Zackery Field
ID: 23031734
CS 70, Summer 2013
Homework 2
Problem 7 [12 Points]

1. [15 Points] Concerning Fermat's Little Theorem

   (a) [7 Points] Prove Fermat's Little Theorem.
   Direct Proof:
   The set of p-1 numbers $\{a * 1, a * 2, \ldots, a * (p-1)\}$for $a \in \{1, 2, \ldots, p-1\}$
   Let two numbers qa, and ra be of the form $q \equiv r(modp)$, it follows that the collection of multiples of a (from the set above) must be unique mod p, and non-zero mod p (non-zero because p is never reached and no member of the set is itself zero). Let S be the multiplication of all the set of p-1 numbers, defined as:

$$S : \{a * 1 * a * 2 * \cdots * a * (p-1)\}$$

   The product S can be rewritten as:

$$\begin{aligned} a^{p-1}(p-1)! &\equiv (p-1)!(modp) \\ a^{p-1} &\equiv 1(modp) \end{aligned}$$

   (b) [5 Points] For every positive integer not necessairly prime, let S_n be the set of integers $a \in \{1, 2, \ldots, n-1\}$ such that $GCD(a, n) = 1$. Then for every $a \in S_n$we have $a^{|S_n|} \equiv 1(modn)$.
   Direct Proof:
   The set of n-1 numbers $S_n \in \{1, 2, \ldots, n-1\}$
   Let two numbers qa, and ra be of the form $q \equiv r(modp)$, it follows that the members of the setS_n above must be unique mod n, and non-zero mod n (non-zero because n is never reached and no member of the set is itself zero). Let T be the multiplication of all the set of n-1 numbers, defined as:

$$T : \{a * 1 * a * 2 * \cdots * a * (n-1)\}$$

   The product T can be rewritten as:

$$\begin{aligned} a^{n-1}(n-1)! &\equiv (n-1)!(modn) \\ a^{n-1} &\equiv 1(modn) \\ a^{n-1} &\equiv a^{|S_n|} \equiv 1(modn) \end{aligned}$$