Homework 3

(Linear congruences and the Chinese Remainder Theorem)

Due Wednesday, October 9 at 11:30am in class.

Note: Be sure to justify your answers. No credit will be given for answers without work/justification. In addition, all written homework assignments should be neat and well-organized; **this assignment has only one part and can be submitted as a single packet**.

(1) For this problem, you may assume the following theorem.

Theorem 1. Let $f(x)$ be a polynomial with integer coefficients. If there exists an integer $n > 1$ such that the congruence $f(x) \equiv 0 \mod (n)$ has no solutions x, then the equation $f(x) = 0$ can have no integer solutions x.

In other words, if $f(x)$ has no zeros modulo n, then $f(x)$ has no integer roots.

(a) Show that the polynomial $x^3 - x + 1$ has no integer roots.
(b) Show that the polynomial $x^3 + x^2 - x + 3$ has no integer roots.
(c) Write the contrapositive of Theorem 1.
(d) Write the converse to the contrapositive from part (c).
(e) Show that the converse of the contrapositive holds for every polynomial of the form $ax + b$ where a and b are integers.
(f) Prove that the congruence $6x^2 + 5x + 1 \equiv 0 \pmod{n}$ has a solution for every positive integer n. (And note that $6x^2 + 5x + 1 = 0$ has no integer solutions.)

(2) Prove that if $ac \equiv bc \pmod{n}$ and $\gcd(c, n) = 1$, then $a \equiv b \pmod{n}$.

(3) Solve each linear congruence or system of linear congruences, if a solution exists. If no solution exists, state why.

(a) $x^2 \equiv 1 \pmod{7}$
(b) $66x \equiv 100 \pmod{121}$
(c) $21x \equiv 14 \pmod{91}$
(d) $x \equiv 5 \pmod{7}$ and $x \equiv 2 \pmod{12}$ and $x \equiv 8 \pmod{13}$

(4) A composite number m is called a Carmichael number if the congruence $a^{m-1} \equiv 1 \pmod{m}$ is true for every number a with $\gcd(a, m) = 1$. Show that $m = 561 = 3 \cdot 11 \cdot 17$ is a Carmichael number.

Fun problem (will not be graded): Try to find another Carmichael number. Do you think that there are infinitely many of them?