Congruences and Modular Arithmetic

Ryan C. Daileda

Trinity University

Number Theory

Introduction

Modular arithmetic is the "arithmetic of remainders."

The somewhat surprising fact is that modular arithmetic obeys most of the same laws that ordinary arithmetic does.

This explains, for instance, homework exercise 1.1.4 on the associativity of remainders.

We will later see that because of this the set of equivalence classes under congruence modulo n can be given the structure of a *ring*.

Congruences

Definition

Let $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$. We say that *a is congruent to b modulo n*, denoted $a \equiv b \pmod{n}$, provided $n | a - b$.

Examples.

- We have: $7 \equiv 22 \pmod{5}$, $-4 \equiv 3 \pmod{7}$, $19 \equiv 119 \pmod{100}$, $37 \equiv 1 \pmod{4}$.
- For any $a, b \in \mathbb{Z}$: $a \equiv b \pmod{1}$.

Notice that:

$$a \equiv b \pmod{n} \quad \Leftrightarrow \quad a - b = nk \quad \Leftrightarrow \quad a = b + nk$$

for some $k \in \mathbb{Z}$.

Our first result concerning congruences should be familiar from Intro to Abstract.

Theorem 1

Let $n \in \mathbb{N}$. Then congruence modulo n is an equivalence relation on $\mathbb{Z}$.

Proof (Sketch). Let $a, b, c \in \mathbb{Z}$.

Reflexivity: Since $n|0$, $a \equiv a \pmod{n}$.

Symmetry: If $n|a-b$, then $n|-(a-b) = b-a$. So $a \equiv b \pmod{n}$ implies $b \equiv a \pmod{n}$.

Transitivity: If $n|a-b$ and $n|b-c$, then $n|(a-b)+(b-c) = a-c$. Thus $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ together imply that $a \equiv c \pmod{n}$. □

Recall that every equivalence relation on a set S *partitions* that set into disjoint subsets (the *equivalence classes*).

Given $n \in \mathbb{N}$, an equivalence class under congruence modulo n is called a *congruence class*.

We will denote the congruence class of $a \in \mathbb{Z}$ by $\overline{a}$ or $a + n\mathbb{Z}$ (whichever is more convenient):

$$\overline{a} = a + n\mathbb{Z} = \{b \in \mathbb{Z} \mid a \equiv b \pmod{n}\} = \{a + nk \mid k \in \mathbb{Z}\}.$$

We will denote the collection of congruence classes by $\mathbb{Z}/n\mathbb{Z}$:

$$\mathbb{Z}/n\mathbb{Z} = \{a + n\mathbb{Z} \mid a \in \mathbb{Z}\}.$$

Before we give more examples, it will be convenient to give a complete description of $\mathbb{Z}/n\mathbb{Z}$.

Theorem 2

Let $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$. Then $a \equiv b \pmod{n}$ iff a and b leave the same remainder when divided by n. In particular, every a is congruent to its remainder when divided by n, and no two distinct remainders are congruent modulo n. Therefore the (distinct) elements of $\mathbb{Z}/n\mathbb{Z}$ are

$$0 + n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}.$$

Remarks. We have the following immediate corollaries.

- $a \equiv 0 \pmod{n}$ iff $n|a$.
- $\left|\mathbb{Z}/n\mathbb{Z}\right| = n$.

Proof of Theorem 2. Write $a = q_1 n + r_1$, $b = q_2 n + r_2$, with $0 \leq r_i < n$.

Then $a - b = (q_1 n + r_1) - (q_2 n + r_2) = (q_1 - q_2)n + (r_1 - r_2)$.

If $a \equiv b \pmod{n}$, then $n|(a - b)$ and we find that

$$n|(a - b) - (q_1 - q_2)n = r_1 - r_2.$$

But $|r_1 - r_2| < n$, so this can only occur if $r_1 - r_2 = 0$ or $r_1 = r_2$.

Conversely, if $r_1 = r_2$, then $a - b = (q_1 - q_2)n$, so that $n|a - b$, and $a \equiv b \pmod{n}$.

The remaining statements follow at once. □

Examples

- If $n = 2$, the only remainders are 0 and 1. According to Theorem 2, we find that $a \equiv b \pmod 2$ iff a and b are both even or both odd. In this case we say a and b have the same *parity*.

- Every integer is congruent to either 0, 1 or 2 modulo 3 (and these options are mutually exclusive).

- Every integer is congruent to (exactly) one of the decimal digits modulo 10. In fact, since every integer whose decimal expansion ends in 0 is divisible by 10, every integer is congruent to its *final* digit modulo 10.

Let $n \in \mathbb{N}$. Theorem 2 tells us that there are exactly n congruence classes modulo n.

A set containing exactly one integer from each congruence class is called a *complete system of residues modulo n*.

Examples.

- The set $\{0, 1, 2, \ldots, n-1\}$ of remainders is a complete system of residues modulo n, by Theorem 2.
- The set $\{0, \pm 1, \pm 2\}$ is a complete system of residues modulo 5.
- More generally, the set $\{a \in \mathbb{Z} : |a| \leq n/2\} \setminus \{-n/2\}$ is a complete system of residues modulo n.

Modular Arithmetic

One of the facts that makes congruences so useful in arithmetic is that they respect the operations of addition and multiplication.

Theorem 3

Let $n \in \mathbb{N}$ and $a, b, c, d \in \mathbb{Z}$. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then:

1. $a + c \equiv b + d \pmod{n}$;
2. $ac \equiv bd \pmod{n}$.

Proof. Write $a - b = nk$ and $c - d = n\ell$ with $k, \ell \in \mathbb{Z}$. Then

$$(a + c) - (b + d) = (a - b) + (c - d) = nk + n\ell = n(k + \ell),$$

so that $a + c \equiv b + d \pmod{n}$.

The proof that multiplication is respected is only slightly less straightforward:

$$\begin{aligned} ac - bd &= ac - ad + ad - bd = a(c-d) + (a-b)d \\ &= an\ell + nkd = n(a\ell + kd), \end{aligned}$$

so that $ac \equiv bd \pmod{n}$. □

Corollary 1

Let $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$. If $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$ for all $k \in \mathbb{N}$.

Proof. Use part 2 of Theorem 3 and induct on k. □

Examples

Example 1

Prove that if $a \in \mathbb{Z}$, then $a^2 \equiv 0, 1 \pmod 4$.

Solution. We know that a is equivalent to one of 0, 1, 2 or 3 modulo 4, so we simply check each case:

$$a \equiv 0 \pmod 4 \quad \Rightarrow \quad a^2 \equiv 0^2 \equiv 0 \pmod 4,$$

$$a \equiv 1 \pmod 4 \quad \Rightarrow \quad a^2 \equiv 1^2 \equiv 1 \pmod 4,$$

$$a \equiv 2 \pmod 4 \quad \Rightarrow \quad a^2 \equiv 2^2 \equiv 0 \pmod 4,$$

$$a \equiv 3 \pmod 4 \quad \Rightarrow \quad a^2 \equiv 3^2 \equiv 1 \pmod 4.$$

Example 2

Prove that $53^{103} + 103^{53}$ is divisible by 39.

Solution. Notice that

$$53 \equiv 14 \equiv -25 \pmod{39},$$
$$103 \equiv 25 \pmod{39},$$

so that

$$53^{103} + 103^{53} \equiv (-25)^{103} + 25^{53} \equiv -5^{206} + 5^{106} \pmod{39}.$$

Now we compute the first few powers of 5 modulo 39:

$5^2 \equiv 25 \pmod{39}$, $5^3 = 125 \equiv 8 \pmod{39}$, $5^4 \equiv 5 \cdot 8 \equiv 1 \pmod{39}$.

Now divide the exponents 206 and 106 by 4:

$$\begin{aligned} -5^{206} + 5^{106} &\equiv -5^{4\cdot 51+2} + 5^{4\cdot 26+2} \pmod{39} \\ &\equiv -(5^4)^{51}5^2 + (5^4)^{26}5^2 \pmod{39} \\ &\equiv -1^{51} \cdot 25 + 1^{26} \cdot 25 \pmod{39} \\ &\equiv -25 + 25 \equiv 0 \pmod{39}. \end{aligned}$$

Remark. When computing the remainder when a^k is divided by n, especially by hand, it is usually best to:

1. Replace a by its remainder when divided by n.
2. Recursively find the remainders when $a^2, a^3, a^4, \ldots$ are divided by n, by multiplying the preceding remainder by a at each stage.

Properties of modular arithmetic ensure that this process yields the correct result.

Cancellation in Modular Arithmetic

Because $\mathbb{Z}$ is a domain, we have the cancellation law

$$ab = ac \text{ and } a \neq 0 \quad \Rightarrow \quad b = c.$$

This law *fails* for modular arithmetic. For instance, we have

$$2 \cdot 3 \equiv 2 \cdot 8 \pmod{10} \text{ and } 2 \not\equiv 0 \pmod{10},$$

yet $3 \not\equiv 8 \pmod{10}$.

The problem is that the common factor 2 and the modulus 10 are not relatively prime.

If we take the GCD into account, we get valid cancellation laws for modular arithmetic.

Lemma 1

Let $n, k \in \mathbb{N}$ and $a, b \in \mathbb{Z}$. Then

$$a \equiv b \pmod{n} \iff ak \equiv bk \pmod{nk}.$$

Proof. If $a \equiv b \pmod{n}$, then $a - b = n\ell$ for some $\ell \in \mathbb{Z}$.

Multiplying through by k yields $ak - bk = nk\ell$, so that $ak \equiv bk \pmod{nk}$.

Conversely, if $ak \equiv bk \pmod{nk}$, then $ak - bk = nk\ell$ for some $\ell \in \mathbb{Z}$.

That is, $k(a - b) = kn\ell$. Since $k \neq 0$, it can be cancelled, yielding $a - b = n\ell$, and hence $a \equiv b \pmod{n}$. □

Euclid's lemma yields the following useful result.

Lemma 2

Let $n \in \mathbb{N}$ and $a, b, c \in \mathbb{Z}$. If $(c, n) = 1$, then

$$ac \equiv bc \pmod{n} \iff a \equiv b \pmod{n}.$$

Proof. If $ac \equiv bc \pmod{n}$, then $n | ac - bc = (a - b)c$.

Since $(c, n) = 1$, Euclid's lemma implies that $n | a - b$, which means $a \equiv b \pmod{n}$.

The reverse implication follows immediately from part 2 of Theorem 3. □

Putting our lemmas together we obtain:

Theorem 4

Let $n \in \mathbb{N}$ and $a, b, c \in \mathbb{Z}$. Then

$$ac \equiv bc \pmod{n} \iff a \equiv b \pmod{n/(c,n)}.$$

Proof. If we write $c = c'(c,n)$ and $n = n'(c,n)$, then we know that $(c', n') = 1$.

By lemmas 1 and 2 we have

$$\begin{aligned} ac \equiv bc \pmod{n} &\Leftrightarrow ac'(c,n) \equiv bc'(c,n) \pmod{n'(c,n)} \\ &\Leftrightarrow ac' \equiv bc' \pmod{n'} \\ &\Leftrightarrow a \equiv b \pmod{n'}. \end{aligned}$$

Since $n' = n/(c,n)$, this completes the proof. □

Moral. We can cancel a common factor in an arbitrary congruence provided we divide the modulus by its GCD with that factor.

Returning to our earlier example, in the congruence

$$2 \cdot 3 \equiv 2 \cdot 8 \pmod{10}$$

we can cancel the 2 provided we replace 10 with

$$\frac{10}{(10,2)} = \frac{10}{2} = 5.$$

This yields the valid congruence

$$3 \equiv 8 \pmod{5}.$$

Before we turn to another example, we point out an important corollary to Theorem 4 (or Lemma 2), which applies whenever the modulus is prime.

Corollary 2

Let $p \in \mathbb{N}$ be prime and let $a, b, c \in \mathbb{Z}$. If $p \nmid c$, then

$$ac \equiv bc \pmod{p} \iff a \equiv b \pmod{p}.$$

Proof. Because p is prime, $p \nmid c$ implies that $(c, p) = 1$. The result follows. □

Example 3

Let $n \in \mathbb{N}$. If $a_1, a_2, \ldots, a_n$ is a complete system of residues modulo n and $(b, n) = 1$, prove that $ba_1, ba_2, \ldots, ba_n$ is also a complete system of residues modulo n.

Solution. To say that $a_1, a_2, \ldots, a_n$ form a complete system of residues modulo n means that

$$\mathbb{Z}/n\mathbb{Z} = \{a_1 + n\mathbb{Z}, a_2 + n\mathbb{Z}, \ldots, a_n + n\mathbb{Z}\},$$

and these are all distinct.

Define $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ by $f(a_i + n\mathbb{Z}) = ba_i + n\mathbb{Z}$. If we can show f is a bijection, we are finished.

Because $Z/n\mathbb{Z}$ is finite, it is sufficient to show f is injective, by the pigeon-hole principle.

So suppose that $f(a_i + n\mathbb{Z}) = f(a_j + n\mathbb{Z})$. Then

$$\begin{aligned} ba_i + n\mathbb{Z} = ba_j + n\mathbb{Z} &\Leftrightarrow ba_i \equiv ba_j \pmod{n} \\ &\Leftrightarrow a_i \equiv a_j \pmod{n} \\ &\Leftrightarrow a_i + n\mathbb{Z} = a_j + n\mathbb{Z}, \end{aligned}$$

where in the second line we have cancelled b in accordance with Lemma 2.

Hence f is injective, and the proof is complete. □

Example. Since $0, 1, 2, 3, 4, 5$ form a complete system of residues modulo 6, and $(5, 6) = 1$, the integers $0, 5, 10, 15, 20, 25$ are also a complete residue system modulo 6.