MATH 25 CLASS 12 NOTES, OCT 17 2011

Contents

1. Simultaneous linear congruences

There is a story (probably apocryphal) about how certain generals from ancient China would count their armies. Suppose a general knows his army has something like 100 soldiers in it, but he is not exactly sure. Instead of sending a person out to manually count each person, he decides to count his soldiers in the following somewhat unusual way. First, he demands that his army lines up in rows of 3, and then he finds that 1 soldier is leftover. Next, he demands that his army lines up in rows of 5, and finds that 4 soldiers are leftover. Finally, he demands that his army lines up in rows of 7, and finds that 5 soldiers are leftover. How does he figure out how many soldiers are in his army?

In terms of the language we are using, we want to find x such that $x \equiv 1 \bmod 3, x \equiv 4 \bmod 5, x \equiv 5 \bmod 7$. How do we find all x (if there are even any) which simultaneously satisfy all these linear congruences?

The next theorem gives the answer.

Theorem 1 (Chinese Remainder Theorem, Theorem 3.10)**.** *Suppose that $n_1, \dots, n_k$ are mutually coprime positive integers, and $a_i, \dots, a_k$ are arbitrary integers. Then the set of simultaneous linear congruences $x \equiv a_1 \bmod n_1, x \equiv a_2 \bmod n_2, \dots, x \equiv a_k \bmod n_k$ has exactly one solution mod $n_1 n_2 \dots n_k = n$.*

Proof. We will actually construct the simultaneous solutions to these congruences and show that it is unique mod n. Let $c_i = n/n_i$. Consider the linear congruence $c_i x \equiv 1 \bmod n_i$. Since $\gcd(c_i, n_i) = 1$, we know this congruence has a (unique) solution $d_i \bmod n_i$. The claim is that $x_0 = a_1c_1d_1 + a_2c_2d_2 + \ldots + a_kc_kd_k$ simultaneously solves all the congruences $x \equiv a_i \bmod n_i$.

First, notice that $n_i | c_j$ for all $j \neq i$, by definition. Therefore $a_jc_jd_j \equiv 0 \bmod n_i$ whenever $j \neq i$. This means that $x_0 \equiv a_ic_id_i \bmod n_i$. But we also know that $c_id_i \equiv 1 \bmod n_i$, so $x_0 \equiv a_i \bmod n_i$, as desired.

We now need to show that this solution is unique mod n. Suppose we have two integers x, x' solving all the simultaneous congruences above. We want to show that $n|(x - x')$. Since $x \equiv x' \bmod n_i$ for all i, we must have $n_i|(x - x')$ for all i. Since the n_i are mutually coprime, this means their product also divides $x - x'$, but $n|(x - x')$ implies $x \equiv x' \bmod n$, as desired. □

This theorem has both theoretical and computational interest. It tells us that a system of simultaneous linear congruences to mutually coprime moduli is equivalent to just one linear congruence to a larger modulus. The theorem also tells us that congruences to relatively prime moduli are 'independent' of each other. The proof also provides a method (albeit a somewhat computationally intensive one, since we need to calculate inverses mod c_i multiple times) for actually finding this solution.

2. Simultaneous linear congruences

The Chinese Remainder Theorem (CRT for short) tells us that we can take a collection of simultaneous linear congruences to mutually coprime moduli and convert them to a single congruence modulo a larger number. The proof gave a method for actually finding this single congruence, but it is computationally intensive. Sometimes there are more ad hoc ways of finding the larger congruence. We begin with a useful and easy fact:

Proposition 1. *Suppose $x \equiv a \bmod n$. Let $m \geq 1$ be any positive integer. Then $x \equiv a, a+n, a+2n, \dots,$ or $a+(m-1)n \bmod (mn)$.*

Proof. If $x \equiv a \bmod n$, then $x = a + kn$ for some integer k. Therefore, we want to show that $x \equiv a + rn \bmod (mn)$ for some $0 \leq r < m$. But this is clear; just take r to be the remainder when we divide k by m: if $k = qm + r$, then $a + kn = a + (qm + r)n = (a + rn) + qmn \equiv a + rn \bmod mn$. □

Examples.

- Find all solutions to $x \equiv 3 \bmod 5, x \equiv 2 \bmod 4$. First, $\gcd(5, 4) = 1$, so these congruences are to mutually coprime moduli. The CRT tells us that the set of simultaneous solutions to these congruences is a single congruence class mod $5 \cdot 4 = 20$. We now want to find that single congruence class.

  The method used to prove the CRT requires us to solve $5x \equiv 1 \bmod 4$ and $4x \equiv 1 \bmod 5$(but not simultaneously). Inspection tells us that $x \equiv 1 \bmod 4, x \equiv 4 \bmod 5$, work. The recipe in the proof then tells us that $x = 3 \cdot 4 \cdot 4 + 2 \cdot 5 \cdot 1 = 58 \equiv 18 \bmod 20$. And indeed one can check that this works.

  However, this is not really the best way to actually find the answer to the original problem. The CRT tells us that there is exactly one solution $x \bmod 20$. On the other hand, we know that $x \equiv 3 \bmod 5, x \equiv 2 \bmod 4$. So we list all the possible values of $x \bmod 20$ which satisfy $x \equiv 3 \bmod 5$: these are $x \equiv 3, 8, 13, 18 \bmod 20$. We then look at this list and find all those which satisfy $x \equiv 2 \bmod 4$; evidently $18 \bmod 20$ is the only one that works. That there is one and only one class mod 20 is no surprise since the CRT tells us that this is what will happen.
- Simultaneously solve $3x \equiv 9 \bmod 12$ and $4x \equiv 2 \bmod 11$. This time we are not given congruences of the form $x \equiv a \bmod n$, but we can reduce the given equations to equivalent congruences which are of this form. For instance, $3x \equiv 9 \bmod 12$ if and only if $x \equiv 3 \bmod 4$. Similarly, $4x \equiv 2 \bmod 11$ has the unique solution $x \equiv 6 \bmod 11$. So our original set of congruences is equivalent to the set of congruences $x \equiv 3 \bmod 4, x \equiv 6 \bmod 11$.

  The CRT tells us that this pair of congruences has exactly one solution mod $4 \cdot 11 = 44$. To find it, suppose $x \bmod 44$ solves both congruences;

$x \equiv 6 \bmod 11$ implies that $x = 6, 17, 28, 39 \bmod 44$, and then from this list we find that the only choice with $x \equiv 3 \bmod 4$ is $39 \bmod 44$.

- Sometimes you can take a single congruence to a big modulus, with big numbers, and then break it up into multiple congruences with smaller moduli and smaller numbers, and then reassemble the answers using the CRT. Let's use this technique on the congruence $19x \equiv 53 \bmod 90$.

  We start by factoring $90 = 2 \cdot 3^2 \cdot 5$. We then break the original congruence into three congruences to smaller moduli:

  $$19x \equiv 53 \bmod 2, 19x \equiv 53 \bmod 9, 19x \equiv 53 \bmod 5.$$

  The advantage to this is that the numbers $19, 71$, which are kind of large, are reduced when we look at smaller moduli. These three congruences are the same as

  $$x \equiv 1 \bmod 2, x \equiv 8 \bmod 9, 4x \equiv 3 \bmod 5.$$

  The last has solutions given by $x \equiv 2 \bmod 5$. So we want to simultaneously solve $x \equiv 1 \bmod 2, x \equiv 8 \bmod 9, x \equiv 2 \bmod 5$. For instance, from $x \equiv 1 \bmod 2, x \equiv 2 \bmod 5$, we find that $x \equiv 7 \bmod 10$. And then this implies that $x \equiv 7, 17, 27, \ldots, 87 \bmod 90$. We pick the one number which is $\equiv 8 \bmod 9$; one finds that the answer is $x \equiv 17 \bmod 90$.

  Of course, you are free to use the method we discussed in the previous class, where one uses the Euclidean algorithm to find solutions to $19x + 90y = 53$. And this example was engineered to be substantially simpler when we broke the original congruence into smaller pieces.

- What do we do if we have simultaneous congruences where the moduli are not mutually coprime? For instance, consider the congruences $x \equiv 11 \bmod 20, x \equiv 5 \bmod 8$. We cannot apply the CRT since $\gcd(20, 8) = 4 \neq 1$. To approach this problem, we break each congruence into multiple congruences to various moduli, using the proposition that if $a \equiv b \bmod n$, and $n = n_1 \ldots n_r$ where the n_i are mutually coprime, then $a \equiv b \bmod n$ is equivalent to the system $a \equiv b \bmod n_i$ where $1 \leq i \leq r$.

  In this case, we cannot break $x \equiv 5 \bmod 8$ into congruences to smaller moduli, since there is no way of nontrivially factoring 8 into two relatively prime numbers. However, we can split $x \equiv 11 \bmod 20$ into the system $x \equiv 11 \equiv 1 \bmod 5, x \equiv 11 \equiv 3 \bmod 4$. So what we want to do now is to simultaneously solve $x \equiv 1 \bmod 5, x \equiv 3 \bmod 4, x \equiv 5 \bmod 8$. The CRT is still inapplicable, since $\gcd(4, 8) \neq 1$. However, consider the pair $x \equiv 3 \bmod 4, x \equiv 5 \bmod 8$. Is there any x which makes both these true? Notice that if $x \equiv 3 \bmod 4$, then $x \equiv 3, 7 \bmod 8$. So it is impossible for any x to simultaneously satisfy both $x \equiv 3 \bmod 4$ and $x \equiv 5 \bmod 8$. Therefore, the original set of congruences has no simultaneous solutions.

The last example brings up the question of precisely what can happen if we have simultaneous congruences to moduli which are not coprime. Let us first think about what happens if we have simultaneous congruences to moduli which are all various prime powers of the same prime p. For instance, in the example above, we had $x \equiv 3 \bmod 2^2, x \equiv 5 \bmod 2^3$. What happens in the general case of two congruences

$x \equiv a_1 \bmod p^{e_1}, x \equiv a_2 \bmod p^{e_2}$? What if there are more than two congruences, all to various moduli which are prime powers of the same prime p?

Proposition 2. *Consider the simultaneous set of congruences* $x \equiv a_1 \bmod p^{e_1}, \ldots, x \equiv a_n \bmod p^{e_n}$*, where* p *is a prime, and* $e_1 \leq e_2 \leq \ldots e_n$*. If* $a_i \equiv a_n \bmod p^{e_i}$ *for all* i*, then this has exactly one solution mod* p^{e_n}*, given by* $x \equiv a_n \bmod p^{e_n}$*. Otherwise this system of congruences has no simultaneous solution.*

Proof. Suppose $a_i \equiv a_n \bmod p^{e_i}$ is true for all i. Let $e = e_n$. If $x \equiv a_n \bmod p^e$, then $x \equiv a_n \bmod p^{e_i}$ as well, since $p^{e_i} | p^e$. Therefore, $x \equiv a_i \bmod p^{e_i}$. So any $x \equiv a_n \bmod p^e$ is a simultaneous solution to our system, and clearly there is only one such solution mod p^e (namely, $a_n \bmod p^e$).

Now suppose that $a_i \not\equiv a_n \bmod p^{e_i}$ for some i. Then there cannot be any solution to our system, because if $x \equiv a_n \bmod p^e$, then $x \equiv a_n \bmod p^{e_i}$ as well, and $x \equiv a_n \bmod p^{e_i}$ is not simultaneously possible with $x \equiv a_i \bmod p^{e_i}$ if $a_i \not\equiv a_n \bmod p^{e_i}$. □

I like to think of this proposition as saying that congruences to moduli which are powers of the same prime must satisfy some sort of 'compatibility' relation if there will be a solution; that is, in the congruences $x \equiv a_i \bmod p^{e_i}$, there are some conditions that the various a_i have to satisfy to have solutions. In contrast, the CRT tells us that linear congruences to mutually coprime moduli impose no compatibility restrictions, at all, for there to be solutions.

Examples.

- Going back to the example with $x \equiv 3 \bmod 4, x \equiv 5 \bmod 8$, we see that the above proposition tells us what we already know, since $5 \not\equiv 3 \bmod 4$.
- Find all solutions to $x \equiv 3 \bmod 5, x \equiv 13 \bmod 25, x \equiv 88 \bmod 125$. Since the moduli are all prime powers of 5, we use the above proposition. We need to check whether $88 \equiv 13 \bmod 25$; since $88 - 13 = 75 = 25 \cdot 3$, this is true, and similarly, $88 \equiv 3 \bmod 5$. Therefore, the above proposition tells us that there is exactly one solution to this system mod 125, and it is $x \equiv 88 \bmod 125$.

The main point of these examples and the above proposition is that a set of congruences to moduli which are all powers of the same prime either have no solution, or have one solution and is given by exactly the congruence in the original system which was to the largest modulus. It is a finite, and fairly straightforward, computation to check which of the two is true.

On the other hand, the CRT gives us a way to take lots of congruences to relatively prime moduli and then piece them together. So one way of approaching a general problem involving linear congruences to different moduli, not necessarily coprime, is to break each apart into several congruences modulo various prime powers, sort these into lists by prime power, determine whether each list has a solution, and if each list does have a solution, reassemble them using the CRT. This sounds sort of complicated, but a few examples should make the idea clear.

Examples.

- Find all simultaneous solutions to $x \equiv 4 \bmod 12, x \equiv 1 \bmod 15, x \equiv 4 \bmod 9$. This looks a little scary, but we start by breaking each congruence into prime power pieces. This yields the system (which is sorted by the original congruence they came from)

$$\begin{aligned}&x \equiv 4 \equiv 0 \bmod 4, x \equiv 4 \equiv 1 \bmod 3,\\&x \equiv 1 \bmod 3, x \equiv 1 \bmod 5,\\&x \equiv 4 \bmod 9.\end{aligned}$$

We sort these by prime power:

$$\begin{aligned}&x \equiv 0 \bmod 4\\&x \equiv 1 \bmod 3, x \equiv 4 \bmod 9\\&x \equiv 1 \bmod 5.\end{aligned}$$

We now ask whether each of these lists, considered one at a time, has a solution. The first and third (to moduli $4, 5$) only consist of one congruence so these obviously have one solution modulo their respective moduli. As for the second list, we check that $4 \equiv 1 \bmod 3$, so this list has solutions given by $x \equiv 4 \bmod 9$. So our original system is equivalent to the system of three congruences

$$x \equiv 0 \bmod 4, x \equiv 4 \bmod 9, x \equiv 1 \bmod 5.$$

At this point, we can use the CRT, since the moduli are mutually coprime, and the CRT tells us that there will be exactly one solution mod $4 \cdot 9 \cdot 5 = 180$. To find this solution, we use the technique we talked about at the beginning of the class. For instance, $x \equiv 4 \bmod 9$ implies that $x \equiv 4, 13, 22, 31 \bmod 36$. We select the one out of these which is $\equiv 0 \bmod 4$, which is clearly 4. So the two congruences $x \equiv 0 \bmod 4, x \equiv 4 \bmod 9$ are equivalent to $x \equiv 4 \bmod 36$. From this, we know that $x \equiv 4, 40, 76, 112, 148 \bmod 180$. We are looking for the one element which is $\equiv 1 \bmod 5$; clearly this is 76 mod 180. So the original system has solution given by $x \equiv 76 \bmod 180$.

- Find all solutions of $x \equiv 7 \bmod 12, x \equiv 10 \bmod 21, x \equiv 5 \bmod 14$. Again, we start by breaking each congruence into its prime power pieces:

$$\begin{aligned}&x \equiv 7 \equiv 3 \bmod 4, x \equiv 7 \equiv 1 \bmod 3,\\&x \equiv 10 \equiv 1 \bmod 3, x \equiv 10 \equiv 3 \bmod 7,\\&x \equiv 5 \equiv 1 \bmod 2, x \equiv 5 \bmod 7.\end{aligned}$$

If we want, we can sort by prime power modulus, but you might have already noticed that we see both $x \equiv 3 \bmod 7$ and $x \equiv 5 \bmod 7$. These cannot simultaneously be true, so the original system has no solutions.