Steven Rosendahl
Homework 10

1. Let ϕ denote Euler's Function.

   (a) Calculate $\phi(22)$.

   $$\phi(22) = \phi(11)\phi(2) = 10 \cdot 1 = 10.$$

   (b) Does there exist $l \in \mathbb{Z}$ such that $a^{7l} \equiv a \mod 22$ for all units $a \in \mathbb{Z}_{22}$? If so, find l. Otherwise, explain why no such l exists.

   We know that we can find an l if $7l \equiv 1 \mod \phi(22)$. Since $gcd(7, 10) = 1$, there is an inverse of 7 in $\mathbb{Z}_{10}$, which is 3. Therefore, $a^{21} \equiv a \mod 22$ for all units $a \in \mathbb{Z}_{22}$.

2. Suppose that $a \in \mathbb{Z}$ is such that $gcd(a, 15) = 1$. If $gcd(k, 8) = 1$, prove that $a^{k^2} \equiv a \mod 15$.

   Suppose $gcd(k, 8) = 1$, and define the set U_8 to be the set of units in $\mathbb{Z}_8$. We want to find k^{-1} such that $k^{-1}k \equiv 1 \mod \phi(15)$, which allows us to say $a^{k^{-1}k} \equiv a \mod 15$. We know that $U_8 = \{1, 3, 5, 7\}$. Since $gcd(k, 8) = 1$, $k \in U_8$. Suppose that $k = 1$. Then $k^{-1} = 1$, so $a^{k^2} \equiv a^1 \equiv a \mod 15$. If $k = 3$, $k^{-1} = 3$, so $a^{k^2} \equiv a^9 \equiv a \mod 15$. If $k = 5$, then $k^{-1} = 5$, and $a^{k^2} \equiv a^{25} \equiv a \mod 15$. If $k = 7$, then $k^{-1} = 7$, so $a^{k^2} \equiv a^{49} \equiv a \mod 15$.

3. Let Ω denote the prime counting map and λ the Liouville function. Prove that $\lambda(x) = \lambda(y)$ if and only if $\Omega(x) \equiv \Omega(y) \mod 2$.

   $\Rightarrow$) Suppose $\lambda(x) = \lambda(y)$. We know

   $$\lambda(a) = \begin{cases} 1, & \Omega(a) \in \{2k | k \in \mathbb{Z}\} \\ -1, & \Omega(a) \in \{2k+1 | k \in \mathbb{Z}\} \end{cases}.$$

   Therefore, the only way $\lambda(x) = \lambda(y)$ is if the parity of $\Omega(x)$ is the same as the parity of $\Omega(y)$. Assume that $\Omega(x), \Omega(y) \in \{2k | k \in \mathbb{Z}\}$. Then $\Omega(x) \equiv \Omega(y) \equiv 0 \mod 2$. Assume $\Omega(x), \Omega(y) \in \{2k+1 | k \in \mathbb{Z}\}$. Then $\Omega(x) \equiv \Omega(y) \equiv 1 \mod 2$. Therefore, if $\lambda(x) = \lambda(y)$, $\Omega(x) \equiv \Omega(y) \mod 2$.

   $\Leftarrow$) Suppose that $\Omega(x) \equiv \Omega(y) \mod 2$. We know that $\lambda(a)$ is defined to be $(-1)^{\Omega(a)}$, so suppose without loss of generality that $\Omega(x), \Omega(y) \in \{2k | k \in \mathbb{Z}\}$. Then $\lambda(x) = (-1)^{2k} = 1$, and $\lambda(y) = (-1)^{2k} = 1$, so $\lambda(x) = \lambda(y)$.

4. Let $i = \sqrt{-1} \in \mathbb{C}$ and define $\rho : \mathbb{N} \to \mathbb{C}$ by $\rho(x) = i^{\Omega(x)}$. Prove that $\rho(x) = \rho(y)$ if and only if $\Omega(x) \equiv \Omega(y) \mod 4$.

   $\Rightarrow$) Suppose $\rho(x) = \rho(y)$. We know that i to a power is either $1, -1, i$, or $-i$. If $\rho(x)$ is to equal $\rho(y)$, then both must equal one of the four variations of i to a power. Suppose $\rho(x) = \rho(y) = 1$. Then $i^{\Omega(x)} = i^{\Omega(y)} = 1$, so $\Omega(x)$ and $\Omega(y)$ must be a multiple of 4. Then $\Omega(x) \equiv \Omega(y) \equiv 0 \mod 4$. If $\rho(x) = \rho(y) = -1$, then $\Omega(x)$ and $\Omega(y)$ must be a multiple of 2 but not a multiple of 4, since being a multiple of 4 would cause $\rho(x) = \rho(y) = 1$. If $\Omega(x)$ and $\Omega(y)$ are multiples of 2 and not multiples of 4, then $\Omega(x) \equiv \Omega(y) \equiv 2 \mod 4$. Suppose that $\rho(x) = \rho(y) = i$. Then $i^{\Omega(x)} = i^{\Omega(y)} = i$. We know that $\Omega(x)$ and $\Omega(y)$ must be in the set $\{4k+1 | k \in \mathbb{Z}\}$, or $\{4k+3 | k \in \mathbb{Z}\}$. Suppose $\Omega(x), \Omega(y) \in \{4k+1 | k \in \mathbb{Z}\}$. Then $i^{\Omega(x)} = i^{\Omega(y)} = i^{4k+1} = i^{4k}i = i$. In this case, we have $\Omega(x) \equiv \Omega(y) \equiv 1 \mod 4$. Finally, suppose that $\Omega(x), \Omega(y) \in \{4k+3 | k \in \mathbb{Z}\}$. Then $i^{\Omega(x)} = i^{\Omega(y)} = i^{4k+3} = i^{4k}(-i) = -i$. In this case, $\Omega(x) \equiv \Omega(y) \equiv 3 \mod 4$. Therefore, if $\rho(x) = \rho(y)$, $\Omega(x) \equiv \Omega(y) \mod 4$.

   $\Leftarrow$) Suppose $\Omega(x) \equiv \Omega(y) \mod 4$. Then $\Omega(x), \Omega(y) \in \{0, 1, 2, 3\}$. If $\Omega(y) = 0$, then $\Omega(x) = 0$, and $\rho(x) = i^0 = 1$ and $\rho(y) = i^0 = 1$, so $\rho(x) = \rho(y)$. If $\Omega(x) = \Omega(y) = 1$, then $\rho(x) = i = \rho(y)$. If $\Omega(x) = \Omega(y) = 2$, then $\rho(x) = -1 = \rho(y)$. If $\Omega(x) = \Omega(y) = 3$, then $\rho(x) = -i = \rho(y)$.

5. Suppose that $f : \mathbb{N} \to \mathbb{C}$ is a function such that $f(xy) = f(x) + f(y)$ for all $x, y \in \mathbb{N}$. If $f(p) = 1$ for all primes p, prove that $f(x) = \Omega(x)$ for all $x \in \mathbb{N}$.

   We know that we can express x and y as

$$x = p_1^{\alpha_1} p_2^{\alpha_2} + \cdots + p_n^{\alpha_n}$$
$$y = p_1^{\beta_1} p_2^{\beta_2} + \cdots + p_n^{\beta_n}.$$

   We can express $f(xy) - f(y)$ as $f(x) + f(y) - f(y) = f(x)$, and we also know

$$\begin{aligned}
f(xy) &= f(p_1^{\alpha_1+\beta_1} p_2^{\alpha_2+\beta_2} + \cdots + p_n^{\alpha_n+\beta_n}) \\
&= f(p_1^{\alpha_1}) + f(p_1^{\beta_1}) + f(p_2^{\alpha_2}) + f(p_2^{\beta_2}) + \cdots + f(p_n^{\alpha_n}) + f(p_n^{\beta_n}) \\
f(xy) - f(y) &= f(x) \\
&= f(p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}) \\
&= f(p_1^{\alpha_1}) + f(p_2^{\alpha_2}) + \cdots + f(p_n^{\alpha_n}) \\
&= \sum_{k=1}^{\alpha_1} f(p_1) + \sum_{k=1}^{\alpha_2} f(p_2) + \cdots + \sum_{k=1}^{\alpha_n} f(p_n) \\
&= \sum_{k=1}^{\alpha_1} 1 + \sum_{k=1}^{\alpha_2} 1 \cdots + \sum_{k=1}^{\alpha_n} 1 \\
&= \alpha_1 + \alpha_2 + \cdots + \alpha_n \\
&= \Omega(x)
\end{aligned}$$

6. For an ordered pair $(a, b) \in \mathbb{N} \times \mathbb{N}$ we define the *Generalized Prime Counting Map* by

$$\overline{\Omega}(a, b) = \Omega(a) - \Omega(b).$$

   If $(a, b), (c, d) \in \mathbb{N} \times \mathbb{N}$ are such that $ad = bc$, prove that $\overline{\Omega}(a, b) = \overline{\Omega}(c, d)$.

   Suppose $ad = bc$. We can write out the prime factorizations of a, b, c, and d as

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$$
$$b = p_1^{\beta_1} p_2^{\beta_2} \dots p_n^{\beta_n}$$
$$c = p_1^{\gamma_1} p_2^{\gamma_2} \dots p_n^{\gamma_n}$$
$$d = p_1^{\delta_1} p_2^{\delta_2} \dots p_n^{\delta_n}.$$

   Then

$$ad = p_1^{\alpha_1+\delta_1} p_2^{\alpha_2+\delta_2} \dots p_n^{\alpha_n+\delta_n}$$
$$bc = p_1^{\beta_1+\gamma_1} p_2^{\beta_2+\gamma_2} \dots p_n^{\beta_n+\gamma_n}.$$

   We can consider $\overline{\Omega}(ad, bc) = \Omega(ad) - \Omega(bc) = 0$. We know $\Omega(ad) - \Omega(bc) = 0$ since $ad = bc$ implies they will have the same prime factorization up to permutation, so the powers of the prime factors of ad will be equivalent to the powers of the prime factors of bc. We now have

$$\begin{aligned}
\Omega(ad) - \Omega(bc) &= (\alpha_1 + \delta_1) + (\alpha_2 + \delta_2) + \cdots + (\alpha_n + \delta_n) - (\beta_1 + \gamma_1) - (\beta_2 + \gamma_2) - \cdots - (\beta_n + \gamma_n) \\
&= (\alpha_1 + \alpha_2 + \cdots + \alpha_n) - (\beta_1 + \beta_2 + \cdots + \beta_n) + (\delta_1 + \delta_2 + \cdots + \delta_n) - (\gamma_1 + \gamma_2 + \cdots + \gamma_n) \\
&= \Omega(a) - \Omega(b) - \Omega(c) + \Omega(d) \\
&= 0.
\end{aligned}$$

   Then $\Omega(a) - \Omega(b) = \Omega(c) - \Omega(d)$, which by definition is $\overline{\Omega}(a, b) = \overline{\Omega}(c, d)$.

7. Let μ be the Möbius Function.

(a) If p and q are distinct primes, prove that $\mu(pq) = 1$.

Since μ is multiplicative, we have that $\mu(xy) = \mu(x)\mu(y)$ when $gcd(x, y) = 1$. Since p and q are distinct, we know that $\mu(pq) = \mu(p)\mu(q)$. By definition of the Möbius function, for a prime ρ we have

$$\mu(\rho) = -\sum_{\substack{d|\rho \\ d\neq\rho}} \mu(\rho) = -\mu(1) = -1,$$

so $\mu(p)\mu(q) = (-1)(-1) = 1$.

(b) If p is prime, prove that $\mu(p^2) = 0$.

From (a), we know that $\mu(\rho) = -1$ for some prime ρ. If we consider p^2, we know that the only divisors are $1, p$, and p^2. By the definition of the Möbius function, we have

$$\mu(p^2) = -\sum_{\substack{d|p^2 \\ d\neq p^2}} \mu(d) = -(\mu(1) + \mu(p)) = -1 + 1 = 0.$$

(c) If p is prime and n is a positive integer, find a formula for the value of $\mu(p^n)$. Prove your answer.

$$\mu(p^n) = \begin{cases} -1, & n = 1 \\ 0, & n > 1 \end{cases}$$

Consider the value of $\mu(p^n)$. We have already shown that $\mu(p) = -1$ for any prime p and that $\mu(p^2) = 0$ for any prime. We can suppose that $\mu(p^n) = 0$ for $n \geq 2$, and $\mu(p^n) = -1$ for $n = 1$. We want to show that $\mu(p^{n+1}) = 0$ for $n \geq 2$. Then

$$\begin{aligned} \mu(p^{n+1}) &= -\sum_{\substack{d|p^{n+1} \\ d\neq p^{n+1}}} \mu(d) \\ &= -(\mu(1) + \mu(p) + \mu(p^2) + \mu(p^3) + \cdots + \mu(p^n)) \\ &= -(1 + (-1) + 0 + 0 + \cdots + 0) \text{ by the inductive hypothesis} \\ &= -(0 + 0 + 0 + \cdots + 0) \\ &= -0 \\ &= 0. \end{aligned}$$