March 28, 2019 Homework 6 due April 11, 2019
Solutions

1. Let a, n be positive integers with $gcd(a,n)=1$. Show that there is an integer k such that $a \cdot a^k \equiv 1 \pmod{n}$.

   Solution. Consider the sequence $a, a^2, \ldots, a^m, \ldots$ and write $a^m = q_m n + r_m$, $0 \le r_m < n$. Clearly elements of the sequence $r_1, r_2, \ldots, r_m, \ldots$ repeat themselves. Let $m' < m''$ be indices such that $r_{m'} = r_{m''}$. In this case $(q_{m''} - q_{m'})n = a^{m''} - a^{m'} = a^{m'}\left(a^{m''-m'} - 1\right)$. Since $gcd(a,n)=1$ one has $n|(a^{m''-m'}-1)$, or $a^{m''-m'} \equiv 1 \pmod{n}$. With $k = m''-m'-1$ the last identity becomes $a \cdot a^k \equiv 1 \pmod{n}$.

2. If $gcd(n,m)=1$, then $\varphi(n)\varphi(m) = \varphi(nm)$.

   Solution. For $0 \le a \le nm-1$, $a = q_n n + r_n$, $0 \le r_n < n$ and $a = q_m m + r_m$, $0 \le r_m < m$ the mapping $f(a) = (r_n, r_m)$ is a bijection. If $0 \le a < nm-1$, $a = q_n n + r_n$, and $a = q_m m + r_m$, then the result follows from the fact that $gcd(a, mn) = 1$ iff $gcd(r_m, m) = 1$ and $gcd(r_n, n) = 1$.

3. Show that if $n > 2$, then $\varphi(n)$ is even.

   Solution. The numbers k with $gcd(n,k)=1$ can be paired with $n-k$, and $gcd(n, n-k)) = 1$.

4. Let n be a positive integer with no square factors (except 1). Show that for each $0 < a < n$ and $1 \le k$ one has $[a]_n^k \ne [0]_n$.

   Solution. Note that $n = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$, with prime p_i and $\alpha_i \ge 1$. 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.

5. True or False? If $a|b$, then $\varphi(a)|\varphi(b)$.

   Solution. Let $b = p_1^{\alpha_1} \ldots p_n^{\alpha_n}$ and $a = p_1^{\beta_1} \ldots p_k^{\beta_n}$ be prime factorizations of b and a (rearranged as needed). Note that $k \le n$, and $1 \le \beta_i \le \alpha_i$, $i = 1, \ldots, k$, and

$$\varphi(b) = b\left(1 - \frac{1}{p_1}\right) \ldots \left(1 - \frac{1}{p_n}\right) \text{ while } \varphi(a) = a\left(1 - \frac{1}{p_1}\right) \ldots \left(1 - \frac{1}{p_k}\right).$$

6. True or False? If $b = ac$, then $\varphi(b) = \varphi(a)\varphi(c)$.

   Solution. If $b = 24$, $a = 2$, $c = 12$, then

   a) $\varphi(24) = 24\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 8$,

   b) $\varphi(2) = 2\left(1 - \dfrac{1}{2}\right) = 1$, and $\varphi(12) = 12\left(1 - \dfrac{1}{2}\right)\left(1 - \dfrac{1}{3}\right) = 4$.

7. Compute $\sum_{d|n} \varphi(d)$ for $n = 12$ and $n = 18$.

   Solution.

   a) $\sum_{d|12} \varphi(d) = \varphi(1) + \varphi(2) + \varphi(3) + \varphi(4) + \varphi(6) + \varphi(12) = 1 + 1 + 2 + 2 + 2 + 4 = 12,$

   b) $\sum_{d|18} = \varphi(d) = \varphi(1) + \varphi(2) + \varphi(3) + \varphi(6) + \varphi(9) + \varphi(18) = 1 + 1 + 2 + 2 + 6 + 6 = 18.$

8. What can be concluded based on results of Problem 7?