Modular Arithmetic Investigations
Pre-class, Week 5

Modular arithmetic (congruences) is another equivalent way of thinking about remainders in long division. Given a natural number $n > 0$ (some people restrict modular arithmetic to $n > 1$), if $n|(a-b)$, then we say that a is *congruent* to b modulo n and write $a \equiv b \pmod{n}$.

1. Determine if the following congruences are true (using the definition of congruency, and preferably without a calculator).

a. $430023 \equiv 23 \pmod{43}$ ✓

b. $23 \equiv 430023 \pmod{43}$ ✓

c. $7823927345612341 \equiv 7112981223576296 \pmod{10}$ ✗

d. $7712927345612341 \equiv 7712981223576296 \pmod{5}$ ✓

e. $a \equiv a \pmod{7}$ (where a is an unknown number) ✓

f. $a \cdot k \equiv 0 \pmod{a}$ (where a is an unknown number) ✓

If $a = q_1 \cdot n + r$ where $0 \leq r < n$, then $a \equiv r \pmod{n}$. If $b = q_2 \cdot n + r$, then we also have $a \equiv b \pmod{n}$. So congruency is an equivalent way of reducing a number to its remainder when divided by n. The way we defined congruency makes easier to deal with negative numbers without worrying about the remainder. The definition and notation we use for congruency provides a powerful and convenient tool when dealing with many types of divisibility problems.

2. Recall the divisibility rule for 3. Using this rule, determine the remainders of 1234567771 and 1112341112 when divided by 3. Express this in mod notation.

$1112341112 \equiv 2 \pmod{3}$

$1234567771 \equiv 1 \pmod{3}$

3. If $a \equiv 4 \pmod{7}$ and $b \equiv 5 \pmod{7}$, then what can you say about $(a+b)$, $(a-b)$ and ab modulo 7? Justify using the definition.

$7 \mid a-4 \qquad 7 \mid b-5$

$a-4 = 7k \qquad b-5 = 7j$

$a = 7k+4 \qquad b = 7j+5$

$a+b = 7k+4+7j+5 = 7(k+j+1)+2$

$a-b = 7k+4-7j-5 = 7(k-j-1)+6$

$ab = (7k+4)(7j+5) = 7(7kj+5k+4j+2)+6$

4. Simplify the expression $25 \cdot 34 + 9 \cdot 8^{12} \pmod{7}$. Justify briefly.

$4 \cdot 6 + 2 \cdot 1 \equiv 5 \pmod{7}$

#3's arguments generalize to show you can reduce "whenever you want" with +, - in mod arith.