Math 113, Summer 2015 Prof. Haiman

**Notes on Euler's function $\phi(n)$**

For each positive integer $n$, Euler's function $\phi(n)$ is defined to be the number of positive integers $k$ less than $n$ which are relatively prime to $n$.

For example, of the positive integers less than 12, four are relatively prime to 12, namely 1, 5, 7, and 11. Therefore $\phi(12) = 4$.

The purpose of these notes is to discuss some properties of $\phi(n)$. The same topics are covered in Section 1.9 of Goodman's book, but I prefer a different and I think somewhat simpler approach.

Before reading these notes, you will need to read Sections 1.6 and 1.7 of Goodman. I will use the same notation as he does for congruence, residue classes, and the system $\mathbb{Z}_n$ of residue classes, with its operations of addition and multiplication modulo $n$. We will make use of the Chinese Remainder Theorem, which is Proposition 1.7.9 in Goodman.

## 1. Multiplicative inverses in $\mathbb{Z}_n$

Recall that each residue class $[a]$ in $\mathbb{Z}_n$ has a unique representative with $a$ in the range $0 \le a < n$. We will begin by showing that the classes $[a]$ which have a multiplicative inverse in $\mathbb{Z}_n$ are exactly those for which $a$ is relatively prime to $n$ (this is Proposition 1.9.9 in Goodman).

First, suppose $a$ is relatively prime to $n$. Since $a$ and $n$ are relatively prime, there are integers $s$ and $t$ such that $1 = sa + tn$. Then $sa \equiv 1 \pmod{n}$, which means $[s][a] = [1]$ in $\mathbb{Z}_n$, so $[s]$ is the required inverse.

For the converse, suppose $a$ is not relatively prime to $n$. Let $d = \gcd(n, a)$. Then $d > 1$, so $l = n/d$ is a positive integer less than $n$, and therefore $[l] \neq [0]$ in $\mathbb{Z}_n$. Now $la = n(a/d)$ is a multiple of $n$, since $d$ divides $a$, so $[l][a] = [0]$ in $\mathbb{Z}_n$. If $[a]$ had a multiplicative inverse $[b]$ we could multiply on both sides by $[b]$ to get $[l] = [0]$ in $\mathbb{Z}_n$, a contradiction.

I will use the notation $\mathbb{Z}_n^\times$ for the set of residue classes $[a]$ in $\mathbb{Z}_n$ which have multiplicative inverses. We have just seen that $\mathbb{Z}_n^\times$ consists of those classes $[a]$ for which $a$ is relatively prime to $n$. The cardinality of the set $\mathbb{Z}_n^\times$ is therefore equal to the number of integers $a$ in the range $0 \le a < n$ which are relatively prime to $n$. But 0 is not relatively prime to $n$ (why not?), so the cardinality of $\mathbb{Z}_n^\times$ is the number of positive integers less than $n$ which are relatively prime to $n$. In other words, $\phi(n) = |\mathbb{Z}_n^\times|$. This fact is the reason why the function $\phi(n)$ is important.

## 2. A formula for $\phi(n)$

*Theorem.* Let the prime factorization of $n$ be $n = p_1^{e_1} \cdots p_k^{e_k}$. Then

$$\phi(n) = \prod_{i=1}^{k} p_i^{e_i - 1}(p_i - 1) \tag{1}$$

Example: the prime factorization of 12 is $2^2 \cdot 3$. According the formula in the theorem, we have $\phi(n) = 2^1(2-1) \cdot 3^0(3-1) = 4$, in agreement with what we found before.

We will prove (1) in two steps. First, we will show that $\phi(n) = p^{e-1}(p-1)$ if $n = p^e$ is a power of a prime.

Second, we will use the Chinese Remainder Theorem to show that if $m$ and $n$ are relatively prime, then $\phi(mn) = \phi(m)\phi(n)$. This implies (by induction on $k$) that if $m_1, \ldots, m_k$ are pairwise relatively prime, then $\phi(m_1 \cdots m_k) = \phi(m_1) \cdots \phi(m_k)$.

Formula (1) will then follow, because if $n = p_1^{e_1} \cdots p_k^{e_k}$, then the factors $m_i = p_i^{e_i}$ are pairwise relatively prime, and $\phi(m_i) = \phi(p_i^{e_i}) = p_i^{e_i-1}(p_i - 1)$.

Now let us consider the case $n = p^e$. Since $p$ is the only prime factor of $n$, a number $a$ is relatively prime to $n$ if and only if $p$ does not divide $a$. There are $p^e$ integers $a$ in the range $0 \le a < p^e$. Of these, $p^{e-1}$ are multiples of $p$, namely the numbers $rp$ for $0 \le r < p^{e-1}$. This leaves $p^e - p^{e-1} = p^{e-1}(p-1)$ integers $0 \le a < n$ relatively prime to $n$, and they are all positive, since $a = 0$ was one of those excluded. This shows that $\phi(n) = p^{e-1}(p-1)$.

It remains to show that if $m$ and $n$ are relatively prime, then $\phi(mn) = \phi(m)\phi(n)$. An integer $x$ is relatively prime to both $m$ and $n$ if and only if $x$ has no prime factor in common with either $m$ or $n$, if and only if $x$ has no prime factor in common with $mn$. So $x$ is relatively prime to both $m$ and $n$ if and only if $x$ is relatively prime to $mn$ (this much is true even if $m$ and $n$ are not relatively prime).

Since we are dealing with more than one modulus at the same time, I will write $[x]_m$, $[x]_n$, or $[x]_{mn}$ to distinguish between residue classes in $\mathbb{Z}_m$, $\mathbb{Z}_n$, or $\mathbb{Z}_{mn}$. Since $m$ and $n$ are relatively prime, the Chinese Remainder Theorem gives a one-to-one correspondence between residue classes $[x]_{mn}$ in $\mathbb{Z}_{mn}$ and pairs $([a]_m, [b]_n)$, with $[a]_m \in \mathbb{Z}_m$ and $[b]_n \in \mathbb{Z}_n$. In the direction from $\mathbb{Z}_{mn}$ to $\mathbb{Z}_m \times \mathbb{Z}_n$, the correspondence simply sends $[x]_{mn}$ to $([x]_m, [x]_n)$.

We have just seen that $x$ is relatively prime to $mn$ if and only if it is relatively prime to both $m$ and $n$. Therefore, in the correspondence given by the Chinese Remainder Theorem, $\mathbb{Z}_{mn}^\times$ corresponds to $\mathbb{Z}_m^\times \times \mathbb{Z}_n^\times$. This shows that $|\mathbb{Z}_{mn}^\times| = |\mathbb{Z}_m^\times| \cdot |\mathbb{Z}_n^\times|$, so $\phi(mn) = \phi(m)\phi(n)$. $\square$

The theorem above is equivalent to Goodman, Proposition 1.9.18(a), although Goodman expresses the formula a bit differently. Goodman's Proposition 1.9.18(b) is what we proved in the second part of the proof given above.

## 3. Euler's theorem

*Theorem.* If $a$ is relatively prime to $n$, then $a^{\phi(n)} \equiv 1 \pmod{n}$.

This is Theorem 1.9.20 in Goodman. He outlines a fairly complicated proof in the exercises to Section 1.9. At the end of Section 1.10 he goes on to explain how it can be deduced more easily from a general theorem of group theory. I will just add a few comments on the explanation Goodman gives in 1.10.

Goodman uses the notation $\Phi(n)$ for the set of residue classes in $\mathbb{Z}_n$ which have multiplicative inverses, which I denoted $\mathbb{Z}_n^\times$. We have seen that this is also the set of classes of integers relatively prime to $n$, and therefore that $|\mathbb{Z}_n^\times| = \phi(n)$.

Now if $[a]$ and $[b]$ in $\mathbb{Z}_n$ have multiplicative inverses, then $[b]^{-1}[a]^{-1}$ is an inverse of $[a][b]$, as you can check. This shows that the subset $\mathbb{Z}_n^\times$ is closed under the operation of multiplication in $\mathbb{Z}_n$. It also contains the multiplicative identity $[1]$ (which is its own inverse). Multiplication is associative in $\mathbb{Z}_n$ and therefore also in $\mathbb{Z}_n^\times$. Therefore, since in $\mathbb{Z}_n^\times$ we have the identity and inverses, $\mathbb{Z}_n^\times$ is a group with the operation of multiplication (this is Goodman, Lemma 1.10.3).

Now we invoke the general theorem (Goodman, Theorem 2.5.6, which we will prove later) that every element $a$ in a finite group of cardinality $g$ satisfies $a^g = e$, where $e$ is the identity element. When the group is $\mathbb{Z}_n^\times$, this becomes $[a]^{\phi(n)} = [1]$, which is another way of writing Euler's theorem.