1 Chinese Remainder Theorem

This is a classic result due to the Chinese mathematician
In his treatise he proposed the problem: find a number (natural number) $x$ such that
\[ x \equiv 2 \pmod{3} \]
\[ x \equiv 3 \pmod{5} \]
\[ x \equiv 2 \pmod{7} \]
His technique to do so is formalized in the Chinese Remainder Theorem stated below.

**Theorem 1.** Let $m_1, m_2, \ldots, m_n$ be such that $\forall i \neq j \hspace{1em} \gcd(m_i, m_j) = 1$, and let $a_1, a_2, \ldots, a_n$ be integers. Let $m = \prod_{i=1}^{n} m_i$ (i.e. $m = m_1 \times m_2 \times \cdots m_n$). Then there is a unique solution $x$, modulo $m$ to the set of congruences
\[ x \equiv a_1 \mod (m_1) \]
\[ x \equiv a_2 \mod (m_2) \]
\[ \vdots \]
\[ x \equiv a_n \mod (m_n) \]

Equivalently, there is a unique integer $x$, $0 \leq x \leq m - 1$ that satisfies the $n$ congruences. The $m_i$ are distinct, pairwise relatively prime numbers. It may help to think of them at first as distinct primes.

**Proof.** For $k = 1, 2, \ldots, n$ let $M_k = m_1 \times m_2 \cdots m_{k-1} \times m_{k+1} \cdots m_n$. $M_k$ is the product of all $m_i$ except $m_k$. Note that we have $M_k = m/m_k$, where the division is legitimate, since $\gcd(m_i, m_j) = 1$ for $i \neq j$. 


Now, \( \gcd(m_k, M_k) = 1 \) (this is true for each of the factors, and we proved that if \( p \mid ab \) then \( p \mid a \lor p \mid b \)).

Therefore, for each \( k \) \( M_k \) has a multiplicative inverse modulo \( m_k \), say \( y_k \). That is \( M_k \cdot y_k \equiv 1 \pmod{m_k} \) (we are using \( \cdot \) instead of \( \times \) to denote multiplication.)

We claim that
\[
x = a_1 \cdot M_1 \cdot y_1 + a_2 \cdot M_2 \cdot y_2 + \cdots + a_n \cdot M_n \cdot y_n
\]
is the required solution.

Note than for \( i \neq j \) \( M_i = 0 \pmod{n_j} \) since \( n_j \) is a factor of \( M_i \).

But that means that, for example for \( i = 1 \) all terms in the sum that defines \( x \) are 0, with the exception of the first term. So \( x \equiv a_1 \cdot M_1 \cdot y_1 \pmod{(m_1)} \)

Similarly, \( x \equiv a_i \pmod{(m_i)} \) for \( i = 2, \ldots, n \).

We shall prove uniqueness shortly.

We can solve the original puzzle: \( m = 3 \times 5 \times 7 = 105 \).
\[
M_1 = 5 \times 7 = 35; \quad M_2 = 21, \quad M_3 = 15. \quad \text{Note that } M_1 \equiv 2(\mod{3}); \quad M_2 \equiv 1(\mod{3});
\]
\[
y_1, \text{ the multiplicative inverse of } M_1 \pmod{3} \text{ is } 2\quad \text{(since } 2 \times 2 = 4 \equiv 1(\mod{3}) \text{). It is easy to see that both } y_2 \text{ and } y_3 \text{ are } 1 \text{ (in different residue classes!)} \text{ as the inverse of } 1 \text{ is always } 1 \text{ in each } \mathbb{Z}_m.
\]

So evaluating \( x = a_1 \cdot M_1 \cdot y_1 + a_2 \cdot M_2 + a_3 \cdot M_3 \) yields
\[
x = 2 \times 2 \times 35 + 3 \times 1 \times 21 + 2 \times 1 \times 15 = 233 \equiv 23(\mod{105})
\]

### 1.1 Uniqueness

We will need a lemma.

**Lemma 2.** If \( \gcd(m_1, m_2) = 1 \), and \( m_1 \mid a \) and \( m_2 \mid a \) then \( m_1 \cdot m_2 \mid a \)

**Proof.** Since \( m_1 \mid a \), \( \exists x : a = m_1 \cdot x \). Since \( m_2 \mid a, m_2 \mid m_1 \cdot x \). But since \( m_1, m_2 \) are relatively prime \( \neg (m_2 \mid m_1) \), so \( m_2 \mid x \), and so \( \exists w : x = m_2 \cdot w \). Substituting, we get \( a = m_1 \cdot x = m_1 \cdot m_2 \cdot w \), and so \( m_1 \cdot m_2 \mid a \)

It is not hard to generalize the lemma to \( k \) pairwise relatively prime \( n_i \).

Now the proof of uniqueness of the solution \( (\mod{m}) \) of the solution in the Chinese Remainder Theorem is easy. Suppose that there are two solutions, \( x_1 \) and \( x_2 \).
It is clear that for $i = 1, 2, \cdots n$ we have $x_1 - x_2 \equiv 0 \pmod{m_i}$.
The lemma above then implies that $x_1 - x_2 \equiv 0 \pmod{m}$.

2 Primes

For convenience we will define primes for positive integers.

Definition 3. $p \in \mathbb{N}, p > 1$, is a prime if $\text{div}(p) = \{1, p\}$

We will look at primes more in later lectures.

2.1 Wilson’s Theorem.

Theorem 4. If $p$ is a prime $(p - 1)! \equiv -1 \pmod{p}$

Proof. Recall the nonzero elements of $\mathbb{Z}_p$ are $\{1, 2, 3, \cdots p - 1\}$, and if $p$ is a prime, all of them have multiplicative inverses.

Lemma 5. Among the $p - 1$ nonzero elements of $\mathbb{Z}_p$ only 1 and $-1$ have the property that they are their own inverses.

Proof. If $x$ is its own inverse, $x^2 \equiv 1 \pmod{p}$. So

$x^2 - 1 \equiv 0 \pmod{p}$

$(x + 1)(x - 1) \equiv 0 \pmod{p}$

So $p|(x + 1)$ or $p|(x - 1)$ (Why? because we saw that $p|a \cdot b \rightarrow (p|a) \lor (p|b)$ when $p$ is a prime.)

If $p|(x + 1)$ then $x \equiv -1 \pmod{p}$, while if $p|(x - 1)$ then $x \equiv 1 \pmod{p}$ (of lemma)

Incidentally recall that $-1 \equiv p - 1 \pmod{p}$.

Now consider the set $\{2, 3, \cdots p - 2\}$. By the lemma, none of these numbers is their own inverse in $\mathbb{Z}_p$. Since they all have inverses, each of them must have an inverse that is in the set. Because inverses are unique, this partitions the set into pairs, of an element and its inverse. (Convince yourself that this works! in particular the cardinality of the set must be even...)

Now consider the product

$2 \cdot 3 \cdots p - 3 \cdot p - 2$, and rearrange it as products of pairs that are inverses of each other. Since each such pair evaluates to 1, we have that

$2 \cdot 3 \cdots p - 3 \cdot p - 2 \equiv 1 \pmod{p}$.
Now \( p - 1)! \equiv 1 \cdot (2 \cdot 3 \cdots p - 3 \cdot p - 2) \cdot (p - 1) \equiv 1 \cdot 1 \cdot (-1) \equiv -1 \pmod{p}. \) \( \square \)