UW Math Circle

April 21, 2016

Remember modular arithmetic: we say that a and b are congruent modulo n and we write $a \equiv b \pmod{n}$ if a and b have the same remainder when you divide then by n, or if n divides $a - b$ with remainder 0.

1. Say what the following numbers are congruent to modulo n.
   (a) $15 \equiv ? \pmod{4}$
   (b) $15 + 7 \equiv ? \pmod{5}$
   (c) $2^3 \equiv ? \pmod{3}$
   (d) $3^4 \equiv ? \pmod{5}$

2. Solve the following equations for x modulo n, or show that there aren't any solutions.
   (a) $2x \equiv 1 \pmod{3}$
   (b) $2x \equiv 1 \pmod{20}$
   (c) $5x \equiv 3 \pmod{15}$
   (d) $4x \equiv 5 \pmod{20}$
   (e) $17x \equiv 1 \mod 19$.

3. For what a does the equation $ax \equiv 1 \pmod{n}$ have a solution when n is equal to $3, 4, 5, 6, 30$?

4. The greatest common divisor of 3 and 5 is 1– and 1 is the greatest common divisor of 3 and $5-3=2$. The greatest common divisor of 15 and 70 is 5. We also see that 5 is the greatest common divisor of 15 and $70-15=55$.

   Prove that if d is the greatest common divisor of a and b and a isn't equal to b, then d is the greatest common divisor of a and $b-a$.

5. Devise a procedure (and prove that it is correct) to find the greatest common divisor of a and b, and to **Hint:** Consider the following example involving 21 and 33.

   - $33 = 21(1) + 12$
   - $21 = 12(1) + 9$
   - $12 = 9(1) + 3$
   - $9 = 3(3) + 0$
   - The greatest common divisor of 33 and 12 is 3.

6. Use your answer to the previous problem to write $ax+by=d$, where x, y are integers and d is the greatest common divisor of a and b.

7. Find the greatest common divisor of 1071 and 462.

8. Devise a criteria for saying when the equation $ax \equiv 1 \pmod{n}$ has a solution, and show that it is correct. You might use induction to show that it is correct.