Lecture 5 - Congruences

One common tool used in solving number-theoretic problems is to consider the remainders obtained after division is performed. We've already used this technique a few times in class (e.g., any time we've written an odd number as $2n+1$), and in this lecture we will make properties of these remainders precise by introducing the theory of congruences.

Let $m \in \mathbb{N}$ be some fixed number. Given any $a \in \mathbb{Z}$, dividing a by m results in one of m different possible remainders. That is, we can write $a = mn + r$ and $r \in \{0, 1, 2, \ldots, m-1\}$ — this is guaranteed by the division algorithm.

If two numbers, $a, b \in \mathbb{Z}$, share the same remainder after dividing by m, we say that a and b are **congruent modulo m** and write $\boxed{a \equiv b \pmod{m}}$. E.g.,

$$8 \equiv 5 \pmod{3}$$
$$29 \equiv 51 \pmod{11}$$
$$7 \equiv -1 \pmod{8}$$

Another way of saying the same thing is $a \equiv b \pmod{m}$ iff $m \mid (a-b)$.

One of the reasons that congruences are a

useful tool is that we can do some arithmetic operations with them. In particular, we have a well-defined notion of addition, subtraction, and multiplication with congruences.

(Congruence modulo m is an example of an equivalence relation, and looking at remainders after division by m splits $\mathbb{Z}$ into m equivalence classes. For example, if $m=6$ our equivalence classes are

$$\{\dots,-18,-12,-6,0,6,12,18,\dots\} =: \bar{0}$$
$$\{\dots,-17,-11,-5,1,7,13,19,\dots\} =: \bar{1}$$
$$\{\dots,-16,-10,-4,2,8,14,20,\dots\} =: \bar{2}$$
$$\{\dots,-15,-9,-3,3,9,15,21,\dots\} =: \bar{3}$$
$$\{\dots,-14,-8,-2,4,10,16,22,\dots\} =: \bar{4}$$
$$\{\dots,-13,-7,-1,5,11,17,23,\dots\} =: \bar{5}$$

We want to define addition, subtraction, and multiplication on these classes. We'll do this by choosing representatives of these classes, but we have to be careful and show our operation doesn't depend on our choice of representative — this is what we mean when we say something is "well-defined.")

Lemma

Addition, subtraction, and multiplication are well-defined for congruence classes modulo m. Precisely, suppose $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ with $a_1 \equiv a_2 \pmod{m}$ and $b_1 \equiv b_2 \pmod{m}$. Then

$$a_1 + b_1 \equiv a_2 + b_2 \pmod{m}$$
$$a_1 - b_1 \equiv a_2 - b_2 \pmod{m}$$
$$a_1 \cdot b_1 \equiv a_2 b_2 \pmod{m}$$

Pf.

We know $m \mid (a_1 - a_2)$ and $m \mid (b_1 - b_2)$, so suppose $a_1 - a_2 = \alpha m$, $b_1 - b_2 = \beta m$. Now consider

$$\begin{aligned} & a_1 + b_1 - (a_2 + b_2) \\ &= a_1 - a_2 + b_1 - b_2 \\ &= \alpha m + \beta m \\ &= (\alpha + \beta) m \end{aligned}$$

and so $m \mid [(a_1 + b_1) - (a_2 + b_2)]$ meaning $a_1 + b_1 \equiv a_2 + b_2 \pmod{m}$. The proofs for subtraction and multiplication are similar. □

The above means that we can do arithmetic (sans division) with congruence classes in a consistent way. For example, note $8 \equiv 14 \pmod{6}$ and $5 \equiv -1 \pmod{6}$. When we add these congruence classes

together, it doesn't matter if we use 8 and $\cancel{5}$, or 14 and -1 — the answer is the same either way:

$$8 + 5 \equiv 13 \pmod 6$$
$$14 + (-1) \equiv 13 \pmod 6.$$

You've probably noticed that division is not mentioned above — that's because division with congruence classes is not (typically) well-defined. For example,

$$7 \cdot 2 \equiv 13 \cdot 2 \pmod{12}$$

but $7 \not\equiv 13 \pmod{12}$ — meaning there's no notion of "½ - division by 2 - when working with congruences modulo 12! Also, notice $6 \cdot 2 \equiv 0 \pmod{12}$, even though $6 \not\equiv 0 \pmod{12}$ nor is $2 \not\equiv 0 \mod 12$!

We can use this arithmetic of congruences to solve equations involving congruences. E.g.

$$x + 5 \equiv 9 \pmod{11}$$
$$\Rightarrow x \equiv 9 - 5 \pmod{11}$$
$$\Rightarrow x \equiv 4 \pmod{11}$$

Even though we don't always have a notion of division for congruence classes, sometimes we can define a division, which is helpful to know when solving congruences

Lemma

Suppose $\gcd(c,m)=1$. Then

$$ac \equiv bc \pmod{m}$$
$$\Rightarrow a \equiv b \pmod{m}$$

Pf

We use the following fact whose proof is an exercise: if x and y are relatively prime and $x \mid yz$, then x must divide z.

As $ac \equiv bc \pmod{m}$, $ac - bc = \alpha m$ for some α. Thus $m \mid (a-b)c$. But as m and c are relatively prime, we must have that $m \mid a-b$, and so $a \equiv b \pmod{m}$. □

Exercise

If x and y are relatively prime, but $x \mid yz$, then $x \mid z$. (Hint: Think about the prime factorizations of x and y.)

This is helpful to know when solving congruences:

What values of x solve the congruence $9x - 7 \equiv 51 \pmod{20}$.

$$\begin{aligned} & 9x - 7 \equiv 51 \pmod{20} \\ \Rightarrow\ & 9x \equiv 58 \pmod{20} \\ \Rightarrow\ & 9x \equiv 18 \pmod{20} \\ \Rightarrow\ & 9x \equiv 9 \cdot 2 \pmod{20} \\ \Rightarrow\ & x \equiv 2 \pmod{20} \end{aligned}$$

Notice that congruences may not have any solutions! For example, there is no x solving the congruence

$$8x \equiv 6 \pmod{12}$$

In principle we can verify this is the case pretty easily since there are only 12 possibilities for x (because we're dealing with congruence classes):

$$\begin{aligned} 8 \cdot 0 &\equiv 0 \pmod{12} \\ 8 \cdot 1 &\equiv 8 \pmod{12} \\ 8 \cdot 2 &\equiv 4 \pmod{12} \\ 8 \cdot 3 &\equiv 0 \pmod{12} \\ 8 \cdot 4 &\equiv 8 \pmod{12} \\ 8 \cdot 5 &\equiv 4 \pmod{12} \\ 8 \cdot 6 &\equiv 0 \pmod{12} \\ 8 \cdot 7 &\equiv 8 \pmod{12} \\ 8 \cdot 8 &\equiv 4 \pmod{12} \\ 8 \cdot 9 &\equiv 0 \pmod{12} \\ 8 \cdot 10 &\equiv 8 \pmod{12} \\ 8 \cdot 11 &\equiv 4 \pmod{12} \end{aligned}$$

While an "exhaustive" calculation (i.e., trying all possibilities) is always possible in principle, it's not very enlightening and could be very slow if m is very large. The following theorem tells us precisely when we have a solution to a congruence of the form $ax \equiv c \pmod{m}$.

Theorem

The congruence

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

has a solution iff $\gcd(a,m) \mid c$.

Pf

- Suppose $ax \equiv c \pmod{m}$ has a solution. Thus $m \mid ax - c$, so for some y,

$$ax - c = my$$
$$\Rightarrow ax - my = c$$

but we know these equations have a solution iff $\gcd(a,m) \mid c$.

- If $\gcd(a,m) \mid c$, then we can solve

$$ax + my = c$$

thus $ax - c = m \cdot (-y)$, so $m \mid ax - c$, and $ax \equiv c \pmod{m}$. □

Notice that congruences have lots of solutions. E.g., $8x \equiv 4 \pmod{12}$ has the following solutions:

$\ldots, -34, -22, -10, 2, 14, 26, 38, 50, \ldots$
$\ldots, -31, -19, -7, 5, 17, 29, 41, 53, \ldots$
$\ldots, -28, -15, -4, 8, 20, 32, 44, 56, \ldots$
$\ldots, -25, -12, -1, 11, 23, 35, 47, 59, \ldots$

However, most of these solutions are congruent to one another: every solution above is congruent, modulo 12, to the other solutions on the same line. Thus there are only 4 incongruent solutions to $8x \equiv 4 \pmod{12}$: every solution to $8x \equiv 4 \pmod{12}$ is congruent to 2, 5, 8 or 11.

Theorem

Suppose $\gcd(a,m) \mid c$. Then

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

has exactly $\gcd(a,m)$ incongruent solutions.

Pf

By our earlier theorems, we know $ax \equiv c \pmod{m}$ has at least one solution: say x_0 is some solution. Then $x_1 = x_0 + \frac{m}{\gcd(a,m)}$ is either a new solution:

$$\begin{aligned} ax_1 &= a\left(x_0 + \frac{m}{\gcd(a,m)}\right) = ax_0 + m\frac{a}{\gcd(a,m)} \\ &\equiv ax_0 + md \pmod{m} \\ &\equiv ax_0 \pmod{m} \\ &\equiv c \pmod{m} \end{aligned}$$

Or it could be congruent to x_0. This would mean $x_1 - x_0 = \frac{m}{\gcd(a,m)}$ is divisible by m, but this can only happen if $\gcd(a,m)$.

In general we could define

$$x_k = x_0 + k \cdot \frac{m}{\gcd(a,m)}$$

and x_k will always be a solution to $ax \equiv c \pmod{m}$ — assuming x_0 is already a solution. It could be, though, that x_k is congruent to an old solution. This will only happen if

$$x_k - x_j \equiv 0 \pmod{m}$$
$$\Rightarrow k \cdot \frac{m}{\gcd(a,m)} - j \cdot \frac{m}{\gcd(a,m)} \equiv 0 \pmod{m}$$
$$\Rightarrow (k-j) \cdot \frac{m}{\gcd(a,m)} \equiv 0 \pmod{m}$$

But this would mean $k-j$ is a multiple of $\gcd(a,m)$. Starting from $j=0$, we have that x_k is a new solution (incongruent to x_i for $0 \le i < k$) precisely when $0 < k < \gcd(a,m)$. Thus there are exactly $\gcd(a,m)$ incongruent solutions to $ax \equiv c \pmod{m}$. □

Notice that if a and m are relatively prime, there is exactly one solution to $ax \equiv c \pmod{m}$ for every c!

We can also consider polynomial congruences, such as $x^2 + 1 \equiv 0 \pmod{10}$. This congruence has solutions $x = 3$ and $x = 7$. Notice that this means, for congruences modulo 10, 3^2 and 7^2 are -1!

Recall the fundamental theorem of algebra which says that a polynomial equation with coefficients in $\mathbb{R}$ (or $\mathbb{C}$) has at most d solutions if d is the degree of the polynomial.

This does not always hold for congruences. For example

$$x^3 + x^2 + 2x \equiv 0 \pmod{8}$$

has five solutions: 0, 2, 4, 5, and 6.

If we consider congruences modulo a prime, however, then the number of solutions is at most the ~~same~~ degree of the polynomial.

<u>Theorem</u>

Let p be a prime number and let $f(x)$ be the polynomial with integer coefficients:

$$f(x) = a_0 x^d + a_1 x^{d-1} + a_2 x^{d-2} + \cdots + a_{d-1} x + a_d$$

where $d \geq 1$ and $a_0 \not\equiv 0 \pmod{p}$. Then there are at most d solutions to

$$f(x) \equiv 0 \pmod{p}.$$

Pf

Suppose not — that is, suppose there exists a polynomial $F(x) = A_0 x^d + \cdots + A_{d-1} x + A_d$ which had $> d$ solutions, and $A_0 \not\equiv 0 \pmod p$. We will show the existence of such a polynomial would result in a contradiction, which means no such polynomial can exist.

Among all the polynomials with more solutions than the degree of the polynomial, choose one of the ones of least degree for F. Suppose $r_1, \ldots, r_{d+1}$ are (incongruent) solutions to $F(x) \equiv 0 \pmod p$.

Let y be any value and notice for any n,

$$x^n - y^n = (x-y) \cdot \sum_{i=0}^{n-1} x^{n-i} y^i$$

$$= (x-y)\left(x^{n-1} + x^{n-2} y + x^{n-3} y^2 + \cdots + x^2 y^{n-3} + x y^{n-2} + y^{n-1}\right)$$

Thus

$$F(x) - F(y) = \sum_{i=0}^{d} A_i x^i - \sum_{i=0}^{d} A_i y^i$$

$$= \sum_{i=0}^{d} A_i (x^i - y^i)$$

$$= \sum_{i=0}^{d} A_i \cdot (x-y) \cdot \sum_{j=0}^{i-1} x^{i-j} y^j$$

$$= (x-y) \cdot \sum_{i=0}^{d} A_i \sum_{j=0}^{i-1} x^{i-j} y^j$$

$$= (x-y) \cdot G(x)$$

Thus

$$F(x) = F(y) + (x-y)\cdot G(x)$$

If we let $y = r_i$ for one of our solutions, then

$$F(x) = (x-r_i)G(x)$$

But if we now plug in $r_j \neq r_i$ for x,

$$(r_j - r_i)G(r_j) \equiv 0 \pmod{p}$$

As $r_j - r_i \not\equiv 0 \pmod{p}$, and $r_j - r_i$ is relatively prime to p, we must have

$$G(r_j) \equiv 0 \pmod{p}$$

We can do this for each $r_j \neq r_i$, so $G(x)$ has at least d solutions. But $G(x)$ is a polynomial of degree at most $d-1$. This contradicts that F was the polynomial of minimal degree with more solutions than the degree of the polynomial!

□