12-14-2022

The Chinese Remainder Theorem

The **Chinese Remainder Theorem** says that certain systems of simultaneous congruences *with different moduli* have solutions. The idea embodied in the theorem was known to the Chinese mathematician Sunzi in the 3rd century A.D. — hence the name.

I'll begin by collecting some useful lemmas.

Lemma 1. Let m and $a_1, \ldots, a_n$ be positive integers. If m is relatively prime to each of $a_1, \ldots, a_n$, then it is relatively prime to their product $a_1 \cdots a_n$.

Proof. If $(m, a_1 \cdots a_n) \neq 1$, then there is a prime p which divides both m and $a_1 \cdots a_n$. Now $p \mid a_1 \cdots a_n$, so p must divide a_i for some i. But p divides both m and a_i, so $(m, a_i) \neq 1$. This contradiction implies that $(m, a_1 \cdots a_n) = 1$. □

For example, 6 is relatively prime to 25, to 7, and to 11. Now $25 \cdot 7 \cdot 11 = 1925$, and $(6, 1925) = 1$.

I showed earlier that the greatest common divisor (a, b) of a and b is *greatest* in the sense that it is divisible by any common divisor of a and b. The next result is the analogous statement for least common multiples.

Lemma 2. Let m and $a_1, \ldots, a_n$ be positive integers. If m is a multiple of each of $a_1, \ldots, a_n$, then m is a multiple of $[a_1, \ldots, a_n]$.

Proof. By the Division Algorithm, there are unique numbers q and r such that

$$m = q \cdot [a_1, \ldots, a_n] + r, \text{ where } 0 \leq r < [a_1, \ldots, a_n].$$

Now a_i divides both m and $[a_1, \ldots, a_n]$, so a_i divides r. Since this is true for all i, r is a common multiple of the a_i smaller than the *least* common multiple $[a_1, \ldots, a_n]$. This is only possible if $r = 0$. Then $m = q \cdot [a_1, \ldots, a_n]$, i.e. m is a multiple of $[a_1, \ldots, a_n]$. □

For instance, 88 is a multiple of 4 and 22. The least common multiple of 4 and 22 is 44, and 88 is also a multiple of 44.

Lemma 3. Let $a_1, \ldots, a_n$ be positive integers. If $a_1, \ldots, a_n$ are pairwise relatively prime (that is, $(a_i, a_j) = 1$ for $i \neq j$), then

$$[a_1, \ldots, a_n] = a_1 \cdots a_n.$$

Proof. Induct on n. The statement is trivially true for $n = 1$, so I'll start with $n = 2$. The statement for $n = 2$ follows from the equation $xy = [x, y](x, y)$:

$$[a_1, a_2] = \frac{a_1 a_2}{(a_1, a_2)} = \frac{a_1 a_2}{1} = a_1 a_2.$$

Now assume $n > 2$, and assume the result is true for n. I will prove that it holds for $n + 1$.

Claim: $[[a_1, \ldots, a_n], a_{n+1}] = [a_1, \ldots, a_n, a_{n+1}]$.

(Some people take this as an iterative *definition* of $[a_1, \ldots, a_n, a_{n+1}]$.) $[a_1, \ldots, a_n, a_{n+1}]$ is a multiple of each of $a_1, \ldots, a_n$, so by Lemma 2 it's a multiple of $[a_1, \ldots, a_n]$. It's also a multiple of a_{n+1}, so

$$[[a_1, \ldots, a_n], a_{n+1}] \,\Big|\, [a_1, \ldots, a_n, a_{n+1}].$$

On the other hand, for $i = 1, \ldots, n$,

$$a_i \,\Big|\, [a_1, \ldots, a_n] \quad \text{and} \quad [a_1, \ldots, a_n] \,\Big|\, [[a_1, \ldots, a_n], a_{n+1}].$$

Therefore,

$$a_i \mid [[a_1, \ldots, a_n], a_{n+1}] .$$

Obviously,

$$a_{n+1} \mid [[a_1, \ldots, a_n], a_{n+1}] .$$

Thus, $[[a_1, \ldots, a_n], a_{n+1}]$ is a common multiple of all the a_i's. Since $[a_1, \ldots, a_n, a_{n+1}]$ is the least common multiple, Lemma 2 implies that

$$[a_1, \ldots, a_n, a_{n+1}] \mid [[a_1, \ldots, a_n], a_{n+1}] .$$

Since I have two *positive* numbers which divide one another, they're equal:

$$[[a_1, \ldots, a_n], a_{n+1}] = [a_1, \ldots, a_n, a_{n+1}].$$

This proves the claim.

Returning to the proof of the induction step, I have

$$[a_1, \ldots, a_n, a_{n+1}] = [[a_1, \ldots, a_n], a_{n+1}] = [a_1 \cdots a_n, a_{n+1}] = a_1 \cdots a_n a_{n+1}.$$

The second equality follows by the induction hypothesis (the statement for n). The third equality follows from Lemma 1 and the result for $n = 2$. □

As an example, 6, 25, and 7 are relatively prime (in pairs). The least common multiple is $[6, 25, 7] = 1050 = 6 \cdot 25 \cdot 7$.

Theorem. (**The Chinese Remainder Theorem**) Suppose m_1, …, m_n are pairwise relatively prime (that is, $(m_i, m_j) = 1$ for $i \neq j$). Then the following system of congruences has a unique solution mod $m_1 m_2 \cdots m_n$:

$$\begin{aligned} x &= a_1 \pmod{m_1} \\ x &= a_2 \pmod{m_2} \\ &\vdots \\ x &= a_n \pmod{m_n} \end{aligned}$$

Notation.

$$x_1 x_2 \cdots \widehat{x_i} \cdots x_n \quad \text{means} \quad x_1 x_2 \cdots x_i \cdots x_n \quad \text{omitting} \quad x_i.$$

For example,

$$x_1 x_2 \cdots \widehat{x_4} \cdots x_6 \quad \text{means} \quad x_1 x_2 x_3 x_5 x_6.$$

This is a convenient (and standard) notation for omitting a single variable term in a product of things. □

Proof. Define

$$p_k = m_1 \cdots \widehat{m_k} \cdots m_n.$$

That is, p_k is the product of the m's with m_k omitted. By Lemma 1, $(p_k, m_k) = 1$. Hence, there are numbers s_k, t_k such that

$$s_k p_k + t_k m_k = 1.$$

In terms of congruences,

$$s_k p_k = 1 \pmod{m_k} .$$

Now let

$$x = a_1 p_1 s_1 + a_2 s_2 p_2 + \cdots + a_n p_n s_n.$$

If $j \neq k$, then $m_k \mid p_j$, so mod m_k all the terms but the k-th term are 0 mod m_k:

$$x = a_k p_k s_k = a_k \cdot 1 = a_k \pmod{m_k}.$$

This proves that x is a solution to the system of congruences (and incidentally, gives a formula for x). Now suppose that x and y are two solutions to the system of congruences.

$$\begin{aligned} x &= a_1 \pmod{m_1} \quad \text{and} \quad y = a_1 \pmod{m_1} \\ x &= a_2 \pmod{m_2} \quad \text{and} \quad y = a_2 \pmod{m_2} \\ &\vdots \\ x &= a_n \pmod{m_n} \quad \text{and} \quad y = a_n \pmod{m_n} \end{aligned}$$

Then

$$x = a_k = y \pmod{m_k} \quad \text{so} \quad x - y = 0 \pmod{m_k} \quad \text{or} \quad m_k \mid x - y.$$

Thus, $x - y$ is a multiple of all the m's, so

$$[m_1, \ldots, m_n] \mid x - y.$$

But the m's are pairwise relatively prime, so by Lemma 3,

$$m_1 \cdots m_n \mid x - y, \quad \text{or} \quad x = y \pmod{m_1 \cdots m_n}.$$

That is, the solution to the congruences is unique mod $m_1 \cdots m_n$. □

Example. Solve

$$\begin{aligned} x &= 2 \pmod 4 \\ x &= 7 \pmod 9 \end{aligned}.$$

$(4, 9) = 1$, so there is a unique solution mod 36. Following the construction of x in the proof,

$$p_1 = 9, \quad 9 \cdot 1 = 1 \pmod 4, \quad \text{so} \quad s_1 = 1$$

$$p_2 = 4, \quad 4 \cdot 7 = 1 \pmod 9, \quad \text{so} \quad s_2 = 7$$

Solution:

$$x = a_1 p_1 s_1 + a_2 p_2 s_2 = 18 + 196 = 214 = 34 \pmod{36}. \quad \square$$

Example. Solve

$$\begin{aligned} x &= 3 \pmod 4 \\ x &= 1 \pmod 5 \\ x &= 2 \pmod 3 \end{aligned}.$$

The moduli are pairwise relatively prime, so there is a unique solution mod 60. This time, I'll solve the system using an iterative method.

$$x = 3 \pmod 4, \quad \text{so} \quad x = 3 + 4s.$$

But $x = 1 \pmod 5$, so

$$\begin{aligned} 3 + 4s &= 1 \pmod 5 \\ 4s &= 3 \pmod 5 \\ 4 \cdot 4s &= 4 \cdot 3 \pmod 5 \\ s &= 2 \pmod 5 \\ s &= 2 + 5t \end{aligned}$$

Hence,

$$x = 3 + 4s = 3 + 4(2 + 5t) = 11 + 20t.$$

Finally, $x = 2 \pmod 3$, so

$$\begin{aligned} 11 + 20t &= 2 \pmod 3 \\ 20t &= -9 = 0 \pmod 3 \\ 2t &= 0 \pmod 3 \\ 2 \cdot 2t &= 2 \cdot 2 \pmod 3 \\ t &= 0 \pmod 3 \end{aligned}$$

Hence, $t = 3u$.
Now put everything back:

$$x = 11 + 20t = 11 + 20(3u) = 11 + 60u, \quad \text{or} \quad x = 11 \pmod{60}. \quad \square$$

Example. Calvin Butterball keeps pet meerkats in his backyard. If he divides them into 5 equal groups, 4 are left over. If he divides them into 8 equal groups, 6 are left over. If he divides them into 9 equal groups, 8 are left over. What is the smallest number of meerkats that Calvin could have?

Let x be the number of meerkats. Then

$$\begin{aligned} x &= 4 \pmod 5 \\ x &= 6 \pmod 8 \\ x &= 8 \pmod 9 \end{aligned}$$

From $x = 4 \pmod 5$, I get $x = 4 + 5a$. Plugging this into the second congruence, I get

$$\begin{aligned} 4 + 5a &= 6 \pmod 8 \\ 5a &= 2 \pmod 8 \\ 5 \cdot 5a &= 5 \cdot 2 \pmod 8 \\ 25a &= 10 \pmod 8 \\ a &= 2 \pmod 8 \end{aligned}$$

Hence, $a = 2 + 8b$. Plugging this into $x = 4 + 5a$ gives

$$x = 4 + 5(2 + 8b) = 14 + 40b.$$

Plugging this into the third congruence, I get

$$\begin{aligned} 14 + 40b &= 8 \pmod 9 \\ 40b &= -6 \pmod 9 \\ 4b &= 3 \pmod 9 \\ 7 \cdot 4b &= 7 \cdot 3 \pmod 9 \\ 28b &= 21 \pmod 9 \\ b &= 3 \pmod 9 \end{aligned}$$

Hence, $b = 3 + 9c$. Plugging this into $x = 14 + 40b$ gives

$$x = 14 + 40(3 + 9c) = 134 + 360c.$$

The smallest positive value of x is obtained by setting $c = 0$, which gives $x = 134$. $\square$

You can sometimes solve a system even if the moduli aren't relatively prime; the criteria are similar to those for solving system of linear Diophantine equations.

Theorem. Consider the system

$$\begin{aligned} x &= a_1 \pmod{m_1} \\ x &= a_2 \pmod{m_2} \end{aligned}.$$

(a) If $(m_1, m_2) \not| a_1 - a_2$, there are no solutions.

(b) If $(m_1, m_2) \mid a_1 - a_2$, there is a unique solution mod $[m_1, m_2]$.

Note that if $(m_1, m_2) = 1$, case (b) automatically holds, and $[m_1, m_2] = m_1 m_2$ — i.e. I get the Chinese Remainder Theorem for $n = 2$.

Proof. (a) I'll prove the contrapositive. Suppose x is a solution to the system of congruences, so

$$x = a_1 \pmod{m_1} \quad \text{and} \quad x = a_2 \pmod{m_2}.$$

The first congruence gives $x - a_1 = 0 \pmod{m_1}$, so $m_1 \mid x - a_1$. Similarly, $m_2 \mid x - a_2$. But $(m_1, m_2) \mid m_1$ and $(m_1, m_2) \mid m_2$, so

$$(m_1, m_2) \mid x - a_1 \quad \text{and} \quad (m_1, m_2) \mid x - a_2.$$

Therefore,

$$(m_1, m_2) \mid (x - a_2) - (x - a_1) = a_1 - a_2.$$

This proves the contrapositive of the assertion, so (a) is true.

(b) First, suppose that if x and y are solutions to the system.

$$x = a_1 \pmod{m_1} \quad \text{and} \quad y = a_1 \pmod{m_1} \quad \text{give} \quad x - y = 0 \pmod{m_1}.$$

Thus, $m_1 \mid x - y$. Similarly, $m_2 \mid x - y$. Since $x - y$ is a multiple of m_1 and m_2, it is a multiple of $[m_1, m_2]$. Thus,

$$x - y = 0 \pmod{[m_1, m_2]}, \quad \text{so} \quad x = y \pmod{[m_1, m_2]}.$$

Thus, any two solutions are congruent mod $[m_1, m_2]$.

Now suppose $(m_1, m_2) \mid a_1 - a_2$, so $a_1 - a_2 = k(m_1.m_2)$ for some $k \in \mathbb{Z}$. Note that

$$\left(\frac{m_1}{(m_1, m_2)}, \frac{m_2}{(m_1, m_2)} \right) = 1.$$

It follows that $\dfrac{m_1}{(m_1, m_2)}$ is invertible mod $\dfrac{m_2}{(m_1, m_2)}$, so there is an integer p such that

$$p \frac{m_1}{(m_1, m_2)} = 1 \pmod{\frac{m_2}{(m_1, m_2)}}.$$

I claim that the following is a solution to the system for all $t \in \mathbb{Z}$:

$$x = a_1 - pkm_1 + t[m_1, m_2].$$

You can obtain this "guess" by working backwards from the system assuming there is a solution, and solving the congruences by basic algebra. I will omit the details.

First, since $m_1 \mid [m_1, m_2]$,

$$x = a_1 - pkm_1 + t[m_1, m_2] = a_1 \pmod{m_1}.$$

This shows that the proposed solution satisfies the first congruence.

Next. I need to reduce $x = a_1 - pkm_1 + t[m_1, m_2] \bmod m_2$ and show that I get a_2. I'll need the following facts. First, since $a_1 - a_2 = k(m_1.m_2)$, we have $a_1 = a_2 + k(m_1, m_2)$.

Second, since $p\dfrac{m_1}{(m_1, m_2)} = 1 \pmod{\dfrac{m_2}{(m_1, m_2)}}$, we have

$$1 - p\frac{m_1}{(m_1, m_2)} = j\frac{m_2}{(m_1, m_2)} \quad \text{for some} \quad j \in \mathbb{Z}.$$

Hence,

$$x = a_1 - pkm_1 + t[m_1, m_2] = a_2 + k(m_1, m_2) - pkm_1 + t[m_1, m_2] =$$

$$a_2 + k(m_1, m_2) - pkm_1 + t[m_1, m_2] = a_2 + k(m_1, m_2)\left(1 - p\frac{m_1}{(m_1, m_2)}\right) + t[m_1, m_2] =$$

$$a_2 + k(m_1, m_2) \cdot j\frac{m_2}{(m_1, m_2)} + t[m_1, m_2] = a_2 + kjm_2 + t[m_1, m_2] = a_2 \pmod{m_2}.$$

This shows that $x = a_1 - pkm_1 + t[m_1, m_2]$ solves the congruences for all $t \in \mathbb{Z}$ — and so $x = a_1 - pkm_1$ is a solution mod $[m_1, m_2]$. Our initial observation shows that this is the only solution mod $[m_1, m_2]$. □

Let's look at an example to show how this works. Suppose we have the system of congruences

$$x = 21 \pmod{24}$$
$$x = 1 \pmod{28}$$

We have $a_1 = 21$, $a_2 = 1$, $m_1 = 24$, and $m_2 = 28$. Since $(24, 28) = 4 \mid 21 - 1$, the condition for a solution is satisfied.

First, $k = \dfrac{a_1 - a_2}{(m_1, m_2)} = \dfrac{20}{4} = 5$.

Next,

$$\frac{m_1}{(m_1, m_2)} = \frac{24}{4} = 6 \quad \text{and} \quad \frac{m_2}{(m_1, m_2)} = \frac{28}{4} = 7.$$

The multiplicative inverse of 6 mod 7 is $p = 6$. (You can find this by trial and error, or using the Extended Euclidean Algorithm.) A solution mod $[m_1, m_2] = [24, 28] = 168$ is

$$x = a_1 - pkm_1 = 21 - 6 \cdot 5 \cdot 24 = -899 = 141 \pmod{168}.$$

You can check that 141 solves the original congruences.

Example. Solve

$$x = 5 \pmod{12}$$
$$x = 11 \pmod{18}.$$

Since $(12, 18) = 6 \mid 11 - 5$, there is a unique solution mod $[12, 18] = 36$. I'll use the iterative method to find the solution.

$$x = 5 \pmod{12}, \quad \text{so} \quad x = 5 + 12s.$$

Since $x = 11 \pmod{18}$,

$$5 + 12s = 11 \pmod{18}$$
$$12s = 6 \pmod{18}$$

Now I use my rule for "dividing" congruences: 6 divides both 12 and 6, and $(6, 18) = 6$, so I can divide through by 6:

$$2s = 1 \pmod{3}.$$

Multiply by 2, and convert the congruence to an equation:

$$s = 2 \pmod{3}, \quad s = 2 + 3t.$$

Plug back in:

$$x = 5 + 12s = 5 + 12(2 + 3t) = 29 + 36t$$
$$x = 29 \pmod{36}$$

□

©2022 by Bruce Ikenaga