MATH 433

Applied Algebra

Lecture 11:
Euler's Theorem.
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 1 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.

Proposition 2 Let k be the order of an integer a modulo n. Then $a^s \equiv a^t \bmod n$ if and only if $s \equiv t \bmod k$.

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.

Proof: Consider two lists of congruence classes modulo p:

$$[1], [2], \ldots, [p-1] \text{ and } [a][1], [a][2], \ldots, [a][p-1].$$

The first one is the list of all elements of G_p. Since a is not a multiple of p, it's class $[a]$ is in G_p as well. It follows that all elements in the second list are from G_p. Also, all elements in the second list are distinct as

$$[a][n] = [a][m] \implies [a]^{-1}[a][n] = [a]^{-1}[a][m] \implies [n] = [m].$$

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

$$[a][1] \cdot [a][2] \cdots [a][p-1] = [1] \cdot [2] \cdots [p-1].$$

Hence $[a]^{p-1}X = X$, where $X = [1] \cdot [2] \cdots [p-1]$.
Note that $X \in G_p$ since G_p is closed under multiplication.
That is, X is invertible. Then $[a]^{p-1}XX^{-1} = XX^{-1}$
$\implies [a]^{p-1}[1] = [1] \implies [a^{p-1}] = [1]$.

Corollary 1 Let p be a prime number. Then $a^p \equiv a \mod p$ for every integer a (that is, $a^p - a$ is a multiple of p).

Corollary 2 Let a be an integer not divisible by a prime number p. Then the order of a modulo p is a divisor of $p - 1$.

Proof: By Fermat's Little Theorem, $a^{p-1} \equiv 1 \mod p$. According to a previously proved proposition, the order of a modulo p divides any positive integer s such that $a^s \equiv 1 \mod p$.

Problem. Find the remainder of 12^{50} after division by 17.

Since 17 is prime and 12 is not a multiple of 17, we have $[12]_{17}^{16} = [1]_{17}$. Then $[12^{50}] = [12]^{50} = [12]^{3\cdot 16+2}$ $= ([12]^{16})^3 \cdot [12]^2 = [12]^2 = [-5]^2 = [25] = [8]$. Hence the remainder is 8.

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**.

Problem. Compute $\phi(100)$.

Since $100 = 2^2 \cdot 5^2$, an integer k is coprime with 100 if and only if it is not divisible by 2 or 5. Among integers from 1 to 100, there are $50 = 100/2$ even numbers and $20 = 100/5$ numbers divisible by 5. Note that some of them are divisible by both 2 and 5. These are exactly numbers divisible by 10. There are $10 = 100/10$ such numbers. We conclude that $\phi(100) = 100 - 50 - 20 + 10 = 40$.

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 $Y \in G_n$. In other words, $f(G_{mn}) = G_m \times G_n$. 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. $\phi(11) = 10$,
$\phi(25) = \phi(5^2) = 5 \cdot 4 = 20$,
$\phi(27) = \phi(3^3) = 3^2 \cdot 2 = 18$,
$\phi(100) = \phi(2^2 \cdot 5^2) = \phi(2^2)\,\phi(5^2) = 2 \cdot 20 = 40$,
$\phi(1001) = \phi(7 \cdot 11 \cdot 13) = (7-1)(11-1)(13-1) = 720$,
$\phi(2023) = \phi(7 \cdot 17^2) = (7-1)(17^2 - 17) = 1632$.

Problem. Determine the last two digits of 3^{2023}.

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

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

Then $[3^{2023}] = [3]^{2023} = [3]^{40 \cdot 50 + 23} = ([3]^{40})^{50}\,[3]^{23} = [3]^{23}$
$= ([3]^5)^4\,[3]^3 = [243]^4\,[3]^3 = [43]^4\,[3]^3 = [(50-7)^2]^2\,[3]^3$
$= [7^2]^2\,[3]^3 = [49]^2\,[3]^3 = [(50-1)^2]\,[3]^3 = [1^2]\,[3]^3 = [27]$.

Thus $3^{2023} = \ldots 27$.