Investigations on Congruence Equations Pre-class, Week 6

In this pre-class, we will investigate when solutions of congruence equations exist, and how to solve the equations in some cases. During the in-class activity, we will see the general theory.

- 1. Determine if it is possible to solve the following equations. You can use any method in this problem, including trying all possible x's. (Note: Since we are trying to solve congruence equations, you only need to try a complete residue system as your possible x's.)
- a. $2x \equiv 4 \pmod{6}$ $\chi = 2$
- **b.** $2x \equiv 3 \pmod{6}$ not possible. 2x is even. Parity is conserved % 6
- c. $4x \equiv 5 \pmod{6}$
- **d.** $4x \equiv 2 \pmod{6}$ $\chi = 2$ 5
- e. $6x \equiv 3 \pmod{9}$ $\not = 2$
- f. $6x \equiv 4 \pmod{9}$ $\land o \vdash P_{o}$
- **2.** In the above problem, you found that $2x \equiv 3 \pmod{6}$ does not have a solution. We will now justify this. Using the definition of congruence modulo 6, write out an integer equation (i.e. an equality, not equivalence) that x has to satisfy. Using this equation, justify why the congruence equation does not have a solution.

$$2x = 6K + 3$$

$$eV \ln = 0 dd$$

3. We have seen that the greatest common divisor of two numbers can be expressed as a linear combination of these numbers. For example, $2 = 2 \cdot 22 - 3 \cdot 14$. Comparing this equation with the integer equation that would result from the congruence equation $14x \equiv 2 \pmod{22}$, find a solution for the congruence equation.

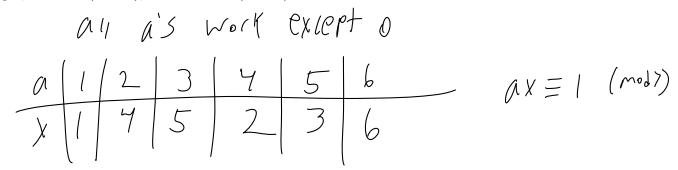
$$14x = 22k+2$$

$$14x - 22k = 2$$

$$14(-3) - 22(-2) = 2$$

$$x = -3 = 19$$

- **4.** A special congruence equation to consider is $2x \equiv 1 \pmod{7}$, or more generally $ax \equiv 1 \pmod{n}$. In a way, we are looking for an x which is the "reciprocal" of a.
- **a.** Let us restrict our attention to modulo 7. For which a can we solve the equation $ax \equiv 1 \pmod{7}$? For example, $2 \cdot 4 \equiv 1 \pmod{7}$, hence $2x \equiv 1 \pmod{7}$ has a solution. What are the other a's that work?



b. Let us now focus on modulo 10. For which a can we solve the equation $ax \equiv 1 \pmod{10}$?

A 1 2 3 4 5 6 7 8 9 X 1 X 7 X X X 3 X 9