Elementary Number Theory : §5

Henry Slayer | University of California, Santa Cruz

Congruence

Congruence is a way of thinking about the integers in a more relational, streamlined, and cyclic way. By fixing a *modulus*, we partition the integers into unique *residues*. The modulus is the reference point, which we pivot off of in terms of divisibility. Simply put, when we say that a is congruent to b modulo m, we're saying that $a - b$ is a multiple of m. Working with congruence lets us cut the integers down to size, and study their properties in a more relative way.

For example, the integers modulo 5 can be described with 5 representatives, the *residue classes* modulo 5. Modulo 5, every integer is congruent to either 0, 1, 2, 3, or 4. Loosely speaking, we can consider the representatives as all possible remainders upon division by the modulus. Hence, in the general case, when we consider the integers modulo m, often denoted $\mathbb{Z}/m$, we use the representative classes: 0, 1, 2, ... $n - 1$.

I remember that the first time I was introduced to congruence, it all felt very confusing. Was an integer still an integer modulo m? What was all of this business about *classes* and *unique systems of representatives*? In truth, they're all the same thing, and in practice, simple modular arithmetic is really just integer arithmetic, except we simplify based on remainders when dividing by the modulus. The richness of the modular worlds will become more apparent when we study quadratic residues and compound congruence. For now, however, we start with some simple definitions.

Definition 1. *Let a and b be integers. Then, a is congruent to b modulo m if $(a-b)$ is divisible by m. We denote this relationship by*

$$a \equiv b \, mod \, m$$

Equivalently, we can say

$$m \mid (a - b)$$

b is the remainder when a is divided by m

Or, $(a - b)$ is a multiple of m.

Well-Definedness of Modular Arithmetic

So, we map the integers to the m unique representatives $0, 1, \ldots m-1$ modulo m, which cycles through the integers like clockwork. However, before we can *do* anything with our new frame of reference, we need to be sure that it is well-defined. That is, we want to be sure that we can actually use residue classes as placeholders for the integers, without losing any information in the process.

Proposition 1. *Operations in modular arithmetic, taking a unique residue class as a distinct representative, are well-defined. In other words, if* $x \equiv \overline{x} \, mod m$, *and* $y \equiv \overline{y} \, mod m$, *then* $x + y \equiv \overline{x} + \overline{y} \, mod m$, *and* $xy \equiv \overline{xy} \, mod m$.

Proof. Suppose that $x \equiv \overline{x}$, and $y \equiv \overline{y}$, modulo m. Then, for integers j and k,

$$x = mj + \overline{x}, \quad y = mk + \overline{y}$$

So, combining terms, $x + y$ can be suggestively written as

$$x + y = \overline{x} + \overline{y} + m(j + k)$$

Which, modulo m, implies that $x + y \equiv \overline{x} + \overline{y} \bmod m$.
We task the reader with proving the multiplicative case, which is much of the same, requiring just a bit more algebraic re-arrangement. □

Properties of Modular Arithmetic

Modular arithmetic enjoys the following basic properties, among more:

(i) If $a \equiv b \bmod m$, $b \equiv a \bmod m$.

(ii) Suppose that $a \equiv b \bmod m$ and $c \equiv d \bmod m$. Then:
$a + c \equiv b + d \bmod m$
$ac \equiv bd \bmod m$

(iii) $ax \equiv ay \bmod m$ implies that $x \equiv y \bmod m$.

In brief, modular arithmetic operates in expected ways, and when the hurdle of shifting from integers-as-integers to integers-as-representatives is overcome, I've found the modular worlds to be quite delightful. Division, modulo m, isn't defined, but, as we'll find, the cyclic nature of modular systems affords a close enough substitute. (EXAMPLE?)

Linear Congruences

Linear congruences are congruences of the form

$$ax \equiv b \bmod m$$

for a given modulus m.As it turns out, these congruences are really only linear diophantine equations in disguise. For $ax \equiv b \bmod m$ is really saying that $ax - b = my$, for integers x and y, which is really just $ax - my = b$. This observation leads us to the following.

Proposition 2. *The congruence*

$$ax \equiv 1 \, mod \, m$$

has a solution if and only if $GCD\,(a, m) = 1$.

Proof. We can prove this simply by translating back and forth between the language of congruences, and the language of linear diophantine equations. Suppose $ax \equiv 1 \bmod m$. Then, $ax - 1 = my$, for some integer y. In turn, this implies that $ax - my = 1$. From previous sections, we know that this equation is solvable if and only if $GCD\,(a, m) = 1$.
Conversely, suppose that $GCD\,(a, m) = 1$. Then, for some choice of integers x and y, $ax + my = 1$. With just a bit of re-arrangement, we can write this as $ax - 1 = m(-y)$, which in turn demonstrates that $ax \equiv 1 \bmod m$. □

Now, if we happen to solve for x in a congruence like the one above, x is considered the *multiplicative inverse* of a, modulo m. Modular inverses are computationally useful, and bring us about as close as we can get to division in the modular world. By the proposition above, we can see that the divisibility relationship between a residue class a and the modulus determines if a will have a multiplicative inverse, or not. However, it is important to observe that inverses come in pairs (or a residue class can be its own inverse, as is always the case with 1).

Proposition 3. *Modulo m, any residue class a has a unique multiplicative inverse b if and only if* $GCD\,(a, m) = 1$. *Furthermore, this inverse is unique.*

Proof. The former part of the statement holds as a direct consequence of the previous proposition, but what of uniqueness? Suppose that an residue class a had two distinct representatives. That is, $ab \equiv ac \equiv 1 \bmod m$. Then,

$$c \equiv 1 \cdot c \equiv (ab) \cdot c \equiv (ac) \cdot b \equiv 1 \cdot b \equiv b$$

And, as $c \equiv b$, they are for all purposes the same residue class in our modular world. □

Solubility of Linear Diophantine Equations

The connections between linear diophantine equations and linear congruences run deep. In particular, modular arithmetic gives us a powerful tool for disproving the existence of solutions to linear diophantine equations.