Linear Congruences

See pages 141-142, especially Theorem 4.17 and Examples 4.19 and 4.20.

Recall that two integers a and b are congruent modulo an integer $m \geq 2$ if $m|(a-b)$, equivalently, $a = mk + b$ for some integer k.

If a and m are relatively prime integers and b is any integer, then the linear congruence $ax \equiv b \bmod m$ is solvable, i.e. there is an integer n such that $an \equiv b \bmod m$. Further, every integer of the form $n + km$, where k is an integer, is also a solution.

Proposition 4.5 ensures that adding an integer to both sides of a (true) congruence and multiplying both sides of a congruence by an integer yield true congruences.

Example. Find all integer solutions to the linear congruence $3x \equiv 4 \bmod 7$.

We would like to multiply both sides of the congruence by an integer s that will "cancel" the 3. (So, in a certain sense, we are looking for a reciprocal for 3.) This means we want $3s \equiv 1$ mod 7.

We list the multiples of 3 until we find one that is one more than a multiple of 7: 3, 6, 9, 12, 15. Since $15 = 2 \cdot 7 + 1$, $15 \equiv 1$ mod 7. Since $15 = 3 \cdot 5$, we choose $s = 5$. We will multiply both sides of the congruence by $s = 5$, knowing that this will "cancel" the 3 on the left side, as follows:

$$\begin{aligned} 3x &\equiv 4 \text{ mod } 7 \\ 5(3x) &\equiv 5(4) \text{ mod } 7 \\ 15x &\equiv 20 \text{ mod } 7 \\ x &\equiv 6 \text{ mod } 7 \end{aligned}$$

The last step follows from the fact that $15 \equiv 1$ mod 7 and $20 \equiv 6$ mod 7.

This means that $x = 6$ is a solution, and any integer of the form $6 + 7k$, for $k \in \mathbb{Z}$ is a solution.

Let's check that this works. First check $x = 6$:

$$3x = 3(6) = 18 = 2 \cdot 7 + 4 \equiv 4 \text{ mod } 7$$

Now, let k be any integer, and check $6 + 7k$:

$$3(6+7k) = 18 + 21k = (2 \cdot 7 + 4) + 21k = 2 \cdot 7 + 3k \cdot 7 + 4 = 7(2+3k) + 4 \equiv 4 \text{ mod } 7$$

Example Find all solutions to the linear congruence $3x \equiv 4$ mod 44.

Our goal is to find an integer s such that $3s \equiv 1$ mod 44, knowing that, if we multiply both sides of the congruence by such an s, the 3 will "cancel," and we will have a solution.

As before we could list multiples of 3 until we found one that worked, but this time we will use the Euclidean Algorithm. Since 3 and 44 are relatively prime, we know that there are integers s and t such that $1 = 3s + 44t$. This implies that $3s = 44(-t) + 1$, i.e. that $3s \equiv 1$ mod 44.

The Euclidean Algorithm I gives:

$$\begin{aligned} \mathbf{44} &= \mathbf{3}(14) + \mathbf{2} \\ \mathbf{3} &= \mathbf{2}(1) + \mathbf{1} \\ \mathbf{2} &= \mathbf{1}(2) \end{aligned}$$

Euclidean Algorithm II gives:

$$\begin{aligned} \mathbf{1} &= \mathbf{3} - \mathbf{2}(1) \\ &= \mathbf{3} - (\mathbf{44} - \mathbf{3}(14))(1) \\ &= (15)(\mathbf{3}) + (-1)(\mathbf{44}) \end{aligned}$$

Thus $s = 15$ and $t = -1$.

So we multiply both sides of the given linear congruence by $s = 15$, as follows:

$$\begin{aligned} 3x &\equiv 4 \mod 44 \\ 15(3x) &\equiv 15(4) \mod 44 \\ 45x &\equiv 60 \mod 44 \\ x &\equiv 16 \mod 44 \end{aligned}$$

We check that $x = 16$ is a solution:

$$3(16) = 48 = 44 + 4 \equiv 4 \mod 44$$

Further, any integer of the form $16 + 44k$, where $k \in \mathbb{Z}$, will be a solution.

Note By this point, it should be clear that $x = sb$ is a solution to $ax \equiv b \mod m$ if s and t are integers satisfying $as + mt = 1$, and that any integer of the form $sb + mk$, for $k \in \mathbb{Z}$, is also a solution.

Systems of Linear Congruences (p 142-143; Thm 4.21 and Ex 4.22 and 4.23)

The Chinese Remainder Theorem says that if m and m' are relatively prime, then the system of linear congruences

$$\begin{aligned} x &\equiv b \mod m \\ x &\equiv b' \mod m' \end{aligned}$$

has a solution, i.e. there is an integer n such that $n \equiv b \mod m$ and $n \equiv b' \mod m'$. Further, if n is such a solution, then so is every integer of the form $n + mm'k$, for $k \in \mathbb{Z}$.

Example Consider the following system of linear congruences:

$$\begin{aligned} x &\equiv 4 \mod 6 \\ x &\equiv 3 \mod 11 \end{aligned}$$

Suppose x is a solution to the system. (We know that such a solution exists, by the CRT.) Then $x = 6y + 4$, for some integer y, since $x \equiv 4 \mod 6$. Thus

$$\begin{aligned} 6y + 4 &\equiv 3 \mod 11 \\ 6y &\equiv -1 \mod 11 \\ 6y &\equiv 10 \mod 11 \end{aligned}$$

To solve this linear congruence for y, we must find an integer s such that $6s \equiv 1 \mod 11$. We list multiples of 6: 6, 12. Since $6 \cdot 2 = 12 = 11 + 1$, we take $s = 2$. We multiply both sides of the congruence by $s = 2$:

$$\begin{aligned} 2(6y) &\equiv 2(10) \mod 11 \\ 12y &\equiv 20 \mod 11 \\ y &\equiv 9 \mod 11 \end{aligned}$$

Thus $y = 9$ is a solution of $6y + 4 \equiv 3 \mod 11$, and $x = 6(9) + 4 = 58$ is a solution of the system.

Let's check that this works:

$$\begin{aligned} 58 &= 6(9) + 4 \equiv 4 \mod 6 \\ 58 &= 11(5) + 3 \equiv 3 \mod 11 \end{aligned}$$

So, yes, $x = 58$ is a solution.

Note that we did not need to take $y = 9$; any integer y of the form $9 + 11k$ for $k \in \mathbb{Z}$ will satisfy $6y + 4 \equiv 3 \mod 11$. Thus any integer $x = 6(9 + 11k) + 4 = 58 + 66k$ is a solution of the system.