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>

In terms of the remainder after dividing by 2, for the elements of $R_2$ we have

<table>
<thead>
<tr>
<th>+</th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

We also have a ‘multiplication table’:

<table>
<thead>
<tr>
<th>×</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>

<table>
<thead>
<tr>
<th>×</th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

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

**Exercise 1** Verify 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.
**Congruence modulo** \( m \)

More generally, let \( m \) be a positive integer.

**Definition.** Integers \( a \) and \( b \) are **congruent modulo** \( m \) if and only if \( a - b \) is divisible by \( m \).

For example,

1. \( 277 \) and \( 2 \) are congruent modulo \( 5 \).
2. \( -3 \) and \( 17 \) are congruent modulo \( 4 \).

We often write this condition as \( m \mid (a - b) \) and we 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 \( m \). E.g., \( -3 \equiv 17 \mod 4 \).

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

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

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 \( m \)). Of course, \( r \in R_m \).

E.g., \( 277 = 5 \cdot 55 + 2 \) and \( 2 \in R_5 \).

Equation (1) implies

\[
a - r = mq.
\]

So, by definition,

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

E.g., \( 277 \equiv 2 \mod 5 \).

In fact, 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 \( a \equiv r \mod m \).

Note that two integers are congruent modulo \( m \) if and only if they have the same remainder after being divided by \( m \).
Example (modulo 3). Let \( m = 3 \). Then \( 20 \equiv 5 \mod 3 \) since \( 20 - 5 = 15 \) is divisible by 3 (note that 20 and 5 both have the remainder 2 after being divided by 3).

1. 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. If \( a \) is congruent to \( b \) modulo \( m \), then \( b \) is congruent to \( a \) modulo \( m \), i.e.,
   \[
   a \equiv b \mod m \implies b \equiv a \mod m.
   \]
   Indeed, \( m | (a - b) \) implies \( m | (b - a) \).

3. 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.,
   \[
   a \equiv b \mod m \quad \text{and} \quad b \equiv c \mod m \implies a \equiv c \mod m.
   \]
   Indeed, \( m | (a - b) \) and \( m | (b - c) \) implies \( m | ((a - b) + (b - c)) \), i.e., \( m | (a - c) \).

Congruence classes modulo \( m \) (for \( m = 3 \))

Example. Again let \( m = 3 \). Congruence modulo 3 divides the integers into 3 categories (classes):

\[
\begin{align*}
[0] & \triangleq \text{integers congruent to 0}, \\
[1] & \triangleq \text{integers congruent to 1}, \\
[2] & \triangleq \text{integers congruent to 2}.
\end{align*}
\]

The set of integers congruent to 0 are those integers which divided by 3 yield a remainder of 0, i.e., they are the multiples of 3:

\[
[0] = \{ \ldots, -9, -6, -3, 0, 3, 6, 9, \ldots \}.
\]

The set of integers congruent to 1 are those integers which divided by 3 yield a remainder of 1, i.e., they are the multiples of 3 plus 1:

\[
[1] = \{ \ldots, -8, -5, -2, 1, 4, 7, 10, \ldots \}.
\]

The set of integers congruent to 2 are those integers which divided by 3 yield a remainder of 1, i.e., they are the multiples of 3 plus 2:

\[
[2] = \{ \ldots, -7, -4, -1, 2, 5, 8, 11, \ldots \}.
\]
Note that each congruence class \([0]\), \([1]\) and \([2]\) is a subset of integers. They are disjoint from one another:

\[
[0] \cap [1] = \emptyset, \quad [0] \cap [2] = \emptyset, \quad [1] \cap [2] = \emptyset
\]

and their union comprises all of the integers:

\[
[0] \cup [1] \cup [2] = \mathbb{Z}.
\]

Another way of saying this is every integer is in exactly one of the three congruence classes \([0]\), \([1]\) and \([2]\).

We can think of congruence as assigning colors to numbers. 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 2** 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 says that:

*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 \(a_1 + b_1 \equiv a_2 + b_2 \mod 3\).*

**Proposition 3 (Eccles 19.1.3)** If \(a_1 \equiv a_2 \mod m\) and \(b_1 \equiv b_2 \mod m\), then

1. \(a_1 + b_1 \equiv a_2 + b_2 \mod m\),
2. \(a_1 - b_1 \equiv a_2 - b_2 \mod m\),
3. \(a_1 b_1 \equiv a_2 b_2 \mod m\).
Linear congruences modulo \( m \)

A linear congruence is an equation of the form

\[ ax \equiv b \mod m. \]

We approach this by working some examples from Eccles’ book.

**Example 19.3.4.** Solve:

\[ 6x \equiv 15 \mod 21. \]

*Note that 3 divides each of 6, 15 and 21.*

**Step 1.** Since 3 divides 6, 15 and 21, this is equivalent to:

\[ 2x \equiv 5 \mod 7. \]

Here we used the following fact:

**Lemma 1.** If \( d \) divides \( a, b \) and \( m \), then

\[ ax \equiv b \mod m \]

is equivalent to

\[ \frac{a}{d}x \equiv \frac{b}{d} \mod \frac{m}{d}. \]

**Step 2.** \( 2x \equiv 5 \mod 7 \) is equivalent to

\[ 2x \equiv 12 \mod 7. \]

Here we used the following fact:

**Lemma 2.** \( ax \equiv b \mod m \) is equivalent to \( ax \equiv b + cm \mod m \) for any integer \( c \).

**Step 3.** \( 2x \equiv 12 \mod 7 \) is equivalent to

\[ x \equiv 6 \mod 7. \]

Here we used the following:

**Lemma 3.** If \( \gcd(a, m) = 1 \), then \( ax \equiv ac \mod m \) is equivalent to

\[ x \equiv c \mod m. \]

From Step 3 we conclude that the equation \( 6x \equiv 15 \mod 21 \) is equivalent to \( x \equiv 6 \mod 7 \). The solutions to this equation are

\[ \{\ldots, -8, -1, 6, 13, 20, \ldots\} = \{6 + 7n \mid n \in \mathbb{Z}\}. \]
**Lemma 1.** If $d$ divides $a$, $b$ and $m$, then

$$ax \equiv b \mod m$$

is equivalent to

$$\frac{a}{d}x \equiv \frac{b}{d} \mod \frac{m}{d}.$$ 

**Proof of Lemma 1.** $ax \equiv b \mod m$ is equivalent to $m \mid (ax - b)$. Since $d$ divides $ax - b$ ($d$ divides both $a$ and $b$), this is equivalent to

$$\frac{m}{d} \mid \frac{ax - b}{d},$$

that is,

$$\frac{m}{d} \mid \left( \frac{a}{d}x - \frac{b}{d} \right),$$

which is equivalent to $\frac{a}{d}x \equiv \frac{b}{d} \mod \frac{m}{d}$. \Box

**Lemma 2.** $ax \equiv b \mod m$ is equivalent to $ax \equiv b + cm \mod m$ for any integer $c$.

**Proof of Lemma 2.**

$$ax \equiv b \mod m$$

$\iff$

$$m \mid (ax - b)$$

$\iff$

$$m \mid (ax - b - cm)$$

$\iff$

$$ax \equiv b + cm \mod m. \Box$$

**Lemma 3.** If $\gcd(a, m) = 1$, then $ax \equiv ac \mod m$ is equivalent to

$$x \equiv c \mod m.$$

**Proof of Lemma 3.**

$$ax \equiv ac \mod m$$

$\iff$

$$m \mid (ax - ac)$$

$\iff$

$$m \mid a(x - c).$$

Since $\gcd(a, m) = 1$, this is equivalent to $m \mid (x - c)$, i.e., $x \equiv c \mod m$. \Box
Example 19.3.3. Solve:

\[ 4x \equiv 12 \mod 14. \]

Note that 4 divides 4 and 12 but not 14. And note \( \gcd(4,14) = 2 \).

By the proposition below, we have that \( 4x \equiv 12 \mod 14 \) is equivalent to \( x \equiv 3 \mod 7 \).

Here is the general result about dividing congruence equations.

**Proposition.** Let \( m \in \mathbb{Z}^+ \) and \( a \in \mathbb{Z} \) and let \( g = \gcd(a,m) \). If \( ab_1 \equiv ab_2 \mod m \), then

\[ b_1 \equiv b_2 \mod \frac{m}{g}. \]

**Proof.** Suppose \( ab_1 \equiv ab_2 \mod m \). Then \( m\mid a(b_1 - b_2) \). This implies \( \frac{m}{g}\mid \frac{a}{g}(b_1 - b_2) \). Since \( \gcd(\frac{m}{g},\frac{a}{g}) = 1 \), we conclude that \( \frac{m}{g}\mid (b_1 - b_2) \). This says that \( b_1 \equiv b_2 \mod \frac{m}{g} \).

**Corollary 1:** Proposition 19.3.1. This the proposition in the case where \( a\mid m \), i.e., \( \gcd(a,m) = a \). (Show this is equivalent to Lemma 1 above.)

**Corollary 2:** Proposition 19.3.2. This the proposition in the case where \( \gcd(a,m) = 1 \). (Show this is equivalent to Lemma 3 above.)