Lecture 9: Congruences

Wednesday, October 22, 2014
8:00 AM

In the previous lecture we defined

$$\mathbb{Z}_n := \{ n\mathbb{Z}, n\mathbb{Z}+1, \dots, n\mathbb{Z}+(n-1)\}.$$

For any integer $\underline{a}$ let $[a]_n := n\mathbb{Z}+a$.

<u>Lemma</u>. The following properties are equivalent:

(i) $[a]_n = [b]_n$.

(ii) $[a]_n \cap [b]_n \neq \emptyset$.

(iii) $a \overset{n}{\equiv} b$.

In particular for any $x \in [a]_n$ we have $[x]_n = [a]_n$.

<u>Def.</u> An element of $[a]_n$ is called a <u>representative</u> of $[a]_n$.

<u>Lemma</u>. $\begin{cases} [a]_n + [b]_n := [a+b]_n \\ [a]_n \cdot [b]_n := [a \cdot b]_n \end{cases}$

are well-defined; i.e. it does NOT depend on the choice of representatives a and b.

<u>Pf.</u> $[a_1]_n = [a_2]_n \Rightarrow \left. a_1 \overset{n}{\equiv} a_2 \right\} \Rightarrow \left\{ a_1+b_1 \overset{n}{\equiv} a_2+b_2 \right.$

Pf. $[a_1]_n = [a_2]_n \Rightarrow a_1 \overset{n}{\equiv} a_2$, $[b_1]_n = [b_2]_n \Rightarrow b_1 \overset{n}{\equiv} b_2$ $\Rightarrow \begin{cases} a_1+b_1 \overset{n}{\equiv} a_2+b_2 \\ a_1 \cdot b_1 \overset{n}{\equiv} a_2 \cdot b_2 \end{cases}$

$$\Rightarrow \begin{cases} [a_1+b_1]_n = [a_2+b_2]_n \\ [a_1 b_1]_n = [a_2 b_2]_n . \end{cases} \qquad \square$$

You have to be extremely careful when you are working with representatives.

Exp. Is $[a]_3 \longmapsto [a]_2$ a well-defined map from $\mathbb{Z}_3$ to $\mathbb{Z}_2$?

Solution. $[0]_3 = [3]_3$, but $[0]_2 \neq [3]_2$. So it is NOT a well-defined map.

$\boxed{Q}$ For what positive integers m and n, the above defined map is well-defined:

$$P_{n,m} : \mathbb{Z}_n \to \mathbb{Z}_m , \ P_{n,m}([a]_n) = [a]_m .$$

Solution. If it is well-defined, then

$$[0]_n = [n]_n \Rightarrow [0]_m = [n]_m$$

$$\Rightarrow n \overset{m}{\equiv} 0$$

$$\Rightarrow m \mid n.$$

If $m \mid n$, then we claim that $\underline{P_{n,m}}$ is well-defined.

$$[a_1]_n = [a_2]_n \Rightarrow a_1 \overset{n}{\equiv} a_2$$

$$\Rightarrow \left.\begin{matrix} n \mid a_1 - a_2 \\ m \mid n \end{matrix}\right\} \Rightarrow m \mid a_1 - a_2$$

$$\Rightarrow a_1 \overset{m}{\equiv} a_2$$

$$\Rightarrow [a_1]_m = [a_2]_m. \quad \blacksquare$$

<u>Chinese Remainder Theorem</u>

Let m and n be two relatively prime positive integers. Then
$$\mathbb{Z}_{mn} \longrightarrow \mathbb{Z}_m \times \mathbb{Z}_n$$
$$[a]_{mn} \longmapsto ([a]_m, [a]_n)$$
is a bijection.

<u>Pf</u>. ① It is well-defined:

$[a]_{mn} \longmapsto [a]_m$ and $[a]_{mn} \longmapsto [a]_n$ are well-defined as $m \mid mn$ and $n \mid mn$.

② It is 1-1.

$$([a]_m, [a]_n) = ([b]_m, [b]_n)$$

$$\Rightarrow \quad a \overset{m}{\equiv} b \quad \text{and} \quad a \overset{n}{\equiv} b$$

$$\Rightarrow \quad \left.\begin{array}{l} m \mid a-b \\ n \mid a-b \end{array}\right\} \Rightarrow \left.\begin{array}{l} \operatorname{lcm}(m,n) \mid a-b \\ \gcd(m,n)=1 \Rightarrow \operatorname{lcm}(m,n) = mn \end{array}\right\}$$

$$\Rightarrow mn \mid a-b \Rightarrow a \equiv b \pmod{mn}$$

$$\Rightarrow [a]_{mn} = [b]_{mn}.$$

③ $\left.\begin{array}{l} |\mathbb{Z}_{mn}| = mn = |\mathbb{Z}_m \times \mathbb{Z}_n| \\ f \text{ is } 1\text{-}1 \end{array}\right\} \Rightarrow f$ is also onto ∎

<u>Cor.</u> Let m and n be two relatively prime positive integers. Then for any integers a and b

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

has a <u>unique</u> solution modulo mn.

<u>Pf</u>. Since the above map is a bijection, for any

a and b, $\exists!\ [x]_{mn} \in \mathbb{Z}_{mn}$ s.t.

$$([x]_n, [x]_m) = ([a]_n, [b]_m)$$

$$\Rightarrow \begin{cases} x \equiv a \pmod n \\ x \equiv b \pmod m). \end{cases}$$

$\blacksquare$

<u>How can we find such a solution?</u>

Suppose $\quad ([x_1]_n, [x_1]_m) = ([1]_n, [0]_m)$

and $\quad ([x_2]_n, [x_2]_m) = ([0]_n, [1]_m)$

$$\Rightarrow ([a x_1 + b x_2]_n, [a x_1 + b x_2]_m)$$

$$= ([a]_n \underbrace{[x_1]_n}_{[1]_n} + [b]_n \underbrace{[x_2]_n}_{[0]_n}, [a]_m \underbrace{[x_1]_m}_{[0]_m} + [b]_m \underbrace{[x_2]_m}_{[1]_m})$$

$$= ([a]_n, [b]_m).$$

So it is enough to find $\underline{x_1}$ and $\underline{x_2}$.

$$\Rightarrow \begin{cases} x_1 \overset{n}{\equiv} 1 \\ x_1 \overset{m}{\equiv} 0 \end{cases} \rightsquigarrow x_1 = mx \text{ for some integer } x.$$

So we need to solve

$$mx \overset{n}{\equiv} 1 \quad ; \quad \text{alternatively } [m]_n [x]_n = [1]_n .$$

<u>Def.</u> We say $[a]_n$ is a unit in $\mathbb{Z}_n$ if

$$\exists [a']_n \in \mathbb{Z}_n \text{ s.t. } [a]_n [a']_n = [1]_n .$$

<u>Corollary</u> $[m]_n$ is a unit in $\mathbb{Z}_n \Leftrightarrow \gcd(m,n)=1$.

<u>Pf.</u> [($\Leftarrow$) Pf 1 by CRT we know the above equation has a solution.]

$$\exists x, \ [m]_n [x]_n = [1]_n \Leftrightarrow \exists x, \ mx \overset{n}{\equiv} 1$$

$$\Leftrightarrow \exists x, y \in \mathbb{Z}, \quad mx - 1 = ny$$

$$\Leftrightarrow \exists x, y \in \mathbb{Z}, \quad mx + ny = 1$$

$$\Leftrightarrow \quad \gcd(m,n) = 1. \qquad \blacksquare$$

One can use Euclid's algorithm to find <u>g.c.d.</u> and a solution to $ax + by = \gcd(a,b)$ in an <u>efficient</u> way. <u>Read it in your book.</u>

<u>What are the solutions of linear equations in $\mathbb{Z}_n$?</u>

$$[a]_n [x]_n = [b]_n \Leftrightarrow ax \overset{n}{\equiv} b$$

It has a solution $\Leftrightarrow \exists x,y\in\mathbb{Z},\ ax-b=ny$

$\Leftrightarrow \exists x,y\in\mathbb{Z},\ b=ax-ny$

$\Leftrightarrow b\in a\mathbb{Z}+n\mathbb{Z}=\gcd(a,n)\mathbb{Z}$

$\Leftrightarrow \gcd(a,n)\mid b.$

<u>Proposition</u>. $[a]_n[x]_n=[b]_n$ has a solution if and only if $\gcd(a,n)\mid b$.

<u>How many solutions does it have?</u>

<u>Exp.</u> $[6]_8[x]_8=[2]_8 \Leftrightarrow 6x\overset{8}{\equiv}2$

(it has a solution as $\gcd(6,8)=2\mid 2$.)

$\Leftrightarrow \exists y\in\mathbb{Z},\quad 8y=6x-2$

$\Leftrightarrow \exists y\in\mathbb{Z},\quad 4y=3x-1$

$\Leftrightarrow \quad 3x\overset{4}{\equiv}1$

$\Leftrightarrow \quad x\overset{4}{\equiv}-1.$

$\Leftrightarrow \quad x=4k-1$ for some integer k

$\Leftrightarrow \quad x\overset{8}{\equiv}-1$ <u>or</u> 3

$\iff [x]_8 = [1]_8$ or $[3]_8$

it has $\underline{\underline{\text{two}}}$ solutions. $\blacksquare$

__Proposition__ (i) $[a]_n [x]_n = [b]_n$ has a solution

if and only if $\gcd(a,n) \mid b$.

(ii) If $d = \gcd(a,n) \mid b$, then $[a]_n [x]_n = [b]_n$

has exactly $\underline{d}$ solutions in $\mathbb{Z}_n$.

(Modulo n/d, it has a unique solution.)

__Pf__.(ii) $[a]_n [x]_n = [b]_n \iff ax \overset{n}{\equiv} b$

$$\iff \exists y \in \mathbb{Z},\quad ny = ax - b$$

$$\iff \left(\frac{n}{d}\right) y = \left(\frac{a}{d}\right)x - \left(\frac{b}{d}\right)$$

$$\iff \left(\frac{a}{d}\right) x \equiv \left(\frac{b}{d}\right) \pmod{\frac{n}{d}}$$

$\gcd\left(\frac{a}{d}, \frac{n}{d}\right) = 1 \Rightarrow \frac{a}{d}$ is a unit in $\mathbb{Z}_{n/d}$

so $\exists\ x_0 \in \mathbb{Z}$ s.t. $\frac{a}{d} x_0 \equiv 1 \pmod{\frac{n}{d}}$

$$\iff x \equiv \left(\frac{b}{d}\right) x_0 \pmod{\frac{n}{d}}$$

$$\iff x = \frac{n}{d}k + \left(\frac{b}{d}\right)x_0 \quad \text{for some integ. } k.$$

$$\iff x \overset{n}{\equiv} \left(\frac{b}{d}\right)x_0 \text{ or}$$

$$\left(\frac{b}{d}\right)x_0 + \frac{n}{d} \text{ or}$$

$$\left(\frac{b}{d}\right)x_0 + 2\frac{n}{d} \text{ or}$$

$$\vdots$$

$$\left(\frac{b}{d}\right)x_0 + (d-1)\frac{n}{d}.$$

$$\blacksquare$$