Elementary Number Theory : §6

Henry Slayer | University of California, Santa Cruz

The Chinese Remainder Theorem

Often, we will be faced with problems or situations in which it is helpful to break congruence down into a system of congruences. Conversely, it can be useful to assemble a single congruence that uniquely describes a system of smaller congruences. Our tool for doing so is the Chinese Remainder Theorem, which allows us to relate congruence across different modulii. Speaking loosely, if our modulus m can be decomposed into coprime factors, say d and e, every congruence modulo m is equivalent to a compound congruence $[a, b] \bmod [d, e]$. The bracket notation means *congruent to **a** modulo **d**, and **b** modulo **e**.* More formally, we can say the following

Theorem 1 (Chinese Remainder Theorem)**.** *If d and e are a pair of coprime numbers, then there exists a bijective correspondence between the set of pairs $[a, b]$, where $0 \leq a < d$, and $0 \leq b < e$, and the set of integers n for which $0 \leq n < de$.*
In other words, the pairs of residues $[a, b]\, mod\, [d, e]$ map uniquely to the residues $n\, mod\, (de)$.

Proof. The sets that we're working with are the same size. So, if we can find an injective map from the set of pairs $[a, b]$ to the set of integers from 0 to $de - 1$, we've found our bijection. So how do we map $n \mapsto [a, b]$? There's a natural choice.
Let $n \mapsto [a, b]$ be defined by the rule that $n \mapsto [a, b]$ if and only if $n \equiv [a, b] \bmod de$.
We need to show that this map is injective, so suppose that we have a pair of values $0 \leq m < de$ and $0 \leq n < de$, such that $n \equiv [a, b] \bmod de$ and $m \equiv [a, b] \bmod [d, e]$. Naturally, then, $n - m \equiv [0, 0] \bmod [d, e]$. In turn, this implies that $n - m$ is a multiple of both d and e. As d and e are coprime, this forces that $n - m$ is a multiple of the least common multiple of d and e. In this case, this means that $n - m$ is a multiple of de. Yet, both m and n are strictly less than de, so their difference $n - m$ is surely less than de. The only multiple of de less than de is 0, so $m - n = 0$, and $m = n$.
Having shown that the map is injective, the fact that our two sets (the set of pairs, and the set of residue classes modulo de) are the same size implies that the map is bijective.
As the map is bijective, this implies that every congruence modulo de corresponds to a unique congruence $[a, b] \bmod [d, e]$, **provided that d and e are coprime**. $\square$

Disassembling and Reassembling Congruence

The extreme utility of the Chinese Remainder Theorem is that it enables us to reduce complex congruences to systems of simpler congruences, and vice versa.

Example 1. *Break* $x \equiv 45 \, mod \, 56$ *into a system of simpler congruences.*

Breaking down congruence couldn't be simpler. All we need to do is find two (or more) co-prime factors of 56. 7 and 8 seem like a good choice. $45 \equiv 3 \, mod \, 7$*, and* $45 \equiv 5 \, mod \, 8$*, so* $45 \equiv [3, 5] \, mod \, [7, 8]$*. Brilliant.*

Example 2. *What is* x*, if...*
x *is no more than 100. Counting by 3, we have one left over.*
Counting by 22, we have three left over.
Counting by 7, we have 4 left over.

We'll start the problem, and leave the reader to finish it.
The statement of the problem implies that $x \equiv 1 \, mod \, 3$*,* $3 \, mod \, 22$*, and* $4 \, mod \, 7$*. Each one of these linear congruences is really hiding a linear diophantine equation, which gives us the following system of equations:*

$$x - 3y = 1$$
$$x - 22z = 3$$
$$x - 7w = 4$$

You do the rest! Hint: use the first two equations to come up with a congruence modulo 66. This can be translated back into the language of linear diophantine equations, and re-combined with the last equation to construct a congruence in terms of 462.

Example 3. *Find all solutions to* $x^2 \equiv 1 \, mod \, 21$*.*

By the CRT, we can decompose this into two congruences, $x^2 \equiv 1 \, mod \, 7$ *and* $x^2 \equiv 1 \, mod \, 3$*. Modulo 7, this means that we have two solutions:* $x \equiv 6$*, or* $x \equiv 1$*. Modulo 3, we also have two solutions,* $x \equiv 1$ *or* $x \equiv 2$*. Two options for each smaller congruence gives us four possible combinations:*

$$x \equiv [1, 1] \, mod \, [3, 7]$$
$$x \equiv [1, 6] \, mod \, [3, 7]$$
$$x \equiv [2, 1] \, mod \, [3, 7]$$
$$x \equiv [2, 6] \, mod \, [3, 7]$$

Respectively, these simpler congruences resolve to $x \equiv 1, \, 8, \, 13, \, 20 \, mod \, 21$*, which characterizes all solutions to* $x^2 \equiv 1 \, mod \, 21$*.*

The last example here characterizes a useful generalization. Solutions to the congruence $x^2 \equiv a \bmod de$ are in one-to-one correspondence with the pairs of solutions (u, v) to the congruences $u^2 \equiv a \bmod d$ and $v^2 \equiv a \bmod e$. In other words, a is a square mod de (meaning $a \equiv x^2$ for some $x \bmod de$) if and only if a is a square modulo d and modulo e. We'll dive into squares (the *quadratic residues*) a bit more further down the road.