**Math 406 Section 4.3: The Chinese Remainder Theorem**

1. **Introduction:** The Chinese Remainder Theorem (CRT) is a tool for solving systems of linear congruences. For example suppose we wished to solve the system:

$$\begin{aligned} 2x &\equiv 3 \bmod 10 \\ x &\equiv 2 \bmod 21 \end{aligned}$$

What could we say about the nature of the solutions?

2. **Lemma:** If $b_1, b_2, ..., b_r$ are pairwise coprime and for each $i$ we have $b_i \mid c$ then $b_1 b_2 ... b_r \mid c$.

**Proof:** Suppose $p^k$ appears in the prime factorization of $b_1 b_2 ... b_r$. Then $p^k$ appears in only one of the $b_i$ since they are pairwise coprime. Then since $b_i \mid c$ we know that $p^j$ appears in the prime factorization of $c$ with $j \geq k$. Thus $b_1 b_2 ... b_r \mid c$. $\mathcal{QED}$

3. **Theorem (The Chinese Remainder Theorem):** Suppose $m_1, m_2, ..., m_r$ are pairwise coprime integers. Then the system:

$$\begin{aligned} x &\equiv a_1 \bmod m_1 \\ x &\equiv a_2 \bmod m_2 \\ \vdots &\quad\ \vdots \\ x &\equiv a_r \bmod m_r \end{aligned}$$

Has a unique solution mod $M = m_1 m_2 ... m_r$.

**Pre-Proof Note:** The proof of this is interesting in that it's constructive, meaning it explicitly tells us how to construct a solution.

**Proof:** For each $i$ define $M_i = M/m_i$, then for each $i$ the equation $M_i y_i \equiv 1 \bmod m_i$ has a unique solution since $\gcd(M_i, m_i) = 1 \mid 1$. Note that $\gcd(M_i, m_i) = 1$ is guaranteed by the pairwise coprimality.

Take all the $y_i$ and construct the integer:

$$M = a_1 M_1 y_1 + a_2 M_2 y_2 + ... + a_r M_r y_r$$

Our claim is that this does the job. To see this note that for any particular $i$ we have $m_i \mid M_j$ for $j \neq i$. This means that $M_j \equiv 0 \bmod m_i$ for each $j \neq i$ and so when we examine $M \bmod m_i$ we are only left with $a_i M_i y_i$ and $a_i M_i y_i \equiv a_i \bmod m_i$.

To show that this $M$ is unique mod $M$ we suppose that $x_1$ and $x_2$ are both solutions. Then for each $i$ we have $x_1 \equiv a_i \equiv x_2 \bmod m_i$ and so $m_i \mid (x_1 - x_2)$. But then since the $m_i$ are pairwise coprime we have $M \mid (x_1 - x_2)$ and so $x_1 \equiv x_2 \bmod M$. $\mathcal{QED}$

**Note 1:** When solving $M_i y_i \equiv 1 \bmod m_i$ we should always reduce $M_i$ first. This can help see the solution more easily. The solution may not be obvious though, but it's just a linear congruence and can be solved with the Euclidean Algorithm.

**Note 2:** If one (or more) of the linear congruences has a coefficient in front of the $x$ then we must solve those linear congruences for $x$ separately first.

**Note 3:** In addition if the $m_i$ are not pairwise coprime then solutions may or may not exist and may or may not be unique, the Chinese Remainder Theorem says nothing.

4. **Example:** Consider the system:

$$x \equiv 2 \bmod 6$$
$$x \equiv 4 \bmod 7$$
$$x \equiv 3 \bmod 25$$

The CRT states that there is a unique solution modulo $(6)(7)(25) = 1050$.

- Put $M_1 = (7)(25) = 175$ then we solve $M_1y_1 \equiv 1 \bmod m_1$ which is $175y_1 \equiv 1 \bmod 6$ which reduces to $1y_1 \equiv 1 \bmod 6$ which has obvious solution $y_1 \equiv 1 \bmod 6$.
- Put $M_2 = (6)(25) = 150$ then we solve $M_2y_2 \equiv 1 \bmod m_2$ which is $150y_2 \equiv 1 \bmod 7$ which reduces to $3y_2 \equiv 1 \bmod 7$ which has solution $y_2 \equiv 5 \bmod 7$.
- Put $M_3 = (6)(7) = 42$ then we solve $M_3y_3 \equiv 1 \bmod m_3$ which is $42y_3 \equiv 1 \bmod 25$ which reduces to $17y_3 \equiv 1 \bmod 25$ which has solution $y_3 \equiv 3 \bmod 25$.

Then we construct:

$$M = (2)(175)(1) + (4)(150)(5) + (3)(42)(3) = 3728 \equiv 578 \bmod 1050$$

5. Application to Cryptography.

Much of this will be more clear when we have talked about the RSA algorithm but we can at least give a high-level overview of how the CRT is used in practice.

In the RSA algorithm Bob picks two large primes $p$ and $q$. He picks $e$ with $\gcd(e, (p-1)(q-1)) = 1$ and calculates $d$ with $de = 1 \bmod (p-1)(q-1)$.

He then calculates $n = pq$ and makes $n$ and $e$ public. He keeps $p, q, d$ private.

When he gets an encrypted message $c$ from Alice he decrypts it to the message $x$ via:

$$x \equiv c^d \bmod pq$$

This is a messy calculation because $pq$ is large.

So what actually happens is that Bob also stores $d_p$ the reduced residue of $d \bmod p-1$ and $d_q$ the reduced residue of $d \bmod q-1$.

Then observe that:

$$x \equiv c^d \bmod pq$$

iff

$$x \equiv c^d \bmod p$$
$$x \equiv c^d \bmod q$$

iff

$$x \equiv c^{d_p} \bmod p$$
$$x \equiv c^{d_q} \bmod q$$

This last iff is because when working with a prime moduli $p$, exponents work mod $p-1$ as we'll see.

So what Bob actually does is calculates the reduced residue of $c^{d_p} \bmod p$ and $c^{d_q} \bmod q$ and then uses the CRT to solve for $x$.