Lecture 9

The Chinese Remainder Theorem

Definition 9.1

Let R, S be rings.
The **direct product** of R and S is the ring

$$R \times S \coloneqq \{(r, s) | r \in R, s \in S\}$$

with ring operations

$$(r_1, s_1) + (r_2, s_2) \coloneqq (r_1 + r_2, s_1 + s_2)$$
$$(r_1, s_1) \cdot (r_2, s_2) \coloneqq (r_1 \cdot r_2, s_1 \cdot s_2)$$

More generally, if $\{R_\alpha | \alpha \in A\}$ is any collection of rings, then the **direct product** of the collection is the ring

$$\bigtimes_{\alpha \in A} R_\alpha \coloneqq \{(r_\alpha)_{\alpha \in A} | r_\alpha \in R_\alpha\}$$

with ring operations

$$(r_\alpha)_{\alpha \in A} + (s_\alpha)_{\alpha \in A} \coloneqq (r_\alpha + s_\alpha)_{\alpha \in A}$$
$$(r_\alpha)_{\alpha \in A} \cdot (s_\alpha)_{\alpha \in A} \coloneqq (r_\alpha \cdot s_\alpha)_{\alpha \in A}$$

Given $a, b \in \mathbb{Z}$, we say they are **relatively prime** if the greatest common divisor is 1. Equivalently, we say a, b are relatively prime if there exists $m, n \in \mathbb{Z}$ such that

$$am + bn = 1$$

.

Definition 9.2

In a commutative ring R with $1 \neq 0$, two ideals $A, B \subset R$ are **comaximal** if $A + B = R$.

Theorem 9.1

Let $A_1, \ldots, A_k \subset R$ be ideals in a commutative ring with $1 \neq 0$.
If they are pairwise comaximal then

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

Proof. We already know that

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

It suffices to show

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

First, consider comaximal ideals A, B.
Let $x \in A \cap B$, then we want to show $x \in A \cdot B$

By comaximality,

$$\exists a \in A, b \in B,\ a + b = 1 \in A + B$$

In particular,

$$x = x \cdot 1 = x \cdot (a + b) = x \cdot a + x \cdot b$$

therefore

$$x \in A \cap B \implies \left.\begin{array}{l} x \in A \implies x \cdot b \in A \cdot B \\ x \in B \implies x \cdot a \in A \cdot B \end{array}\right\} \implies x \cdot a + x \cdot b \in A \cdot B$$

Hence $x \in A \cdot B \implies A \cap B \subset A \cdot B$, and we can conclude

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

The general case follows if we can show

$$A = A_1,\ B = A_2 \cdot A_3 \cdot \ldots \cdot A_k$$

are comaximal; we can do this with induction.
By assumption of comaximality A_1, A_i are comaximal for all $i \in \{2, \ldots, k\}$ therefore

$$\begin{aligned} &\exists x_2 \in A_1,\ y_2 \in A_2, \quad \text{s.t.} \quad 1 = x_2 + y_2 \\ &\exists x_3 \in A_1,\ y_3 \in A_3, \quad \text{s.t.} \quad 1 = x_3 + y_3 \\ &\qquad\qquad \vdots \\ &\exists x_k \in A_1,\ y_k \in A_k, \quad \text{s.t.} \quad 1 = x_k + y_k \end{aligned}$$

and this implies

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

and we conclude $A_1, A, 2 \cdot \ldots A_k$ are comaximal. ■

Theorem 9.2: Chinese Remainder Theorem

Let $A_1, \ldots A_k \subset R$ ideals in a commutative ring with $1 \neq 0$.
The map

$$\begin{aligned} \phi \colon R &\to (R/A_1) \times (R/A_2) \times (R/A_3) \times \cdots \times (R/A_k) \\ r &\mapsto (r + A_1, r + A_2, r + A_3, \ldots, r + A_k) \end{aligned}$$

is a ring homomorphism with $\operatorname{Ker} \phi = A_1 \cap A_2 \cap \cdots \cap A_k$.
If they are pairwise comaximal, then ϕ is surjective.

Corollary 9.1

If $A_1, \ldots, A_k \subset R$ are pairwise comaximal ideals in a commutative ring with $1 \neq 0$, then there is an isomorphism of rings

$$R/(A_1 \cdot \ldots \cdot A_k) \cong R/(A_1 \cap A_2 \cap \cdots \cap A_k) \cong (R/A_1) \times (R/A_2) \times (R/A_3) \times \cdots \times (R/A_k)$$

Corollary 9.2

Let n be a positive integer with factorization into unique primes

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

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 9.1 Here are factorizations of two integer modulo rings:

$$\mathbb{Z}/30\mathbb{Z} \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z})$$
$$\mathbb{Z}/168\mathbb{Z} \cong (\mathbb{Z}/8\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/7\mathbb{Z})$$