MATH 433

Applied Algebra

Lecture 5:
Chinese remainder theorem.
Fermat's little theorem.
Euler's theorem.

Congruence classes

Given an integer a, the **congruence class of** a **modulo** n is the set of all integers congruent to a modulo n: $[a]_n = \{a + nk : k \in \mathbb{Z}\}$.

The set of all congruence classes modulo n is denoted $\mathbb{Z}_n$.

The arithmetic operations on $\mathbb{Z}_n$ are defined as follows. For any integers a and b, we let

$$[a]_n + [b]_n = [a + b]_n,$$
$$[a]_n - [b]_n = [a - b]_n,$$
$$[a]_n \times [b]_n = [ab]_n.$$

Invertible congruence classes

We say that a congruence class $[a]_n$ is **invertible** (or the integer a is **invertible modulo** n) if there exists a congruence class $[b]_n$ such that $[a]_n[b]_n = [1]_n$. If this is the case, then $[b]_n$ is called the **inverse** of $[a]_n$ and denoted $[a]_n^{-1}$.

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

The set of all invertible congruence classes in $\mathbb{Z}_n$ is denoted G_n or $\mathbb{Z}_n^*$. This set is closed under multiplication.

Chinese Remainder Theorem

Theorem Let $n, m \geq 2$ be relatively prime integers and a, b be any integers. Then the system of congruences

$$\begin{cases} x \equiv a \mod n, \\ x \equiv b \mod m, \end{cases}$$

has a solution. Moreover, this solution is unique modulo nm.

Proof: Since $\gcd(n, m) = 1$, we have $sn + tm = 1$ for some integers s, t. Let $c = bsn + atm$. It is easy to check that c is a solution. Also, any element of $[c]_{nm}$ is a solution. Conversely, if x is a solution, then $n|(x - c)$ and $m|(x - c)$, which implies that $nm|(x - c)$, i.e., $x \in [c]_{nm}$.

Corollary Let $n_1, n_2, \dots, n_k \geq 2$ be pairwise coprime integers and $a_1, a_2, \dots, a_k$ be any integers. Then the system of congruences $x \equiv a_i \mod n_i$, $1 \leq i \leq k$, has a solution which is unique modulo $n_1 n_2 \dots n_k$.

Problem. Solve simultaneous congruences

$$\begin{cases} x \equiv 3 \bmod 12, \\ x \equiv 2 \bmod 29. \end{cases}$$

The moduli 12 and 29 are coprime. First we use the Euclidean algorithm to represent 1 as an integral linear combination of 12 and 29:

$$\left(\begin{array}{cc|c} 1 & 0 & 12 \\ 0 & 1 & 29 \end{array}\right) \to \left(\begin{array}{cc|c} 1 & 0 & 12 \\ -2 & 1 & 5 \end{array}\right) \to \left(\begin{array}{cc|c} 5 & -2 & 2 \\ -2 & 1 & 5 \end{array}\right)$$

$$\to \left(\begin{array}{cc|c} 5 & -2 & 2 \\ -12 & 5 & 1 \end{array}\right) \to \left(\begin{array}{cc|c} 29 & -12 & 0 \\ -12 & 5 & 1 \end{array}\right).$$

Hence $(-12) \cdot 12 + 5 \cdot 29 = 1$. Let $x_1 = 5 \cdot 29 = 145$, $x_2 = (-12) \cdot 12 = -144$. Then

$$\begin{cases} x_1 \equiv 1 \bmod 12, \\ x_1 \equiv 0 \bmod 29. \end{cases} \qquad \begin{cases} x_2 \equiv 0 \bmod 12, \\ x_2 \equiv 1 \bmod 29. \end{cases}$$

It follows that one solution is $x = 3x_1 + 2x_2 = 147$. The other solutions form the congruence class of 147 modulo $12 \cdot 29 = 348$.

Problem. Solve simultaneous congruences

$$\begin{cases} x \equiv 1 \bmod 3, \\ x \equiv 2 \bmod 4, \\ x \equiv 3 \bmod 5. \end{cases}$$

First we solve the first two congruences. Let $x_1 = 4$, $x_2 = -3$. Then $x_1 \equiv 1 \bmod 3$, $x_2 \equiv 0 \bmod 3$, $x_1 \equiv 0 \bmod 4$, $x_2 \equiv 1 \bmod 4$. It follows that $x_1 + 2x_2 = -2$ is a solution. The general solution is $x \equiv -2 \bmod 12$.

Now it remains to solve the system

$$\begin{cases} x \equiv -2 \bmod 12, \\ x \equiv 3 \bmod 5. \end{cases}$$

We need to represent 1 as an integral linear combination of 12 and 5: $1 = (-2) \cdot 12 + 5 \cdot 5$. Then a particular solution is $x = 3 \cdot (-2) \cdot 12 + (-2) \cdot 5 \cdot 5 = -122$. The general solution is $x \equiv -122 \bmod 60$, which is the same as $x \equiv -2 \bmod 60$.

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 $[a]_n, [a]_n^2, [a]_n^3, \ldots$ contains repetitions. Hence for some integers $0 < r < s$ we will have

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

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 $a^{p-1} \equiv 1 \bmod p$ 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, it's 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 $a^p \equiv a \mod p$ 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: Let k be the order of a modulo p. We have $p-1 = kq + r$, where q is the quotient and r is the remainder of $p-1$ by k. By Fermat's little theorem, $[a]^{p-1} = [1]$. Then $[a]^r = [a]^{p-1-kq} = [a]^{p-1}([a]^k)^{-q} = [1]$. Since $0 \leq r < k$, it follows that $r = 0$.

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.

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.

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 $[a]^m X X^{-1} = X X^{-1}$
$\implies [a]^m[1] = [1] \implies [a^m] = [1]$. Recall that $m = \phi(n)$.