MCS 150 Homework 6

1. Let $n \in \mathbb{Z}^+$. The *multiplicative order* of an integer x modulo n is defined as the least $k \in \mathbb{Z}^+$ such that
$$x^k \equiv 1 \pmod{n}.$$
   (a) Not every integer has a multiplicative order. Play with some examples and formulate a conjecture about which integers do and which do not. Prove your conjecture. (Hint: List the powers $x, x^2, x^3, \ldots$. They cannot all be different modulo n. Choose $l \neq z$ so that $x^l \equiv x^z \pmod{n}$ and use this to show that there must be a power of x that is congruent to 1 modulo n.)
   (b) Let p be a prime number. Experiment with the multiplicative order of integers modulo p. What do you notice? State your conjecture, but you do not need to prove it.

2. Let $n \in \mathbb{Z}^+$. Consider the second degree congruence equation $x^2 \equiv 1 \pmod{n}$. Obviously, any integer $x \equiv 1 \pmod{n}$ or $x \equiv -1 \pmod{n}$ satisfies this equation.
   (a) Find an example to show that it is possible for this congruence equation to have solutions other than ± 1 modulo n.
   (b) Prove that if p is any prime number then the only solutions of $x^2 \equiv 1 \pmod{p}$ are integers $x \equiv \pm 1 \pmod{p}$.

3. Let $n \in \mathbb{Z}^+$. On the last homework, you noticed that if $n = p^k$ for some prime number p and $k \in \mathbb{Z}^+$, then the number of units among the canonical representatives $0, 1, \ldots, n-1$ is $p^k - p^{k-1}$.
   (a) Now suppose n is any integer, i.e. not necessarily prime or a prime power. Play with some examples until you can formulate a conjecture about the number of units among the canonical representatives $0, 1, \ldots, n-1$ modulo n.
   (b) Let $m, n \in \mathbb{Z}^+$ such that m and n are relatively prime. Let M be the number of units among the canonical representatives $0, 1, \ldots, m-1$ modulo m and let N be the number of units among the canonical representatives $0, 1, \ldots, n-1$ modulo n. Prove that the number of units among the canonical representatives $0, 1, \ldots, mn-1$ modulo mn is MN.
   (c) Prove your conjecture from part (a). (Hint: the result you proved in part (b) should be very helpful.)