Steven Rosendahl
Homework 9

1. Directly calculate $\sum_{d|12} \phi(d)$ and verify that you obtain 12 as your answer.

$$\begin{aligned}\sum_{d|12} \phi(d) &= \phi(1) + \phi(2) + \phi(3) + \phi(4) + \phi(6) + \phi(12)\\ &= 1 + 1 + 2 + 2 + 2 + 4\\ &= 12\end{aligned}$$

2. Suppose that $p_1, p_2, \ldots, p_N$ are distinct primes. Prove that

$$\frac{\phi(p_1p_2 \ldots p_N)}{p_1p_2 \ldots p_N} = \prod_{n=1}^{N} \left(1 - \frac{1}{p_n}\right)$$

$$\begin{aligned}\frac{\phi(p_1p_2 \ldots p_N)}{p_1p_2 \ldots p_N} &= \frac{\phi(p_1)\phi(p_2) \ldots \phi(p_N)}{p_1p_2 \ldots p_N}\\ &= \prod_{n=1}^{N} \frac{\phi(p_n)}{p_n}\\ &= \prod_{n=1}^{N} \frac{p_n - 1}{p_n}\\ &= \prod_{n=1}^{N} \left(1 - \frac{1}{p_n}\right)\end{aligned}$$

3. Find a value of n such that $\phi(n)/n < 1/4$. What do you think is a good strategy for choosing n so that $\phi(n)/n$ is close to zero?

   One value for which this holds true is $n = 210$. $\phi(210)$ is 48, and $48/210 = 8/35 < 1/4$. One strategy for finding these numbers would be to pick values for which $\phi(n)$ is small but has many unique prime factors.

4. Suppose that p is prime and m and n are non-negative integers.

   (a) Prove that $\phi(p^{m+n}) \geq \phi(p^m)\phi(p^n)$.

   We can consider $\phi(p^{m+n})$. If we let $m+n = j$, then we have $\phi(p^j)$, which can be expressed as $p^j - p^{j-1}$. If we consider $\phi(p^m)\phi(p^n)$, we have

$$\begin{aligned}\phi(p^m)\phi(p^n) &= (p^m - p^{m-1})(p^n - p^{n-1})\\ &= p^{m+n} - 2p^{m+n-1} + p^{m+n-2}\\ &= p^j - 2p^{j-1} + p^{j-2}.\end{aligned}$$

   If we compare the two values, we get

$$\begin{aligned}p^j - p^{j-1} &\overset{?}{\geq} p^j - 2p^{j-1} + p^{j-2}\\ p^{j-1} &\geq p^{j-2}.\end{aligned}$$

   We know this is true since $m, n > 0$, so $j > 0$.

   (b) Under what additional assumptions on m and n do we obtain $\phi(p^{m+n}) = \phi(p^m)\phi(p^n)$?

   If either m or n, but not both m and n are zero, then we have $\phi(p^{m+0}) = \phi(p^m)\phi(p^0) = \phi(p^m)$ or $\phi(p^{0+n}) = \phi(p^0)\phi(p^n) = \phi(p^n)$.

5. Suppose that a and b are positive integers.

   (a) Prove that $\phi(ab) \geq \phi(a)\phi(b)$.

   Suppose that a and b are not relatively prime and consider the product $\phi(a)\phi(b)$. Then

$$\begin{aligned}
\phi(a)\phi(b) &< \phi(p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r})\phi(p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r}) \\
&= \phi(p_1^{\alpha_1})\phi(p_2^{\alpha_2}) \dots \phi(p_r^{\alpha_r})\phi(p_1^{\beta_1})\phi(p_2^{\beta_2})\phi(p_r^{\beta_r}) \\
&= \prod_{i=1}^{r} \left(p_i^{\alpha_i} - p_i^{\alpha_i - 1}\right) \prod_{i=1}^{r} \left(p_i^{\beta_i} - p_i^{\beta_i - 1}\right) \\
&= \prod_{i=1}^{r} p_i^{\alpha_i} \left(1 - \frac{1}{p_i}\right) \prod_{i=1}^{r} p_i^{\beta_i} \left(1 - \frac{1}{p_i}\right) \\
&= ab \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)^2 .
\end{aligned}$$

   We can also consider the function $\phi(ab)$.

$$\begin{aligned}
\phi(ab) &= \phi(p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r} p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r}) \\
&= \phi(p_1^{\alpha_1+\beta_1} p_2^{\alpha_2+\beta_2} \dots p_r^{\alpha_r+\beta_r}) \\
&= \phi(p_1^{\alpha_1+\beta_1})\phi(p_2^{\alpha_2+\beta_2}) \dots \phi(p_r^{\alpha_r+\beta_r}) \\
&= \prod_{i=1}^{r} p_i^{\alpha_i+\beta_i} - p_i^{\alpha_i+\beta_i} \frac{1}{p} \\
&= \prod_{i=1}^{r} p_i^{\alpha_i+\beta_i} \left(1 - \frac{1}{p_i}\right) \\
&= ab \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).
\end{aligned}$$

   Since

$$\phi(ab) = ab \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) > ab \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)^2 > \phi(a)\phi(b),$$

   we have

$$\phi(ab) > \phi(a)\phi(b).$$

   If $gcd(a, b) = 1$, then we can say $\phi(ab) = \phi(a)\phi(b)$. Therefore $\phi(ab) \geq \phi(a)\phi(b)$.

   (b) Prove that $\phi(ab) = \phi(a)\phi(b)$ if and only if $gcd(a, b) = 1$.

   $\Rightarrow$) Suppose $\phi(ab) = \phi(a)\phi(b)$ implies $gcd(a, b) > 1$. We know from (a) that when a and b are not relatively prime, $\phi(ab) > \phi(a)\phi(b)$, which is a direct contradiction to $\phi(ab) = \phi(a)\phi(b)$. Therefore $\phi(ab) = \phi(a)\phi(b)$ implies $gcd(a, b) = 1$.

   $\Leftarrow$) Suppose $gcd(a, b) = 1$. Then a and b are relatively prime, so $\phi(ab) = \phi(a)\phi(b)$ by the theorem.

6. Suppose that n is a positive integer and k is any integer.

   (a) Prove that $gcd(n, k) = 1$ if and only if $gcd(n, n - k) = 1$.

   $\Leftarrow$) Suppose that $gcd(n, k) > 1$. Then $gcd(n, k) = q$, so $q \mid n$ and $q \mid k$, $n = qa$ and $k = qb$ for some $a, b \in \mathbb{Z}$. Then $n - k = pa - pb = p(a - b)$, so $p \mid n - k$, which implies that $gcd(n, n-k) > 1$. Therefore, by contrapositive, $gcd(n, k) = 1$ implies $gcd(n, n-k) = 1$.

   $\Rightarrow$) Suppose $gcd(n, n - k) > 1$. Then there exists $p \in \mathbb{Z}$ such that $p \mid n$ and $p \mid k$. Then $n = pa$ and $k = pb$ for some $a, b \in \mathbb{Z}$. We can express $n - k = pa - pb = p(a - b)$, so $p \mid (n - k)$ and $p \mid n$, and $gcd(n, n - k) > 1$.

(b) Prove that $\phi(n)$ is an even integer for all $n \geq 3$.

By definition, the totient function counts the number of units in $\mathbb{Z}_n$. Suppose that $n \geq 3$. If we take any element k from $\mathbb{Z}_n$, we know by (a) that if k is relatively prime to n, then $n-k$ is relatively prime to n. Therefore, if k is a unit in $\mathbb{Z}_n$, then $n-k$ is also a unit in $\mathbb{Z}_n$. If n is odd, then we know that there will not be any situation where $n-k=k$, since that would imply that $n=2k$, or n is even which is a contradiction. Then for every unit k in $\mathbb{Z}_n$, we can find another unit $n-k$ also in $\mathbb{Z}_n$, which means there are an even number of units in $\mathbb{Z}_n$, so $\phi(n) \in \{2j \mid j \in \mathbb{Z}\}$ when n is odd. If n is even, however, there may be a unit k in $\mathbb{Z}_n$ such that $k=n-k$. If this is the case, then this unit will be the same as $n/2$. Since it is a unit, then $gcd(n/2, n) = 1$. We saw that n was even, so we can say $n = 2l,\ l \in \mathbb{Z}$. Then $gcd(2l/2, 2l) = gcd(l, 2l) \neq 1$, so there cannot be a unit k in an even $\mathbb{Z}_n$ such that $k = n-k$.

7. If n is a positive integer prove that $\phi(n) = 2$ if and only if $n \in \{3, 4, 6\}$.

$\Rightarrow$) Suppose $\phi(n) = 2$ and let $k \in \mathbb{Z} > 2$ and $l \in \mathbb{Z} > 1$. We want to consider the case where $n = 2^k 3^l$, so $\phi(n) = \phi(2^k 3^l) = (2^k - 2^{k-1})(3^l - 3^{l-1})$. This can be further simplified to $2^k(1/2)3^l(2/3) = 2^k 3^l(1/3) > 2$ for $l > 1$ and $k > 2$. Therefore we only have $\{1, 2, 3, 4, 6, 12\}$ to consider. Since $\phi(1) = \phi(2) = 1$ and $\phi(12) = 4$, we can eliminate those values. However, $\phi(3) = \phi(4) = \phi(6) = 2$, so $\phi(n) = 2$ when $n \in \{3, 4, 6\}$.

$\Leftarrow$) Suppose $n \in \{3, 4, 6\}$. Then $\phi(3) = 2$, $\phi(4) = 2$, and $\phi(6) = 2$.