MODULAR ARITHMETIC II: CONGRUENCES AND DIVISION

MATH CIRCLE (BEGINNERS) 02/05/2012

Modular arithmetic. Two whole numbers a and b are said to be *congruent modulo* n, often written $a \equiv b \pmod{n}$, if they give the same remainders when divided by n. In other words, the difference $a - b$ is divisible by n. For instance, when you divide 16 by 3, you get 5 remainder 1; and when you divide 22 by 3 you get 7 remainder 1. Since the remainders are the same (1), we say that $16 \equiv 22 \pmod{3}$. Note that another way of checking this is that $16 - 22 = -6$, which is divisible by 3.

Examples:

$5 \equiv 1 \pmod{2}$ ... because $5 - 1 = 4$ is divisible by 2.

$6 \equiv 2 \pmod{4}$ ... because $6 - 2 = 4$ is divisible by 4.

$12 \equiv 0 \pmod{3}$ because $12 - 0 = 12$ is divisible by 3. In general, saying that x is congruent to zero modulo n ("$x \equiv 0 \pmod{n}$") is just another way of saying that x is divisible by n.

$7 \equiv -3 \pmod{5}$ ... because $7 - (-3) = 10$ is divisible by 5.

The word *congruent* means "the same" or "equivalent." Congruences are useful because many of their properties are similar to properties of ordinary equality. They tell us that certain properties of numbers depend only on their remainder, not on the actual number itself.

Properties of Congruences:

(1) $a \equiv a \pmod{d}$
(2) $a \equiv b \pmod{d}$ implies $b \equiv a \pmod{d}$
(3) If $a \equiv b \pmod{d}$ and $b \equiv c \pmod{d}$, then $a \equiv c \pmod{d}$.
(4) If $a \equiv a' \pmod{d}$ and $b \equiv b' \pmod{d}$, then
- $a \pm b \equiv a' \pm b' \pmod{d}$
- $ab \equiv a'b' \pmod{d}$

Suppose I wanted to define an unusual kind of addition for fractions—I'll call it *crazy-addition* and write it with a little circle around the plus sign, and it works like this:

$$\frac{a}{b} \oplus \frac{c}{d} = \frac{a+c}{b+d}$$

Problem 1. How does this compare to the usual formula for addition? The usual formula is:

$$\frac{a}{b} + \frac{c}{d} =$$

Problem 2. The crazy-addition formula is simpler than the usual formula for adding fractions. Why don't we use it instead? (There could be more than one reason...)

Here's one good reason we don't use crazy-addition: It doesn't work to represent fractions different ways! Take the fractions $\frac{1}{2} = \frac{2}{4}$ and $\frac{2}{3} = \frac{6}{9}$.

Problem 3. Compute:

$$\frac{1}{2} \oplus \frac{2}{3} =$$

Now compute:

$$\frac{2}{4} \oplus \frac{6}{9} =$$

I (crazy-)added the same two numbers each time–are the results equal?

(Right, they're not equal!) We should step back and worry a bit about modular arithmetic. I've said that it's just fine to add and subtract and multiply remainders, and that $3 \equiv 7 \equiv 11 \equiv -1 \pmod 4$, but how do I know that adding and multiplying actually *works?*

That is to say, even though $3 \equiv 11 \pmod 4$ and $2 \equiv 18 \pmod 4$, how do I know that

$$3 + 2 \equiv 11 + 18 \pmod 4 \qquad \text{and} \qquad 3 \cdot 2 \equiv 11 \cdot 18 \pmod 4?$$

Remember, with crazy-addition, this sort of thing DIDN'T work; when I crazy-added different-but-equal representations, I got UNEQUAL answers. Why couldn't the same thing happen with modular addition (or multiplication)?

Let's prove that addition and multiplication work...

If an integer a is divisible by n, it means that we can write $a = qn$ for some other integer q. If a has a remainder of r upon division by n (where r is between 0 and $n-1$ inclusive), it means that we can write

$$a =$$

And if $a \equiv a' \pmod n$, it means they both have the same remainder... so I could write

$$a' =$$

(Careful... Don't use the variable q twice in different places to mean possibly-different numbers! Pick another variable for the second time, say q'.)

Now if $b \equiv b' \pmod n$ it means we can write...

It's fine to add, subtract, and multiply remainders modulo n. (We just proved it!) But division is trickier...

DIVISION DIFFICULTY #1: Sometimes there is not a unique answer!

Problem 4. Fill in the blanks:

$$[2]_4 \cdot [1]_4 = [\quad\ ]_4$$

$$[2]_4 \cdot [3]_4 = [\quad\ ]_4$$

What should $[2]_4/[2]_4$ be? Or what's the problem here?

DIVISION DIFFICULTY #2: Sometimes two nonzero numbers multiply to give 0!

Problem 5. Give at least two different examples, using two different modulus, of two nonzero numbers multiplying to give 0.

Problem 6. Can you find a modulus where it's never the case that two nonzero numbers multiply to 0? Write down the multiplication table for your modulus to be sure. Is it the only one, or are there others?

In the ordinary numbers, dividing is the same thing as multiplying by the inverse.

- If I want to divide by 3, I may as well *multiply* by $\frac{1}{3}$.
- If I want to divide by $\frac{1}{8}$, I can *multiply* by 8.
- If I want to divide by $\frac{2}{5}$, I can always *multiply* by $\frac{5}{2}$.

In ordinary numbers, the multiplicative inverse of x is a number y such that $x \cdot y = 1$.

We can think about multiplicative inverses in modular-arithmetic world too! For example, in modulus 5, we have

$$[2]_5 \cdot [3]_5 = [6]_5 = [1]_5,$$

so 2 and 3 are inverses of each other modulo 5.

Problem 7. Fill in the blanks where possible, or if there is no inverse write "No inverse exists!"

(1) $[3]_8 \cdot [\quad]_8 = [1]_8$

(2) $[5]_7 \cdot [\quad]_7 = [1]_7$

(3) $[6]_{11} \cdot [\quad]_{11} = [1]_{11}$

(4) $[2]_{12} \cdot [\quad]_{12} = [1]_{12}$

(5) $[8]_{15} \cdot [\quad]_{15} = [1]_{15}$

(6) $[9]_{15} \cdot [\quad\ ]_{15} = [1]_{15}$

(7) $[2]_{1000} \cdot [\quad\ ]_{1000} = [1]_{1000}$