3-30-2008

Congruences and Modular Arithmetic

- a is **congruent to** b **mod** n means that $n \mid a - b$. Notation: $a = b \pmod{n}$.
- Congruence mod n is an **equivalence relation**. Hence, congruences have many of the same properties as ordinary equations.
- Congruences provide a convenient shorthand for divisibility relations.

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

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

Write $a = b \pmod{m}$ to mean 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.

Example. $101 = 3 \pmod{2}$ and $2 = 101 \pmod{3}$. $\square$

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 $b = a (\bmod m)$.

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

Proof. I'll prove transitivity by way of example. 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 $a = c \pmod{m}$. $\square$

Example. Consider congruence mod 3. There are 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 $\mathbb{Z}$.)

When you're doing things mod 3, it is if there were only 3 numbers. I'll grab one number from each of the classes to **represent** the classes; for simplicity, I'll use 0, 2, and 1.

Here is an addition table for the classes in terms of these representatives:

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

Here's an example: $2 + 1 = 0$, because $2 + 1 = 3$ as integers, and 3's congruence class is represented by 0. This is the table for **addition mod** 3.

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 **least nonnegative system of residues mod** n, and it is the set of representatives I'll usually use.

(Sometimes I'll get sloppy and call it the **least positive system of residues**, even though it includes 0.) □

Proposition. Suppose $a = b \pmod{m}$. Then

$$a \pm c = b \pm c \pmod{m} \quad \text{and} \quad ac = bc \pmod{m}\,.$$

Proof. I'll prove (part of) the first congruence as an example. Suppose $a = b \pmod{m}$. Then $a - b = km$ for some k, so

$$(a + c) - (b + c) = km.$$

But this implies that $a + c = b + c \pmod{m}$. □

Example. Solve the congruence

$$2x + 11 = 7 \pmod{3}\,.$$

First, reduce all the coefficients mod 3:

$$2x + 2 = 1 \pmod{3}\,.$$

Next, add 1 to both sides, using the fact that $2 + 1 = 0 \pmod{3}$:

$$2x = 2 \pmod{3}\,.$$

Finally, multiply both sides by 2, using the fact that $2 \cdot 2 = 4 = 1 \pmod{3}$:

$$x = 1 \pmod{3}\,.$$

That is, any number in the set $\{\ldots, -5, -2, 1, 4, \ldots\}$ will solve the original congruence. □

Remark. Notice that I accomplished *division* by 2 (in solving $2x = 2 \pmod{3}$ by *multiplying* by 2. The reason this works is that, mod 3, 2 is its own *multiplicative inverse.*

Recall that two numbers x and y are **multiplicative inverses** if $x \cdot y = 1$ and $y \cdot x = 1$. For example, in the rational numbers, $\dfrac{3}{5}$ and $\dfrac{5}{3}$ are multiplicative inverses. *Division by a number is defined to be multiplication by its multiplicative inverse.* Thus, division by 3 *means* multiplication by $\dfrac{1}{3}$.

In the integers, only 1 and -1 have multiplicative inverses. When you perform a "division" in $\mathbb{Z}$ — such as dividing $2x = 6$ by 2 to get $x = 3$ — you are actually factoring and using the Zero Divisor Property:

$$2x = 6, \quad 2x - 6 = 0, \quad 2(x - 3) = 0, \quad x - 3 = 0, \quad x = 3.$$

(I used the Zero Divisor Property in making the third step: Since $2 \neq 0$, $x - 3$ must be 0.)

In doing modular arithmetic, however, many numbers may have multiplicative inverses. In these cases, you can perform division by multiplying by the multiplicative inverse.

Here is a multiplication table mod 3, using the standard residue system $\{0, 1, 2\}$:

$*$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

You can construct similar tables for other moduli. For example, 2 and 3 are multiplicative inverses mod 5, because $2 \cdot 3 = 1 \pmod 5$. So if you want to "divide" by 3 mod 5, you multiply by 2 instead.

This doesn't always work. For example, consider

$$2x = 4 \pmod 6.$$

2 does not have a multiplicative inverse mod 6; that is, there is no k such that $2k = 1 \pmod 6$. You can check by trial that the solutions to the equation above are $x = 2 \pmod 6$ and $x = 5 \pmod 6$ — just look at $2x \pmod 6$ for $x = 0, 1, 2, 3, 4, 5$. $\square$

Proposition. Suppose $a = b \pmod m$ and $c = d \pmod m$. Then

$$a + c = b + d \pmod m \quad \text{and} \quad ac = bd \pmod m.$$

Note that you can use the second property and induction to show that if $a = b \pmod m$, then

$$a^n = b^n \pmod m \quad \text{for all} \quad n \geq 1.$$

Proof. Suppose $a = b \pmod m$ and $c = d \pmod m$. Then $m \mid a - b$ and $m \mid c - d$, so by properties of divisibility,

$$m \mid (a - b) + (c - d) = (a + c) - (b + d).$$

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

To prove the second equation, note that $m \mid a - b$ and $m \mid c - d$ imply that there are integers j and k such that

$$mj = a - b \quad \text{and} \quad mk = c - d.$$

Therefore,

$$a = b + mj \quad \text{and} \quad c = d + mk.$$

Multiplying these two equations, I obtain

$$\begin{aligned} ac &= (b + mj)(d + mk) \\ ac &= bd + m(dj + bk + mjk) \\ ac - bd &= m(dj + bk + mjk) \end{aligned}$$

Hence, $m \mid ac - bd$, so $ac = bd \pmod m$. $\square$

Example. What is the least positive residue of $99^{10} \pmod 7$?

$99 = 1 \pmod 7$, so

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

Example. 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 $i \ne 0, p$. 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,

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