MATH 433

Applied Algebra

Lecture 11:
Euler's phi-function.

Order of a congruence class

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, i.e., if $\gcd(a, n) = 1$.

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.

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.

Corollary Let a be an integer not divisible by a prime number p. Then the order of a modulo p is a divisor of $p - 1$.

Euler's Theorem

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

Theorem (Euler) 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 $\phi(n)$.

Proof of Euler's Theorem

Proof: Let $[b_1], [b_2], \ldots, [b_m]$ be the list of all elements of G_n. Note that $m = \phi(n)$. Consider another list:

$$[a][b_1], [a][b_2], \ldots, [a][b_m].$$

Since $\gcd(a, n) = 1$, the congruence class $[a]_n$ is in G_n as well. Hence the second list also consists of elements from G_n. Also, all elements in the second list are distinct as

$$[a][b] = [a][b'] \implies [a]^{-1}[a][b] = [a]^{-1}[a][b'] \implies [b] = [b'].$$

It follows that the second list consists of the same elements as the first (arranged in a different way). Therefore

$$[a][b_1] \cdot [a][b_2] \cdots [a][b_m] = [b_1] \cdot [b_2] \cdots [b_m].$$

Hence $[a]^m X = X$, where $X = [b_1] \cdot [b_2] \cdots [b_m]$.
Note that $X \in G_n$ since G_n is closed under multiplication.
That is, X is invertible. Then $[a]^m XX^{-1} = XX^{-1}$
$\implies [a]^m[1] = [1] \implies [a^m] = [1]$. Recall that $m = \phi(n)$.

Euler's phi function

The number of elements in G_n, the set of invertible congruence classes modulo n, is denoted $\phi(n)$. In other words, $\phi(n)$ counts how many of the numbers $1, 2, \ldots, n$ are coprime with n. $\phi(n)$ is called **Euler's ϕ-function** or **Euler's totient function**.

Proposition 1 If p is prime, then $\phi(p^s) = p^s - p^{s-1}$.

Proposition 2 If $\gcd(m, n) = 1$, then $\phi(mn) = \phi(m)\,\phi(n)$.

Theorem Let $n = p_1^{s_1} p_2^{s_2} \ldots p_k^{s_k}$, where $p_1, p_2, \ldots, p_k$ are distinct primes and $s_1, \ldots, s_k$ are positive integers. Then

$$\phi(n) = p_1^{s_1-1}(p_1 - 1)p_2^{s_2-1}(p_2 - 1)\ldots p_k^{s_k-1}(p_k - 1).$$

Sketch of the proof: The proof is by induction on k. The base of induction is Proposition 1. The induction step relies on Proposition 2.

Proposition If $\gcd(m,n) = 1$, then $\phi(mn) = \phi(m)\,\phi(n)$.

Proof: Let $\mathbb{Z}_m \times \mathbb{Z}_n$ denote the set of all pairs (X, Y) such that $X \in \mathbb{Z}_m$ and $Y \in \mathbb{Z}_n$. We define a function $f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ by the formula $f([a]_{mn}) = ([a]_m, [a]_n)$. Since m and n divide mn, this function is well defined (does not depend on the choice of the representative a). Since $\gcd(m,n) = 1$, the Chinese Remainder Theorem implies that this function establishes a one-to-one correspondence between the sets $\mathbb{Z}_{mn}$ and $\mathbb{Z}_m \times \mathbb{Z}_n$.

Furthermore, an integer a is coprime with mn if and only if it is coprime with m and with n. Therefore the function f also establishes a one-to-one correspondence between G_{mn} and $G_m \times G_n$, the latter being the set of pairs (X, Y) such that $X \in G_m$ and $Y \in G_n$. It follows that the sets G_{mn} and $G_m \times G_n$ consist of the same number of elements. Thus $\phi(mn) = \phi(m)\,\phi(n)$.

Examples. $\phi(11) = 10$,
$\phi(25) = \phi(5^2) = 5 \cdot 4 = 20$,
$\phi(27) = \phi(3^3) = 3^2 \cdot 2 = 18$,
$\phi(100) = \phi(2^2 \cdot 5^2) = \phi(2^2)\,\phi(5^2) = 2 \cdot 20 = 40$,
$\phi(1001) = \phi(7 \cdot 11 \cdot 13) = \phi(7)\,\phi(11)\,\phi(13)$
$\quad = 6 \cdot 10 \cdot 12 = 720.$

Problem. Determine the last two digits of 3^{2019}.

The last two digits form the remainder under division by 100. Since $\phi(100) = 40$, we have

$$3^{40} \equiv 1 \bmod 100.$$

Then $[3^{2019}] = [3]^{2019} = [3]^{40\cdot 50+19} = ([3]^{40})^{50}\,[3]^{19}$
$= [3]^{19} = ([3]^7)^3([3]^2)^{-1} = [2187]^3[9]^{-1} = [-13]^3[-11]$
$= [169][143] = [67]$. Hence $3^{2019} = \ldots 67$.