Homework 7

Some notes on the homework assignment:

- Remember to acknowledge your collaborators and cite your sources. The template has a section built in for you to do this (see the comments in the template).
- Remember to let me know if you can't do your peer review this week (for any reason)!
- I know this looks long, but the problems are broken up into parts to break things into bite-sized pieces
- You will probably want to use the result of problem 1 in problem 2b.

Here's the schedule of when things are due for this assignment.

Component Due	**Date**
Draft of Solutions	Thursday, May 26
Peer Review	Tuesday, May 31
Final Copy	Friday, June 3

And finally, here are the problem statements.

1. *Suppose that m and k are positive integers and that k is relatively prime to $\varphi(m)$. Suppose also that m has a primitive root. Use Theorem 9.17 (or other methods) to show that the function*

$$f : \left(\mathbb{Z}/m\mathbb{Z}\right)^{\times} \to \left(\mathbb{Z}/m\mathbb{Z}\right)^{\times}$$
$$x \mapsto x^k$$

is injective.

2. *Suppose that k and n are positive integers. In this problem, you will show that the set*

$$S = \{0, 1^k, 2^k, 3^k, \ldots, (n-1)^k\}$$

forms a complete set of residues modulo n if n is square-free and $(k, \lambda(n)) = 1$. The converse is true too, but I won't make you show that here.

   (a) *Show that the only element of S which is congruent to 0 modulo n is 0.*

   (b) *Suppose $1 \leqslant x, y \leqslant n-1$ and p is a prime factor of n. Show that if $x^k \equiv y^k \mod n$, then $x \equiv y \mod p$.*

   (c) *Conclude that S forms a complete set of residues modulo n.*

3. (a) *Suppose $f(x_1, \ldots, x_n)$ is a polynomial with integer coefficients. Show that if there exist integers $(k_1, \ldots, k_n)$ so that $f(k_1, \ldots, k_n) = 0$, then there exists a solution to $f(x_1, \ldots, x_n) \equiv 0 \mod m$ for every positive integer m. What is the contrapositive of this statement?*

   (b) *Show that there are no solutions in integers to $x^2 + y^2 = 3z^2$*

4. *Classify all right triangles whose sides have integer lengths and whose area equals its perimeter.*