BLACKSBURG MATH CIRCLE: SATURDAY, SEPTEMBER 12, 2015

Elements of number theory

1. Prove that $1^n + 2^n + \ldots + (n-1)^n$ is divisible by n for any odd $n > 1$.

2. **Fermat-Wiles theorem**: If n is an integer greater than 2, the equation $x^n + y^n = z^n$ has no positive integer solutions (x, y, z).

3. Twin prime conjectures: There are infinitely many primes p such that
   (a) (**Euclid**, 300BC) $p + 2$ is also prime;
   (b) (**Germain**, 1825) $2p + 1$ is aslo prime.

4. If a and d are integers and $d \neq 0$, show that we can divide a by d to obtain a *quotient* q and a *remainder* r, i.e.
$$a = q \cdot d + r \text{ such that } 0 \leq r < |d|.$$

Definition 1. If $a = dq$ for some non-zero integers a, d, and q, we say that d and q *divide* a or that d and q are *divisors* of a, and write $d|a$ and $q|a$.

5. Pick your favorite psitive integer d. If integers a_1 and a_2 have remainders r_1 and r_2 when divided by d, is it always true that

   (a) $a_1 + a_2$ has remainder $r_1 + r_2$ when divided by d?

   (b) $a_1 - a_2$ has remainder $r_1 - r_2$ when divided by d?

   (c) $a_1 \cdot a_2$ has remainder $r_1 \cdot r_2$ when divided by d?

   (d) a_1/a_2 has remainder r_1/r_2 when divided by d?

Definition 2. Let d be a positive integer. Two numbers a and b are called *congruent modulo* d if they have the same remainder when divided by d, i.e. $a = q \cdot d + r$ and $b = p \cdot d + r$. We denote this by $a \equiv b (\operatorname{mod} d)$.

6. What does the world modulo d looks like? For $d = 5$, the world consists of 5 'trees', each named after one of the 5 possible remainders. Find formulas describing all numbers residing in each tree. How about the general d?

Lemma 1. Let a and b be integers. In the world mod d

(a) $d|a$ iff $a \equiv 0(\text{mod}\, d)$;
(b) a is congruent to its own remainder (mod d);
(c) $a \equiv b(\text{mod}\, d)$ iff $d|(a-b)$.

Lemma 2. Let a, b and c be integers. Then

(a) Reflexivity $a \equiv a(\text{mod}\, d)$;
(b) Symmetry $a \equiv b(\text{mod}\, d)$ implies $b \equiv a(\text{mod}\, d)$;
(c) Transitivity $a \equiv b(\text{mod}\, d)$ and $b \equiv c(\text{mod}\, d)$ implies $a \equiv c(\text{mod}\, d)$.

Lemma 3. $a \equiv b(\text{mod}\, d)$ and $c \equiv e(\text{mod}\, d)$, then

(a) $a + c \equiv b + e(\text{mod}\, d)$;
(b) $a - c \equiv b - e(\text{mod}\, d)$;
(c) $a \cdot c \equiv b \cdot e(\text{mod}\, d)$.

Corollary 1. If $a \equiv b(\text{mod}\, d)$, then for all natural numbers h and k

(a) $a \pm h \equiv b \pm h(\text{mod}\, d)$ and $a \cdot h \equiv b \cdot h(\text{mod}\, d)$;
(b) $a^k \equiv b^k(\text{mod}\, d)$.

7. Find the remainder of $2^{2015}(\text{mod}\, 3)$ and $2^{2015}(\text{mod}\, 5)$.