11-5-2018

Modular Arithmetic

Definiton. Let a, b, and m be integers. a is **congruent to** b **mod** m if $m \mid a - b$; that is, if

$$a - b = km \text{ for some integer } k.$$

Notation: $a = b \pmod{m}$ means that a is congruent to b mod m. m is called the **modulus** of the congruence; I will almost always work with positive moduli.

Note that $a = 0 \pmod{m}$ if and only if $m \mid a$. Thus, modular arithmetic gives you another way of dealing with divisibility relations.

For example:

$101 = 3 \pmod{2}$ because $2 \mid 101 - 3 = 98$.

$19 = -17 \pmod{12}$ because $12 \mid 19 - (-17) = 36$.

Proposition. Congruence mod m is an **equivalence relation**:

(a) (**Reflexivity**) $a = a \pmod{m}$ for all a.

(b) (**Symmetry**) If $a = b \pmod{m}$, then $b = a \pmod{m}$.

(c) (**Transitivity**) If $a = b \pmod{m}$ and $b = c \pmod{m}$, then $a = c \pmod{m}$.

Proof. Since $m \mid 0 = a - a$, it follows that $a = a \pmod{m}$.

Suppose $a = b \pmod{m}$. Then $m \mid a - b$, so $m \mid b - a$. Hence, $b = a \pmod{m}$.

Suppose $a = b \pmod{m}$ and $b = c \pmod{m}$. Then there are integers j and k such that

$$a - b = jm, \quad b - c = km.$$

Add the two equations:

$$a - c = (j + k)m.$$

This implies that $a = c \pmod{m}$. □

Example. (a) List the elements of the equivalence classes relative to congruence mod 3.

(b) Using 0, 1, and 2 to represent these equivalence classes, construct addition and multiplication tables mod 3.

(a) The equivalence classes are the 3 **congruence classes**:

$$\{\ldots, -3, 0, 3, 6, \ldots\}, \quad \{\ldots - 4, -1, 2, 5, \ldots\}, \quad \{\ldots - 5, -2, 1, 4, \ldots\}.$$

Each integer belongs to exactly one of these classes. Two integers in a given class are congruent mod 3. (If you know some group theory, you probably recognize this as constructing $\mathbb{Z}_3$ from $\mathbb{Z}$.) □

(b)

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

For example, $2 + 1 = 0$, because $2 + 1 = 3$ as integers, and the congruence class of 3 is represented by 0. Likewise, $2 \cdot 2 = 4$ as integers, and the congruence class of 4 is represented by 1. $\square$

I could have chosen different representatives for the classes — say 3, -4, and 4. A choice of representatives, one from each class, is called a **complete system of residues mod** 3. But working mod 3 it's natural to use the numbers 0, 1, and 2 as representatives — and in general, if I'm working mod n, the obvious choice of representatives is the set $\{0, 1, 2, \ldots, n-1\}$. This set is called the **standard residue system mod** n, and it is the set of representatives I'll usually use. Thus, the standard residue system mod 6 is $\{0, 1, 2, 3, 4, 5\}$.

Theorem. Suppose $a = b \pmod{m}$ and $c = d \pmod{m}$. Then:

(a) $a + c = b + d \pmod{m}$ and $a - c = b - d \pmod{m}$.

(b) $ac = bd \pmod{m}$.

Proof. I'll prove the first congruence as an example. Suppose $a = b \pmod{m}$ and $c = d \pmod{m}$. Then $a - b = jm$ and $c - d = km$ for some $j, k \in \mathbb{Z}$, so

$$(a + c) - (b + d) = jm - km = (j - k)m.$$

This implies that $a + c = b + d \pmod{m}$. $\square$

Example. Solve the congruence

$$7x + 1 = 2(2x + 8) \pmod{11}.$$

$$\begin{aligned} 7x + 1 &= 2(2x + 8) \pmod{11} \\ 7x + 1 &= 4x + 16 \pmod{11} \\ 7x + 1 &= 4x + 5 \pmod{11} \\ 3x &= 4 \pmod{11} \end{aligned}$$

There are no "fractions" mod 11. I want to divide by 3, and to do this I need to multiply by the multiplicative inverse of 3. So I need a number k such that $k \cdot 3 = 1 \pmod{11}$. A systematic way of finding such a number is to use the **Extended Euclidean algorithm**. In this case, I just use trial and error. Obviously, $k = 0$ and $k = 1$ won't work, so I'll start at $k = 2$:

$$2 \cdot 3 = 6 \pmod{11}, \quad 3 \cdot 3 = 9 \pmod{11}, \quad 4 \cdot 3 = 12 = 1 \pmod{11}.$$

Thus, I need to multiply the equation by 4:

$$\begin{aligned} 4 \cdot 3x &= 4 \cdot 4 \pmod{11} \\ 12x &= 16 \pmod{11} \qquad \square \\ x &= 5 \pmod{11} \end{aligned}$$

Definition. x and y are **multiplicative inverses** mod n if $xy = 1 \pmod{n}$.

Notation: $x = y^{-1} \pmod{n}$ or $y = x^{-1} \pmod{n}$. *Do not use fractions.*

Example. (a) Find $6^{-1} \pmod{17}$.

(b) Prove that 6 does not have a multiplicative inverse mod 8.

(a) $6 \cdot 3 = 18 = 1 \pmod{17}$, so $6^{-1} = 3 \pmod{17}$. $\square$

(b) Suppose $6x = 1 \pmod{8}$. Then

$$\begin{aligned} 4 \cdot 6x &= 4 \cdot 1 \pmod{8} \\ 24x &= 4 \pmod{8} \\ 0 &= 4 \pmod{8} \end{aligned}$$

This contradiction shows that 6 does not have a multiplicative inverse mod 8. $\square$

Example. Reduce $996 \cdot 997 \cdot 998 \cdot 999 \pmod{1000}$ to a number in $\{0, 1, \ldots, 999\}$.

$$996 \cdot 997 \cdot 998 \cdot 999 = (-4)(-3)(-2)(-1) = 24 \pmod{1000}. \quad \square$$

Example. Reduce $99^{10} \pmod{7}$ to a number in $\{0, 1, 2, 3, 4, 5, 6\}$.

$99 = 1 \pmod{7}$, so

$$99^{10} = 1^{10} = 1 \pmod{7}. \quad \square$$

Example. Show that if p is prime, then

$$(x + y)^p = x^p + y^p \pmod{p}.$$

By the Binomial Theorem,

$$(x + y)^p = \sum_{i=0}^{p} \binom{p}{i} x^i y^{p-i}.$$

A typical coefficient $\binom{p}{i} = \dfrac{p!}{i!\,(p-i)!}$ is divisible by p for $i \neq 0, p$. So going mod p, the only terms that remain are x^p and y^p.

For example

$$(x + y)^2 = x^2 + y^2 \pmod{2} \quad \text{and} \quad (x + y)^3 = x^3 + y^3 \pmod{3}.$$

The result is *not* true if the modulus is not prime. For example,

$$(1 + 1)^4 = 0 \pmod{4}, \quad \text{but} \quad 1^4 + 1^4 = 2 \pmod{4}. \quad \square$$
