

MATH 433

Applied Algebra

Lecture 10:

Order of a congruence class.

Fermat's Little Theorem.

Powers of a congruence class

Let $[a] \in \mathbb{Z}_n$ be a congruence class modulo n . The powers $[a]^k$, $k = 1, 2, \dots$ are defined inductively: $[a]^1 = [a]$ and $[a]^k = [a]^{k-1}[a]$ for $k > 1$.

Theorem 1 $[a]^{k+m} = [a]^k[a]^m$ and $[a]^{km} = ([a]^k)^m$ for all $k, m \geq 1$.

In the case when $[a]$ is invertible, we also let $[a]^0 = [1]$ and $[a]^{-k} = ([a]^{-1})^k$ for each $k \geq 1$.

Theorem 2 If $[a]$ is invertible, then $[a]^{k+m} = [a]^k[a]^m$ and $[a]^{km} = ([a]^k)^m$ for all $k, m \in \mathbb{Z}$.

Finite multiplicative order

A congruence class $[a]_n$ is said to have **finite (multiplicative) order** if $[a]_n^k = [1]_n$ for some positive integer k . 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., a is coprime with n).

Proof: If $[a]_n$ has finite order k , then $[1]_n = [a]_n^k = [a]_n [a]_n^{k-1}$, which implies that $[a]_n^{-1} = [a]_n^{k-1}$.

Conversely, suppose that $[a]_n$ is invertible. Since the set \mathbb{Z}_n is finite, the sequence $[a]_n, [a]_n^2, [a]_n^3, \dots$ contains repetitions. Hence for some integers $0 < r < s$ we will have

$$[a]_n^r = [a]_n^s \implies [a]_n^r [a]_n^{-r} = [a]_n^s [a]_n^{-r} \implies [1]_n = [a]_n^{s-r}.$$

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

Proof: If $s = k\ell$, where $\ell \in \mathbb{Z}$, then

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

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 $r = 0$.

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

Proof: If $s \equiv t \pmod{k}$, then $s - t = \ell k$, $\ell \in \mathbb{Z}$. It follows that $[a^s] = [a]^s = [a]^{t+\ell k} = [a]^t([a]^k)^\ell = [a]^t[1]^\ell = [a]^t = [a^t]$.

Conversely, if $[a^s] = [a^t]$, then

$$[a]^{s-t} = [a]^s[a]^{-t} = [a]^s([a]^t)^{-1} = [a^s][a^t]^{-1} = [1].$$

By Proposition 1, $s - t$ is a multiple of k .

Examples. • $G_7 = \{[1], [2], [3], [4], [5], [6]\}$.

$$[1]^1 = [1],$$

$$[2]^2 = [4], [2]^3 = [8] = [1],$$

$$[3]^2 = [9] = [2], [3]^3 = [2][3] = [6], [3]^4 = [2]^2 = [4],$$

$$[3]^5 = [4][3] = [5], [3]^6 = [3][5] = [1].$$

$$[4]^2 = [16] = [2], [4]^3 = [4][2] = [1].$$

$$[5]^2 = [25] = [4], [5]^3 = [4][5] = [-1], [5]^4 = [-1][5] = [2],$$

$$[5]^5 = [2][5] = [3], [5]^6 = [3][5] = [1].$$

$$[6]^2 = [-1]^2 = [1].$$

Thus $[1]$ has order 1, $[6]$ has order 2, $[2]$ and $[4]$ have order 3, and $[3]$ and $[5]$ have order 6.

• $G_{12} = \{[1], [5], [7], [11]\}$.

$$[1]^1 = [1], [5]^2 = [25] = [1], [7]^2 = [-5]^2 = [25] = [1],$$

$$[11]^2 = [-1]^2 = [1].$$

Thus $[1]$ has order 1 while $[5]$, $[7]$, and $[11]$ have order 2.

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

Proof: Consider two lists of congruence classes modulo p :

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

The first one is the list of all elements of G_p . Since a is not a multiple of p , its class $[a]$ is in G_p as well. Hence the second list also consists of elements 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 $a^p \equiv a \pmod{p}$ 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, $a^{p-1} \equiv 1 \pmod{p}$. According to a previously proved proposition, the order of a modulo p divides any positive integer s such that $a^s \equiv 1 \pmod{p}$.

Problem. Find the remainder of 12^{50} under 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.