Class Activity, Week 7
Chinese Remainder Theorem

As you saw in pre-class, if we are given a system of the form $x \equiv r (\text{mod } n_1)$ and $x \equiv r (\text{mod } n_2)$ with $\gcd(n_1, n_2) = 1$, or more generally, a system of the form

$$x \equiv r \pmod{n_1},\ x \equiv r \pmod{n_2},\ x \equiv r \pmod{n_3},\ \ldots,\ x \equiv r \pmod{n_k},$$

with $\gcd(n_i, n_j) = 1$ for all $i \neq j$, then $x \equiv r \pmod{n_1 n_2 \cdots n_k}$ is the unique solution modulo $n_1 n_2 \cdots n_k$. The reason for the uniqueness is because if both x, y modulo n_1, n_2 satisfy the system, then $x - y \equiv 0 \pmod{n_1}$ and $x - y \equiv 0 \pmod{n_2}$, leading to $x \equiv y \pmod{n_1 n_2}$ since $\gcd(n_1, n_2) = 1$.

What about systems where the right hand sides are not necessarily the same value for each modulus? For example, suppose we need to solve $x \equiv 2 \pmod 3$ and $x \equiv 3 \pmod 5$. Are such systems always solvable? To answer this question we use the Chinese Remainder Theorem.

Theorem 1: (Chinese Remainder Theorem) Suppose $n_1, n_2, \ldots, n_k$ are pairwise relatively prime and $r_1, r_2, \ldots, r_k$ are any numbers. Then, there exists a solution for

$$\begin{aligned} x &\equiv r_1 \pmod{n_1} \\ x &\equiv r_2 \pmod{n_2} \\ &\vdots \\ x &\equiv r_k \pmod{n_k} \end{aligned}$$

Furthermore, x is unique modulo $n = n_1 n_2 \cdots n_k$.

proof: We first show that a solution exists. Since $\gcd(\frac{n}{n_i}, n_i) = 1$ for any i, we can find a solution for $\frac{n}{n_i} \cdot x \equiv r_i \pmod{n_i}$. Let us pick one solution and call that s_i. Now, consider $x_0 = \frac{n}{n_1} \cdot s_1 + \frac{n}{n_2} \cdot s_2 + \cdots + \frac{n}{n_k} \cdot s_k$. For each $j \neq i$, n_j divides $\frac{n}{n_i}$. For example, n_1 divides $\frac{n}{n_2}$ because n contains a factor of n_1. Using this, for any i,

$$x_0 \equiv \frac{n}{n_i} \cdot s_i \equiv r_i \pmod{n_i}$$

because of the way we chose s_i. Therefore, x_0 is a solution for the given system.

Now to show uniqueness modulo n, suppose there are two solutions x_1 and x_2. Since both are solutions to the system of equations, we find that

$$\begin{aligned} x_1 - x_2 &\equiv 0 \pmod{n_1} \\ x_1 - x_2 &\equiv 0 \pmod{n_2} \\ &\vdots \\ x_1 - x_2 &\equiv 0 \pmod{n_k} \end{aligned}$$

Since $\gcd(n_i, n_j) = 1$, we know that $x_1 - x_2 \equiv 0 \pmod n$, and hence the solution to the system given in the theorem is unique modulo n. □

This proof is a constructive proof, giving us a recipe to solve a system and not just telling us a solution exists. So to solve a system of congruences, we execute the following steps:

- For each ith equation of the system, find $\frac{n}{n_i}$, where n_i is the modulus in that equation and n is the product of all moduli.
- Solve for $\frac{n}{n_i} \cdot x \equiv r_i \pmod{n_i}$. Call this solution s_i.
- Add all the $\frac{n}{n_i} \cdot s_i$'s. This sum is a solution for the system.

Let us apply these steps to solve one example system. Suppose we want to solve

$$x \equiv 2 \pmod 3 \text{ and } x \equiv 3 \pmod 5 .$$

Then $n = 3 \cdot 5 = 15$. So for the first equation, $i = 1$, we have $\frac{n}{n_1} = 5$ (first step). We need to solve $\frac{n}{n_1}x \equiv r_1 \pmod{n_1}$, which becomes $5x \equiv 2 \pmod 3$ when we substitute the values. This congruence equation simplifies to $2x \equiv 2 \pmod 3$, and a solution is $s_1 = 1$ (second step). We repeat the first two steps for each i, so we move onto $i = 2$. First $\frac{n}{n_2} = 3$, and we need to solve, $\frac{n}{n_2}x \equiv r_2 \pmod{n_2}$, i.e. $3x \equiv 3 \pmod 5$. Again, a solution is $s_2 = 1$.
After the first two steps are completed for each i, we put the solution together as described in step 3. A solution for the system is $5 \cdot 1 + 3 \cdot 1$, i.e. $x \equiv 8 \pmod{15}$.
Notice that when we substitute the expression $5 \cdot 1 + 3 \cdot 1$ in place of x in the first congruence equation, we get $5 \cdot 1 + 3 \cdot 1 \equiv 2 \pmod 3$, which simplifies to $5 \cdot 1 \equiv 2 \pmod 3$ because the second term contains 3. Since $s_1 = 1$ was chosen to satisfy $5s_1 \equiv 2 \pmod 3$, the equation holds. Because of the way we constructed the solution, when used in each congruence equation, all but one of the terms will cancel and by choosing s_i in a specific way, we can ensure the solution to work for all equations.

1. Use the Chinese Remainder Theorem method to solve the following systems of congruence equations:

a.
$$\begin{aligned} x &\equiv 3 \pmod 5 \\ x &\equiv 4 \pmod 7 \end{aligned}$$

b.
$$\begin{aligned} x &\equiv 4 \pmod 9 \\ x &\equiv 5 \pmod{14} \end{aligned}$$

c.
$$\begin{aligned} x &\equiv 1 \pmod 3 \\ x &\equiv -2 \pmod 5 \\ x &\equiv 4 \pmod 7 \end{aligned}$$

d.
$$\begin{aligned} x &\equiv 3 \pmod 5 \\ x &\equiv 4 \pmod 7 \\ x &\equiv 5 \pmod 9 \end{aligned}$$

Chinese Remainder Theorem is a special case of the following theorem, which we state without proof.

Theorem 2: The system

$$\begin{aligned} x &\equiv r_1 \pmod{n_1} \\ x &\equiv r_2 \pmod{n_2} \\ &\vdots \\ x &\equiv r_k \pmod{n_k} \end{aligned}$$

is solvable if and only if $\gcd(n_i, n_j)$ divides $r_i - r_j$. Furthermore, the solution is unique modulo $\text{lcm}(n_1, n_2, \cdots, n_k)$.

We can also consider a more generalized linear system of the form

$$\begin{aligned} a_1x &\equiv r_1 \pmod{n_1} \\ a_2x &\equiv r_2 \pmod{n_2} \\ &\vdots \\ a_kx &\equiv r_k \pmod{n_k} \end{aligned}$$

In order to solve this system, we first solve for x modulo n_i for every i, and then use the Chinese Remainder Theorem. So in order for the system to have a solution, we need $\gcd(a_i, n_i)$ to divide r_i for every i using Theorem 1 in the previous week's class activity.

2. Solve the system:
$$\begin{aligned} 2x &\equiv 5 \pmod 7 \\ 4x &\equiv 2 \pmod 6 \\ x &\equiv 3 \pmod 5 \end{aligned}$$

3. Solve the system:
$$\begin{aligned} 5x &\equiv 2 \pmod 3 \\ 2x &\equiv 4 \pmod{10} \\ 4x &\equiv 7 \pmod 9 \end{aligned}$$

Fermat's Little Theorem

Recall that we defined the **order** of a modulo n, to be the smallest positive integer k such that $a^k \equiv 1 \pmod n$. For $n = p$ prime, it turns out we can define the order for all a not a multiple of p. In fact, we have the following information about all non-zero $a \pmod p$.

Theorem 3: (Fermat's Little Theorem) If p is prime and $a \not\equiv 0 \pmod p$, then

$$a^{p-1} \equiv 1 \pmod p .$$

proof: Consider the following numbers modulo p: $a, 2a, 3a, \ldots, (p-1)a$. We claim that these numbers are distinct modulo p. Suppose $i \cdot a \equiv j \cdot a \pmod p$ for $i \neq j$. This congruence is equivalent to $p | a(i-j)$. Since $p \not| a$, it means $p|(i-j)$, which is not possible since both i, j are less than or equal to $(p-1)$.

Therefore, the numbers $a, 2a, 3a, \ldots, (p-1)a$ must equal the numbers $1, 2, \ldots, (p-1)$ (modulo n) arranged randomly. Hence the product of $a, 2a, 3a, \ldots, (p-1)a$ must equal the product of $1, 2, \ldots, (p-1)$ modulo n, i.e.

$$1 \cdot 2 \cdot 3 \cdots (p-1) \equiv a \cdot 2a \cdot 3a \cdots (p-1)a \pmod n \equiv a^{p-1} 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod n$$

Since $1 \cdot 2 \cdot 3 \cdots (p-1)$ is not divisible by p, we can cancel that from both sides leaving us with $a^{p-1} \equiv 1 \pmod n$. □

4. Check that $a^6 \equiv 1 \pmod 7$ for all $a \not\equiv 0$ modulo 7.

Fermat's Little Theorem implies (as we will show later) that given a prime p and an $a \not\equiv 0 \pmod p$, the order of a divides $p-1$. In some cases the order is exactly $p-1$, and so we can express any number as a^r for some r modulo p. This is an important structural property of residue classes for prime moduli. We will see implications of this later as well.

Fermat's Little Theorem can also be expressed as follows, which allows $a \equiv 0 \pmod p$ to be included in the statement:

Corollary: For any prime p and any a, we have

$$a^p \equiv a \pmod p .$$

A generalization of Fermat's Little Theorem is the following.

Theorem 4: (Euler-Fermat Theorem) If $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod n$.

5. Find $\phi(15)$ and check if $a^{\phi(15)} \equiv 1 \pmod{15}$ holds for $a = 2, 4, 7$.

6. Modify the proof of the Fermat's Little Theorem to prove the Euler-Fermat Theorem.

Note: The use of *order* in defining these terms is no accident because the order of a mod n is the order of the element a in the multiplicative group of integers mod n, as you might have seen/will see in MTH 450. This group has $\phi(n)$ elements. Euler-Fermat Theorem then says that the order of any element in the group divides the order of the group (Lagrange's theorem). In the special case of n prime, we also have that the multiplicative group is cyclic.