Lecture 11: the Euler ϕ-function

In the light of the previous lecture, we shall now look in more detail at the function defined there. Let $n \geq 1$ be a natural number. Recall that we defined $\phi(n)$ to be the number of natural numbers $1 \leq m \leq n$ and coprime to n. This function is called *Euler's ϕ-function.*

For example, let's calculate $\phi(12)$. The numbers $1, 5, 7, 11$ are all the numbers that are less than 12 and coprime with it. We deduce that $\phi(12) = 4$.

We shall prove two important theorems about this function. Here is the first. Another proof of this theorem will follow once we have proved the Chinese Remainder Theorem.

Theorem 0.1. *If* $\gcd(a, b) = 1$ *then* $\phi(ab) = \phi(a)\phi(b)$.

Proof. Let $1 \leq a' \leq a$ and $\gcd(a', a) = 1$: there are $\phi(a)$ such numbers. Let $1 \leq b' \leq b$ and $\gcd(b', b) = 1$: there are $\phi(b)$ such numbers. Think in terms of fractions $\frac{a'}{a}$ and $\frac{b'}{b}$. If we add them together we get $\frac{a'b+ab'}{ab}$. Consider the number $a'b + ab'$. I claim that it is coprime to ab. To see what let $p \mid ab$ and $p \mid a'b + ab'$. By Gauss's lemma, since a and b are coprime we have that $p \mid a$ or $p \mid b$. Suppose the former, without loss of generality. Then it is easy to see that this implies that $p \mid a'b$. Now a' and a are coprime and so this implies that $p \mid b$. But this contradicts the fact that a and b are coprime.

Put $f_{a',b'} = r$ where r is the remainder when $a'b + ab'$ is divided by ab. Thus $a'b + ab' = qab + r$ where $0 \leq r < ab$. I claim that $\gcd(r, ab) = 1$. But this follows immediately from the argument behind Eulcid's algorithm.

We now show that if $f_{a',b'} = f_{a'',b''}$ then $a' = a''$ and $b' = b''$. Our assumption implies that

$$(a' - a'')b + (b' - b'')a = sab$$

where s is an integer. We see now that a must divide $(a' - a'')b$ but a and b are coprime and so a divides $a' - a''$. But this can only happen if $a' = a''$. Similarly, $b' = b''$.

We have therefore shown that

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

To prove the reverse inequality, let $1 \leq c \leq ab$ where $\gcd(c, ab) = 1$. Since a and b are coprime, we may find x and y integers such that $1 = ax + by$. Thus $c = a(cx) + b(cy)$. Put $b' \equiv cx \pmod{b}$ and $a' \equiv cy \pmod{a}$. It is easy to check that $c \equiv ab' + a'b \pmod{ab}$. Also $\gcd(a', a) = 1$ and $\gcd(b', b) = 1$. This proves the reverse inequality. $\square$

Functions $f\colon \mathbb{N}\backslash\{0\} \to \mathbb{C}$ are called *arithmetic functions*. Such functions play an important role in mathematics. An arithmetic function is said to be *multiplicative* if $\gcd(a,b)=1$ implies $f(ab)=f(a)f(b)$. Thus the above theorem shows that ϕ is multiplicative. Let's see why this is a desirable property. By the Fundamental Theorem of Arithmetic, the number n has a prime factorization

$$p = p_1^{e_1}\dots p_m^{e_m}$$

where the p_i are distinct primes. Since distinct prime powers are coprime we have that

$$\phi(n) = \phi(p_1^{e_1})\dots\phi(p_m^{e_m}).$$

Thus calculating $\phi(n)$ reduces to calculating ϕ of a power of a prime.

Lemma 0.2. *If p is a prime, and $n = p^e$ then*

$$\phi(n) = p^e - p^{e-1} = n(1-\frac{1}{p}).$$

Proof. How many non-zero natural numbers are there less than or equal to p^e? The answer is p^e. Which numbers are less than or equal to p^e and *not* coprime to p^e. It will be all those numbers $1 \leq m \leq p^e$ such that $p \mid m$. There are p^{e-1} such numbers and so the number of numbers less than or equal to p^e and coprime to it is $p^e - p^{e-1}$. □

Combining this result with our theorem above we have the following.

Theorem 0.3.

$$\phi(n) = n\prod_{p|n}(1-\frac{1}{p})$$

where the product is taken over all distinct prime divisors of n.

We now come to our second main theorem. Before we state and prove we shall motivate it by means of an example. Let's take $n = 12$ and we consider all the fraction with numerators between 1 and 12

$$\frac{1}{12},\frac{2}{12},\frac{3}{12},\frac{4}{12},\frac{5}{12},\frac{6}{12},\frac{7}{12},\frac{8}{12},\frac{9}{12},\frac{10}{12},\frac{11}{12},\frac{12}{12}.$$

Now write these fractions in their lowest terms

$$\frac{1}{12},\frac{1}{6},\frac{1}{4},\frac{1}{3},\frac{5}{12},\frac{1}{2},\frac{7}{12},\frac{2}{3},\frac{3}{4},\frac{5}{6},\frac{11}{12},\frac{1}{1}.$$

Now partition this set of fractions according to their denominators

$$\frac{1}{1},$$

$$\frac{1}{2},$$

$$\frac{1}{3}, \frac{2}{3},$$
$$\frac{1}{4}, \frac{3}{4},$$
$$\frac{1}{6}, \frac{5}{6},$$
$$\frac{1}{12}, \frac{5}{12}, \frac{7}{12}, \frac{11}{12}.$$

We had 12 fractions originally and we haven't lost any and so

$$12 = 1 + 1 + 2 + 2 + 2 + 4$$

since we have a partition. Now observe that $\phi(12) =$ and $\phi(6) = 2$ and $\phi(4) = 2$ and $\phi(3) = 2$ and $\phi(2) = 1$ and $\phi(1) = 1$ and that the denominators are all the divisors of 12.

Theorem 0.4.

$$\sum_{d|n} \phi(d) = n$$

where the sum is taken over all divisors of n.

Proof. There are n fractions $\frac{m}{n}$ where $1 \leq m \leq n$. Write each such fraction in its lowest terms and denote the set of n fractions that arises by X. The set X has n elements. Thus we write

$$\frac{m}{n} = \frac{m'}{n'}$$

where $\gcd(m', n') = 1$. Let $d = \gcd(m, n)$. Then $n = dn'$ and $m = dm'$. It follows that $n' \mid n$.

On the other hand if $n' \mid n$ and $\frac{m'}{n'}$ is a fraction in its lowest terms and $\frac{dm'}{n}$, where $n = dn'$, is one of our original fractions.

It follows that the set X consists of all fractions in their lowest terms whose denominators divide n. we may therefore partition the set X according to the denominators to get a set of blocks; each block consists of all the fractions in their lowest terms over a fixed denominators d and there are $\phi(d)$ of those.

The result is now clear. $\square$