Example: Prove $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

Proof. Define $\varphi: \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ by $n \longmapsto ([n]_2, [n]_3)$. Let $n, m \in \mathbb{Z}$. We have that:

$$\begin{aligned}\varphi(m+n) &= ([m+n]_2, [m+n]_3) \\ &= ([m]_2 + [m]_3, [n]_2 + [n]_3) \\ &= \varphi(m) + \varphi(n).\end{aligned}$$

So φ is a homomorphism. Let $([a]_2, [b]_3) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Consider $n = 3a + 4b \in \mathbb{Z}$. Then $\varphi(n) = \varphi(3a+4b) = ([3a+4b]_2, [3a+4b]_3) = ([3a]_2, [4b]_3) = ([a]_2, [b]_3)$. Hence φ is surjective.

Let $m \in \operatorname{Ker}\varphi$. Then $\varphi(m) = ([0]_2, [0]_3)$, which implies $([m]_2, [m]_3) = ([0]_2, [0]_3)$. So $[m]_2 = [0]_2$ and $[m]_3 = [0]_3$; i.e., $2 \mid m$ and $3 \mid m$. Since 2 and 3 are coprime, $6 \mid m$, so $m = 6k$ for some $k \in \mathbb{Z}$. Thus $m \in 6\mathbb{Z}$, hence $\operatorname{Ker}\varphi \subseteq 6\mathbb{Z}$.

Let $n \in 6\mathbb{Z}$. Then $\varphi(n) = ([n]_2, [n]_3) = ([0]_2, [0]_3)$. Hence $6\mathbb{Z} \subseteq \operatorname{Ker}\varphi$. Thus $\operatorname{Ker}\varphi = 6\mathbb{Z}$, and by the first isomorphism theorem $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. $\square$

Lemma: Let $\gcd(m,n) = 1$. There is a unique simultaneous solution mod mn to the equations:

$$x \equiv a_1 \pmod m$$
$$x \equiv a_2 \pmod n$$

Proof. We have $x \equiv a_1 \pmod m)$*, which is equivalent to

$$x = a_1 + mk. \qquad (1)$$

We want k so that $a_1 + mk \equiv a_2 \pmod n$, or equivalently,

$$mk \equiv a_2 - a_1 \pmod n. \qquad (2)$$

Since $\gcd(m,n) = 1$, there exists an $\tilde{m} \in \mathbb{Z}$ s.t. $\tilde{m}m \equiv m\tilde{m} \equiv 1 \pmod n$†. From Equation (2), consider $\tilde{m}mk = k = \tilde{m}(a_2 - a_1)$. Substituting k into Equation (1) yields $\boxed{x = a_1 + m\tilde{m}(a_2 - a_1)}$, which solves the equations:

$$a_1 + m\tilde{m}(a_2 - a_1) \equiv a_1 \pmod m.^*$$
$$a_1 + m\tilde{m}(a_2 - a_1) \overset{\dagger}{\equiv} a_1 + (a_2 - a_1) \equiv a_2 \pmod n. \quad \text{From } m\tilde{m} \equiv 1 \pmod n \quad \square$$

Theorem: (Chinese Remainder Theorem) Let $m, n \in \mathbb{Z}_{\geq 1}$ with $\gcd(m,n) = 1$. Then $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

Proof. The proof follows similarly to our first example. $\square$

Theorem: (Fundamental Theorem of Finitely Generated Abelian Groups) Let G be a finite abelian group. Then G is a product of cyclic groups.

Proof. The proof of this theorem is outside the scope of this course. $\square$

Theorem: Let $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ with p_i's prime and $p_i \neq p_j$, $e_i \geq 1$. Then:

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \mathbb{Z}/p_2^{e_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{e_r}\mathbb{Z}.$$

Proof. CRT and induction. See Galois Theory. $\square$

Example:

1) $|G| = 4$. Then $G \cong \mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
2) $|G| = 6$. Then $G \cong \mathbb{Z}/6\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.
3) $|G| = 36$. Note that $36 = 2^2 \cdot 3^2$. The permutations of its prime factors are:

$$(2,2,3,3) \longrightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$$
$$(2^2,3,3) \longrightarrow \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$$
$$(2,2,3^2) \longrightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$$
$$(2^2,3^2) \longrightarrow \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \cong \mathbb{Z}/36\mathbb{Z}.$$

Since $\gcd(2,18) \neq 1$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z} \ncong \mathbb{Z}/36\mathbb{Z}$. Similarly, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$ does not have an element of order 36!