Chinese remainder theorem

Let A be a commutative ring. We consider the homomorphism

$$f : A \to \prod_{i=1}^{n} A/\mathfrak{a}_i$$

where $\mathfrak{a}_1, \cdots, \mathfrak{a}_n \subset A$ are ideals. We are interested in the injectivity and surjectivity of f.

Injectivity

Proposition

We have $\ker(f) = \cap \mathfrak{a}_i$

Proof.

Follows from $\ker(A \to A/\mathfrak{a}) = \mathfrak{a}$ for any ideal $\mathfrak{a} \subset A$. $\square$

Surjectivity

Proposition

Suppose that $\mathfrak{a}_i + \mathfrak{a}_j = A$ if $i \neq j$. Then, f is surjective.

To prove the proposition, it suffices to find $y_1, \cdots, y_n \in A$ such that

$$y_i \equiv \begin{cases} 1 & (\text{mod } \mathfrak{a}_i) \\ 0 & (\text{mod } \mathfrak{a}_j) \text{ if } i \neq j. \end{cases}$$

Existence of $y_1, \cdots, y_n$

By symmetry, it suffices to show the existence of y_n. For each $i = 1, 2, \cdots, n-1$,

$$\mathfrak{a}_i + \mathfrak{a}_n = A$$

implies

$$x_i + z_i = 1 \tag{1}$$

for some $x_i \in \mathfrak{a}_i$ and $z_i \in \mathfrak{a}_n$. Then, we have

$$(1) \Rightarrow x_i \equiv 1 (\text{mod } \mathfrak{a}_n)$$
$$\text{and}$$
$$x_i \in \mathfrak{a}_i \Rightarrow x_i \equiv 0 (\text{mod } \mathfrak{a}_i).$$

Take $y_n = x_1 x_2 \cdots x_{n-1}$.

Chinese remainder theorem

As a consequence, we obtain:-

Theorem

Suppose that $\cap \mathfrak{a}_i = 0$ *and that* $\mathfrak{a}_i + \mathfrak{a}_j = A$ *if* $i \neq j$. *Then,* f *is an isomorphism.*

Question

Let $N = p_1^{e_1} \cdots p_n^{e_n}$, where e_i is a positive integer and p_i's are distinct primes. Can you deduce that

$$f : \mathbb{Z}/N\mathbb{Z} \to \prod_{i=1}^{n} \mathbb{Z}/p_i^{e_i}\mathbb{Z}?$$

is an isomorphism from the Chinese remainder theorem?