The Chinese Remainder Theorem

<u>Defn</u>: Let R, S be rings

The <u>direct product</u> of R and S is the ring

$$R \times S := \{(r,s) \mid r \in R,\ s \in S\}$$

$$(r_1, s_1) + (r_2, s_2) := (r_1 + r_2,\ s_1 + s_2)$$

$$(r_1, s_1) \cdot (r_2, s_2) := (r_1 \cdot r_2,\ s_1 \cdot s_2)$$

More generally, if $\{R_\alpha \mid \alpha \in A\}$ is any collection of rings

The <u>direct product</u> of the collection is the ring

$$\bigtimes_{\alpha \in A} R_\alpha := \{(r_\alpha)_{\alpha \in A} \mid r_\alpha \in R_\alpha\}$$

$$(r_\alpha)_{\alpha \in A} + (s_\alpha)_{\alpha \in A} := (r_\alpha + s_\alpha)_{\alpha \in A}$$

$$(r_\alpha)_{\alpha \in A} \cdot (s_\alpha)_{\alpha \in A} := (r_\alpha \cdot s_\alpha)_{\alpha \in A}.$$

Given $a, b \in \mathbb{Z}$, we say they are <u>relatively prime</u> if the greatest common divisor is 1.

Equivalently, we say a, b are relatively prime if $\exists\, m, n \in \mathbb{Z}$

s.t. $am + bn = 1$.

<u>Defn</u>: In a comm. ring R w/ $1 \neq 0$.

Two ideals A and $B \subset R$ are <u>comaximal</u> if $A + B = R$

Thm: Let $A_1, \ldots, A_k \subset R$ ideals in a comm. ring w/ $1 \neq 0$

If they are pairwise comaximal

Then $A_1 \cdot A_2 \cdots A_k = A_1 \cap A_2 \cap \cdots \cap A_k$

Pf: we already know that

$$A_1 \cdot A_2 \cdots A_k \subset A_1 \cap A_2 \cap \cdots \cap A_k$$

It suffices to show

$$A_1 \cap A_2 \cap \cdots \cap A_k \subset A_1 \cdot A_2 \cdots A_k.$$

First, consider comaximal ideals A, B.

Let $x \in A \cap B$. we want to show $x \in A \cdot B$

By comaximality $\Longrightarrow \exists\, a \in A,\ b \in B$ st. $a + b = 1 \in A + B$

In particular $\Longrightarrow$ $x = x \cdot 1 = x \cdot (a+b) = x \cdot a + x \cdot b$

$x \in A \cap B \Longrightarrow$ $x \in A \Longrightarrow x \cdot b \in A \cdot B$; $x \in B \Longrightarrow x \cdot a \in A \cdot B$ $\Longrightarrow x \cdot a + x \cdot b \in A \cdot B$

$\Longrightarrow x \in A \cdot B \Longrightarrow A \cap B \subset A \cdot B$

$\Longrightarrow A \cdot B = A \cap B$

The general case follows if we can show

$A = A_1$, $B = A_2 \cdot A_3 \cdots A_k$ are comaximal

(by induction)

By assumption of comaximality

A_1, A_2 comaximal

A_1, A_3 comaximal

$\vdots$ $\vdots$

A_1, A_k comaximal

$\Longrightarrow \exists\ x_2 \in A_1\ \ y_2 \in A_2$ s.t. $1 = x_2 + y_2$

$x_3 \in A_1,\ y_3 \in A_3$ s.t. $1 = x_3 + y_3$

$\vdots$

$x_k \in A_1,\ y_k \in A_k$ s.t. $1 = x_k + y_k$

$$\Longrightarrow 1 = (x_2+y_2)\cdot(x_3+y_3)\cdot \_\_\_ \cdot(x_k+y_k) \in A_1 + (A_2 \cdot \_\_\_ \cdot A_k)$$

$\Longrightarrow$ $A_1,\ A_2 \cdot \_\_\_ A_k$ comaximal $\square$

Thm: (Chinese Remainder Theorem)

Let $A_1, \_\_\_, A_k \subset R$ ideals in a comm. ring w/ $1 \neq 0$.

The map

$$\phi : R \longrightarrow (R/A_1) \times (R/A_2) \times (R/A_3) \times \_\_\_ \times (R/A_k)$$
$$r \longmapsto (r + A_1,\ r + A_2,\ r + A_3,\ \_\_\_,\ r + A_k)$$

is a ring homomorphism w/ $\operatorname{Ker}\phi = A_1 \cap A_2 \cap \_\_\_ \cap A_k$

If they are pairwise comaximal

Then ϕ is surjective

Cor: If $A_1, \ldots, A_k \subset R$ are pairwise comaximal ideals in a comm. ring w/ $1 \neq 0$

Then there is an isomorphism of rings

$$R/(A_1 \cdots A_k) \cong R/(A_1 \cap A_2 \cap \cdots \cap A_k) \cong (R/A_1) \times (R/A_2) \times \cdots \times (R/A_k)$$

Cor: Let n be a positive integer w/ factorization into unique primes

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

Then $\mathbb{Z}/n\mathbb{Z} \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}) \times (\mathbb{Z}/p_2^{\alpha_2}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z})$

Example: $\mathbb{Z}/30\mathbb{Z} \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z})$

$\mathbb{Z}/168\mathbb{Z} \cong (\mathbb{Z}/8\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/7\mathbb{Z})$

Pf: (of CRT)

we want to see

$$\phi : R \to (R/A_1) \times \cdots \times (R/A_k)$$
$$r \mapsto (r + A_1, \ldots, r + A_k)$$

① $\ker \phi = A_1 \cap \cdots \cap A_k$

② If $A_1, \ldots, A_k$ are pairwise comaximal then ϕ is surjective.

we prove this for $k=2$, and the generalize

① $A, B \subset R$ ideals

$$\phi: R \longrightarrow (R/A) \times (R/B)$$
$$r \longmapsto (r+A, r+B)$$

Let $r \in \operatorname{Ker} \phi$: Then $\begin{matrix} r+A = 0+A \\ r+B = 0+B \end{matrix} \Longrightarrow \begin{matrix} r \in A \\ r \in B \end{matrix} \Longrightarrow r \in A \cap B.$

If $r \in A \cap B$, then $\begin{matrix} r \in A \\ r \in B \end{matrix} \Longrightarrow \begin{matrix} r+A = 0+A \\ r+B = 0+B \end{matrix} \Longrightarrow r \in \operatorname{Ker}\phi$

② If A, B are comaximal

$\Longrightarrow \exists\ x \in A,\ y \in B$ s.t. $1 = x+y$

$\Longrightarrow \begin{matrix} 1-x = y \in B \\ 1-y = x \in A \end{matrix} \Longrightarrow \begin{matrix} 1+A = y+A \\ 1+B = x+B \end{matrix}$

$$\Longrightarrow \phi(x) = (x+A, x+B) = (0+A, 1+B)$$
$$\phi(y) = (y+A, y+B) = (1+A, 0+B).$$

So if we have any element $(r+A, s+B) \in R/A \times R/B$

Then $(r+A, s+B) = (r+A, 0+B) + (0+A, s+B)$

$$= (r+A, r+B)\cdot(1+A, 0+B) + (s+A, s+B)\cdot(0+A, 1+B)$$
$$= \phi(r)\cdot\phi(y) + \phi(s)\cdot\phi(x)$$
$$= \phi(ry+sx) \Longrightarrow \phi \text{ surj.}$$

More generally, if $A_1, \_\_ A_k \subset R$ are ideals

Let $A = A_1, \quad B = A_2 \cdot A_3 \cdots A_k$

Then we have a homomorphism

$$\phi_1 : R \longrightarrow R/A \times R/B, \quad Ker\,\phi_1 = A_1 \cap B$$

Now $A_2/B, \; A_3/B, \_\_ A_k/B \subset R/B$ are ideals

Take $A' = A_2/B, \; B' = (A_3/B)\cdot(A_4/B) \cdots (A_k/B)$
$= (A_3 \cdot A_4 \cdots A_k)/B$

Then we get a homomorphism

$$\phi_2 : R/B \longrightarrow (R/B)/A' \times (R/B)/B', \quad Ker\,\phi_2 = A' \cap B'$$

By an isomorphism theorem

$$(R/B)/A' = (R/B)/(A_2/B) \cong R/A_2$$

$$(R/B)/B' = (R/B)/(A_3 \cdot A_4 \cdots A_k/B) \cong R/A_3 \cdots A_k$$

$$\hat{\phi}_2 = (Id, \phi_2) \circ \phi_1 : R \longrightarrow R/A_1 \times R/A_2 \times R/(A_3 \cdots A_k)$$

Proceeding inductively on k, we end up with

$$\phi : R \longrightarrow R/A_1 \times R/A_2 \times \_\_ \times R/A_k$$

and the surjectivity when $A_1, \_\_ A_k$ pairwise comaximal

follow essentially because $A_1, A_2 \_\_ A_k$ are comaximal $\square$