TW 314 Lecture 29 (We 26 Apr 2017)

The Euler Phi Function

For a positive integer m, let $\mathbb{Z}_m^*$ denote the set of integers a with $0 < a < m$ such that a is relatively prime to m.

Clearly, $\mathbb{Z}_m^* = \mathbb{Z}_m - \{0\} = \{1, 2, \ldots, m-1\}$ if and only if m is prime. By Theorem 4 (and the fact that $\gcd(m,a) = 1$ and $\gcd(m,b) = 1$ implies $\gcd(m, ab) = 1$) we have that ...

Theorem 5 For a positive integer m, $(\mathbb{Z}_m^*, \cdot)$ is an abelian group, where $\cdot$ is modulo m multiplication.

The **Euler phi function** is defined by

$\phi(m)$ = the number of positive integers less than m that are relatively prime to m, that is

$$\phi(m) = |\mathbb{Z}_m^*|.$$

Clearly, if p is prime, then $\phi(p) = p - 1$.

Example: Since $\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$, $\phi(12) = 4$.

Our next task is to find an explicit formula for $\phi(m)$. We need the following basic result.

Lemma 6 If m and n are relatively prime, then $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$ if and only if $a \equiv b \pmod{mn}$.

Proof: Prove this as an exercise.

Proposition 7 If m and n are relatively prime, then $\phi(mn) = \phi(m)\phi(n)$.

Proof: Define the function $f: \mathbb{Z}_{mn}^* \to \mathbb{Z}_m^* \times \mathbb{Z}_n^*$ by $f(a) = (a \pmod{m}, a \pmod{n})$.

We show that f is a bijection, for then $\phi(mn) = |\mathbb{Z}_{mn}^*| = |\mathbb{Z}_m^*| \times |\mathbb{Z}_n^*| = \phi(m)\phi(n)$.

f is an injection: Suppose $f(a) = f(b)$.

Then $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$.
Therefore $a \equiv b \pmod{mn}$, that is, $a = b$ in $\mathbb{Z}_{mn}^*$.

f is a surjection: Suppose $a \in \mathbb{Z}_m^*$ and $b \in \mathbb{Z}_n^*$, that is, $\gcd(m,a) = 1$ and $\gcd(n,b) = 1$. To show that there exists an $x \in \mathbb{Z}_{mn}^*$ such that $f(x) = (a,b)$, we need to show that there exists a solution to the equations

$$x \equiv a \pmod{m} \quad \text{—①}$$
$$x \equiv b \pmod{n} \quad \text{—②}$$

By ①, $x = a + km$ for some integer k, and then by ②, $b \equiv a + km \pmod{n}$. Let $k = t + ln$ for integers t and l. Then $x = a + mt + lmn$, and therefore $x \equiv a + mt \pmod{mn}$. It follows that $x \in \mathbb{Z}_{mn}^*$ and x satisfies equations ① and ②.

■