March 14, 2019 Homework 5 due March 28, 2019
Solutions

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 $0 \le r < n$ 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 $A \bigcap B = \emptyset$.

Solution. Since for $i = 1, 2, \dots$ one has $0 \le (c^i a) < n$ the set A contains at most n elements. There are indeces i and $i + j$, $j \ge 1$, so that $(c^i a) = (c^{i+j} a)$, and $c^i a(c^j - 1)$ is divisible by n. Since $\gcd(c^i a, n) = 1$ this means that $n|(c^j - 1)$ for a positive j. We denote such smallest positive integer j by s (this s is called the **multiplicative order of** a). That is $n|(c^s - 1)$, and for $1 \le j < s$ one has $n \not|(c^j - 1)$.

This yields $|A| = s$, and, since s does not depend on a, also $|B| = s$. Finally if $(c^i a) = (c^j b)$, then

$$A = \left\{(c^i a), (c^{i+1} a), \dots, (c^{i+s-1} a)\right\} = \left\{(c^j b), (c^{j+1} b), \dots, (c^{j+s-1} b)\right\} = B.$$

2. Let a, b, and n 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 $s|\varphi(n)$.

Solution. For each c such that $0 \le c < n - 1$ and $\gcd(c, n) = 1$ the set S_c contains s elements. If the number of distinct sets S_c is k, then $\varphi(n) = ks$.

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

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

   $$x^2 \equiv 1 \pmod{p} \Rightarrow p|(x^2-1) \Rightarrow p|(x-1) \text{ or } p|(x+1) \Rightarrow x = np \pm 1,\ n = 0, \pm 1, \pm 2, \dots.$$

   b) If $a \not\equiv 0, 1 \pmod{p}$, and $ab \equiv 1 \pmod{p}$, then $p \not|(a - b)$.
   Solution. If $ab \equiv 1 \pmod{p}$, and $a \equiv b \pmod{p}$, then $a^2 \equiv 1 \pmod{p}$. Due to part a) above $a \equiv 1 \pmod{p}$, or $a \equiv 0 \pmod{p}$.

   c) $(p - 1)! \equiv -1 \pmod{p}$.
   Solution. Pair each $1 \le a < p$ with its inverse.

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

Solution. If $0 \le a < p$, and $a^2 - a = pq$, then $p|a(a - 1)$, and $p|gcd(p, a)gcd(p, a - 1)$. This yields $a = 0$, or $a = 1$.

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

   Solution. Let $b = b_1 b_2$ with $gcd(b_1, b_2) = 1$, and $sb_1 + tb_2 = 1$. If $x = tb_2$, then $x^2 - x = tb_2(tb_2 - 1) = -tb_2 tb_1 = -t^2 b$.

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 $[a]_n^k \neq [0]_n$.

   Solution. Note that $n = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$, with prime p_i and $\alpha_i \geq 1$. Lack of square factors yields $\alpha_1 = \cdots = \alpha_m = 1$, and $n = p_1 \cdots p_m$. If $[a]_n^k = [0]_n$, then $n|a^k$ and $p_i|a^k$, $i = 1, \ldots, m$. This yields $p_i|a$, $i = 1, \ldots, m$, and $a = q \cdot p_1 \cdots p_m = qn$. This contradiction completes the proof.