Chinese Remainder Theorem

Kevin James

Definition

Suppose that R is a ring and that $A, B \trianglelefteq R$. We say that A and B are <u>comaximal</u> if $A + B = R$.

Theorem

Suppose that R is a ring and that $A_1, \ldots, A_k \trianglelefteq R$. The map $\pi : R \to R/A_1 \times \cdots \times R/A_k$ defined by $\pi(r) = (r + A_1, \ldots, r + A_k)$ is a ring homomorphism with $\ker(\pi) = A_1 \cap \cdots \cap A_k$. Thus

$$R/A_1 \cap \cdots \cap A_k \cong \pi(R).$$

If the ideals $A_1, \ldots, A_k$ are pairwise comaximal then π is surjective and $A_1 \cap \cdots \cap A_k = A_1 A_2 \ldots A_k$ and in this case

$$R/A_1 \ldots A_k \cong R/A_1 \times \cdots \times R/A_k.$$

Corollary

Suppose that $n \in \mathbb{N}$ *and that* $n = p_1^{a_1} \dots p_k^{a_k}$. *Then,*

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{a_k}\mathbb{Z}.$$

Further we have the isomorphism of multiplicative groups.

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{a_1}\mathbb{Z})^\times \times \cdots \times \left(\mathbb{Z}/p_k^{a_k}\mathbb{Z}\right)^\times,$$

which implies that $\phi(n) = \phi(p_1^{a_1}) \cdot \cdots \cdot \phi(p_k^{a_k})$.