MATH 433

Applied Algebra

Lecture 4:
Modular arithmetic (continued).
Linear congruences.

Congruences

Let n be a postive integer. The integers a and b are called **congruent modulo** n if they have the same remainder when divided by n. An equivalent condition is that n divides the difference $a - b$.

Notation. $a \equiv b \bmod n$ or $a \equiv b \pmod{n}$.

Examples. $12 \equiv 4 \bmod 8$, $24 \equiv 0 \bmod 6$, $31 \equiv -4 \bmod 35$.

Proposition 1 If $a \equiv b \bmod n$ then for any integer c,
(i) $a + cn \equiv b \bmod n$;
(ii) $a + c \equiv b + c \bmod n$;
(iii) $ac \equiv bc \bmod n$.

Proposition 2 Let $a, b, c, n \in \mathbb{Z}$, $n > 0$.
(i) If $ac \equiv bc \bmod n$ and $\gcd(c, n) = 1$, then $a \equiv b \bmod n$.
(ii) If $c > 0$ and $ac \equiv bc \bmod nc$, then $a \equiv b \bmod n$.

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 $[a]_n = \{a + nk : k \in \mathbb{Z}\}$.

Examples. $[0]_2$ is the set of even integers, $[1]_2$ is the set of odd integers, $[2]_4$ is the set of even integers not divisible by 4.

If n divides a positive integer m, then every congruence class modulo n is the union of m/n congruence classes modulo m. For example, $[2]_4 = [2]_8 \cup [6]_8$.

The congruence class $[0]_n$ is called the **zero congruence class**. It consists of the integers divisible by n.

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

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

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

We need to check that these operations are well defined, namely, they do not depend on the choice of representatives a, b for the congruence classes.

Proposition If $a \equiv a' \mod n$ and $b \equiv b' \mod n$, then **(i)** $a+b \equiv a'+b' \mod n$; **(ii)** $a-b \equiv a'-b' \mod n$; **(iii)** $ab \equiv a'b' \mod n$.

Proof: Since n divides $a-a'$ and $b-b'$, it also divides $(a+b)-(a'+b') = (a-a')+(b-b')$, $(a-b)-(a'-b') = = (a-a')-(b-b')$, and $ab - a'b' = a(b-b')+(a-a')b'$.

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 $[a]_n^{-1}$.

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 $[1]_7^2 = [2]_7[4]_7 = [3]_7[5]_7 = [6]_7^2 = [1]_7$.

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

Proof: **(i)** Suppose that $[b]_n$ and $[b']_n$ are inverses of $[a]_n$. Then $[b]_n = [b]_n[1]_n = [b]_n[a]_n[b']_n = [1]_n[b']_n = [b']_n$.

(ii) $([a]_n[b]_n)([a]_n^{-1}[b]_n^{-1}) = [a]_n[a]_n^{-1} \cdot [b]_n[b]_n^{-1}$
$= [1]_n[1]_n = [1]_n$.

(iii) is a reformulation of the first part of **(ii)**.

(iv) If $[a]_n$ is invertible and $[a]_n[b]_n = [0]_n$, then
$[b]_n = [1]_n[b]_n = [a]_n^{-1}[a]_n[b]_n = [a]_n^{-1}[0]_n = [0]_n$.

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.

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

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

Hence $(-3) \cdot 107 + 14 \cdot 23 = 1$. It follows that

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

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

Linear congruences

Linear congruence is a congruence of the form $ax \equiv b \bmod n$, where x is an integer variable. We can regard it as a linear equation in $\mathbb{Z}_n$: $[a]_n X = [b]_n$.

Theorem The linear congruence $ax \equiv b \bmod n$ has a solution if and only if $d = \gcd(a, n)$ divides b. If this is the case then the solution set consists of d congruence classes modulo n that form a single congruence class modulo n/d.

Proof: If x is a solution then $ax = b + kn$ for some $k \in \mathbb{Z}$. Hence $b = ax - kn$, which is divisible by $\gcd(a, n)$.

Conversely, assume that d divides b. Then the linear congruence is equivalent to $a'x \equiv b' \bmod m$, where $a' = a/d$, $b' = b/d$ and $m = n/d$. In other words, $[a']_m X = [b']_m$. Now $\gcd(a', m) = \gcd(a/d, n/d) = \gcd(a, n)/d = 1$. Hence $[a']_m$ is invertible. Then the solution set is $X = [a']_m^{-1}[b']_m$, a congruence class modulo n/d.

Problem 1. Solve the congruence
$12x \equiv 6 \bmod 21.$

$\iff 4x \equiv 2 \bmod 7 \iff 2x \equiv 1 \bmod 7$
$\iff [x]_7 = [2]_7^{-1} = [4]_7$
$\iff [x]_{21} = [4]_{21}$ or $[11]_{21}$ or $[18]_{21}$.

Problem 2. Solve the congruence
$23x \equiv 6 \bmod 107.$

The numbers 23 and 107 are coprime. We already know that $[23]_{107}^{-1} = [14]_{107}$.
Hence $[x]_{107} = [23]_{107}^{-1}[6]_{107} = [14]_{107}[6]_{107} = [84]_{107}$.