1 Chinese Remainder Theorem

Using the techniques of the previous section, we have the necessary tools to solve congruences of the form \( ax \equiv b \pmod{n} \). The Chinese Remainder Theorem gives us a tool to consider multiple such congruences simultaneously.

First, let’s just ensure that we understand how to solve \( ax \equiv b \pmod{n} \).

**Example 1.** Find \( x \) such that \( 3x \equiv 7 \pmod{10} \)

**Solution.** Based on our previous work, we know that 3 has a multiplicative inverse modulo 10, namely \( 3^{\varphi(10)-1} \). Moreover, \( \varphi(10) = 4 \), so the inverse of 3 modulo 10 is \( 3^3 \equiv 27 \equiv 7 \pmod{10} \). Hence, multiplying both sides of the above equation by 7, we obtain

\[
3x \equiv 7 \pmod{10} \\
\iff 7 \cdot 3x \equiv 7 \cdot 7 \pmod{10} \\
\iff x \equiv 49 \equiv 9 \pmod{10}
\]

Hence, the solution is \( x \equiv 9 \pmod{10} \).

**Example 2.** Find \( x \) such that \( 3x \equiv 6 \pmod{12} \).

**Solution.** Uh oh. This time we don’t have a multiplicative inverse to work with. So what to do? Well, let’s take a look at what this would mean. If \( 3x \equiv 6 \pmod{12} \), that means \( 3x - 6 \) is divisible by 12, so there is some \( k \in \mathbb{Z} \) such that \( 3x - 6 = 12k \). Now that we’re working in the integers, we can happily divide by 3, and we thus obtain that \( x - 2 = 4k \). Hence, we have that \( x \equiv 2 \pmod{4} \) solves the desired congruence.

Proposition 1. Let \( n \in \mathbb{N} \), and let \( a, b \in \mathbb{Z} \). The congruence \( ax \equiv b \pmod{n} \) has a solution for \( x \) if and only if \( \gcd(a, n) | b \), again by Bezout’s Lemma.

Moreover, the strategy we used in Example 2 will in general work. Suppose that we have \( ax \equiv b \pmod{n} \), and we have that \( \gcd(a, n) = d \). Then in order that this has a solution, we know that \( b \) is divisible by \( d \). In particular, there exist integers \( a', b', n' \) such that \( a = a'd, b = b'd, n = n'd \). We can then work as we did in Example 2 to rewrite this equation as \( a'x \equiv b' \pmod{n'} \).
Example 3. Find $x$, if possible, such that

$$2x \equiv 5 \pmod{7},$$

and $3x \equiv 4 \pmod{8}$

Solution. First note that 2 has an inverse modulo 7, namely 4. So we can write the first equivalence as

$$x \equiv 4 \cdot 5 \equiv 6 \pmod{7}.$$ 

Hence, we have that $x = 6 + 7k$ for some $k \in \mathbb{Z}$.

Now we can substitute this in for the second equivalence:

$$3x \equiv 4 \pmod{8}$$

$$3(6 + 7k) \equiv 4 \pmod{8}$$

$$18 + 21k \equiv 4 \pmod{8}$$

$$2 + 5k \equiv 4 \pmod{8}$$

$$5k \equiv 2 \pmod{8}.$$ 

Recalling that 5 has an inverse modulo 8, namely 5, we thus obtain

$$k \equiv 10 \equiv 2 \pmod{8}.$$ 

Hence, we have that $k = 2 + 8j$ for some $j \in \mathbb{Z}$.

Plugging this back in for $x$, we have that $x = 6 + 7k = 6 + 7(2 + 8j) = 20 + 56j$ for some $j \in \mathbb{Z}$.

In fact, any choice of $j$ will work here. Hence, we have that $x$ is a solution to the system of congruences if and only if $x \equiv 20 \pmod{56}$.

Example 4. Find $x$, if possible, such that

$$x \equiv 3 \pmod{4},$$

and $x \equiv 0 \pmod{6}$.

Solution. Let’s work as we did above. From the first equivalence, we have that $x = 3 + 4k$ for some $k \in \mathbb{Z}$. Then, the second equivalence implies that $3 + 4k \equiv 0 \pmod{6}$, and hence $4k \equiv -3 \equiv 3 \pmod{6}$. However, this is impossible, since we know that $\gcd(4, 6) = 2$ and $2 \nmid 3$.

Ok, so not every system of congruences will have a solution, but our strategy of trying to solve them will reveal when there is no solution also.

Notice the problem that occurred here: when we considered the first equivalence, we ended up with a coefficient of 4 in front of the $k$. Since 4 is not relatively prime to 6, there was a chance that the next equivalence would not have a solution, and indeed that is what happened. In general this will be the case: if we consider two equivalences of the form

$$x \equiv b_1 \pmod{n_1}$$

$$x \equiv b_2 \pmod{n_2},$$

then the method we developed above will take the following approach: first, write $x = b_1 + kn_1$. Plug that in to the second equation to obtain $kn_1 \equiv b_2 - b_1 \pmod{n_2}$. If $n_1$ and $n_2$ share factors, then we may not be able to solve this equivalence, per Proposition. Hence, we can demand that $n_1$ and $n_2$ are relatively prime, and this should solve that problem.

Continuing, then, if we assume that $n_1$ and $n_2$ are relatively prime, we have reduced this system to $kn_1 \equiv b_2 - b_1 \pmod{n_2}$. Then we obtain $kn_1 - b_2 + b_1 = jn_2$ for some $j \in \mathbb{Z}$. Rearranging, we have $kn_1 - jn_2 = b_2 - b_1$. Since $n_1$ and $n_2$ are relatively prime, we know from Bezout’s Lemma that we will be
able to solve this equation for $k$ and $j$. Once we know $k$ and $j$, we can then backsolve to give us a solution for $x$.

This strategy of considering relatively prime moduli, in general, will yield a solution to this problem. The general form is given by the following theorem.

**Theorem 1.** Let $n_1, n_2, \ldots, n_k$ be a set of pairwise relatively prime natural numbers, and let $b_1, b_2, \ldots, b_k \in \mathbb{Z}$. Put $N = n_1 n_2 \ldots n_k$, the product of the moduli. Then there is a unique $x \pmod{N}$ such that $x \equiv b_i \pmod{n_i}$ for all $1 \leq i \leq k$.

Note that working mod $N$ should be unsurprising; this is how we ended up in the first example as well. You can see that the method of backsolving for $x$ will end up multiplying the moduli together.

**Proof.** For each $i$ with $1 \leq i \leq k$, put $m_i = \frac{N}{n_i}$. Notice that since the moduli are relatively prime, and $n_i$ is the product of all the moduli other than $n_i$, we have that $n_i \perp m_i$, and hence $m_i$ has a multiplicative inverse modulo $n_i$, say $y_i$. Moreover, note that $m_i$ is a multiple of $n_j$ for all $j \neq i$.

Put $x = y_1 b_1 m_1 + y_2 b_2 m_2 + \cdots + y_k b_k m_k$.

Notice that for each $i$ with $1 \leq i \leq k$, we obtain

\[
x \equiv y_1 b_1 m_1 + y_2 b_2 m_2 + \cdots + y_k b_k m_k \pmod{n_i} \\
\equiv y_i b_i m_i \pmod{n_i} \quad \text{ (since each $m_j$ with $j \neq i$ is a multiple of $n_i$)} \\
\equiv b_i \pmod{n_i} \quad \text{ (since $y_i$ is an inverse to $m_i$ modulo $n_i$).}
\]

Therefore, we have that $x \equiv b_i \pmod{n_i}$ for all $1 \leq i \leq k$.

Finally, we wish to show uniqueness of the solution \( x \pmod{N} \). Suppose that $x$ and $y$ both solve the congruences. Then we have that for each $i$, $n_i$ is a divisor of $x - y$. Since the $n_i$ are relatively prime, this means that $N$ is a divisor of $x - y$, and hence $x - y$ are congruent modulo $N$. \qed

**Example 5.** Use the Chinese Remainder Theorem to find an $x$ such that

\[
x \equiv 2 \pmod{5} \\
x \equiv 3 \pmod{7} \\
x \equiv 10 \pmod{11}
\]

**Solution.** Set $N = 5 \times 7 \times 11 = 385$. Following the notation of the theorem, we have $m_1 = N/5 = 77$, $m_2 = N/7 = 55$, and $m_3 = N/11 = 35$.

We now seek a multiplicative inverse for each $m_i$ modulo $n_i$. First: $m_1 \equiv 77 \equiv 2 \pmod{5}$, and hence an inverse to $m_1 \pmod{n_1}$ is $y_1 = 3$.

Second: $m_2 \equiv 55 \equiv 6 \pmod{7}$, and hence an inverse to $m_2 \pmod{n_2}$ is $y_2 = 6$.

Third: $m_3 \equiv 35 \equiv 2 \pmod{11}$, and hence an inverse to $m_3 \pmod{n_3}$ is $y_3 = 6$.

Therefore, the theorem states that a solution takes the form:

\[
x = y_1 b_1 m_1 + y_2 b_2 m_2 + y_3 b_3 m_3 = 3 \times 2 \times 77 + 6 \times 3 \times 55 + 6 \times 10 \times 35 = 3552.
\]

Since we may take the solution modulo $N = 385$, we can reduce this to 87, since $2852 \equiv 87 \pmod{385}$. 

---

3
**Example 6.** Find all solutions \(x\), if they exist, to the system of equivalences:

\[
\begin{align*}
2x &\equiv 6 \pmod{14} \\
3x &\equiv 9 \pmod{15} \\
5x &\equiv 20 \pmod{60}
\end{align*}
\]

**Solution.** As in Example 2, we first wish to reduce this, where possible, using the strategy outlined following the statement of Proposition 1. Since \(\gcd(2, 14) = 2\), we can cancel a 2 from all terms in the first equivalence to write \(x \equiv 3 \pmod{7}\). Likewise, we simplify the other two equivalences to reduce the entire system to

\[
\begin{align*}
x &\equiv 3 \pmod{7} \\
x &\equiv 3 \pmod{5} \\
x &\equiv 4 \pmod{12}
\end{align*}
\]

We can now follow the strategy of the Chinese Remainder Theorem. Following the notation in the theorem, we have

\[
\begin{align*}
m_1 &= 5 \cdot 12 = 60 \equiv 4 \pmod{7}; \quad y_1 \equiv 4^5 \equiv 1024 \equiv 2 \pmod{7} \\
m_2 &= 7 \cdot 12 = 84 \equiv 4 \pmod{5}; \quad y_2 \equiv 4^3 \equiv 64 \equiv 4 \pmod{5} \\
m_3 &= 7 \cdot 5 = 35 \equiv 11 \pmod{12}; \quad y_3 \equiv 11^3 \equiv (-1)^3 \equiv -1 \equiv 11 \pmod{12}.
\end{align*}
\]

Hence, we have \(x = y_1 m_1 b_1 + y_2 m_2 b_2 + y_3 m_3 b_3 = 2 \cdot 60 \cdot 3 + 4 \cdot 84 \cdot 3 + 11 \cdot 35 \cdot 4 = 2908\).

Hence, we have any solution \(x \equiv 2908 \equiv 388 \pmod{420}\).