

MATH 433  
Applied Algebra

**Lecture 9:**  
**Chinese Remainder Theorem.**

## Linear congruences

**Linear congruence** is a congruence of the form  $ax \equiv b \pmod{n}$ , where  $x$  is an integer variable.

We can regard it as a linear equation in  $\mathbb{Z}_n$ :

$$[a]_n X = [b]_n, \text{ where } X = [x]_n.$$

**Theorem 1** 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  $X = [a]_n^{-1} [b]_n$ .

**Theorem 2** The linear congruence  $ax \equiv b \pmod{n}$  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  $n$ .

## Chinese Remainder Theorem

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

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

of congruences 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  $c = bsn + atm$ . Then

$$\begin{aligned} c &= bsn + a(1 - sn) = a + (b - a)sn \equiv a \pmod{n}, \\ c &= b(1 - tm) + atm = b + (a - b)tm \equiv b \pmod{m}. \end{aligned}$$

Therefore  $c$  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.,  $x \in [c]_{nm}$ .

**Problem.** Solve simultaneous congruences  $\begin{cases} x \equiv 3 \pmod{12}, \\ x \equiv 2 \pmod{29}. \end{cases}$

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:

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

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

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

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 a system of congruences 
$$\begin{cases} x \equiv 3 \pmod{12}, \\ x \equiv 2 \pmod{10}. \end{cases}$$

The system has no solutions. Indeed, any solution of the first congruence must be an odd number while any solution of the second congruence must be an even number.

**Problem.** Solve a system of congruences 
$$\begin{cases} x \equiv 6 \pmod{12}, \\ x \equiv 2 \pmod{10}. \end{cases}$$

The general solution of the first congruence is  $x = 6 + 12y$ , where  $y$  is an arbitrary integer. Substituting this into the second congruence, we obtain  $6 + 12y \equiv 2 \pmod{10} \iff 12y \equiv -4 \pmod{10} \iff 6y \equiv -2 \pmod{5} \iff y \equiv 3 \pmod{5}$ . Thus  $y = 3 + 5k$ , where  $k$  is an arbitrary integer. Then  $x = 6 + 12y = 6 + 12(3 + 5k) = 42 + 60k$  or, equivalently,  $x \equiv 42 \pmod{60}$ .

Note that the solution is unique modulo 60, which is the least common multiple of 12 and 10.

## Chinese Remainder Theorem (generalized)

**Theorem** 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

$$\begin{cases} x \equiv a_1 \pmod{n_1}, \\ x \equiv a_2 \pmod{n_2}, \\ \dots\dots\dots \\ x \equiv a_k \pmod{n_k} \end{cases}$$

has a solution which is unique modulo  $n_1 n_2 \dots n_k$ .

*Idea of the proof:* The theorem is proved by induction on  $k$ . The base case  $k = 1$  is trivial. The induction step uses the usual Chinese Remainder Theorem.

**Problem.** Solve simultaneous congruences

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

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

Now it remains to solve the system

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

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  $x \equiv -122 \pmod{60}$ , which is the same as  $x \equiv -2 \pmod{60}$ .

**Problem.** Solve a system of congruences

$$\begin{cases} 2x \equiv 3 \pmod{15}, \\ x \equiv 2 \pmod{31}. \end{cases}$$

We begin with solving the first linear congruence. Since  $\gcd(2, 15) = 1$ , all solutions form a single congruence class modulo 15. Namely,  $x$  is a solution if  $[x]_{15} = [2]_{15}^{-1}[3]_{15}$ . We find that  $[2]_{15}^{-1} = [8]_{15}$ . Hence  $[x]_{15} = [8]_{15}[3]_{15} = [24]_{15} = [9]_{15}$ . Equivalently,  $x \equiv 9 \pmod{15}$ .

Now the original system is reduced to

$$\begin{cases} x \equiv 9 \pmod{15}, \\ x \equiv 2 \pmod{31}. \end{cases}$$

Next we represent 1 as an integral linear combination of 15 and 31:  $1 = (-2) \cdot 15 + 31$ . It follows that one solution to the system is  $x = 2 \cdot (-2) \cdot 15 + 9 \cdot 31 = 219$ . All solutions form the congruence class of 219 modulo  $15 \cdot 31 = 465$ .