March 14, 2019 Homework 5 due March 28, 2019

1. Let a, b, c, and n be positive integers such that

$$\gcd(a,n) = \gcd(b,n) = \gcd(c,n) = 1.$$

If $a = qn + r$ with $0 \leq r < n$ then we shall denote r by $(a)_n$, or just by (a) if there is no ambiguity concerning n. Let $A = \{(a), (ca), (c^2a), \dots\}$ and $B = \{(b), (cb), (c^2b), \dots\}$. Show that A and B are finite sets, $|A| = |B|$, and either $A = B$, or $A \bigcap B = \emptyset$.

2. Let n be a positive integer. Denote the number of positive integers less than n and relatively prime to n by $\varphi(n)$. Let a, b be positive integers such that $\gcd(a,n) = \gcd(b,n) = 1$. Consider the set $S_a = \{(a), (ba), (b^2a), \dots\}$ (see Problem 1). Let $s = |A|$. Show that $s|\varphi(n)$.

3. Let $p > 2$ be a prime number.

   a) Find all solutions for $x^2 \equiv 1 \pmod{p}$.

   b) If $a \not\equiv 0, 1 \pmod{p}$, and $ab \equiv 1 \pmod{p}$, then $p \not| (a - b)$.

   c) $(p-1)! \equiv -1 \pmod{p}$.

4. Let p be a prime number. If $[a]_p^2 = [a]_p$, then $[a]_p = [0]_p$, or $[a]_p = [1]_p$.

5. If b is not a prime number find $x \neq 0, 1$ that solves $[x]_b^2 = [x]_b$.

6. Let n be a positive integer with no non zero square factors. Show that for each $0 < a < n$ and $1 \leq k$ one has $[a]_n^k \neq [0]_n$.