§1 Lecture 11-15

Example 1.1

$$\mathbb{Z}_3[x]/I \text{ where } I = \langle x^2 + 2 \rangle$$
$$(x^2 + I) + (2 + I) = (x^2 + 2 + I) = (0 + I)$$
$$(2 + I) + (1 + I) = (0 + I)$$
$$\text{so } (x^2 + I) = -(2 + I) = (1 + I)$$
$$\underbrace{((2x + 1) + I)}_{\text{Non zero}} \underbrace{((x + 1) + I)}_{\text{Non zero}} = (2x^2 + 2x + x + 1 + I) = (2x^2 + 1 + I)$$
$$= (x^2 + I) + (x^2 + I) + (1 + I) = (1 + I) + (1 + I) + (1 + I) = (0 + I)$$

Hence $\mathbb{Z}_3[x]/I$ is not an integral domain.

Theorem 1.2 (The Chinese Remainder Theorem)
Let $n_1, n_2, n_3, \dots, n_k$ be positive integers with $\gcd(n_i, n_j) = 1$ for $i \neq j$.

Then for any $a_1, a_2, a_3, \dots, a_k$, the following has a solution:

$$\begin{aligned} x &\equiv_{n_1} a_1 \\ x &\equiv_{n_2} a_2 \\ &\vdots \\ x &\equiv_{n_k} a_k \end{aligned}$$

Moreover, for any two solutions x and x', $x \equiv x' \mod (n_1 n_2 \cdots n_k)$.

Example 1.3
Generally, $\mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$ if $\gcd(p, q) = 1$.

For example, $\mathbb{Z}_7 \times \mathbb{Z}_8 \cong \mathbb{Z}_{56}$.

Proof. Consider the homomorphism $\varphi : \mathbb{Z} \to \mathbb{Z}_7 \times \mathbb{Z}_8$ defined by

$$\varphi(a) = ([a]_7, [a]_8)$$

$$\begin{aligned} \varphi(a+b) &= ([a+b]_7, [a+b]_8) = ([a]_7 + [b]_7, [a]_8 + [b]_8) \\ &= ([a]_7, [a]_8) + ([b]_7, [b]_8) = \varphi(a) + \varphi(b) \end{aligned}$$

$$\varphi : \mathbb{Z} \to G \qquad \varphi(n) = g^n \text{ where } g = (1, 1)$$

φ is surjective by the chinese remainder theorem. Indeed fo any a_1, a_2, there exists x such that $x \equiv_7 a_1$ and $x \equiv_8 a_2$ so $\varphi(x) = (a_1, a_2)$.

Note 1.4. $[a]_7$ means $a \mod (7)$.

What is $\ker(\varphi)$?

$\ker(\varphi) = 7\mathbb{Z} \cap 8\mathbb{Z} = 56\mathbb{Z}$ by the first isomorphism theorem. Because we know that $\varphi(\mathbb{Z}) = \mathbb{Z}_7 \times \mathbb{Z}_8$, and that by the first isomorphism theorem, $\varphi(\mathbb{Z}) \cong \mathbb{Z}/\ker(\varphi)$. And $\varphi(\mathbb{Z}) = \mathbb{Z}_7 \times \mathbb{Z}_8 \cong \mathbb{Z}_{56} = \mathbb{Z}/\mathbb{Z}_{56}$. $\square$

Lemma 1.5 (16.41)
Let m and n be positive integers with $\gcd(m, n) = 1$. Then for all $a, b \in \mathbb{Z}$,

$$x \equiv_m a$$
$$x \equiv_n b$$

has a solution.

Moreover, the solution is unique $\mod (mn)$. i.e. if x_1 and x_2 are solutions, then $x_1 \equiv_{mn} x_2$.

Example 1.6

$$x \equiv_7 6$$
$$x \equiv_8 4$$

has solution 20. The full set of solutions is $20 + 56\mathbb{Z}$.

Proof. We know that $x \equiv_m a$ has solutions of the form $\{a + mp : p \in \mathbb{Z}\}$. We must find solutions such that

$$a + mp \equiv_n b \Rightarrow mp \equiv_n b - a$$

But $\gcd(m, n) = 1$ implies that there exists s, t such that $1 = sm + tn$. i.e. s is the multiplicative inverse of m in $\mathbb{Z}_n$. Hence

$$smp \equiv_n s(b - a)$$
$$\Rightarrow p \equiv_n s(b - a)$$

Therefore we have found x which satisfies $x \equiv_m a$ and $x \equiv_n b$. □

Suppose x_1 and x_2 are both solutions. Then:

$$x_1 - x_2 \equiv_m 0$$
$$x_1 - x_2 \equiv_n 0$$

Hence $m \mid (x_1 - x_2)$ and $n \mid (x_1 - x_2)$ so $mn \mid (x_1 - x_2)$.