MATH 433

Applied Algebra

Lecture 7:
Modular arithmetic.
Invertible congruence classes.

Congruence classes

Given an integer a, the **congruence class of** a **modulo** n is the set of all integers congruent to a modulo n.

Notation. $[a]_n$ or simply $[a]$. Also denoted $a + n\mathbb{Z}$ as $[a]_n = \{a + nk : k \in \mathbb{Z}\}$.

For any integers a and b, the congruence classes $[a]_n$ and $[b]_n$ either coincide, or else they are disjoint.

The set of all congruence classes modulo n is denoted $\mathbb{Z}_n$. It consists of n elements $[0]_n, [1]_n, [2]_n, \dots, [n-1]_n$, which form a partition of the set $\mathbb{Z}$.

Modular arithmetic

Modular arithmetic is an arithmetic on the set $\mathbb{Z}_n$ for some $n \geq 1$. The arithmetic operations on $\mathbb{Z}_n$ are defined as follows. For any integers a and b, we let

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

Theorem The arithmetic operations on $\mathbb{Z}_n$ are well defined, namely, they do not depend on the choice of representatives a, b for the congruence classes.

Proof: Let a' be another representative of $[a]_n$ and b' be another representative of $[b]_n$. Then $a' \equiv a \bmod n$ and $b' \equiv b \bmod n$. According to a previously proved proposition, this implies $a' + b' \equiv a + b \bmod n$, $a' - b' \equiv a - b \bmod n$ and $a'b' \equiv ab \bmod n$. In other words, $[a' + b']_n = [a + b]_n$, $[a' - b']_n = [a - b]_n$ and $[a'b']_n = [ab]_n$.

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 $[a]_n^{-1}$. Also, we say that b is the (multiplicative) **inverse of** a **modulo** n.

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

A nonzero congruence class $[a]_n$ is called a **zero-divisor** if $[a]_n[b]_n = [0]_n$ for some $[b]_n \neq [0]_n$.

Examples. • In $\mathbb{Z}_6$, the congruence classes $[1]_6$ and $[5]_6$ are invertible since $[1]_n^2 = [5]_6^2 = [1]_6$. The classes $[2]_6$, $[3]_6$, and $[4]_6$ are zero-divisors since $[2]_6[3]_6 = [4]_6[3]_6 = [0]_6$.

• In $\mathbb{Z}_7$, all nonzero congruence classes are invertible since $[1]_7^2 = [2]_7[4]_7 = [3]_7[5]_7 = [6]_7^2 = [1]_7$.

Properties of invertible congruence classes

Theorem **(i)** If $[a]_n$ is invertible, then $[a]_n^{-1}$ is also invertible and $([a]_n^{-1})^{-1} = [a]_n$.
(ii) The inverse $[a]_n^{-1}$ is always unique.
(iii) If $[a]_n$ and $[b]_n$ are invertible, then the product $[a]_n[b]_n$ is also invertible and $([a]_n[b]_n)^{-1} = [a]_n^{-1}[b]_n^{-1}$.
(iv) Zero-divisors are not invertible.

Proof: **(i)** Let $[b]_n = [a]_n^{-1}$. Then $[b]_n[a]_n = [a]_n[b]_n = [1]_n$, which means that $[a]_n = [b]_n^{-1}$.

(ii) Suppose that $[b]_n$ and $[b']_n$ are both inverses of $[a]_n$. Then $[b]_n = [b]_n[1]_n = [b]_n[a]_n[b']_n = [1]_n[b']_n = [b']_n$.

(iii) We only need to show that $([a]_n[b]_n)([a]_n^{-1}[b]_n^{-1}) = [1]_n$. Indeed, $([a]_n[b]_n)([a]_n^{-1}[b]_n^{-1}) = [a]_n[a]_n^{-1}\cdot[b]_n[b]_n^{-1} = [1]_n[1]_n = [1]_n$.

(iv) If $[a]_n$ is invertible and $[a]_n[b]_n = [0]_n$, then $[b]_n = [1]_n[b]_n = [a]_n^{-1}[a]_n[b]_n = [a]_n^{-1}[0]_n = [0]_n$.
Therefore $[a]_n$ cannot be a zero-divisor.

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

Proof: Let $d = \gcd(a, n)$. If $d > 1$ then n/d and a/d are integers, $[n/d]_n \neq [0]_n$, and $[a]_n[n/d]_n =$ $= [an/d]_n = [a/d]_n[n]_n = [a/d]_n[0]_n = [0]_n$. Hence $[a]_n$ is a zero-divisor.

Now consider the case $\gcd(a, n) = 1$. In this case 1 is an integral linear combination of a and n: $ma + kn = 1$ for some $m, k \in \mathbb{Z}$. Then
$[1]_n = [ma + kn]_n = [ma]_n = [m]_n[a]_n$.
Thus $[a]_n$ is invertible and $[a]_n^{-1} = [m]_n$.

Problem. Find the inverse of 23 modulo 107.

Numbers 23 and 107 are coprime (they are actually prime). We use the matrix method to represent 1 as an integral linear combination of these numbers.

$$\left(\begin{array}{cc|c} 1 & 0 & 107 \\ 0 & 1 & 23 \end{array}\right) \to \left(\begin{array}{cc|c} 1 & -4 & 15 \\ 0 & 1 & 23 \end{array}\right) \to \left(\begin{array}{rr|c} 1 & -4 & 15 \\ -1 & 5 & 8 \end{array}\right)$$
$$\to \left(\begin{array}{rr|c} 2 & -9 & 7 \\ -1 & 5 & 8 \end{array}\right) \to \left(\begin{array}{rr|c} 2 & -9 & 7 \\ -3 & 14 & 1 \end{array}\right) \to \left(\begin{array}{rr|c} 23 & -107 & 0 \\ -3 & 14 & 1 \end{array}\right)$$

From the 2nd row of the last matrix we read off that $(-3) \cdot 107 + 14 \cdot 23 = 1$. It follows that

$[1]_{107} = [(-3) \cdot 107 + 14 \cdot 23]_{107} = [14 \cdot 23]_{107} = [14]_{107}[23]_{107}$.

Thus $[23]_{107}^{-1} = [14]_{107}$.