Linear Congruences

**Theorem.** Let \( d = (a, m) \), and consider the equation

\[
ax = b \pmod{m}.
\]

(a) If \( d \nmid b \), there are no solutions.

(b) If \( d \mid b \), there are exactly \( d \) distinct solutions \( \pmod{m} \).

**Proof.** Observe that

\[
ax = b \pmod{m} \iff ax + my = b \text{ for some } y.
\]

Hence, (a) follows immediately from the corresponding result on linear Diophantine equations. The result on linear Diophantine equations which corresponds to (b) says that if \( x_0 \) is a particular solution, then there are infinitely many integer solutions

\[
x = x_0 + \frac{m}{d} t.
\]

I need to show that of these infinitely many solutions, there are exactly \( d \) distinct solutions \( \pmod{m} \). Suppose two solutions of this form are congruent \( \pmod{m} \):

\[
x_0 + \frac{m}{d} t_1 = x_0 + \frac{m}{d} t_2 \pmod{m}.
\]

Then

\[
\frac{m}{d} t_1 = \frac{m}{d} t_2 \pmod{m}.
\]

Now \( \frac{m}{d} \) divides both sides, and \( \left( \frac{m}{d}, m \right) = \frac{m}{d} \), so I can divide this congruence through by \( \frac{m}{d} \) to obtain

\[
t_1 = t_2 \pmod{d}.
\]

Going the other way, suppose \( t_1 = t_2 \pmod{d} \). This means that \( t_1 \) and \( t_2 \) differ by a multiple of \( d \):

\[
t_1 - t_2 = kd.
\]

So

\[
\frac{m}{d} t_1 - \frac{m}{d} t_2 = \frac{m}{d} \cdot kd = km.
\]

This implies that

\[
\frac{m}{d} t_1 = \frac{m}{d} t_2 \pmod{m}.
\]

So

\[
x_0 + \frac{m}{d} t_1 = x_0 + \frac{m}{d} t_2 \pmod{m}.
\]

Let me summarize what I’ve just shown. I’ve proven that two solutions of the above form are equal \( \pmod{m} \) if and only if their parameter values are equal \( \pmod{d} \). That is, if I let \( t \) range over a complete system of residues \( \pmod{d} \), then \( x_0 + \frac{m}{d} t \) ranges over all possible solutions \( \pmod{m} \). To be very specific, all the solutions \( \pmod{m} \) are given by

\[
x_0 + \frac{m}{d} t \pmod{m} \quad \text{for} \quad t = 0, 1, 2, \ldots, d - 1.
\]

---

**Example.** Solve \( 6x = 7 \pmod{8} \).
Since \((6, 8) = 2 \nmid 7\), there are no solutions. \(\Box\)

**Example.** Solve \(3x = 7 \pmod{4}\).

Since \((3, 4) = 1 \mid 7\), there will be 1 solutions mod 4. I’ll find it in three different ways.

**Using linear Diophantine equations.**

\[
3x = 7 \pmod{4} \implies 3x + 4y = 7 \quad \text{for some } y.
\]

By inspection \(x_0 = 1, y_0 = 1\) is a particular solution. \((3, 4) = 1\), so the general solution is

\[
x = 1 + 4t, \quad y = 1 - 3t.
\]

The \(y\) equation is irrelevant. The \(x\) equation says

\[
x = 1 \pmod{4}.
\]

**Using the Euclidean algorithm.** Since \((3, 4) = 1\), some linear combination of 3 and 4 is equal to 1. In fact,

\[
(-1) \cdot 3 + 1 \cdot 4 = 1.
\]

This tells me how to juggle the coefficient of \(x\) to get \(1 \cdot x\):

\[
\begin{align*}
4x &\equiv 0 \pmod{4} \\
-3x &\equiv 7 \pmod{4} \\
x &\equiv 1 \pmod{4}
\end{align*}
\]

(I used the fact that \(7 = -1 \pmod{4}\).

**Using inverses mod 4.** Here is a multiplication table mod 4:

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

I see that \(3 \cdot 3 = 1 \pmod{4}\), so I multiply the equation by 3:

\[
3x = 7 \pmod{4}, \quad x = 21 = 1 \pmod{4}. \quad \Box
\]

**Theorem.** Let \(d = (a, b, m)\), and consider the equation

\[
ax + by = c \pmod{m}.
\]

(a) If \(d \nmid c\), there are no solutions.

(b) If \(d \mid c\), there are exactly \(md\) distinct solutions mod \(m\).

I won’t give the proof; it follows from the corresponding result on linear Diophantine equations.
**Example.** Solve

\[ 2x + 6y = 4 \pmod{10}. \]

\((2, 6, 10) = 2 \mid 4\), so there are \(2 \cdot 10 = 20\) solutions mod 10. I’ll solve the equation using a reduction trick similar to the one I used to solve two variable linear Diophantine equations.

The given equation is equivalent to

\[ 2x + 6y + 10z = 4 \quad \text{for some} \quad z. \]

Set

\[ w = \frac{2}{(2, 6)} x + \frac{6}{(2, 6)} y. \]

Then

\[(2, 6)w + 10z = 4, \quad 2w + 10z = 4, \quad w + 5z = 2.\]

\(w_0 = -3, \ z_0 = 1\), is a particular solution. The general solution is

\[ w = -3 + 5s, \quad z = 1 - s. \]

Substitute for \(w\):

\[ \frac{2}{(2, 6)} x + \frac{6}{(2, 6)} y = -3 + 5s, \quad x + 3y = -3 + 5s. \]

\(x_0 = 5s, \ y_0 = -1\), is a particular solution. The general solution is

\[ x = 5s + 3t, \quad y = -1 - t. \]

\(t = 0, 1, \ldots, 9\) will produce distinct values of \(y\) mod 10. Note, however, that \(s\) and \(s + 2r\) produce \(5s\) and \(5s + 10r\), which are congruent mod 10. That is, adding a multiple of 2 to a given value of \(s\) makes the \(5s\) term in \(x\) repeat itself mod 10. So I can get all possibilities for \(x\) mod 10 by letting \(s = 0, 1\).

All together, the distinct solutions mod 10 are

\[ x = 5s + 3t, \quad y = -1 - t, \quad \text{where} \quad s = 0, 1 \quad \text{and} \quad t = 0, 1, \ldots, 9. \quad \square \]

**Remarks:** I saw the particular solution \(x_0 = 5s, \ y_0 = -1\) by inspection. In general, you can get one using the Extended Euclidean algorithm. For example, in this case

\[ 1 = (1, 3) = 1 \cdot (-2) + 3 \cdot 1. \]

Multiply by \(-3 + 5s\) (to match \(x + 3y = -3 + 5s\)) to get

\[-3 + 5s = 1 \cdot [-2(-3 + 5s)] + 3 \cdot (-3 + 5s).\]

So a particular solution is \(x_0 = -2(-3 + 5s) = 6 - 10s\) and \(y_0 = -3 + 5s\).

In general, it can be tricky to determine the parameter ranges which give the correct number of solutions; it may require some trial-and-error, or careful analysis of the general solution.