Math 580/780I Notes 7

Euler's Theorem and Wilson's Theorem:

- Definition and Notation. For a positive integer n, we define $\phi(n)$ to be the number of positive integers $\le n$ which are relatively prime to n. The function ϕ is called Euler's ϕ-function.

- **Examples.** $\phi(1) = 1$, $\phi(2) = 1$, $\phi(3) = 2$, $\phi(4) = 2$, $\phi(p) = p - 1$ for every prime p, and $\phi(pq) = (p-1)(q-1)$ for all primes p and q

- **Theorem 12 (Euler).** *For every positive integer n and every integer a relatively prime to n, we have $a^{\phi(n)} \equiv 1 \pmod{n}$.*

- **Proof:** If $n = 1$, the result is clear. We suppose as we may then that $n > 1$. Let $a_1, a_2, \dots, a_{\phi(n)}$ be the $\phi(n)$ positive integers $\le n$ relatively prime to n. Consider the numbers

$$a_1 a, a_2 a, \dots, a_{\phi(n)} a. \qquad (*)$$

Note that no two numbers in $(*)$ are congruent modulo n since $(a, n) = 1$ and $a_i a \equiv a_j a \pmod{n}$ implies $a_i \equiv a_j \pmod{n}$ so that $i = j$. Now, fix $j \in \{1, 2, \dots, \phi(n)\}$. There are integers q and r such that $a_j a = nq + r$ and $0 \le r < n$. Since $(a_j a, n) = 1$ and $n > 1$, we obtain $r \ne 0$ and $(r, n) = 1$. Thus, $r = a_k$ for some $k \in \{1, 2, \dots, \phi(n)\}$. Hence, for each $j \in \{1, 2, \dots, \phi(n)\}$, there is a $k \in \{1, 2, \dots, \phi(n)\}$ for which $a_j a \equiv a_k \pmod{n}$. Since the numbers $a_j a$ are distinct modulo n, we deduce that the numbers in $(*)$ are precisely $a_1, a_2, \dots, a_{\phi(n)}$ in some order. Therefore,

$$a_1 a_2 \cdots a_{\phi(n)} \equiv (a_1 a)(a_2 a) \cdots (a_{\phi(n)} a) \equiv a^{\phi(n)} a_1 a_2 \cdots a_{\phi(n)} \pmod{n}.$$

Since $\gcd(a_1 a_2 \cdots a_{\phi(n)}, n) = 1$, we obtain $a^{\phi(n)} \equiv 1 \pmod{n}$ as desired.

- **Theorem 13 (Wilson).** *For every prime p, $(p-1)! \equiv -1 \pmod{p}$.*

- **Proof:** If $p = 2$, the result is clear. We consider now the case $p > 2$. Let $S = \{1, 2, \dots, p-1\}$. For every $a \in S$, there is a unique $a' \in S$ satisfying $a'a \equiv 1 \pmod{p}$. If $a = 1$ or $a = p-1$, then $a' = a$. The converse statement also holds since $a' = a$ implies $(a-1)(a+1) = a^2 - 1$ is divisible by p so that $a \equiv 1 \pmod{p}$ or $a \equiv p - 1 \pmod{p}$. The remaining elements of S can be grouped in $(p-3)/2$ pairs (a, a'), say $(a_1, a_1'), \dots, (a_{(p-3)/2}, a'_{(p-3)/2})$, so that

$$(p-1)! \equiv 1 \times (p-1) \times (a_1 a_1') \cdots (a_{(p-3)/2} a'_{(p-3)/2}) \equiv 1 \times (p-1) \equiv -1 \pmod{p}.$$

- **Comment:** The converse of Wilson's Theorem also holds.

Homework:

(1) Calculate $\phi(12)$ and $\phi(18)$.

(2) Given that $\phi(825) = 400$, what is the remainder when $2^{10012010}$ is divided by 825?

(3) Let p be a prime. Explain why $(p-2)! \equiv 1 \pmod{p}$.

(4) Show that $a^{18} \equiv 1 \pmod{756}$ for every integer a which is relatively prime to 756. (Note that $\phi(756) = 216$ is significantly larger than 18.)