L20: Chinese Remainder Theorem

Thm (Chinese remainder thm)

Let $m, n \in \mathbb{Z}$ be coprime, i.e. $(m,n) = 1$

Then $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

Pf Define group hom $\varphi: \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$
$\ell \mapsto (\bar{\ell}, \bar{\ell})$

Claim $\ker \varphi = mn\mathbb{Z}$

Pf "$\supseteq$": ✓

"$\subseteq$": $(m,n) = 1 \Rightarrow \exists a, b$ s.t. $am + bn = 1$

Let $\ell \in \ker \varphi \Rightarrow \ell = 0 \pmod m$ $\quad \ell = km$
$\ell = 0 \pmod n$ $\quad \ell = k'n$

$\Rightarrow \ell = \ell am + \ell bn = k'nam + kmbn = (k'a + kb) \cdot mn$ □

$\Rightarrow \varphi$ induces an injective group hom $\bar{\varphi}: \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

Since $|\mathbb{Z}/mn\mathbb{Z}| = mn = |\mathbb{Z}/m\mathbb{Z}| \cdot |\mathbb{Z}/n\mathbb{Z}|$, $\bar{\varphi}$ is an isom.

Ex
- $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
- $\mathbb{Z}/15\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$
- $\mathbb{Z}/4\mathbb{Z} \not\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
- $\mathbb{Z}/p_1^{k_1} \cdots p_\ell^{k_\ell}\mathbb{Z} \cong \mathbb{Z}/p_1^{k_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_\ell^{k_\ell}\mathbb{Z}$

Good to know: $\bar{\varphi}$ has an "explicit inverse"

$\bar{\varphi}^{-1}$: $(1,0) \mapsto bn$
$(0,1) \mapsto am$
$(p,q) \mapsto pbn + qam$