34 The Chinese Remainder Theorem

In this section, we investigate how to solve equations that involve modular equivalences.

Solving One Equation

We start with an easy example.

Example 34.1
Solve the equation

$$x \equiv 4 \pmod{11}.$$

Solution. This asks for all integers x so that $x - 4$ is a multiple of 11 (i.e., $x - 4 = 11k$ for some integer k). We can rewrite this as $x = 4 + 11k$ where k can be any integer.
So the solutions are: $\ldots, -18, -7, 4, 15, 26, \ldots$.

Let's now work on a more complicated example. We solve the following.

Example 34.2
Solve the equation

$$3x \equiv 4 \pmod{11}. \tag{28}$$

Suppose, just for a moment, that we had a solution x_0 to the equation $3x \equiv 4\,(11)$. Now consider the integer $x_1 = x_0 + 11$. If we substitute x_1 for x in Equation (28), we get

$$3x_1 = 3(x_0 + 11) = 3x_0 + 33 \equiv 3x_0 \equiv 4 \pmod{11}$$

so x_1 is also a solution. Thus, if we add or subtract any multiple of 11 to a solution to Equation (28), we obtain another solution to Equation (28). So if there is a solution, then there is a solution in $\{0, 1, 2, \ldots, 10\} = \mathbb{Z}_{11}$. Once we find all the solutions in $\mathbb{Z}_{10}$, we have found all solutions to the equation.

Now there are only 11 possible values of x we need to try, and it might be simplest just to try all the possibilities to find the answer. However, we want to generalize this method to problems where the modulus is a great deal larger than 11.

We seek a number $x \in \mathbb{Z}_{11}$ for which $3x \equiv 4\ (11)$. But notice:

$$3x \equiv 4\ (11) \quad \Longleftrightarrow \quad (3x) \bmod 11 = 4 \quad \Longleftrightarrow \quad 3 \otimes x = 4$$

where $\otimes$ is modular multiplication in $\mathbb{Z}_{11}$. How do we solve the equation $3 \otimes x = 4$ in $\mathbb{Z}_{11}$? We would like to divide both sides by 3. Do we get $x = \frac{4}{3}$? Nonsense! That is not how we divide in $\mathbb{Z}_{11}$. We multiply both sides of $3 \otimes x = 4$ by 3^{-1}. Now by the methods of Section 33, we can calculate $3^{-1} = 4$, and so

$$3 \otimes x = 4 \quad \Rightarrow \quad 4 \otimes 3 \otimes x = 4 \otimes 4 \quad \Rightarrow \quad 1 \otimes x = 5 \quad \Rightarrow \quad x = 5$$

(because $12 \bmod 11 = 1$ and $16 \bmod 11 = 5$).

Let's check this answer in Equation (28). We substitute $x = 5$ and we calculate:

$$3x = 15 \equiv 4 \pmod{11}$$

and so 5 is a solution. Furthermore, there are no other solutions in $\mathbb{Z}_{11}$. If $x' \in \mathbb{Z}_{11}$ were another solution, we would have $3 \otimes x' = 4$, and when we $\otimes$ both sides by 4, we would find $x' = 5$.

Although 5 is the only solution in $\mathbb{Z}_{11}$, it is not the only solution to Equation (28). If we add any multiple of 11 to 5, we get another solution. The full set of solutions is $\{5 + 11k : k \in \mathbb{Z}\} = \{\ldots, -17, -6, 5, 16, 27, \ldots\}$. This completes the solution to Example 34.2.

We summarize what we have learned in the following result.

Proposition 34.3

Let $a, b, n \in \mathbb{Z}$ with $n > 0$. Suppose a and n are relatively prime and consider the equation:

$$ax \equiv b \pmod{n}.$$

The set of solutions to this equation is

$$\{x_0 + kn : k \in \mathbb{Z}\}$$

where $x_0 = a_0^{-1} \otimes b_0$, $a_0 = a \bmod n$, $b_0 = b \bmod n$, and $\otimes$ is modular multiplication in $\mathbb{Z}_n$. The integer x_0 is the only solution to this equation in $\mathbb{Z}_n$.

We have essentially done the proof by solving Equation (28). Please write out the proof yourself using our solution to Equation (28) as a guide.

It is not hard to extend Proposition 34.3 to solve equations of the form

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

where a and n are relatively prime.

Solving Two Equations

Now we solve a pair of congruence equations in different moduli. The type of problem we solve is

$$\begin{aligned} x &\equiv a \pmod{m} \quad \text{and} \\ x &\equiv b \pmod{n}. \end{aligned}$$

Let's work out the solution to the following problem.

Example 34.4

Solve the pair of equations:

$$\begin{aligned} x &\equiv 1 \pmod{7} \quad \text{and} \\ x &\equiv 4 \pmod{11}. \end{aligned}$$

In other words, we want to find all integers x that satisfy both these equations. Let's begin with the first equation. Since $x \equiv 1\ (7)$, we can write

$$x = 1 + 7k$$

for some integer k. We can substitute $1 + 7k$ for x in the second equation: $x \equiv 4\,(11)$. This gives

$$1 + 7k \equiv 4 \pmod{11} \quad \Rightarrow \quad 7k \equiv 3 \pmod{11}.$$

The problem now reduces to a single equation in k. We apply Proposition 34.3. To solve this equation, we need to $\otimes$ both sides by 7^{-1} working in $\mathbb{Z}_{11}$. In $\mathbb{Z}_{11}$ we find that $7^{-1} = 8$. We calculate in $\mathbb{Z}_{11}$:

We can check that $7^{-1} = 8$ by calculating $7 \otimes 8 = (7 \cdot 8) \bmod 11 = 56 \bmod 11 = 1$.

$$7 \otimes k = 3 \quad \Rightarrow \quad 8 \otimes 7 \otimes k = 8 \otimes 3 \quad \Rightarrow \quad k = 2.$$

Furthermore, if we increase or decrease $k = 2$ by any multiple of 11, we again have a solution to $1 + 7k \equiv 4\,(11)$.

We are nearly done. Let's write down what we have. We know that we want all values of x with

$$x = 1 + 7k$$

and k can be any integer of the form

$$k = 2 + 11j$$

where j is any integer. Combining these two, we have

$$x = 1 + 7k = 1 + 7(2 + 11j) = 15 + 77j \qquad (\forall j \in \mathbb{Z}).$$

In other words, the solution set to the equations in Example 34.4 is $\{x \in \mathbb{Z} : x \equiv 15\ (77)\}$.

To check that this is correct, notice that

$$15 \equiv 1 \pmod{7} \qquad \text{and} \qquad 15 \equiv 4 \pmod{11}.$$

Furthermore, if x is increased or decreased by any multiple of 77, both equations remain valid because 77 is a multiple of both 7 and 11.

Theorem 34.5 (Chinese Remainder)

Let a, b, m, n be integers with m and n positive and relatively prime. There is a unique integer x_0 with $0 \le x_0 < mn$ which solves the pair of equations

$$\begin{aligned} x &\equiv a \pmod{m} \quad \text{and} \\ x &\equiv b \pmod{n}. \end{aligned}$$

Furthermore, every solution to these equations differs from x_0 by a multiple of mn.

We saw all the steps to prove the Chinese Remainder Theorem when we solved the system in Example 34.4. The general proof follows the method of that example.

Proof. From the equation $x \equiv a\ (m)$, we know that $x = a + km$ where $k \in \mathbb{Z}$. We substitute this into the second equation $x \equiv b\ (n)$ to get

$$a + km \equiv b\ (n) \quad \Rightarrow \quad km \equiv b - a\ (n)$$

and we want to solve this for k. Note that adding or subtracting a multiple of n to $b - a$ or to m does not change this equation. So we let

$$\begin{aligned} m' &= m \bmod n \quad \text{and} \\ c &= (b - a) \bmod n. \end{aligned}$$

Since m and n are relatively prime, so are m' and n (see Exercise 32.12). Thus solving $km \equiv b - a\ (n)$ is equivalent to solving $km' \equiv c\ (n)$. To find a solution in $\mathbb{Z}_n$, we solve, in $\mathbb{Z}_n$,

$$k \otimes m' = c.$$

Since m' is relatively prime to n, we can $\otimes$ both sides by its reciprocal to get

$$k = (m')^{-1} \otimes c.$$

Let $d = (m')^{-1} \otimes c$, so the values for k that we want are $k = d + jn$ for all integers j.

Finally, we substitute $k = d + jn$ into $x = a + km$ to get

$$x = a + km = a + (d + jn)m = a + dm + jnm$$

where $j \in \mathbb{Z}$ is arbitrary. We have shown that the original system of two equations reduces to the single equation

$$x \equiv a + dm \pmod{mn}$$

and the conclusions follow. ☺

Example 34.6

Suppose we want to solve a system of three equations. For example, solve for all x:

$$\begin{aligned} x &\equiv 3 \pmod{9}, \\ x &\equiv 5 \pmod{10}, \quad \text{and} \\ x &\equiv 2 \pmod{11}. \end{aligned}$$

Solution: We can solve the first two equations by the usual method

$$\left.\begin{aligned} x &\equiv 3\ (9) \\ x &\equiv 5\ (10) \end{aligned}\right\} \quad \Rightarrow \quad x \equiv 75\ (90).$$

Now we combine this result with the last equation and again solve by the usual method.

$$\left.\begin{aligned} x &\equiv 75\ (90) \\ x &\equiv 2\ (11) \end{aligned}\right\} \quad \Rightarrow \quad x \equiv 255\ (990).$$

Recap

We investigated how to solve equations of the form $ax + b \equiv c\ (n)$ as well as systems of equations of the form $x \equiv a\ (m)$ and $x \equiv b\ (n)$ where m and n are relatively prime.

EXERCISES

1. Solve the following for all integers x.
   (a) $3x \equiv 17$ (mod 20).
   (b) $2x + 5 \equiv 7$ (mod 15).
   (c) $10 - 3x \equiv 2$ (mod 23).
   (d) $100x \equiv 74$ (mod 127).
2. Solve the following systems of equations.
   (a) $x \equiv 4\ (5)$ and $x \equiv 7\ (11)$.
   (b) $x \equiv 34\ (100)$ and $x \equiv -1\ (51)$.
   (c) $x \equiv 3\ (7)$, $x \equiv 0\ (4)$, and $x \equiv 8\ (25)$.
   (d) $3x \equiv 8\ (10)$ and $2x + 4 \equiv 9\ (11)$.
3. Explain why it is important for a and n to be relatively prime in the equation $ax \equiv b\ (n)$. Specifically, you should
   (a) Create an equation of the form $ax \equiv b\ (n)$ that has no solutions.
   (b) Create an equation of the form $ax \equiv b\ (n)$ that has more than one solution in $\mathbb{Z}_n$.
4. For the pair of equations $x \equiv a\ (m)$ and $x \equiv b\ (n)$, explain why it is important that m and n be relatively prime. Where in the proof of Theorem 34.5 did we use this fact?

   Give an example of a pair of equations $x \equiv a\ (m)$ and $x \equiv b\ (n)$ that has no solution.