Modular Arithmetic

Modular arithmetic is a way of systematically ignoring differences involving a multiple of an integer. If \( n \) is an integer, two integers are equal mod \( n \) if they differ by a multiple of \( n \); it is as if multiples of \( n \) are "set equal to 0".

Definition. Let \( n \), \( x \), and \( y \) be integers. \( x \) is congruent to \( y \) mod \( n \) if \( n \mid x - y \). The notation

\[
x = y \pmod{n}
\]

means that \( x \) is congruent to \( y \) mod \( n \).

Example.

\[
7 = 1 \pmod{6}, \quad \text{since} \quad 6 \mid 7 - 1.
\]

\[
57 = -13 \pmod{7}, \quad \text{since} \quad 7 \mid 57 - (-13).
\]

A number is even if and only if it’s congruent to 0 mod 2; a number is odd if and only if it’s congruent to 1 mod 2.

The following proposition says that you can work with modular equations in many of the ways that you work with ordinary equations.

Proposition. Let \( n \in \mathbb{Z} \).

(a) If \( a = b \pmod{n} \) and \( c = d \pmod{n} \), then

\[
a + c = b + d \pmod{n}.
\]

(b) If \( a = b \pmod{n} \) and \( c = d \pmod{n} \), then

\[
ac = bd \pmod{n}.
\]

(c) If \( a = b \pmod{n} \), then

\[
ac = bc \pmod{n}.
\]

Proof.

- You can often prove statements about congruences by reducing them to statements about divisibility.
- You can often prove statements about divisibility by reducing them to equations.

(a) Suppose \( a = b \pmod{n} \) and \( c = d \pmod{n} \).

\( a = b \pmod{n} \) means \( n \mid a - b \) and \( c = d \pmod{n} \) means \( n \mid c - d \). By properties of divisibility,

\[
n \mid (a - b) + (c - d) = (a + c) - (b + d).
\]

Therefore, \( a + c = b + d \pmod{n} \).

(b) Suppose \( a = b \pmod{n} \) and \( c = d \pmod{n} \).

\( a = b \pmod{n} \) means \( n \mid a - b \), which means \( a - b = jn \) for some \( j \in \mathbb{Z} \). \( c = d \pmod{n} \) means \( n \mid c - d \), which means \( c - d = kn \) for some \( k \in \mathbb{Z} \). Thus, \( a = b + jn, c = d + kn \), and hence

\[
ac = (b + jn)(d + kn) = bd + bkn + djn + jkn^2 = bd + n(bk + dj + jk) = bd + n(kd + aj).
\]
This gives \( ac - bd = n(kk + dj + jkn) \), so \( n \mid ac - bd \), and hence \( ac = bd \pmod{n} \).

(c) Suppose \( a = b \pmod{n} \). This means that \( n \mid a - b \). By properties of divisibility,

\[
 n \mid (a - b)c = ac - bc.
\]

Therefore, \( ac = bc \pmod{n} \). □

Example. Solve \( 3x + 4 = 2x + 8 \pmod{9} \).

In this case, I’ll solve the modular equation by adding or subtracting the same thing from both sides.

\[
\begin{align*}
3x + 4 &= 2x + 8 \pmod{9} \\
-4 &= 4 \pmod{9} \\
3x &= 2x + 4 \pmod{9} \\
-x &= 4 \pmod{9}
\end{align*}
\]

The solution is \( x = 4 \pmod{9} \). □

The next result says that congruence \( \pmod{n} \) is an **equivalence relation**.

**Proposition.**

(a) (Reflexivity) \( a = a \pmod{n} \) for all \( a \in \mathbb{Z} \).

(b) (Symmetry) Let \( a, b \in \mathbb{Z} \). If \( a = b \pmod{n} \), then \( b = a \pmod{n} \).

(c) (Transitivity) Let \( a, b, c \in \mathbb{Z} \). If \( a = b \pmod{n} \) and \( b = c \pmod{n} \), then \( a = c \pmod{n} \).

**Proof.** (a) If \( a \in \mathbb{Z} \), then \( n \mid a - a \), so \( a = a \pmod{n} \).

(b) If \( a = b \pmod{n} \), then \( n \mid a - b \), so \( n \mid -(a - b) = b - a \). Therefore, \( b = a \pmod{n} \).

(c) Suppose \( a = b \pmod{n} \) and \( b = c \pmod{n} \). \( a = b \pmod{n} \) means \( n \mid a - b \); \( b = c \pmod{n} \) means \( n \mid b - c \). Therefore,

\[
 n \mid (a - b) + (b - c) = a - c.
\]

Hence, \( a = c \pmod{n} \). □

An equivalence relation on a set gives rise to a **partition** of the set into equivalence classes. In the case of congruence \( \pmod{n} \), an equivalence class consists of integers congruent to each other \( \pmod{n} \).

**Definition.** \( \mathbb{Z}_n \) (read “\( \mathbb{Z} \pmod{n} \)”) is the set of equivalence classes under congruence \( \pmod{n} \).

**Example.** Consider the equivalence relation of congruence \( \pmod{3} \) on \( \mathbb{Z} \). The integers break up into three
*disjoint* sets:

```
| -10 | -9 | -8 | -7 | -6 | -5 | -4 | -3 | -2 | -1 |  0 |  1 |  2 |  3 |  4 |  5 |  6 |  7 |  8 |  9 | 10 |
```

```
| -10 | -7 | -4 | -1 |  2 |  5 |  8 |
```

```
| -9 | -6 | -3 |  0 |  3 |  6 |  9 |
```

```
| -8 | -5 | -2 |  1 |  4 |  7 | 10 |
```

All the elements of a given set are congruent mod 3, and no element in one set is congruent mod 3 to an element of another. The sets divide up the integers like three puzzle pieces.

It’s cumbersome to write and use equivalence classes as is, since each equivalence class is a set (infinite, in this case). It’s customary to choose a *representative* from each equivalence class and use the representatives to do arithmetic. I’ll choose

0 from \{ \ldots, -9, -6, -3, 0, 3, 6, 9, \ldots \},

1 from \{ \ldots, -8, -5, -2, 1, 4, 7, 10, \ldots \},

2 from \{ \ldots, -7, -4, -1, 2, 5, 8, 11, \ldots \}.

I’ll abuse notation and write

\[ \mathbb{Z}_3 = \{ 0, 1, 2 \}. \]

\( \mathbb{Z}_3 \) is called the **cyclic group of order** 3. The “cyclic” nature of \( \mathbb{Z}_3 \) can be visualized by arranging the integers in a spiral, with each congruence class on a ray.

![Spiral Diagram](image)

When you do arithmetic in \( \mathbb{Z}_3 \), it is as if you count in a circle: 0, 1, 2, then back to 0 again.

You can form other cyclic groups in an analogous way. For example,

\[ \mathbb{Z}_6 = \{ 0, 1, 2, 3, 4, 5 \}. \]

You can do arithmetic in \( \mathbb{Z}_n \) by adding and multiplying as usual, but **reducing the results mod** \( n \).
Example. Here are the addition and multiplication tables for \( \mathbb{Z}_3 \):

\[
\begin{array}{c|ccc}
+ & 0 & 1 & 2 \\
\hline
0 & 0 & 1 & 2 \\
1 & 1 & 2 & 0 \\
2 & 2 & 0 & 1 \\
\end{array}
\quad
\begin{array}{c|cccc}
\cdot & 0 & 1 & 2 \\
\hline
0 & 0 & 0 & 0 \\
1 & 0 & 1 & 2 \\
2 & 0 & 2 & 1 \\
\end{array}
\]

For example, as integers \( 2 + 2 = 4 \). I divide \( 4 \) by the modulus \( 3 \) and get a remainder of \( 1 \). Hence, \( 2 + 2 = 1 \).

Likewise, \( 2 \cdot 2 = 4 = 1 \) in \( \mathbb{Z}_3 \). \( \square \)

Example.

\[
\begin{align*}
6 \cdot 7 &= 9 \text{ in } \mathbb{Z}_{11}.
13 + 19 &= 11 \text{ in } \mathbb{Z}_{21}.
-8 &= 9 \text{ in } \mathbb{Z}_{17}.
\end{align*}
\]

Strictly speaking, \(-8\) is not in \(\mathbb{Z}_{17}\). The last statement is just another way of saying \(-8 \equiv 9 \pmod{17}\). \( \square \)

I showed earlier how to use algebraic operations to solve simple modular equations. How would you solve something like this:

\[
6x = 13 \pmod{25}?
\]

I’d like to divide both sides by \( 6 \), but I only know how to add and multiply. I can subtract, but that’s because I can add additive inverses. Well, division is multiplication by the multiplicative inverse; what is a multiplicative inverse mod \( 25 \)?

Definition. Let \( a, b \in \mathbb{Z}_n \). \( a \) and \( b \) are multiplicative inverses if \( ab = 1 \pmod{n} \) (or \( ab = 1 \) in \( \mathbb{Z}_n \)).

If \( a \) is the multiplicative inverse of \( b \), you can write \( a = b^{-1} \) — but don’t write \( \frac{1}{b} \), that’s bad manners.

Example. \( 6 \) and \( 2 \) are multiplicative inverses mod \( 11 \), because \( 6 \cdot 2 = 1 \pmod{11} \).

\( 1 \) is always its own multiplicative inverse.

On the other hand, \( 8 \) does not have a multiplicative inverse mod \( 12 \). You can see that by trying cases:

\[
\begin{array}{c|ccccc}
\multicolumn{6}{c}{n} \\
\hline
8n \pmod{12} & 0 & 1 & 2 & 3 & 4 \\
\hline
n & 6 & 7 & 8 & 9 & 10 \\
\hline
8n \pmod{12} & 0 & 8 & 4 & 0 & 8 \\
\end{array}
\]

No number multiplied by \( 8 \) gives \( 1 \) mod \( 12 \).

I could try all the possibilities because the numbers were small. How would you do this kind of problem if the numbers were larger?

One approach is to simply appeal to the result following this example. However, I can also give a proof by contradiction.

Suppose that \( 8 \) has a multiplicative inverse mod \( 12 \). Let \( x \) be the multiplicative inverse. Then \( 8x = 1 \pmod{12} \). Multiplying both sides by \( 3 \), I get

\[
24x = 3 \pmod{12}, \quad \text{or} \quad 0 = 3 \pmod{12}.
\]
This is a contradiction, since 0 and 3 do not differ by a multiple of 12. Therefore, 8 does not have a multiplicative inverse mod 12. □

**Proposition.** $m \in \mathbb{Z}_n$ has a multiplicative inverse if and only if $(m, n) = 1$.

**Proof.** Suppose $m \in \mathbb{Z}_n$ has a multiplicative inverse, so

$$km = 1 \text{ for some } k \in \mathbb{Z}_n.$$ 

I can regard this as a statement in $\mathbb{Z}$:

$$km = 1 \pmod{n}.$$ 

This means that $km$ and 1 differ by a multiple of $n$:

$$km - 1 = an \text{ for some } a \in \mathbb{Z}.$$ 

Thus,

$$km - an = 1.$$ 

This is a linear combination of $m$ and $n$ which gives 1. Therefore, $(m, n) = 1$. Conversely, suppose $(m, n) = 1$. I may find integers $a$ and $b$ such that

$$am + bn = 1.$$ 

That is,

$$am = 1 \pmod{n}.$$ 

Now regarded as an equation in $\mathbb{Z}_n$, this says

$$am = 1 \text{ in } \mathbb{Z}_n.$$ 

That is, $m$ is a unit with multiplicative inverse $a$. □

**Example.** Find the multiplicative inverse of 31 in $\mathbb{Z}_{52}$.

Note that $(31, 52) = 1$. Apply the Extended Euclidean Algorithm:

<table>
<thead>
<tr>
<th>a</th>
<th>q</th>
<th>y</th>
</tr>
</thead>
<tbody>
<tr>
<td>52</td>
<td></td>
<td>5</td>
</tr>
<tr>
<td>31</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>21</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>10</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>10</td>
<td>0</td>
</tr>
</tbody>
</table>

Thus,

$$1 = 3 \cdot 52 + (-5) \cdot 31.$$ 

In $\mathbb{Z}_{52}$, 52 = 0 and $-5 = 47$. The equation says $1 = 47 \cdot 31$. Thus, 47 is the multiplicative inverse of 31 in $\mathbb{Z}_{52}$. □
Theorem. If \((a, n) = 1\), then the equation
\[
ax = b \quad \text{in} \quad \mathbb{Z}_n
\]
has a unique solution.

Proof. If \((a, n) = 1\), then \(a\) has a multiplicative inverse \(a^{-1}\) in \(\mathbb{Z}_n\). Thus, \(aa^{-1} = 1\) in \(\mathbb{Z}_n\).

First, this means that \(x = a^{-1}b\) is a solution, since
\[
a(a^{-1}b) = (aa^{-1})b = 1 \cdot b = b.
\]

Second, if \(x'\) is another solution, then \(ax' = b\). Multiplying both sides by \(a^{-1}\), I get
\[
a^{-1}ax' = a^{-1}b, \quad x' = a^{-1}b.
\]

That is, \(x' = x\). This means the solution is unique. \(\square\)

Example. Solve
\[
13x = 12 \quad \text{(mod 15)}.
\]

There is a solution, since \((13, 15) = 1\). I need to find a multiplicative inverse for 13 mod 15.

\[
\begin{array}{ccc}
a & q & y \\
15 & - & 7 \\
13 & 1 & 6 \\
2 & 6 & 1 \\
1 & 2 & 0 \\
\end{array}
\]

The Extended Euclidean Algorithm says that
\[
(-6)(15) + (7)(13) = 1.
\]

Hence, \(7 \cdot 13 = 1 \quad \text{(mod 15)}\), i.e. 7 is the multiplicative inverse of 13 mod 15.

Multiply the original equation by 7:
\[
7 \cdot 13x = 7 \cdot 12 \quad \text{(mod 15)}, \quad x = 84 = 9 \quad \text{(mod 15)}. \quad \square
\]

©1999 by Bruce Ikemaga