Chinese Remainder Theorem and Systems of Congruences

Brian Zhang

primeri.org

Contents

§1 Review

In our Modular Arithmetic I handout, we went over modular linear congruences. For those of you not familiar with these, it is recommended that you go back and read that handout. Just for review and for convenience, we'll redefine them here.

§1.1 "Re"-definitions

Linear Congruence

A **Linear Congruence** is a special kind of congruence, where

$$ax + b \equiv c \pmod{m}$$

and we want to solve for x.

Note that these are very similar to linear equations, but with a congruence sign instead of an equals sign. However, unlike linear equations not all linear congruences have solutions. For example, the congruence $2x \equiv 5 \pmod{8}$ does not have any solutions, since it is impossible for an even number to be congruent to an odd number. We can guarantee that there is a solution when a is relatively prime to m. If they are not relatively prime, and $\gcd(a, m) = d$, then:

- There will be a solution when d divides $b - c$.
- Otherwise, there will not be solutions.

When solving linear congruences or systems of them, you may find modular inverses useful.

Modular Inverses

A **modular inverse** of an integer b modulo m is an integer b^{-1} such that

$$b \cdot b^{-1} \equiv 1 \pmod{m}$$

More simply, we refer to b^{-1} as an **inverse**.

However, b^{-1} modulo m does not exist when $\gcd(b, m) > 1$. Finally, here is an example taken from the Modular Arithmetic handout for review.

Example 1.3

Find all solutions to $48x - 115 \equiv 291 \pmod{13}$.

Solution. We can first isolate the variable, by adding 115 to both sides of the congruence:

$$48x \equiv 406 \pmod{13}$$

Note that $48 \equiv 9 \pmod{13}$, and $406 \equiv 3 \pmod{13}$, so

$$9x \equiv 3 \pmod{13}$$

Since $9^{-1} \equiv 3 \pmod{13}$, then we can multiply both sides by 9^{-1} and get

$$x \equiv 3 \cdot 9^{-1} \equiv 3 \cdot 3 \equiv 9 \pmod{13}$$

so $\boxed{x \equiv 9 \pmod{13}}$ is our solution. □

§2 Theory

The Chinese Remainder Theorem is a powerful tool that aids us in solving congruences. It basically tells us if our congruences are solvable or not.

§2.1 The Chinese Remainder Theorem

Just like solving linear congruences is similar to solving linear equations, solving systems of congruences is similar to solving systems of equations. The following theorem, the Chinese Remainder Theorem, guarantees that we will have a solution when solving systems of congruences with the following properties.

Theorem 2.1 (Chinese Remainder Theorem)
Let $m_1, m_2, \ldots m_n$ be pairwise relatively prime positive integers, and $M = m_1 m_2 \ldots m_n$. For any integers $y_1, y_2, \ldots y_n$, there exists an integer x such that

$$\begin{aligned} x &\equiv y_1 \pmod{m_1}, \\ x &\equiv y_2 \pmod{m_2}, \\ x &\equiv y_3 \pmod{m_3}, \\ &\vdots \\ x &\equiv y_n \pmod{m_n} \end{aligned}$$

and x is unique modulo M.

§2.2 Actually Solving

However, knowing that a solution exists is very different from actually solving the system of congruences. We're going to go over a number of examples on how we deal with these systems.

Example 2.2
Find all solutions to the system of linear congruences

$$\begin{aligned} n &\equiv 1 \pmod{2} \\ n &\equiv 3 \pmod{5} \end{aligned}$$

Solution. We can start by writing what we are given about n in the form of equations:

$$\begin{aligned} n &= 2a + 1 \\ n &= 5b + 1 \end{aligned}$$

for integers a and b. We can combine these two equations to get the relation

$$5b + 3 = 2a + 1$$

In order to find more out about the possible values of a and b individually, we try to isolate either variable. By looking at each side of the equation in modulo 2 and modulo 5, we can extract some nontrivial information. First, we do modulo 2. By taking both sides of the equation modulo 2 and after simplification, we get

$$b + 1 \equiv 1 \pmod{2} \Rightarrow b \equiv 0 \pmod{2}$$

This means that we can write b as $2c$ for some integer c. Now, we rewrite what we know about n in terms of c:

$$n = 5b + 3 = 5(2c) + 3 = 10c + 3$$

Thus, $n \equiv 3 \pmod{10}$. It is easy to check that this curve of solutions does work, so we are done. □

Note how the modulo of the answer is equivalent to the product of the modulos of the two equations we are given.

Example 2.3
Find all solutions to the system of linear congruences

$$x \equiv 1 \pmod{3}$$
$$x \equiv 2 \pmod{4}$$

Solution. From the system of congruences, we have

$$x = 3a + 1 = 4b + 2$$

for integers a and b. Now, we look at the equation $3a + 1 = 4b + 2$ in modulo 3:

$$1 \equiv b + 2 \pmod{3} \Rightarrow b \equiv 2 \pmod{3}$$

This means that $b = 3c + 2$ for some integer c. Thus, we have

$$x = 4b + 2 = 4(3c + 2) + 2 = 12c + 10$$

so $x \equiv 10 \pmod{12}$ is the solution to the system of congruences. □

Here is an example of when a system of congruences does not have a solution.

Example 2.4
Find all solutions to the system of linear congruences

$$a \equiv 2 \pmod{6}$$
$$a \equiv 3 \pmod{9}$$

Solution. According to they system of linear congruences,

$$a = 6x + 2 = 9y + 3$$

By taking modulo 6, we get

$$2 \equiv 3y + 3 \pmod{6} \Rightarrow 3y \equiv 5 \pmod{6}$$

which means that $3y = 6z + 5$ for some integer z. Now, taking this equation modulo 3 we get

$$0 \equiv 2 \pmod{3}$$

This is clearly false, so there are no solutions for z. Similarly, there are no solutions for a. □

Now, we take a look at solving multiple linear congruences.

Example 2.5
Find all solutions to the system of linear congruences

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

Solution. What we are going to do for three systems of congruences is solve it in steps. We first find the solution to 2 of them at once, and then find the integers that satisfy the solution to 2 of them and the third congruence. We already determined in Example 6 the solution to congruences 1 and 2, so all we need to do is to find the solution to the congruences $x \equiv 10 \pmod{12}$ and $x \equiv 4 \pmod 5$. But this is just a system of 2 congruences, which we know how to solve!

We get that

$$x = 12a + 10 = 5b + 4$$

By taking modulo 5, we get

$$2a \equiv 4 \pmod 5 \Rightarrow a \equiv 2 \pmod 5$$

which means that $a = 5c + 2$ for some integer c. Thus,

$$x = 12a + 10 = 12(5c + 2) + 10 = 60c + 34$$

so $x \equiv 34 \pmod{60}$ is our solution. □

Example 2.6
Find all solutions to the system of linear congruences

$$\begin{aligned} x &\equiv 1 \pmod 3 \\ x &\equiv 1 \pmod 4 \\ x &\equiv 1 \pmod 5 \end{aligned}$$

Solution. This example is very similar to the previous example, and we could just do something similar to what we did earlier. However, there is something much smarter we can do.

Notice that for each of the congruences, x is congruent to 1 in some modulo. This means that if we multiply the 3 numbers, $3 \cdot 4 \cdot 5 = 60$, x will still be congruent to 1 in modulo 60. And that's it! The only solution is $x \equiv 1 \pmod{60}$. □

Now, time for a word problem.

Example 2.7
Find all numbers less than 100 such that they leave a remainder of 1 when divided by 3 and a remainder of 2 when divided by 4.

Solution. We want to convert the words of this problem into mathematical equations. Lets first take a look at the condition that n has a remainder of 1 when divided by 3. This just means that the number n is congruent to 1 mod 3. Similarly, n is also congruent to 2 mod 4. So we just want to solve

$$\begin{aligned} x &\equiv 1 \pmod 3 \\ x &\equiv 2 \pmod 4 \end{aligned}$$

which is the system of congruences in Example 6. Thus, $x \equiv 10 \pmod{12}$, so the numbers that work are $\boxed{10, 22, 34, 46, 58, 70, 82, 94}$. □

§3 Exercises

Exercise 3.1. Solve the system of linear congruences:

$$\begin{aligned} x &\equiv 3 \pmod{8} \\ x &\equiv 5 \pmod{9} \end{aligned}$$

Exercise 3.2. Solve the system of linear congruences:

$$\begin{aligned} 3x &\equiv 2 \pmod{4} \\ 2x &\equiv 4 \pmod{7} \end{aligned}$$

Hint: If you're stuck, try using the techniques taught in the modular arithmetic handout to simplify the congruences into something you know how to work with.

Exercise 3.3. Find the largest integer less than 400 that leaves a remainder of 2 when divided by 3 and a remainder of 4 when divided by 7.

Exercise 3.4. How many integers between 1 and 100 leave a remainder of 2 when divided by 4 and also a remainder of 4 when divided by 5?

Exercise 3.5 (MathCounts). A marching band has more than 100 members, but fewer than 200 members. When they line up in rows of 4 there is one extra person; when they line up in rows of 5 there are two extra people; and when they line up in rows of 7 there are three extra people. How many people are in this marching band?

Exercise 3.6. A natural number leaves a remainder of 7 when divided by 11 and a remainder of 10 when divided by 2. Find the remainder when the number is divided by 66.

Exercise 3.7 (AHSME 1993/18). Adam and Ben start their new jobs on the same day. Adam's schedule is 3 workdays followed by 1 rest day. Ben's schedule is 7 workdays followed by 3 rest days. On how many of their first 1000 days do both have rest days on the same day?

Exercise 3.8. A band of 17 pirates stole a chest of gold coins. When they tried to divide the fortune into equal portions, 3 coins remained. In the ensuing brawl over who should get the extra coins, one pirate was forced to walk the plank. The wealth was redistributed, but this time an equal division left 10 coins. Again, an argument broke out in which another pirate was forced to walk the plank. But now the total amount of money was evenly distributed among the remaining pirates. What was the least number of coins that could have been stolen?

Exercise 3.9. How many four-digit integers either leave a remainder of 2 when divided by 7, or a remainder of 4 when divided by 5, but not both?