# Lecture 7 — The Chinese Remainder Theorem

It is of course very easy to find a value $x$ satisfying

$$x \equiv c \pmod{m}$$

for any constant $c$: just take $x = c$. But suppose we wanted to find an $x$ solving this congruence for two different values of $m$ at the same time. I.e., is there an $x \in \mathbb{Z}$ which simultaneously satisfies both of the following congruences?

$$x \equiv c \pmod{m_1}$$
$$x \equiv c \pmod{m_2}$$

As an example, try to find an $x$ such that

$$x \equiv 3 \pmod{17}$$
$$x \equiv 3 \pmod{11}$$

After a little thought it's not too hard to find a solution: $x$ has to have the form $x = 17\alpha + 3$ and the form $x = 11\beta + 3$. To reconcile these, just take $\alpha = 11$ and $\beta = 17$.

$$\begin{aligned} x &= 11 \cdot 17 + 3 \\ &= 187 + 3 \\ &= 190. \end{aligned}$$

As another example, let's find an $x \in \mathbb{Z}$ such that

$$x \equiv 2 \pmod{9}$$
$$x \equiv 2 \pmod{15}$$

Of course, $x = 15 \cdot 9 + 2 = 137$ does the trick.

(Actually, an even easier solution is $x = 2$ — and $x = 3$ for the first example.)

Now let's try something a little bit harder: Is there an $x \in \mathbb{Z}$ with

$$x \equiv 7 \pmod{5}$$
$$x \equiv 7 \pmod{11}$$

Using the same process as above, $x = 62$ is what we want. Notice, however, the above could be rewritten as

$$x \equiv 2 \pmod{5}$$
$$x \equiv 7 \pmod{11}$$

We already know 62 makes this happen, but the answer might be harder to see if we write our first congruence as $x \equiv 2 \pmod{5}$ instead of $x \equiv 7 \pmod{5}$.

What about

$$x \equiv 3 \pmod{9}$$
$$x \equiv 28 \pmod{16}$$

Notice we can rewrite this as

$$x \equiv 3 \pmod{9}$$
$$x \equiv 12 \pmod{16}$$

This becomes

$$x \equiv 12 \pmod{9}$$
$$x \equiv 12 \pmod{16}$$

and so

$$x = 16 \cdot 9 + 12$$
$$= 156$$

Let's do one more example before we try to understand the general situation. Is there an $x \in \mathbb{Z}$ such that

$$x \equiv 19 \pmod{42}$$
$$x \equiv 15 \pmod{30}$$

How should we proceed in finding such an $x$ — or showing no such $x$ exists?

Well if $x \equiv 19 \pmod{42}$, then $x$ has the form $x = 42\alpha + 19$ for some $\alpha \in \mathbb{Z}$. Plugging this into the second congruence gives

$$42\alpha + 19 \equiv 15 \pmod{30}$$
$$\Rightarrow 42\alpha \equiv -4 \pmod{30}$$
$$\Rightarrow 42\alpha \equiv 26 \pmod{30}$$

Hence

$$42\alpha = 30\beta + 26$$

for some $\beta \in \mathbb{Z}$. However, writing this as $42\alpha + 30\gamma = 26$ (so $\beta = -\gamma$), we see

that there is no solution! If there were a solution $x \in \mathbb{Z}$ to

$$x \equiv 19 \pmod{42}$$
$$x \equiv 15 \pmod{30}$$

then there would also be a solution $\alpha, \gamma \in \mathbb{Z}$ to

$$42\alpha + 30\gamma = 26$$

But this equation has no solution since 26 is not a multiple of $\gcd(42, 30) = 6$!

What makes this last example, where there was no solution, to the previous examples where there was a solution? In all of our previous examples the moduli (the numbers we mod out by) were relatively prime, but this was not the case in the last example. As long as the moduli are relatively prime we will be able to find a solution to the congruence.

This result of solving congruences, provided we mod out by numbers which are relatively prime was known to ancient Chinese mathematicians, and for this reason is sometimes called the Chinese remainder theorem.

**Thm** (The Chinese Remainder Theorem)

Let $m$ and $n$ be relatively prime numbers and let $a, b \in \mathbb{Z}$ be any integers. Then there exists a solution to the system of congruence equations,

$$x \equiv a \pmod{m}$$
$$x \equiv b \pmod{n}$$

Furthermore, there is exactly one $x$ in $0 \leq x < mn$ solving these congruences.

**Pf**

Solutions to $x \equiv a \pmod{m}$ all have the form $x = m\alpha + a$. Plugging this into $x \equiv b \pmod{n}$ gives

$$m\alpha + a \equiv b \pmod{n}$$
$$\Rightarrow m\alpha \equiv b - a \pmod{n}$$

Thus $m\alpha = n\beta + b - a$ for some $\beta$, and we thus want to find $\alpha, \beta \in \mathbb{Z}$ solving

$$m\alpha - n\beta = b - a$$

As $m$ and $n$ are relatively prime, such a solution exists.

As $m$ and $n$ are relatively prime, there is only one congruence class, call it $\gamma$, solving

$$m\gamma \equiv b - a \pmod{n}$$

and so we may take $0 \leq \gamma < n$. Hence $x = m\gamma + a$, and $0 \leq \gamma < n$ implies $m\gamma < mn \leq m(n-1) = mn - m$.

Thus, taking $a < m$, $x \leq mn - m + a$ and $x < mn$. □

With the Chinese remainder theorem at our disposal, we are now ready to show how to calculate Euler's totient function. Recall

$$\varphi(n) = \#\{a \mid 1 \leq a \leq n, \gcd(a,n) = 1\}$$

$$\varphi(p) = p - 1 \text{ if } p \text{ is prime}$$

$$\varphi(p^k) = p^k - p^{k-1} \text{ if } p \text{ is prime.}$$

The following result is key for having an effective way to compute $\varphi$:

Theorem

If $m$ and $n$ are relatively prime, then $\varphi(mn) = \varphi(m)\varphi(n)$.

Pf

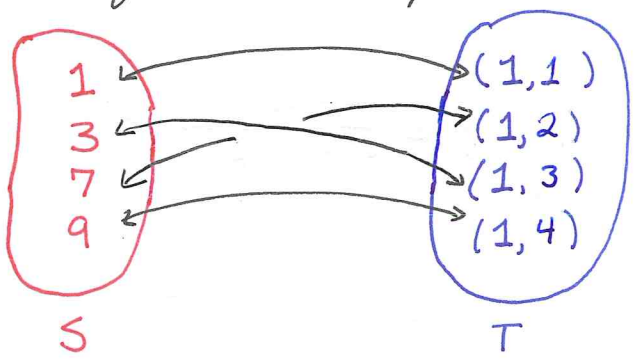
To show this result, we will establish a 1-1 correspondence between two sets:

$S := \{a \mid 1 \leq a \leq mn \ \gcd(a, mn) = 1\}$, and

$T := \{(b,c) \mid 1 \leq b \leq m, \ 1 \leq c \leq n, \gcd(b,m) = \gcd(c,n) = 1\}$.

That is, we'll show there's a way to match up each element of $S$ with an element of $T$ such that

- Every element of $S$ is matched up with a unique element of $T$, and
- every element of $T$ is matched up with a unique element of $S$.




The sets $S$ and $T$ for $m=2, n=5$

Constructing such a 1-1 correspondence shows that $S$ and $T$ have the same size. This will prove our theorem because $\#S = \varphi(mn)$ and $\#T = \varphi(m)\varphi(n)$. [In general, the collection of all pairs $(x,y)$ where $x \in X$ and $y \in Y$ has $\#X \cdot \#Y$ elements because for each of the $\#X$ options we have for $x$ in $(x,y)$, we have $\#Y$ options for the $y$. Thus there are

$$\underbrace{\#Y + \#Y + \cdots + \#Y}_{\#X \text{ times}} = \#X \cdot \#Y$$

pairs.]

To a value $a \in S$ (so, $\gcd(a, mn) = 1$) we associate an element $(b,c) \in T$ where $b \equiv a \pmod{m}$ and $c \equiv a \pmod{n}$.

Notice such a $(b,c)$ does exist in $T$. As $a$ has no common factors w/ $mn$, it has no common factors with neither $m$ nor $n$. (If $d|a$ and $d|m$, then obviously $d|mn$.)

Furthermore, $a$ is a solution to

$$x \equiv b \pmod{m}$$
$$x \equiv c \pmod{n}$$

which by the Chinese remainder theorem means $a$ is the only solution in $0 \leq x < mn$. This shows us each $a \in S$ is associated to a unique $(b,c) \in T$.

The Chinese remainder theorem also allows us to associate elements of $S$ to elements of $T$. Given $(b,c) \in T$, the Chinese remainder theorem guarantees us a unique solution, $0 \leq x < mn$ to

$$x \equiv b \pmod{m}$$
$$x \equiv c \pmod{n}$$

and we'll take this unique solution to be our associated $a \in S$. (Exercise: Show $a$ must be relatively prime to $mn$ if $a \equiv b \pmod{m}$ and $a \equiv c \pmod{n}$. To do this, use pf by contradiction: suppose $\gcd(a,m) \neq 1$ and show that would contradict $a \equiv b \pmod{m}$.)

This establishes a one-to-one correspondence between $S$ and $T$, thus $\#S = \#T$. As $\#S = \varphi(mn)$ and $\#T = \varphi(m)\varphi(n)$, we have that

$$\varphi(mn) = \varphi(m)\varphi(n)$$

provided $\gcd(m,n) = 1$. □

We now have an easy way of determining $\varphi(n)$, provided we have the prime factorization of $n$.

Pf

If $n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$ for distinct primes $p_1, \ldots, p_m$, then

$$\varphi(n) = \varphi(p_1^{k_1} \cdots p_m^{k_m})$$

$$= \varphi(p_1^{k_1}) \cdots \varphi(p_m^{k_m})$$

$$= [p_1^{k_1} - p_1^{k_1-1}] \cdot \ldots \cdot [p_m^{k_m} - p_m^{k_m-1}]$$

Pf

Exercise.

Using this theorem,

$$\varphi(360) = \varphi(8) \cdot \varphi(9) \cdot \varphi(5)$$
$$= \varphi(2^3) \cdot \varphi(3^2) \cdot \varphi(5)$$
$$= (2^3 - 2^2) \cdot (3^2 - 3) \cdot 4 = 4 \cdot 6 \cdot 4 = 96.$$