The Chinese Remainder Theorem
and
Back Substitution

sjLin

August 25, 2021

Systems of linear congruences arise in many contexts. For example, as we will see later, they are the basis for a method that can be used to perform arithmetic with large integers. Such systems can even be found as word puzzles in the writings of ancient Chinese and Hindu mathematicians, such as that given in Example 4.

Example 4

In the first century, the Chinese mathematician Sun-Tsu asked:

There are certain things whose number is unknown. When divided by 3, the remainder is 2; when divided by 5, the remainder is 3; and when divided by 7, the remainder is 2. What will be the number of things?

This puzzle can be translated into the following question: What are the solutions of the systems of congruences

$$x \equiv 2 \pmod 3$$

$$x \equiv 3 \pmod 5$$

$$x \equiv 2 \pmod 7$$

We will solve this system, and with it Sun-Tsu's puzzle, later in this section.

#

The Chinese remainder theorem, named after the Chinese heritage of problems involving systems of linear congruences, states that when the moduli of a system of linear congruences are pairwise relatively prime, there is a unique solution of the system modulo the product of the moduli.

Theorem 2 The Chinese Remainder Theorem

Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime positive integers greater than one and $a_1, a_2, \ldots, a_n$ arbitrary integers.. Then the system

$$x \equiv a_1 \pmod m_1$$

$$x \equiv a_2 \pmod m_2$$

$$\ldots$$

$$x \equiv a_n \pmod m_n$$

has a unique solution modulo $m = m_1 m_2 \ldots m_n$. (That is, there is a solution x with $0 \leq x < m$, and all other solutions are congruent modulo m to this solution.)

Proof:

To establish this theorem, we need to show that a solution exists and that it is unique modulo m. We will show that a solution exists by describing a way to construct this solution; showing that the solution is unique modulo m is Exercise 30.

To construct a simultaneous solution, first let

$$M_k = m/m_k$$

for $k = 1, 2, \ldots, n$. That is, M_k is the product of the moduli except for m_k. Because m_i and m_k have no common factors greater than 1 when $i \neq k$, it follows that $\gcd(m_k, M_k) = 1$. Consequently, by Theorem 1, we know that there is an integer y_k, an inverse of M_k modulo m_k, such that

$$M_k y_k \equiv 1 \pmod{m_k}.$$

To construct a simultaneou solution, form the sum

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_n M_n y_n.$$

$$M_k \times y_i \equiv 1 \pmod{m_k}$$

Using Eulidean Algorithm to find y_i

$$M_k = a m_k + b$$

$$\cdots \rightarrow$$

$$1 = M_k \times y_i + s \times m_k$$

$$M_i y_i \equiv 1 \pmod{m_k}$$

We will now show that x is a simultaneous solution. First, note that because $M_j \equiv 0 \pmod m_k$ whenever $j \neq k$, all terms except the kth term in this sum are congruent to 0 modulo m_k. Because $M_k y_k \equiv 1 \pmod m_k$ we see that

$$x \equiv a_k M_k y_k \equiv a_k \pmod m_k$$

for $k = 1, 2, \ldots, n$. We have shown that x is a simultaneous solution to the n congruences.

#

Example 5 illustrates how to use the construction given in our proof of the Chinese reminader theorem to solve a system of ocngruences. We will solve the system given in Example 4, arising in Sun-Tsu's puzzle.

Example 5

$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$
$$x \equiv 2 \pmod 7$$

To solve the system of congruences in Example 4, first let $m = 3 \cdot 5 \cdot 7 = 105$, $M_1 = m/3 = 35$, $M_2 = m/5 = 21$, and $M_3 = m/7 = 15$. We see that 2 is an inverse of $M_1 = 35$ modulo 3, because $35 \cdot 2 \equiv 2 \cdot 2 \equiv 1 \pmod 3$;
1 is an inverse of $M_2 = 21$ modulo 5, because $21 \equiv 1 \pmod 5$;
and 1 is an inverse of $M_3 = 15 \pmod 7$, because $15 \equiv 1 \pmod 7$. The solutions to this system are those x such that

$$x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1$$
$$= 233 \equiv 23 \pmod{105}$$

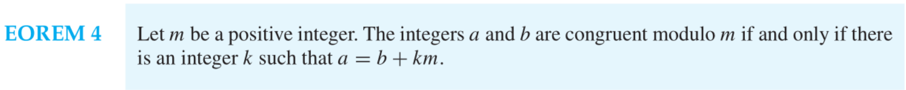
It follows that 23 is the smallest positive integer that is a simultaneous oslution. We conclude that 23 si the smallest positive integer that leaves a remainder of 2 when divided by 3, a remainder of 3 when divided by 5, and a remainder of 2 when divided by 7.

#

Although the construction in Theorem 2 provides a gerneral method for solving systems of linear congruences with pairwise relatively prime moduli, it can be easier to solve a system using a different method. Example 6 illustrates the use of a method known as back substitution.

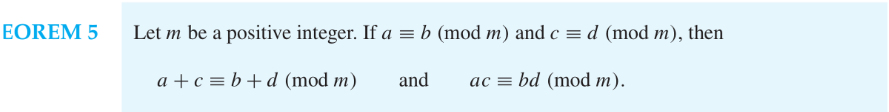
Example 6

Use the method of back substitution to find all integers x such that $x \equiv 1 \pmod 5$, $x \equiv 2 \pmod 6$, and $x \equiv 3 \pmod 7$.



EOREM 4

Let m be a positive integer. The integers a and b are congruent modulo m if and only if there is an integer k such that $a = b + km$.



EOREM 5

Let m be a positive integer. If $a \equiv b \pmod m$ and $c \equiv d \pmod m$, then

$$a + c \equiv b + d \pmod m \qquad \text{and} \qquad ac \equiv bd \pmod m.$$

Solution:

Solution: By Theorem 4 in Section 4.1, the first congruence can be rewritten as an equality, $x = 5t + 1$ where t is an integer. Substituting this expression for x into the second congruence tells us that

$$5t + 1 \equiv 2 \pmod{6},$$

which can be easily solved to show that $t \equiv 5 \pmod{6}$ (as the reader should verify). Using Theorem 4 in Section 4.1 again, we see that $t = 6u + 5$ where u is an integer. Substituting this expression for t back into the equation $x = 5t + 1$ tells us that $x = 5(6u + 5) + 1 = 30u + 26$. We insert this into the third equation to obtain

$$30u + 26 \equiv 3 \pmod{7}.$$

Solving this congruence tells us that $u \equiv 6 \pmod{7}$ (as the reader should verify). Hence, Theorem 4 in Section 4.1 tells us that $u = 7v + 6$ where v is an integer. Substituting this expression for u into the equation $x = 30u + 26$ tells us that $x = 30(7v + 6) + 26 = 210u + 206$. Translating this back into a congruence, we find the solution to the simultaneous congruences,

$$x \equiv 206 \pmod{210}.$$ ◀