Linear Congruences

In ordinary algebra, an equation of the form $ax = b$ (where a and b are given real numbers) is called a linear equation, and its solution $x = b/a$ is obtained by multiplying both sides of the equation by $a^{-1} = 1/a$.

The subject of this lecture is how to solve any *linear congruence*

$$ax \equiv b \pmod{m}$$

where a, b are given integers and m is a given positive integer.

For a simple example, you can easily check by inspection that the linear congruence

$$6x \equiv 4 \pmod{10}$$

has solutions $x = 4, 9$. Already we see a difference from ordinary algebra: linear congruences can have more than one solution!

Are these the *ONLY* solutions? No. In fact, any integer which is congruent to either 4 or 9 mod 10 is also a solution. You should check this for yourself now.

So any integer of the form $4 + 10k$ or of the form $9 + 10k$ where $k \in \mathbb{Z}$ is a solution to the given linear congruence. The above linear congruence has *infinitely many* integer solutions.

The is a general principle at work here. *Solutions to linear congruences are always entire congruence classes.* If any member of the congruence class is a solution, then all members are. This is a simple consequence of the properties of congruences proved in a previous lecture.

This means that although the congruence $6x \equiv 4 \pmod{10}$ had infinitely many integer solutions, the solutions fall into congruence classes, and there are only two of those: $[4]_{10}$ and $[9]_{10}$.

Whenever a linear congruence has any solutions, it has infinitely many. The solutions fall into congruence classes, and there are only a finite number of congruence classes that solve the congruence.

Here is the key observation which enables us to solve linear congruences.

By definition of congruence, $ax \equiv b \pmod{m}$ iff $ax - b$ is divisible by m. Hence, $ax \equiv b \pmod{m}$ iff $ax - b = my$, for some integer y. Rearranging the equation to the equivalent form $ax - my = b$ we arrive at the following result.

Lemma. *Solving the congruence $ax \equiv b \pmod{m}$ is equivalent to solving the linear diophantine equation $ax - my = b$.*

Since we already know how to solve linear diophantine equations, this means we can apply that knowledge to solve linear congruences.

Theorem. *Let a, b be any integers and let m be a positive integer. Let $d = \gcd(a, m)$. If $d \nmid b$ then the linear congruence $ax \equiv b \pmod{m}$ has no solutions. If $d \mid b$ then the linear congruence $ax \equiv b \pmod{m}$ has exactly d solutions, where by "solution" we mean a congruence class mod m.*

Comment. Later in this lecture we will see that all the solutions can be joined together to form a single congruence class mod m/d.

Proof of the theorem. Solving the congruence $ax \equiv b \pmod{m}$ is equivalent to solving the linear diophantine equation $ax - my = b$. If $d \nmid b$ then the diophantine equation has no solutions, so the congruence has no solutions, either. If $d \mid b$ then the solutions of the diophantine equation take the form

$$x = x_0 + (m/d)t, \qquad y = y_0 + (a/d)t$$

where (x_0, y_0) is any particular solution (obtained from the Euclidean algorithm, for instance).

To finish the proof, observe that as t runs through the values $0, 1, \ldots, d-1$ (the residues mod d) the congruence classes $[x_0 + (m/d)t]_m$ run through *all* the solutions. (There are no other solutions because the classes just repeat for higher and lower values of t.) □

Example. Returning to the example $6x \equiv 4 \pmod{10}$, we solve it by first guessing the solution $x_0 = 4$ by trial and error. Then the theorem tells us that $[x_0 + (10/2)t]_{10}$ for $t = 0, 1$ gives the complete solution set. Thus, $x = [4]_{10}$ and $[9]_{10}$ is the complete solution.

Notice that we could write this as: $x \equiv 4, 9 \pmod{10}$. This congruence describes exactly the same set of integers as the union of the congruence classes $[4]_{10}$, $[9]_{10}$.

Even better: we can write the complete solution as: $x \equiv 4 \pmod{5}$. This single congruence describes the set of all integer solutions, as you should check. In other words, we have

$$[4]_{10} \cup [9]_{10} = [4]_5.$$

Example. Let's solve $230x \equiv 1081 \pmod{12167}$. We start by applying the Euclidean algorithm to compute $d = \gcd(230, 12167) = 23$. Since $d \mid 1081$ there are solutions. The extended Euclidean algorithm gives the particular solution $(s_0, t_0) = (53, 1)$ to the diophantine equation $230s - 12167t = 23$, and scaling by $47 = 1081/23$ we get the particular solution $(x_0, y_0) = (2491, 47)$ to the diophantine equation $230x - 12167y = 1081$. So $x_0 = 2491$ solves the original given congruence. In this case, $m/d = 529$. Thus, with $m = 12167$, the set of residue classes

$$\{[2491 + 529t]_m : t = 0, 1, 2, \ldots, 22\}$$

gives the complete solution set to the congruence.

Thus with $m = 12167$ we get solutions $[a]_m$ for $a = 2491$, 3020, 3549, 4078, 4607, 5136, 5665, 6194, 6723, 7252, 7781, 8310, 8839, 9368, 9897, 10426, 10955, 11484, 12013, 12542, 13071, 13600, 14129 and no others.

We can also say that (still with $m = 12167$) we get solutions $[a]_m$ for $a = 2491$, 3020, 3549, 4078, 4607, 5136, 5665, 6194, 6723, 7252, 7781, 8310, 8839, 9368, 9897, 10426, 10955, 11484, 12013, 375, 904, 1433, 1962.

This is because $12542 \equiv 375$, $13071 \equiv 904$, $13600 \equiv 1433$, and $14129 \equiv 1962 \pmod{m}$.

When dealing with congruence classes, we can always replace any representative by another one!

Incidentally, we can also write the complete solution obtained above as a single congruence class mod 529. The complete solution is given by $x \equiv 375 \pmod{529}$. Again, the union of all 23 congruence classes mod m is a single congruence class mod m/d.

The examples suggest a simpler method to solve a linear congruence, which should always produce a single congruence class mod m/d (assuming $d \mid m$).

The remainder of this lectures explores this idea.

As a special case of the theorem, let me point out that if $d = \gcd(a, m) = 1$ then the linear congruance $ax \equiv b \pmod{m}$ has a unique solution class.

In the special case $\gcd(a, m) = 1$, we can always solve the congruence by finding the *inverse* of $[a]_m$ and then multiplying both sides of the congruence by the inverse to obtain the unique solution. This is a satisfying idea because it is so similar to what we do in ordinary high school algebra to solve linear equations.

Definition. An *inverse* of a mod m is any integer c such that $a \cdot c \equiv 1 \pmod{m}$. We write $a^{-1} \bmod m = c$, or $[a]_m^{-1} = [c]_m$ for the modular inverse just defined, when it exists.

An inverse of a mod m exists iff $\gcd(a, m) = 1$. Proving this is a good exercise.

Example. Suppose we are given the congruence $11x \equiv 15 \pmod{20}$. Observe that $d = \gcd(11, 20) = 1$. Thus $11x \equiv 15 \pmod{20}$ has a *unique* solution class. Observe that $11 \cdot 11 \equiv 1 \pmod{20}$, so $[11]_{20} \cdot [11]_{20} = [1]_{20}$ and $[11]_{20}^{-1} = [11]_{20}$. This tells us that we can solve the given congruence simply by multiplying both sides by 11 and reducing numbers mod 20. Here we go:

$$\begin{aligned} 11x &\equiv 15 \pmod{20} \\ 11 \cdot 11x &\equiv 11 \cdot 15 \pmod{20} \\ 121x &\equiv 165 \pmod{20} \\ x &\equiv 5 \pmod{20}. \end{aligned}$$

This proves that $x = [5]_{20}$ is the unique solution to the given congruence $11x \equiv 15 \pmod{20}$.

So we can always solve $ax \equiv b \pmod{m}$ in case $\gcd(a, m) = 1$ simply by multiplying both sides by the inverse of $[a]_m$ (i.e., canceling the a factor). Of course, to *find* the inverse of a in general requires the extended Euclidean algorithm to solve the corresponding diophantine equation $as - mt = 1$; then $c = s \bmod m$ will be an inverse of a mod m. It should be noted that if m is

small enough then trial and error works pretty well to find an inverse, since there are few possibilities to check.

In fact, the technique of multiplying by an inverse can be used to solve *any* linear congruence $ax \equiv b \pmod{m}$, even when $d = \gcd(a, m) \neq 1$.

Let us see why.

Assume that $d = \gcd(a, m)$ divides b. Solving the congruence $ax \equiv b \pmod{m}$ is equivalent to solving the diophantine equation $ax - my = b$. But we can divide both sides of the equation by d to get a *reduced* diophantine equation

$$Ax - My = B \quad \text{where } A = \frac{a}{d}, M = \frac{m}{d}, B = \frac{b}{d}.$$

The solutions to the reduced diophantine equation are exactly the same as the solutions to the original one. Thus, solving $ax \equiv b \pmod{m}$ is equivalent to solving

$$Ax \equiv B \pmod{M}.$$

This congruence satisfies the condition $\gcd(A, M) = 1$, and thus can be solved by finding an inverse of A mod M and multiplying both sides by that inverse.

Example. Let's again solve $230x \equiv 1081 \pmod{12167}$ (which we solved earlier) using this new approach. We start by applying the Euclidean algorithm to compute $d = \gcd(230, 12167) = 23$. Next, we reduce the congruence to the equivalent congruence $10x \equiv 47 \pmod{529}$ by dividing by d. We now have $\gcd(10, 529) = 1$, so we can solve by multiplying by 10^{-1} mod 529. We can find the inverse by finding any solution to the diophantine equation $10x - 529y = 1$ and then throwing away y. For instance, the extended Euclidean algorithm gives $(x, y) = (53, 1)$ so $10^{-1} \equiv 53 \mod 529$.

Multiplying the reduced congruence $10x \equiv 47 \pmod{529}$ by the inverse 53 gives the (unique!) solution $x \equiv 53 \cdot 47 \equiv 375 \pmod{529}$.

You should verify for yourself that the union of the congruence classes $[a]_m$ for $a = 2491, 3020, 3549, 4078, 4607, 5136, 5665, 6194, 6723, 7252, 7781, 8310, 8839, 9368, 9897, 10426, 10955, 11484, 12013, 375, 904, 1433, 1962$ (which we got before) gives exactly the same set of integers as the single congruence class $[375]_{529}$.