Modular Math:

A. Modular math is simply working with MOD. MOD is the remainder after dividing by a specific value. For example, 35 MOD 3 = 2 since the remainder after 35 is divided by 3 is 2.

B. Modular math works with congruencies. It is true that 35 MOD 3 = 2, but it is also true that this is congruent to 32 MOD 3 or even 26 MOD 3, since they all produce the same value of 2 after being divided by 3.

C. In general, n MOD a $\equiv$ (n + ab) MOD a, where b is any integral. So 35 MOD 3 $\equiv$ (35 + 3b) MOD 3. If b = -4, then we learn that 35 MOD 3 $\equiv$ 23 MOD 3, which we can see is true since they both produce the value 2.

D. Number sense uses this in a few different forms.

Ex [1] 2x $\equiv$ 3 MOD 7, $0<x<12$, then x = _____

a. On problems like these, think of this as being 2x $\equiv$ 3a + 7. We are looking for a value of a that produces an integer value for x that is between 0 and 12. Basically, we are adding multiples of 7 to 3 until a value can be found for x in the given range.

b. Go through each value mentally (usually starting with 0) until you find a value that works. With a = 0, we get x = $^3/_2$ which is not an integer. With a = 1, we get x = 5 which is in the range. So x = 5.

Ex [2] 13^{14} divided by 5 has a remainder of _____

a. One property of MOD's is that a^b MOD n $\equiv$ (a MOD n)^b MOD n. So for this problem, we know that 13 MOD 5 = 3. So we can first think of this as being 3^{14} MOD 5.

b. There are several ways to go from here. I would probably then say this is equal to 9^7 MOD 5. We know that 9^0 ends in a 1 and 9^1 ends in a 9. After this the last digit repeats itself. So $9^n \equiv 9^{n \text{ MOD } 2}$. So $9^7 \equiv 9^1$ which has a remainder of 4 after dividing by 5.

c. The answer is 4.

d. The goal of these types of problems is to reduce the value using congruencies, until you get something that is easy to compute. In this case, we got 9 MOD 5. Sometimes, you can know the answer earlier. It just takes a lot of practice.

E. Sometimes, there are special cases where finding the answer is easier.

1. We know from a theorem (Euler's Totient Theorem) that a^b MOD b = a, if a and b are *relatively prime*.

Ex [1] 15^{17} MOD 17 = ________

a. The answer is 15 since 15 and 17 are relatively prim e.