Concepts of Math: Recitation 27 (Irina's Lecture)

December 2, 2015

The Chinese Remainder Theorem

If $\{n_1, n_2, \ldots, n_r\}$ is a set of natural numbers that are pairwise relatively prime, and $\{a_1, a_2, \ldots a_r\}$ is a set of any r integers, then the system of congruences $x \equiv a_i \pmod{n_i}$ has a unique solution modulo $N = n_1 n_2 \ldots n_r$. To find this solution, let $N_i = N/n_i$. Then solve the congruences $N_i y_i \equiv 1 \pmod{n_i}$. The solution is

$$x \equiv \sum_{j=1}^{r} a_j N_j y_j.$$

1. Find all the integers that are congruent to 1 mod 7, 2 mod 8, and 5 mod 9. Which solution has the smallest absolute value?

2. Suppose that $x \equiv 3 \pmod{6}$, $x \equiv 4 \pmod{7}$, and $x \equiv 5 \pmod{8}$. Explain why the Chinese Remainder Theorem does not apply to compute x. Transform the problem to an equivalent problem where the Chinese Remainder Theorem can be used and solve this problem.

Wilson's Theorem

If p is prime, then $(p-1)! \equiv -1 \pmod{p}$.

1. Prove the converse of Wilson's Theorem. If $p \in \mathbb{N}$, $p \geq 2$, and $(p-1)! \equiv -1 \pmod{p}$, then p is prime.

Subtle work with congruence relations

1. This problem appeared in the last recitation notes. If you did not do it last time, please do it now. In class we proved the following lemma: if p is a prime number and $a^2 \equiv 1 \pmod{p}$, then $a \equiv 1 \pmod{p}$ of $a \equiv -1 \pmod{p}$. Show that this statement is not true when p is not prime. For example $5^2 \equiv 1 \pmod{12}$. However neither $5 \equiv 1 \pmod{12}$ nor $5 \equiv -1 \pmod{12}$ is true.

2. Here are operations that can be performed on congruences. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a + c \equiv b + d \pmod{n}$, $a - c \equiv b - d \pmod{n}$, and $ac \equiv bd \pmod{n}$. If $k \in \mathbb{N}$, then $a^k \equiv b^k \pmod{n}$. Give examples.

3. This was done earlier, but needs to be done again. One cannot just divide both sides of a congruence by an integer, that is $ab \equiv ac \pmod{n}$ 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 take a root of both sides of a congruence, that is $a^k \equiv b^k \pmod{n}$ does not imply that $a \equiv b \pmod{n}$. For example $9 \equiv 4 \pmod{5}$ is true, however $3 \equiv 2 \pmod{3}$ is false.

4. Solve the system $x - y \equiv 2 \pmod{10}$, $x + y \equiv 8 \pmod{10}$. Add the two equations side by side:
$$2x \equiv 0 \pmod{10}.$$
Note that $\gcd(2, 10) = 2$, there are two congruence class solutions. $x \equiv 0 \pmod{10}$ and $x \equiv 5 \pmod{10}$. Find the corresponding y's and verify your solutions.

5. Solve the system $2x + y \equiv 5 \pmod{10}$, $x - 3y \equiv 9 \pmod{10}$.