MATH 433

Applied Algebra

Lecture 6:
Euler's totient function.
Public key systems.

Finite multiplicative order

$\mathbb{Z}_n$: the set of all congruence classes modulo n.
G_n: the set of all invertible congruence classes modulo n.

Theorem A nonzero congruence class $[a]_n$ is invertible if and only if $\gcd(a, n) = 1$.

A congruence class $[a]_n$ has **finite order** if $[a]_n^k = [1]_n$ for some integer $k \geq 1$. The smallest k with this property is called the **order of** $[a]_n$. We also say that k is the **order of** a **modulo** n.

Theorem A congruence class $[a]_n$ has finite order if and only if it is invertible.

Proposition Let k be the order of an integer a modulo n. Then $a^s \equiv 1 \bmod n$ if and only if s is a multiple of k.

Proof: If $s = kt$, where $t \in \mathbb{Z}$, then

$$[a]_n^s = ([a]_n^k)^t = [1]_n^t = [1]_n.$$

Conversely, let $[a]_n^s = [1]_n$. We have $s = kq + r$, where q is the quotient and r is the remainder of s by k. Then

$$[a]^r = [a]^{s-kq} = [a]^s([a]^k)^{-q} = [1].$$

Since $0 \leq r < k$, it follows that $r = 0$.

Fermat's Little Theorem Let p be a prime number. Then $a^{p-1} \equiv 1 \bmod p$ for every integer a not divisible by p.

Euler's Theorem Let $n \geq 2$ and $\phi(n)$ be the number of elements in G_n. Then $a^{\phi(n)} \equiv 1 \bmod n$ for every integer a coprime with n.

Corollary Let a be an integer coprime with an integer $n \geq 2$. Then the order of a modulo n is a divisor of $\phi(n)$.