MODULAR ARITHMETIC: CONGRUENCES

MATH CIRCLE (BEGINNERS) 01/29/2012

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
- $a \pm b \equiv a' \pm b' \pmod{d}$
- $ab \equiv a'b' \pmod{d}$

Problem 1. For each of the numbers, below, find a number between 0 and $n-1$ that it's equivalent to.

For example: If the problem asks $17 \equiv \quad \pmod 6$, you would write $17 \equiv 5 \pmod 6$.

(a) $17 \equiv \quad \pmod 5$

(b) $29 \equiv \quad \pmod{10}$

(c) $433551 \equiv \quad \pmod 2$

(d) $315 \equiv \quad \pmod{21}$

(e) $91 \equiv \quad \pmod{13}$

(f) $-10 \equiv \quad \pmod 6$

If you remember the rules for addition and multiplication of evens and odds, that was just a special case of congruences, namely congruences modulo 2. Remember the rules for addition and multiplication:

EVEN + EVEN = EVEN
EVEN + ODD = ODD
ODD + EVEN = ODD
ODD + ODD = EVEN

EVEN $\times$ EVEN = EVEN
EVEN $\times$ ODD = EVEN
ODD $\times$ EVEN = EVEN
ODD $\times$ ODD = ODD

Or, in table form:

+	EVEN	ODD
EVEN	EVEN	ODD
ODD	ODD	EVEN

$\times$	EVEN	ODD
EVEN	EVEN	EVEN
ODD	EVEN	ODD

Modulo 2, every even number is congruent to zero, and every odd number is congruent to 1. So thinking in terms of congruences we could rewrite these tables:

+	0	1
0	0	1
1	1	0

$\times$	0	1
0	0	0
1	0	1

Remember, now 0 stands for *every* even number, and 1 stands for *every* odd number.

Problem 2. Fill in the addition and multiplication tables in the cases of modulus $n = 4$ and $n = 5$.

Modulo 4:

+	0	1	2	3
0				
1				
2				
3				

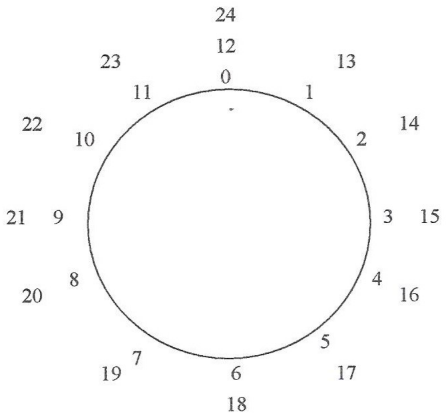
$\times$	0	1	2	3
0				
1				
2				
3				

Modulo 5:

+	0	1	2	3	4
0					
1					
2					
3					
4					

$\times$	0	1	2	3	4
0					
1					
2					
3					
4					

Geometric representation. To represent numbers modulo n use a circle divided into n equal parts. Any integer divided by n gives one of the remainders $0, 1, \ldots, n-1$. Place these numbers at equal intervals on the circumference of the circle. Every integer is congruent modulo n to one of those numbers and is geometrically represented by one of those points. If you look at a regular clock, you see something very similar with $n = 12$. But we usually use 0 instead of 12 when we are working modulo 12:



Problem 3. Use modular arithmetic to solve the following:

(a) A biology experiment starts at 2 p.m. and lasts 80 hours. At what time of the day will the experiment end?

(b) What day of the week will your birthday be in 2013? (Don't forget 2012 is a leap year... this matters in case your birthday is in January or February!)

Problem 4. In decimal notation, we write numbers as powers of 10. For instance, 7302 is a shorthand way of writing the number

$$7 \times 1000 + 3 \times 100 + 0 \times 10 + 2 \times 1 = 7 \times 10^3 + 3 \times 10^2 + 0 \times 10^1 + 2 \times 10^0.$$

In general, we write numbers that look like $a_k a_{k-1} \dots a_1 a_o$, where the a_i's are the digits, and that represents:

$$a_k \times 10^k + a_{k-1} \times 10^{k-1} + \dots + a_1 \times 10^1 + a_0 \times 10^0$$

Use this and modular arithmetic to explain the following divisibility tests:

(a) A number is divisible by 3 exactly when the sum of its digits is divisible by 3. (Hint: $10 \equiv 1 \pmod 3$...)

(b) A number is divisible by 11 exactly when the *alternating* sum of its digits is divisible by 11. (Hint: $10 \equiv -1 \pmod{11}$.

Problem 5. Use properties of congruences:

(a) To what number between 0 and 6 inclusive is the product $11 \cdot 18 \cdot 2322 \cdot 13 \cdot 19$ congruent modulo 7?

(b) To what number between 0 and 12 inclusive is the product $3 \cdot 7 \cdot 11 \cdot 17 \cdot 23 \cdot 29 \cdot 113$ congruent to modulo 13?