Concepts of Math: Recitation 25 (Irina's Lecture)

November 30, 2015

Modular Arithmetic

1. Use the Binomial Theorem to find the last two digits of 39^{202}. *Hint:* $39^{202} = (40-1)^{202}$. Use binomial expansion. Note that all but the last two terms are divisible by 100.

2. Note that $ab \equiv ac \pmod{n}$ does not necessarily imply $b \equiv c \pmod{n}$. For example $4 \equiv 2 \pmod{2}$ is true, however $2 \equiv 1 \pmod{2}$ is false. It is not ok to divide both sides of a congruence by an integer. Also $a^k \equiv b^k \pmod{n}$ does not imply that $a \equiv b \pmod{n}$. For example $4 \equiv 1 \pmod{3}$ is true, however $2 \equiv 1 \pmod{3}$ is false. It is not ok to take a root of both sides of a congruence.

3. In class we proved that if $\gcd(a, n) = 1$, then equation $ax \equiv b \pmod{n}$ has one congruence $\pmod{n}$ class solution. Solve $54x \equiv 3 \pmod{35}$. Note that this is the same as solving the linear Diophantine equation $54x - 3 = 35y$, which is the same as $54x - 35y = 3$. Solve this equation using the Euclidean algorithm. Your final answer will be $x \equiv 2 \pmod{35}$.

4. Consider the equation $ax \equiv b \pmod{n}$. Prove that this equation has a solution if and only if b is divisible by $\gcd(a, n)$. Use the fact that $ax \equiv b \pmod{n}$ is equivalent to the linear Diophantine equation $ax - ny = b$ which, as we know, has a solution if and only if b is divisible by $\gcd(a, n)$.

5. Show that if $x \equiv 1 \pmod{2}$, then either $x \equiv 1 \pmod{6}$, or $x \equiv 3 \pmod{6}$, or $x \equiv 5 \pmod{6}$. One congruence class $\pmod{2}$ is equivalent to the union of three congruence classes $\pmod{6}$. In general one congruence class $\pmod{n}$ is equivalent to the union of k congruence classes $\pmod{nk}$.

6. Consider the equation $ax \equiv b \pmod{n}$. Suppose that b is divisible by $g = \gcd(a, n)$. Prove that this equation has g distinct congruence $\pmod{n}$ class solutions. Use the fact that $ax \equiv b \pmod{n}$ is equivalent to the linear Diophantine equation $ax - ny = b$. We have $a = kg$, $n = lg$, $b = mg$, where $k, l, m \in \mathbb{Z}$ and $\gcd(k, l) = 1$. Divide both sides of $ax - ny = b$ by g to get $kx - ly = m$, where $\gcd(k, l) = 1$. This implies that $lx \equiv m \pmod{l}$. By the lemma proved in class this equation has one congruence $\pmod{l}$ class solution, thus the solution is the union of g congruence $\pmod{n}$ class solutions.

7. Find all the solutions of $6x \equiv 3 \pmod{27}$. The answer should be a union of congruence (mod 27) class solutions.

8. If there is time left, please tell the students a little history about Fermat's last theorem.