MATH 115, SUMMER 2012
LECTURE 7

JAMES MCIVOR

1. Solving Congruences

Today we begin our study of finding solutions x to expressions of the form

$$f(x) \equiv 0 \mod m$$

where f is a polynomial with integer coefficients. We will not able to say exactly what x is, but we would like to at least determine the possible congruence classes of x modulo m. As we will see, this is not easy.

We study today only linear equations. First, what are the solutions to

$$ax \equiv 0 \mod m,$$

where a is fixed and x is our variable? You'd like to divide both sides by a but you may not be able to! Sometimes you can, namely when a is prime to m (since that's the condition that a have a multiplicative inverse mod m) and then you just get the one solution $x \equiv 0 \mod m$. Let's look at an example where you can't.

Example 1.1. Solve $2x \equiv 0 \mod 6$.

We have obviously $x \equiv 0 \mod m$. But also by inspection $x \equiv 3 \mod 6$ works, and no others do. Notice that here $a = 2$, $m = 6$, and so $(a, m) = 2$. Moreover, our other solution, 3, is actually $m/(a, m)$. This works in general.

Lemma 1. *Let $g = (a, m)$. The congruence $ax \equiv b \mod m$ has no solution if g does not divide b, and a unique solution mod $\frac{m}{g}$ if $g|b$.*

Proof. Maybe "torus" picture.

Concretely, we want to find $x, y \in \mathbb{Z}$ such that $ax + my = b$. Divide through by $g = (a, m)$ to get.

$$\frac{a}{g}x + \frac{m}{g}y = \frac{b}{g}$$

This clearly shows that if $b \not| g$, then there are no such x and y, so our congruence has no solution. On the other hand, if g *does* divide b, then the above equation says

$$\frac{a}{g}x \equiv \frac{b}{g} \mod \frac{m}{g}$$

Now $\frac{a}{g}$ and $\frac{m}{g}$ (note they're both integers) are relatively prime, so $\frac{a}{g}$ has an inverse mod $\frac{m}{g}$, and multiplying through by this inverse, call it a' gives

$$x \equiv a'\frac{b}{g} \mod \frac{m}{g}$$

Since the multiplicative inverse is unique up to the modulus (which is now $\frac{m}{g}$), we're done.

□

That's all there is to say about solving one linear congruence - either there's a unique solution mod $\frac{m}{g}$ or there's no solution, depending on the relationship between b and (a, m). Following the proof also shows how to construct solutions explicitly. (Do this in section!)

2. Chinese Remainder Theorem

Now we try to solve sytems of linear equations. We consider a system of congruences of the form

$$\begin{aligned} x \equiv& a_1 \mod m_1 \\ x \equiv& a_2 \mod m_2 \\ &\vdots \\ x \equiv& a_k \mod m_k \end{aligned}$$

Draw picture.

The answer to this question is in the following important theorem

Theorem 1 (Chinese Remainder Theorem)**.** *In the system above, if the m_i are pairwise relatively prime, then the system has a solution x, which is unique modulo $m_1 m_2 \cdots m_k$.*

Proof. Write $m = m_1 \cdots m_k$ for short. Each m/m_i is prime to m_i, since the m_j are relatively prime in pairs. Thus m/m_i has an inverse mod m_i, call this inverse b_i. Then the solution is

$$x = \sum_{i=1}^{k} \frac{m}{m_i} b_i a_i,$$

because if you reduce it mod m_i, all terms except the ith one drop out, and when working mod m_i, $\frac{m}{m_i} b_i \equiv 1$,leaving just $x \equiv a_i$.

□

There are many proofs, but this one is good because if you understand it, then you know how explicitly construct solutions. Let's see how.

3. Applications/Examples

Example 3.1. Solve the system of congruences

$$\begin{aligned} x \equiv& 3 \mod 4 \\ x \equiv& 1 \mod 5 \\ x \equiv& 2 \mod 3 \end{aligned}$$

Note that the three moduli are prime in pairs, so there is a solution, and it should be unique modulo $4 \cdot 5 \cdot 3 = 60$. To find it, we have to find inverses to the three numbers $m/m_1 = 60/4 = 15$, $m/m_2 = 60/5 = 12$, and $m/m_3 = 60/3 = 20$ mod 4,5, and 3, respectively.

What's an inverse to 15 mod 4? Well, we might as well reduce 15 to 3, and then it's easy to see that 3 is its own inverse, since $3 \cdot 3 = 9 \equiv 1 \mod 4$. Similarly, to find an inverse to 12 mod 5, we reduce 12 to 2, and then we see that 3 is the inverse, since $2 \cdot 2 = 6 \equiv 1 \mod 5$. For the last one, 20 reduces to 2 mod 3, which is its own inverse. So we have the three inverses $b_1 = b_2 = 3$ and $b_3 = 2$. Thus our answer is

$$x = \sum \frac{m}{m_i} b_i a_i = 15 \cdot 3 \cdot 3 + 12 \cdot 3 \cdot 1 + 20 \cdot 2 \cdot 2 = 135 + 36 + 80$$

which we can consider mod 60 to give $15 + 36 + 20 = 71 \equiv 11 \mod 60$.

Here is a different point of view on the theorem, which is more abstract-algebraic in nature. Consider the above example, and imagine that the numbers $a_1 = 3, a_2 = 1, a_3 = 2$ were changed. What possible values could they take? In the theorem, they are allowed to be any integers, but we work only up to congruence mod the various m_i, so the only distinct situations that can arise are

$$a_1 = 0, 1, 2, 3, \qquad a_2 = 0, 1, 2, 3, 4, \qquad a_3 = 0, 1, 2$$

These are just three complete residue systems for the three moduli. For each such choice, the theorem says there's a unique number x mod 60. So you give me a triple (a_1, a_2, a_3) and I give you a unique solution mod 60, that is, a number from 0 to 59. So the theorem says there's a bijection

$$\{0, 1, 2, 3\} \times \{0, 1, 2, 3, 4\} \times \{0, 1, 2\} \leftrightarrow \{0, 1, 2, 3, \ldots, 58, 59\},$$

where "$\times$" means cartesian product of sets[1].

Come back to this next theorem once we know what isomorphisms are - skipped for now...

As a final application, we now consider congruences of higher degree, that is, expressions of the form

$$f(x) \equiv 0 \mod m,$$

where $f(x) = a_n x^n + \ldots + a_1 x + a_0$ is a polynomial with integer coefficients. The **degree** of this congruence is the largest k for which $a_k \not\equiv 0 \mod m$. The first question to ask is: how many solutions are there, if any? This obviously depends on the modulus, so we ask how the number of solutions changes when we multiply moduli.

Theorem 2. *If $f(x) \equiv 0 \mod m_1$ has a_1 solutions (mod m_1) and $f(x) \equiv 0 \mod m_2$ has a_2 solutions (mod m_2), and if a_1, a_2 are relatively prime, then $f(x) \equiv 0 \mod m_1 m_2$ has $a_1 a_2$ solutions mod $m_1 m_2$.*

The theorem is very important - it tells us how to calculate the number of solutions using the prime factorization of the modulus.

Proof. - Idea: construct bijection between solutions of $f(x) \equiv 0 \mod m_1 m_2$ and pairs (x_1, x_2), where x_i is a solution of $f(x) \equiv 0 \mod m_i$.

- 1) Given a sol'n mod $m_1 m_2$, it reduces mod m_1 and mod m_2 give x_1 and x_2, respectively. (Don't need $(m_1, m_2) = 1$ here).

- 2) Conversely, start with a pair of solutions: $f(x_1) \equiv 0 \mod m_1$ and $f(x) \equiv 0 \mod m_2$. The pair (x_1, x_2) corresponds to a unique residue class x mod $m_1 m_2$ by CRT (used relatively prime hypothesis here). Explicitly, we solve $x \equiv x_1 \mod m_1$ and $x \equiv x_2 \mod m_2$: we get a unique solution mod $m_1 m_2$.

- The key fact is that this x reduces to x_i mod m_i. Because it means if we start with a solution x mod $m_1 m_2$, then reduce it mod m_1, m_2, then lift back up to the

[1] Actually each of these are rings, as we'll see, and this can be taken as a cartesian product of rings, and the bijection is actually an isomorphism of rings!

larger modulus, we get our original x (up to ocngruence mod $m_1 m_2$). Thus we have a bijection. $\square$

- Do examples of counting solutions with this theorem in section!