The Chinese Remainder Theorem

Marc Cahay

Department of Electrical and Computer Engineering
University of Cincinnati

June 18, 2024

Basics

Although the Chinese Remainder Theorem gives us the tools to solve several congruences of the form $ax \equiv b \pmod{m}$, let's make sure we know how to do the most basic step: solving only one such congruence.

One Congruence

Examples

Example 1: Find x such that $3x \equiv 7 \pmod{10}$.
You can use Euclid's algorithm or Euler's totient function to find that the inverse of 3 modulo 10 is 7. Multiplying both sides of the congruence by this number, you get

$$3 \cdot 7 \cdot x \equiv 49 \pmod{10} \Longleftrightarrow x \equiv 9 \pmod{10}.$$

Example 2: Find x such that $3x \equiv 6 \pmod{12}$.
3 does not have a multiplicative inverse modulo 12 as $\gcd(3, 12) = 3$. We can use Euclid's algorithm on the equation $3x - 12k = 6 \Leftrightarrow x - 2 = 4k$ (by the definition of modular arithmetic) to receive $x \equiv 2 \pmod{4}$.

Exception

Example 3: Find x such that $3x \equiv 7 \pmod{12}$.
This isn't possible. Rearranging this expression into the equation $3x - 7 = 12k \Leftrightarrow 3x - 12k = 7$, since $\gcd(3, 12)$ does not divide 7, there are no solutions (by Bezout's Lemma, proved on Euclid's Algorithm slides.)

A corollary of Bezout's Lemma can easily be inferred from these examples.

Corollary

There only exist solutions to the congruence $ax \equiv b \pmod{m}$, *where* $n \in \mathbb{N}$ *and* $a, b \in \mathbb{Z}$, *if and only if* $\gcd(a, m) \mid b$.

Two Equations

Let's try this with two equations.

Example 4: Find x if $2x \equiv 5 \pmod 7$ and $3x \equiv 4 \pmod 7$.
Let's tackle the first equation. 2 has a multiplicative inverse modulo 7: namely, 4, so $2 \cdot 4 \cdot x \equiv 6 \pmod 7 \Leftrightarrow x \equiv 6 \pmod 7 \Leftrightarrow x = 7k - 6$.