MATH 433

Applied Algebra

Lecture 8:
Linear congruences.

Modular arithmetic

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 $\mathbb{Z}_n$. It consists of n elements.

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 is 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 a **multiplicative inverse of a modulo n**.

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.

Linear congruences

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

In the case $b = 1$, solving the linear congruence is equivalent to finding the inverse of the congruence class $[a]_n$. In the case $b = 0$, it is equivalent to determining if $[a]_n$ is a zero-divisor.

Theorem If the congruence class $[a]_n$ is invertible, then the equation $[a]_n X = [b]_n$ has a unique solution in $\mathbb{Z}_n$, which is $X = [a]_n^{-1}[b]_n$.

Proof: Suppose $X \in \mathbb{Z}_n$ is a solution of the equation. Then $[a]_n^{-1}([a]_n X) = [a]_n^{-1}[b]_n$. We have

$$[a]_n^{-1}([a]_n X) = ([a]_n^{-1}[a]_n)X = [1]_n X = X.$$

Conversely, if $X = [a]_n^{-1}[b]_n$, then

$$[a]_n X = [a]_n([a]_n^{-1}[b]_n) = ([a]_n[a]_n^{-1})[b]_n = [1]_n[b]_n = [b]_n.$$

Problem 1. Solve the congruence
$23x \equiv 6 \bmod 107$.

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

Problem 2. Solve the congruence $3x \equiv 5 \bmod 15$.

The congruence has no solutions. Indeed, $3x - 5 \equiv 1 \bmod 3$ so that $3x - 5$ is never divisible by 3. As a consequence, $3x - 5$ is not divisible by 15.

Problem 3. Solve the congruence $3x \equiv 6 \bmod 15$.

Checking all 15 elements of $\mathbb{Z}_{15}$, we find solutions:
$x \equiv 2 \bmod 15$, $x \equiv 7 \bmod 15$, and $x \equiv 12 \bmod 15$.
Equivalently, x is a solution if and only if $x \equiv 2 \bmod 5$.

More properties of congruences

Proposition 1 Let $a, b \in \mathbb{Z}$ and $c, n \in \mathbb{P}$. Then the congruence $ac \equiv bc \mod nc$ is equivalent to $a \equiv b \mod n$.

Indeed, $ac \equiv bc \mod nc$ means that $\dfrac{ac - bc}{nc}$ is an integer while $a \equiv b \mod n$ means that $\dfrac{a - b}{n}$ is an integer.

Proposition 2 Let $a, b \in \mathbb{Z}$ and $c, n \in \mathbb{P}$. If $ac \equiv bc \mod n$ and $\gcd(c, n) = 1$, then $a \equiv b \mod n$.

Indeed, $ac \equiv bc \mod n$ means that $ac - bc = (a - b)c$ is divisible by n. Since $\gcd(c, n) = 1$, it follows that $a - b$ is divisible by n.

Theorem The linear congruence $ax \equiv b \mod n$ 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 the congruence has a solution x, 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 $a'x \equiv b' \mod m$, where $a' = a/d$, $b' = b/d$ and $m = n/d$. In other words, $[a']_m X = [b']_m$, where $X = [x]_m$.

We have $\gcd(a', m) = \gcd(a/d, n/d) = \gcd(a, n)/d = 1$. Hence the congruence class $[a']_m$ is invertible. By a previously proved theorem, all solutions x of the linear congruence form a single congruence class modulo m, $X = [a']_m^{-1}[b']_m$. This congruence class splits into d distinct congruence classes modulo $n = md$.

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

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

Problem. Find all integer solutions of the equation $12x - 21y = 6$.

For any integer solution of the equation, the number x is a solution of the linear congruence $12x \equiv 6 \bmod 21$. By the above, $x \equiv 4 \bmod 7$, that is, $x = 4 + 7k$ for some $k \in \mathbb{Z}$. Then $y = (12x - 6)/21 = (12(4 + 7k) - 6)/21 = 2 + 4k$, which is also integer. Thus the general integer solution is $x = 4 + 7k$, $y = 2 + 4k$, where $k \in \mathbb{Z}$.