In the previous lecture we defined

\[ \mathbb{Z}_n := \{ n \mathbb{Z}, n \mathbb{Z} + 1, \ldots, n \mathbb{Z} + (n-1) \mathbb{Z} \} \]

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

**Lemma.** The following properties are equivalent:

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

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

(iii) \( a \equiv b \). 

In particular, for any \( x \in [a]_n \) we have \( [x]_n = [a]_n \).

**Def.** An element of \( [a]_n \) is called a representative of \( [a]_n \).

**Lemma.** \( [a]_n + [b]_n := [a+b]_n \)

\( [a]_n \cdot [b]_n := [a \cdot b]_n \)

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

**Pf.** \( [a_1]_n = [a_2]_n \Rightarrow a_1 \equiv a_2 \Rightarrow a_1 + b_1 \equiv a_2 + b_2 \).
Proof. \([a_1]_n = [a_2]_n \Rightarrow a_1 \equiv a_2 \Rightarrow \exists a_1 + b_1 \equiv a_2 + b_2\)

\([b_1]_n = [b_2]_n \Rightarrow b_1 \equiv b_2 \Rightarrow \exists a_1 \cdot b_1 \equiv a_2 \cdot b_2\)

\[\Rightarrow \exists [a_1 + b_1]_n = [a_2 + b_2]_n\]

\[\exists [a_1 \cdot b_1]_n = [a_2 \cdot b_2]_n. \quad \square\]

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

**Example.** \([a]_3 \rightarrow [a]_2\) 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.

**Q.** For what positive integers \(m\) and \(n\), the above defined map is well-defined:

\(\phi_{nm}: \mathbb{Z}_n \rightarrow \mathbb{Z}_m, \phi_{nm}(\lfloor a \rfloor_n) = \lfloor a \rfloor_m\).

**Solution.** If it is well-defined, then

\([0]_n = [n]_n \Rightarrow [0]_m = [n]_m\).
\[ \Rightarrow \quad n \equiv 0 \]

\[ \Rightarrow \quad m \mid n. \]

If \( m \mid n \), then we claim that \( \mathbb{P}_{n,m} \) is well-defined.

\[ [a_1]_n = [a_2]_n \Rightarrow a_1 \equiv a_2 \]

\[ \Rightarrow \quad n \mid a_1-a_2 \quad \Rightarrow \quad m \mid a_1-a_2 \]

\[ m \mid n \]

\[ \Rightarrow a_1 \equiv a_2 \]

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

**Chinese Remainder Theorem**

Let \( m \) and \( n \) be two relatively prime positive integers. Then \( \mathbb{Z}_{mn} \rightarrow \mathbb{Z}_m \times \mathbb{Z}_n \)

\[ [a]_{mn} \mapsto ([a]_m, [a]_n) \]

is a bijection.

**Proof.** 1) It is well-defined:

\[ [a]_{mn} \rightarrow [a]_m \quad \text{and} \quad [a]_{mn} \rightarrow [a]_n \]

are well-defined as \( m \mid mn \) and \( n \mid mn \).
2. It is 1-1.

\[
([a]_m, [a]_n) = ([b]_m, [b]_n) \implies a \equiv b \mod m \quad \text{and} \quad a \equiv b \mod n
\]

\[
\implies \quad m \mid a - b \implies \text{lcm}(m,n) \mid a - b
\]

\[
\quad \text{and} \quad n \mid a - b \implies \text{gcd}(m,n) = 1 \implies \text{lcm}(m,n) = mn
\]

\[
\implies mn \mid a - b \implies a \equiv b \mod mn
\]

\[
\implies [a]_{mn} = [b]_{mn}
\]

3. \( |\mathbb{Z}_{mn}| = mn = |\mathbb{Z}_m \times \mathbb{Z}_n| \iff f \text{ is also onto} \)

\[
\implies f \text{ is } 1-1
\]

Cor. Let \( m \) and \( n \) be two relatively prime positive integers. Then for any integers \( a \) and \( b \)

\[
\begin{align*}
\begin{cases}
x \equiv a \mod m \\
x \equiv b \mod n
\end{cases}
\end{align*}
\]

has a unique solution modulo \( mn \).

\[\text{Pf. Since the above map is a bijection, for any} \]

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

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

\[\Rightarrow \begin{cases} x \equiv a \pmod{n} \\ x \equiv b \pmod{m}. \end{cases} \]

How can we find such a solution?

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

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

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

\[= ([a]_n \cdot [x_1]_n + [b]_n \cdot [x_2]_n, [a]_m \cdot [x_1]_m + [b]_m \cdot [x_2]_m)\]

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

So it is enough to find \( x_1 \) and \( x_2 \).

\[\Rightarrow \begin{cases} x_1 \equiv 1 \\ x_1 \sim 0 \end{cases} \quad \Rightarrow x_1 = mx \quad \text{for some} \quad \text{integer } x.
\]

So we need to solve
$$m \cdot x \equiv 1 \pmod{n} \implies \text{alternatively } [m]_n [x]_n = [1]_n.$$ 

**Def.** We say $[a]_n$ is a unit in $\mathbb{Z}_n$ if

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

**Corollary** $[m]_n$ is a unit in $\mathbb{Z}_n \iff \gcd(m,n) = 1.$

**Pf.** [(\Leftarrow) Pf.] by CRT we know the above equation has a solution.]

$$\exists x, \ [m]_n [x]_n = [1]_n \iff \exists x, \ m \cdot x \equiv 1 \pmod{n}$$

$$\iff \exists x, y \in \mathbb{Z}, \ m \cdot x - 1 = n \cdot y$$

$$\iff \exists x, y \in \mathbb{Z}, \ m \cdot x + n \cdot y = 1$$

$$\iff \gcd(m,n) = 1.$$ 

One can use Euclid’s algorithm to find $\gcd$ and a solution to $ax + by = \gcd(a,b)$ in an efficient way. Read it in your book.

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

$$[a]_n [x]_n = [b]_n \iff a \cdot x \equiv b \pmod{n}$$
It has a solution \( \iff \exists x, y \in \mathbb{Z}, \ ax - b = ny \)

\( \iff \exists x, y \in \mathbb{Z}, \ b = ax - ny \)

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

\( \iff \gcd(a, n) \mid b. \)

**Proposition.** \([a]_n \ [x]_n = [b]_n \) has a solution if and only if \( \gcd(a, n) \mid b. \)

**How many solutions does it have?**

**Exp.** \([6]_8 \ [x]_8 = [2]_8 \iff 6x \equiv 2 \)

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

\( \iff \exists y \in \mathbb{Z}, \ 8y = 6x - 2 \)

\( \iff \exists y \in \mathbb{Z}, \ 4y = 3x - 1 \)

\( \iff 3x \equiv 1 \)

\( \iff x \equiv -1 \)

\( \iff x = 4k - 1 \) for some integer \( k \)

\( \iff x \equiv -1 \ \text{or} \ 3 \)
\[ [x]_8 = [1]_8 \text{ or } [3]_8 \]

it has two solutions.

Proposition (i) \( [a]_n \cdot [x]_n = [b]_n \) has a solution if and only if \( \gcd(a, n) \mid b \).

(ii) If \( d = \gcd(a, n) \mid b \), then \( [a]_n \cdot [x]_n = [b]_n \) has exactly \( \frac{d}{d} \) solutions in \( \mathbb{Z}_n \).

((Modulo \( \frac{n}{d} \), it has a unique solution.)

Prove (ii) \( [a]_n \cdot [x]_n = [b]_n \iff ax \equiv b \mod n \)

\[ \iff \exists y \in \mathbb{Z}, \ n \ y = ax - b \]

\[ \iff (\frac{n}{d}) \ y = (\frac{a}{d})x - (\frac{b}{d}) \]

\[ \iff \left( \frac{a}{d} \right) x \equiv \left( \frac{b}{d} \right) \left( \mod \frac{n}{d} \right) \]

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

so \( \exists x_0 \in \mathbb{Z} \) s.t. \( \frac{a}{d} x_0 \equiv 1 \left( \mod \frac{n}{d} \right) \)

\[ \iff x \equiv \left( \frac{b}{d} \right) x_0 \left( \mod \frac{n}{d} \right) \]
\[ x = \frac{n}{d} k + \left( \frac{b}{d} \right) x_0 \text{ for some integer } k. \]

\[ x \equiv \left( \frac{b}{d} \right) x_0 \text{ or } \left( \frac{b}{d} \right) x_0 + \frac{n}{d} \text{ or } \left( \frac{b}{d} \right) x_0 + 2 \frac{n}{d} \text{ or } \left( \frac{b}{d} \right) x_0 + (d-1) \frac{n}{d}. \]