Solving Congruence Equations
Class activity, Week 6

In this activity, we will consider congruence equations. As we saw in the Week 5 class activity, solving $ax \equiv b \pmod{n}$ is equivalent to solving $ax - b = kn$, which can be rewritten as the linear Diophantine equation $ax + n(-k) = b$. This Diophantine equation has a solution if and only if $\gcd(a, n)$ divides b.

Recall how we found solutions to Diophantine equations:
Suppose $b = \ell \cdot \gcd(a, n)$. Express $\gcd(a, n)$ as a linear combination of a and n, and then multiply both sides by ℓ to express b as a linear combination of a and n. For example, to solve for x in $4x \equiv 2 \pmod{6}$, we need to find a k so that $4x - 2 = 6k$, in other words $4x + 6(-k) = 2$. So to find a solution x we first express the greatest common divisor as a linear combination $6 - 4 = 2$. From this expression we find that $x = -1$.

As with Diophantine equations, there are infinitely many solutions to a congruence equation expressed in the form $x_k = x_0 + \dfrac{kn}{\gcd(a, n)}$ from Theorem 2 of Week 3 class activity. To check that x_k is also a solution, observe that

$$ax_k = ax_0 + \frac{a}{\gcd(a, n)}kn\,.$$

Since $\gcd(a, n)|a$, $\dfrac{a}{\gcd(a, n)}$ is an integer. Therefore, $ax_k \equiv ax_0 \pmod{n} \equiv b \pmod{n}$.

So, to solve $10 \cdot x \equiv 35 \pmod{75}$, we first rewrite it as a Diophantine equation:

$$10x - 35 = 75k \qquad \longrightarrow \qquad 10x - 75k = 35$$

Note that $\gcd(10, 75) = 5$ and $5|35$, so this equation has a solution. First, express 5 as a linear combination of 75 and 10, which doesn't require Euclidean algorithm in this case since it's easy to see $5 = 75 - 7 \cdot 10$. Then we multiply both sides by 7 to get

$$35 = 75 \cdot 7 - (7 \cdot 7) \cdot 10$$

Expressed in mod, this means $10(-49) \equiv 35 \pmod{75}$. If we want a positive x, we can use $10 \cdot 26 \equiv 35 \pmod{75}$. Note that there are other solutions, using the above formula. The other x solutions are $x_k = 26 + \frac{k \cdot 75}{5} = 26 + 15k$. For example, for $k = 1$, we get $x = 41$; $k = 2$ gives $x = 56$; and so on.

1. Let us now find solutions to each of the following equations using this idea. For each, find all integer solutions of the corresponding Diophantine equation and determine if your solution is unique with respect to the modulo you're working in.

a. $7x \equiv 9 \pmod{15}$ $\gcd(7, 15) = (1 = (15 - 2 \cdot 7) \cdot 9 \longrightarrow 9 = 9 \cdot 15 - 9 \cdot 2 \cdot 7$
$= 135 - (18)7 \longrightarrow x = -18$
$\equiv -3$
$\equiv 12$
$\sqrt{1|9}$
$x = 12 + 15k$

b. $9x \equiv 39 \pmod{42}$ $\gcd(9, 42) = (3 = 42 \cdot 2 - 9 \cdot 9) \cdot 13 \longrightarrow 39 = 42 \cdot 2 \cdot 13 - 9 \cdot 13 \cdot 9$
$x \equiv -117 \equiv 9$
$\sqrt{3|39}$
$x = 9 + k\frac{42}{3} = 9 + 14k$

c. $14x \equiv 42 \pmod{63}$ $\gcd(14, 63) = (7 = 63 - 14 \cdot 4)6 \longrightarrow 42 = 63 \cdot 6 - 6 \cdot 4 \cdot 14$
$x \equiv -24 \equiv 39$
$\sqrt{7|42}$
$x = 39 + k\frac{63}{7} = 39 + 9k$

Even though we have infinitely many solutions x_k, modulo n, some of these x_k's end up being the same. The solutions can be listed as $x_0, x_0 + \frac{n}{\gcd(a,n)}, x_0 + \frac{2n}{\gcd(a,n)}, \ldots$. To find the number of distinct solutions consider when the list starts repeating (modulo n), i.e. when $x_0 \equiv x_0 + \frac{r \cdot n}{\gcd(a,n)} \pmod{n}$. For this to hold $\frac{r \cdot n}{\gcd(a,n)}$ has to be congruent to 0 modulo n, i.e. it has to be divisible by n. The first time this happens is when $r = \gcd(a,n)$. Therefore, for $k = 0, 1, \ldots, (\gcd(a,n) - 1)$, we have different solutions, for a total of $\gcd(a,n)$ solutions. This finishes the proof of the following theorem.

Theorem 1: The congruence $ax \equiv b \pmod{n}$ has a solution if and only if $\gcd(a,n)$ divides b. In this case, the number of solutions modulo n is exactly $\gcd(a,n)$.

Corollary: The congruence $ax \equiv b \pmod{n}$ has a unique solution (modulo n) if $\gcd(a,n) = 1$.

Corollary: If p is prime and a is not divisible by p, the congruence $ax \equiv b \pmod{p}$ has a unique solution (modulo p).

Another way to see how many solutions we have for a congruence equation is by reducing the equation as in the following theorem.

Theorem 2: Assume $d = \gcd(a,n)$ divides b. Then $ax \equiv b \pmod{n}$ if and only if $\frac{a}{d} \cdot x \equiv \frac{b}{d} \pmod{\frac{n}{d}}$.

proof: Note that $ax \equiv b \pmod{n}$ is equivalent to $ax - b = kn$ for some integer k. By dividing both sides by $d \neq 0$, this equation is equivalent to $\frac{a}{d} \cdot x - \frac{b}{d} = k \cdot \frac{n}{d}$. Therefore x is a solution for $\frac{a}{d} \cdot x \equiv \frac{b}{d} \pmod{\frac{n}{d}}$. Similarly, the converse is true. □

Corollary: If $d = \gcd(a,n)$ divides b, the number of solutions of $ax \equiv b \pmod{n}$ is $\gcd(a,n)$.

proof: Suppose x is a solution for $ax \equiv b \pmod{n}$. Then from Theorem 2, x is a solution for $\frac{a}{d} \cdot x \equiv \frac{b}{d} \pmod{\frac{n}{d}}$. Say x_0 is a solution modulo $\frac{n}{d}$. Then, all other solutions are of the form $x_0 + k \cdot \frac{n}{d}$. As before, we see that for $k = 0, 1, \ldots, (d-1)$ we get different solutions modulo n. Therefore, there are d solutions modulo n. □

Consider now a special congruence equation: $ax \equiv ab \pmod{n}$. If $\gcd(a,n) = 1$, then according to the first corollary of Theorem 1, there is only one solution for the congruence equation modulo n. Therefore, any solution x satisfies $x \equiv b \pmod{n}$.

Corollary: If $\gcd(a,n) = 1$ and $ax \equiv ab \pmod{n}$, then $x \equiv b \pmod{n}$.

For the last corollary, consider another special congruence equation: $ax \equiv 1 \pmod{n}$. A solution for this equation is called an *inverse* of a. From Theorem 1, we know that for an inverse to exist $\gcd(a,n)$ must equal 1. In that case, we also have a unique inverse.

Corollary: Given a modulo n, there exists an inverse for a if and only if $\gcd(a,n) = 1$. In that case, the inverse is unique.

Given n, the number of positive integers that are less or equal to than n and relatively prime to n is denoted by $\phi(n)$. More specifically,

$$\phi(n) = |\{x : 1 \leq x \leq n \text{ and } \gcd(x, n) = 1\}|$$

where $|\cdot|$ denotes the number of elements. From the above corollary, we see that modulo n, the number of residue classes which have inverses is equal to $\phi(n)$.

2 a. Find the inverse b for 5 modulo 14.

3

b. Using the fact that $5b \equiv 1 \pmod{14}$, solve the congruence equation $5x \equiv 12 \pmod{14}$.

$3 \cdot 12 \equiv 8$

We use a^{-1} to represent the residue class of the inverse of a modulo n. So, from your work above $5^{-1} \equiv$ 3 (mod 14).

3. Given a prime number p, how many residue classes have inverses? (Note: You might want to start by trying specific cases such as $p = 3, 5, 7$.)

$p-1$ (all except [p])

Corollary: For a prime p, $\phi(p) =$ $p-1$. In other words, all positive integers less than p are coprime with p.

4. (Optional) Can you figure out what $\phi(pq)$ is where p, q are primes?

$pq - \frac{pq}{p} - \frac{pq}{q} + 1 = pq - q - p + 1 = (p-1)(q-1)$

We will later see how to calculate $\phi(n)$ for any integer n.

$\phi(pqr) = pqr - \frac{pqr}{p} - \frac{pqr}{q} - \frac{pqr}{r} + \frac{pqr}{pq} + \frac{pqr}{pr} + \frac{pqr}{qr} - 1$

$= pqr - qr - pr - pq + r + q + p - 1$

$= (p-1)(q-1)(r-1)$

$\phi(p^2) = p^2 - p = p(p-1)$

$\phi(p^3) = p^3 - p^2 = p^2(p-1)$

$\phi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1)$

$\phi(p^2q) = p^2q - pq - p^2 + p = p(pq - q - p + 1) = p(p-1)(q-1)$

$\phi(p^{n_1}q^{n_2}) = p^{n_1-1}q^{n_2-1}(p-1)(q-1)$

$\phi(n) = \phi(p_1^{n_1}p_2^{n_2}\cdots p_k^{n_k}) = p_1^{n_1-1}p_2^{n_2-1}\cdots (p_1-1)(p_2-1)\cdots$