Math 406 Section 4.2: Solving Linear Congruences

---

1. **Introduction:**

   Solving congruences is hard and so we will begin with linear congruences:

   $$ax \equiv b \bmod m$$

2. **Do Solutions Exist:**

   Consider that for $x \in \mathbb{Z}$ we have $ax \equiv b \bmod m$ iff there is some $y \in \mathbb{Z}$ such that

   $$ax + my = b$$

   in other words if b is a linear combination of a and m, and this will happen exactly when $\gcd(a, m) \mid b$.

   So for starters we can say that $ax \equiv b \bmod m$ has solutions iff $\gcd(a, m) \mid b$.

3. **Finding One Solution:**

   Once we know this, how can we find one solution for starters? Well we can use the Euclidean Algorithm to solve $ax' + my' = \gcd(a, m)$ and then scale both sides to get b on the right and then the coefficient of a will be our x. We'll typically call this x_0 and write it as the least nonnegative residue mod m.

   Example:

   Consider $4x \equiv 6 \bmod 50$. We have $\gcd(4, 50) = 2 \mid 6$ so that solutions exist. First we use the Euclidean Algorithm to solve:

   $$4x' + 50y' = 2$$

   This gives us $x' = -12$ and $y' = 1$, in other words:

   $$4(-12) + 50(1) = 2$$

   and hence:

   $$4(-36) + 50(3) = 6$$

   So one solution is $x = -36$ and we can see this:

   $$4(-36) \equiv 6 \bmod 50$$

   We'll replace this by the least nonnegative residue $x_0 \equiv 14 \bmod 50$.

4. **Finding All Solutions:**

So now we need to ask if there are other solutions. Suppose we have one, so we have $ax_0 \equiv b \bmod m$. What can we say if x is another solution?

Well suppose $x \in \mathbb{Z}$ is another solution, then we can say:

$$ax \equiv b \bmod m$$

which by subtracting implies:

$$a(x - x_0) \equiv 0 \bmod m$$

This then implies that:

$$x - x_0 \equiv 0 \bmod m/\gcd(m, a)$$

And this implies that:

$$x = x_0 + k\left(\tfrac{m}{\gcd(m,a)}\right) \text{ for } k \in \mathbb{Z}.$$

So we know that if we have another solution then the solution must look like this. However are all these solutions and do they differ?

Well, suppose that we choose $k \in \mathbb{Z}$ and let:

$$x = x_0 + k\left(\frac{m}{\gcd(m, a)}\right)$$

Then observe that:

$$\begin{aligned}
ax &\equiv a(x_0 + k\left(\frac{m}{\gcd(m, a)}\right) \bmod m \\
&\equiv ax_0 + ak\left(\frac{m}{\gcd(m, a)}\right) \bmod m \\
&\equiv b + k\left(\frac{ma}{\gcd(m, a)}\right) \bmod m \\
&\equiv b + k(\operatorname{lcm}(m, a)) \bmod m \\
&\equiv b + k(0) \bmod m \\
&\equiv b \bmod m
\end{aligned}$$

Thus all of these are in fact solutions.

5. **Incongruent solutions mod m**

Lastly, when are they unique mod m?

Well first suppose that we have two solutions, one with k_1 and one with k_2. Then if the solutions are congruent mod m then:

$$\begin{aligned}
x_0 + k_1\left(\frac{m}{\gcd(m,a)}\right) &\equiv x_0 + k_2\left(\frac{m}{\gcd(m,a)}\right) \mod m \\
k_1\left(\frac{m}{\gcd(m,a)}\right) &\equiv k_2\left(\frac{m}{\gcd(m,a)}\right) \mod m \\
k_1 &\equiv k_2 \mod \frac{m}{\gcd(m, m/\gcd(m,a))} \\
k_1 &\equiv k_2 \mod \frac{m}{m/\gcd(m,a)} \\
k_1 &\equiv k_2 \mod \gcd(m,a)
\end{aligned}$$

(Note that $\gcd(m, m/gcd(m,a)) = m/gcd(m,a)$ since $m/gcd(m,a)$ divides both.)

On the other hand if $k_1 \equiv k_2 \mod \gcd(m,a)$ then $k_1 = k_2 + \alpha\gcd(m,a)$ for some $\alpha \in \mathbb{Z}$ and then:

$$\begin{aligned}
x_0 + k_1\left(\frac{m}{\gcd(m,a)}\right) &= x_0 + (k_2 + \alpha\gcd(m,a))\left(\frac{m}{\gcd(m,a)}\right) \\
&\equiv x_0 + k_2\left(\frac{m}{\gcd(m,a)}\right) \mod m
\end{aligned}$$

It follows that solutions differ iff $k_1 \not\equiv k_2 \mod \gcd(m,a)$.

6. **Summary Theorem:**

The linear congruence $ax \equiv b \bmod m$ has solutions iff $\gcd(a, m) \mid b$. If it does then one solution x_0 can be found via the Euclidean Algorithm and then there are $\gcd(m, a)$ distinct solutions mod m which are given by:

$$x \equiv x_0 + k\left(\frac{m}{\gcd(m,a)}\right) \bmod m \text{ for } k = 0, 1, ..., \gcd(m, a) - 1$$

It's typical that for small lists of solutions we will explicitly list each and replace each with its least nonnegative residue if necessary. For large lists of solutions this can get a bit unwieldy.

(a) **Example:**

Our example from earlier, $4x \equiv 6 \bmod 50$, has $\gcd(4, 50) = 2 \mid 6$ and so there are exactly two distinct solutions mod 50. We found one to be $x_0 = 14$ and therefore all solutions have the form:

$$x \equiv 14 + k\left(\frac{50}{\gcd(50,4)}\right) \bmod 50 \text{ for } k = 0, 1$$

That is $x \equiv 14 + 25k \bmod 50$ for $k = 0, 1$, or $x \equiv 14, 39 \bmod 50$.

(b) **Example:**

Consider the linear congruence $20x \equiv 15 \bmod 65$. Since $\gcd(20, 65) = 5 \mid 15$ there are exactly 5 distinct solutions mod 65.

We can obtain one by first using the Euclidean Algorithm to solve:

$$20x' + 65y' = 5$$

This gives us:

$$20(-3) + 65(1) = 5$$

Hence:

$$20(-9) + 65(3) = 15$$

Thus we have $20(-9) \equiv 15 \bmod 65$ and so $x_0 \equiv -9 \bmod 65$ is one solution but we could use the least nonnegative residue solution $x_0 \equiv 56 \bmod 65$.

Therefore all solutions have the form:

$$x \equiv 56 + k\left(\frac{65}{\gcd(65,20)}\right) \bmod 65 \text{ for } k = 0, 1, 2, 3, 4$$

That is $x \equiv 56 + 13k \bmod 65$ for $k = 0, 1, 2, 3, 4$. If we did want to replace these by their least nonnegative residues we would need to list them as $x \equiv 56, 69, 82, 95, 108 \bmod 65$ and replace them to get $x \equiv 56, 4, 17, 30, 43 \bmod 65$.