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 $f(x) \equiv 0 \pmod{n}$ 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.
Consider this polynomial modulo 2:

$$0^3 - 0 + 1 \equiv 1 \pmod{2}$$

and

$$1^3 - 1 + 1 \equiv 1 \pmod{2}.$$

So, if $x \in [0]$ or $x \in [1]$ modulo 2, then $f(x) \in [1]$ modulo 2. So $f(x) \equiv 0$ has no solutions (mod 2) and by the theorem $f(x) = 0$ has no integer solutions.

(b) Show that the polynomial $x^3 + x^2 - x + 3$ has no integer roots.
Consider this polynomial modulo 5:

$$\begin{aligned} 0^3 + 0^2 - 0 + 3 &\equiv 3 \pmod{5} \\ 1^3 + 1^2 - 1 + 3 &\equiv 4 \pmod{5} \\ 2^3 + 2^2 - 2 + 3 = 13 &\equiv 3 \pmod{5} \\ 3^3 + 3^2 - 3 + 3 = 36 &\equiv 1 \pmod{5} \\ 4^3 + 4^2 - 4 + 3 = 79 &\equiv 4 \pmod{5}. \end{aligned}$$

So, $f(x) \notin [0]$ modulo 5 for any $x \in [0], [1], [2], [3]$, or $[4]$ modulo 5. So $f(x) \equiv 0$ has no solutions (mod 5) and by the theorem $f(x) = 0$ has no integer solutions.

(c) Write the contrapositive of Theorem 1.
Let $f(x)$ be a polynomial with integer coefficients. If the equation $f(x) = 0$ has an integer solution, then for every $n > 1$ the congruence $f(x) \equiv 0 \pmod{n}$ has a solution.

(d) Write the converse to the contrapositive from part (c).
Let $f(x)$ be a polynomial with integer coefficients. If for every $n > 1$ the congruence $f(x) \equiv 0 \pmod{n}$ has a solution, then the equation $f(x) = 0$ has an integer solution.

(e) Show that the converse of the contrapositive holds for any polynomial of the form $ax + b$ where a and b are integers.

Proof. Suppose the $f(x) = ax + b$ where a and b are integers and that, for every $n > 1$, the congruence $f(x) \equiv 0 \pmod{n}$ has a solution. Then we have that, for every n, the congruence $ax \equiv -b \pmod{n}$ has a solution. This is a linear congruence, and we know that it has a solution if and only if $\gcd(a, n) \mid (-b)$. Since there is a solution for every $n > 1$, the congruence has a solution for $n = |a|$. Then it must be that $\gcd(a, |a|) = a \mid (-b)$. Thus the equation $ax + b = 0$ has an integer solution: $x = -b/a$. □

(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.)

Proof. Let $n > 1$ be an integer and note that $6x^2 + 5x + 1 = (3x + 1)(2x + 1)$. The congruence

$$3x \equiv -1 \pmod{k}$$

has a solution if and only if $\gcd(3, k) = 1$. Similarly, the congruence

$$2x \equiv -1 \pmod{k}$$

has a solution if and only if $\gcd(2, k) = 1$. Write $n = 2^e m$ where $2^e \,||\, n$ and note that $\gcd(2^e, m) = 1$. Then we have that

$$3x \equiv -1 \pmod{2^e}$$

has a solution, say x_1, and

$$2x \equiv -1 \pmod{m}$$

has a solution, say x_2. Since $\gcd(2^e, m) = 1$, by the CRT, the simultaneous congruences

$$x \equiv x_1 \pmod{2^e}$$
$$x \equiv x_2 \pmod{m}$$

have a common solution x. Thus $2^e \mid (3x + 1)$ and $m \mid (2x + 1)$, and we have that $2^e m = n \mid (2x + 1)(3x + 1)$, as desired. □

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

Proof. Suppose that a, b, c are integers and $n > 1$ a natural number such that

$$ac \equiv bc \pmod{n}.$$

Then we know that $n \mid (ac - bc)$, i.e., for some integer q,

$$nq = ac - bc = (a - b)c.$$

Then we have that

$$\frac{nq}{c} = a - b$$

is an integer. Since $\gcd(c, n) = 1$, it must be that $c \mid q$ and so q/c is an integer. Thus we see that $n \mid (a - b)$ and so $a \equiv b \pmod{n}$. □

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

(a) $x^2 \equiv 1 \pmod{7}$
We can solve this by plugging in values $0, 1, 2, \ldots, 6$. We find that $x \equiv 1, 6 \pmod{7}$.

(b) $66x \equiv 100 \pmod{121}$
Since $\gcd(66, 121) = 11$ and $11 \nmid 100$, this congruence has not solution.

(c) $21x \equiv 14 \pmod{91}$ Since $\gcd(21, 91) = 7$ and $7 \mid 14$, we know that there are many solutions: 7 congruence classes modulo 91. Applying the Lemma (a) from class, we can divide by 7 to get

$$3x \equiv 2 \pmod{13}.$$

Now, just by inspection, we might notice that if $x = 5$, this congruence is true. So the solution is the class of [5] modulo 13 or the classes

$$[5], [18], [31], [44], [57], [70], [83]$$

modulo 91.

(d) $x \equiv 5 \pmod{7}$ and $x \equiv 2 \pmod{12}$ and $x \equiv 8 \pmod{13}$
Since 7, 12, and 13 are pairwise coprime, we can apply the Chinese Remainder Theorem. First, we find a particular solution, for example $x = 866$ (use the proof of CRT to find this). Then the solutions are all contained in the class [866] modulo $1092 = 12 \cdot 13 \cdot 7$.

(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.
Suppose that $\gcd(a, 561) = 1$. Then $\gcd(a, 3) = \gcd(a, 11) = \gcd(a, 17) = 1$. From Fermat's Little Theorem, we know that

$$a^2 \equiv 1 \pmod{3}$$
$$a^{10} \equiv 1 \pmod{11}$$
$$a^{16} \equiv 1 \pmod{17}.$$

Thus

$$a^{560} = (a^2)^{280} \equiv 1 \pmod{3}$$
$$a^{560} = (a^{10})^{56} \equiv 1 \pmod{11}$$
$$a^{560} = (a^{16})^{35} \equiv 1 \pmod{17}.$$

So consider the system

$$x \equiv 1 \pmod 3$$
$$x \equiv 1 \pmod{11}$$
$$x \equiv 1 \pmod{17}.$$

This clearly has a solution for $x = 1$. By the CRT, the congruence class [1] modulo $3 \cdot 11 \cdot 17 = 561$ contains all solutions to this system. Thus, since a^{560} is also a solution to this system, $a^{560} \in [1]$. In other words, $a^{560} \equiv 1 \pmod{561}$.

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