4. The Chinese Remainder Theorem:

Classic result in number theory: Let $n_1, \dots, n_k \in \mathbb{Z}^+$, pairwise coprime.

For any sequence $a_1, \dots, a_k \in \mathbb{Z}$, $\exists\, x \in \mathbb{Z}$ that solves the system

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ \vdots \\ x \equiv a_k \pmod{n_k}. \end{cases}$$

Moreover, all solutions are congruent modulo $N = n_1 n_2 \cdots n_k$.

This is in fact a special case of a much more general result.

Let R, S be rings. It is easy to define $R \oplus S$, and $R_1 \oplus \cdots \oplus R_n$ in the obvious fashion. This is comm. iff each R_i is, and has $1 = (1, \dots, 1)$ iff each R_i has 1.

Recall that if $H \leq G$, then $x \equiv y \pmod{H}$ iff $y^{-1}x \in H$ (or $x - y \in H$ if G is additive & abelian).

If I is an ideal of R, then write $x \equiv \bmod I$ iff $x - y \in I$.

If I, J are ideals, then $IJ = (ab : a \in I,\ b \in J)$
$= \{a_1 b_1 + \dots + a_k b_k : a_i \in I,\ b_i \in J\}$.

Note: $IJ \subseteq I \cap J$.

Example: $(9)(6) = (54) \subseteq \mathbb{Z}$ (product)
$(9) \cap (6) = (18) \subseteq \mathbb{Z}$ (lcm)
$(9) + (6)$ (gcd)

Similarly, we can define $\hat{\prod}_{i=1}^{} I_i$ in the obvious manner.

Motivation: In $\mathbb{Z}$, $(x, y) = 1$ iff $\exists\, a, b \in \mathbb{Z}$ s.t. $ax + by = 1 \in U(\mathbb{Z})$
or equivalently, $(x) + (y) = \mathbb{Z}$.

Prop 4.1 (The case for 2 ideals): Let R be a ring with 1, I, J ideals of R s.t. $I+J=R$. Then for any $r_1, r_2 \in R$, $\exists\ r \in R$ s.t. $r-r_1 \in I$ and $r-r_2 \in J$, i.e., $\exists\ r \in R$ that solves the system:

$$\begin{cases} x \equiv r_1 \mod I \\ x \equiv r_2 \mod J. \end{cases}$$

Pf: Write $1 = a+b$, $a \in I$, $b \in J$, and set $r = r_2 a + r_1 b$.

Claim: This works.

$$r - r_1 = (r - r_1 b) + r_1(b-1) = r_2 a + r_1(b-1) = r_2 a - r_1 a$$
$$= (r_2 - r_1)a \in I \ \checkmark$$

$$r - r_2 = (r - r_2 a) + r_2(a-1) = r_1 b + r_2(a-1) = r_1 b - r_2 b$$
$$= (r_1 - r_2)b \in J \ \checkmark$$

□

Prop 4.2 (The Chinese Remainder Theorem): Let R be a ring with 1 & $I_1, \dots, I_n$ ideals s.t. $I_j + I_k = R$ if $j \neq k$. Then for any $r_1, \dots, r_n \in R$, $\exists\ r \in R$ s.t. $x = r$ solves the system

$$\begin{cases} x \equiv r_1 \mod I_1 \\ \vdots \\ x \equiv r_n \mod I_n \end{cases}$$

Moreover, any 2 solutions are congruent modulo $I_1 \cap \dots \cap I_n$.

Pf: For $j = 2, \dots, n$, write $1 = a_j + b_j$ $a_j \in I_1$, $b_j \in I_j$.

Then, $1 = 1^{n-1} = (a_2 + b_2)(a_3 + b_3) \cdots (a_n + b_n) \in I_1 + \prod_{j=2}^{n} I_j = R$.

Now apply Prop 4.1: $\exists\ s_1 \in R$ s.t. $\begin{cases} s_1 \equiv 1 & \bmod I_1 \\ s_1 \equiv 0 & \bmod \hat{\prod}_{j=2} I_j \end{cases}$

Since $\hat{\prod}_{j=2} I_j \subseteq I_k$ $(k>1)$, $s_1 \equiv 0 \bmod I_k$ $(k>1)$.

Choose s_k similarly, i.e., so $\begin{cases} s_k \equiv 1 & \bmod I_k \\ s_k \equiv 0 & \bmod \prod_{j\neq k} I_j \end{cases}$

Now, set $r = \hat{\sum}_{k=1} r_k s_k$. Claim: This works.

Note: $r - r_j = \sum_{i\neq j} r_i s_i + r_j (s_j - 1)$ $\quad 1 \leq j \leq n$

$s_i \equiv 0 \bmod I_j$ $\qquad$ $(s_j - 1) \equiv 0 \bmod I_j$

If $s \in R$ is another solution, then $s \equiv r_j \equiv r \bmod I_j$, so by definition, $s \equiv r \bmod \hat{\bigcap}_{j=1} I_j$. □

Cor 4.3: Let $I_1, \ldots, I_n$ be ideals of R. Then $\exists$ ring homom

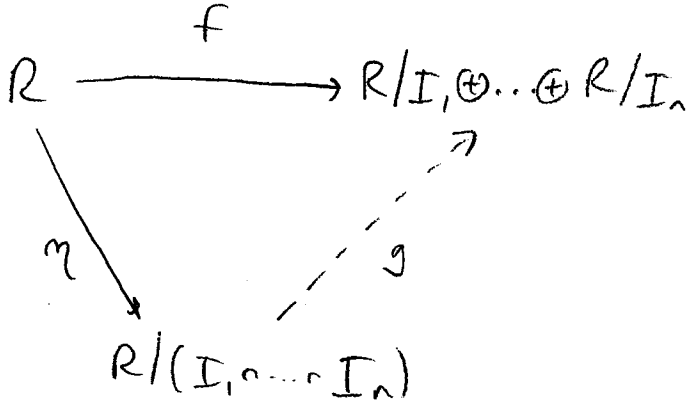
$$g: R/(I_1 \cap \cdots \cap I_n) \hookrightarrow R/I_1 \oplus \cdots \oplus R/I_n.$$

Moreover, if $1 \in R$ and $I_j + I_k = R$ $\forall j \neq k$, then g is an isom.

Pf: Define $f: R \to R/I_1 \oplus \cdots \oplus R/I_n$ by $f(r) = (r+I_1, \ldots, r+I_n)$.

This is clearly a homom, &

$\ker f = I_1 \cap \cdots \cap I_n$.



4

By the FHT for rings, $\exists!$ g that we seek.
(Exercise: show g is 1-1).

If R has 1 and $I_j + I_k = R$ for all $j \neq k$, then g is onto by the Chinese Remainder Theorem, so g is an isomorphism. □

Note:
- Surjectivity of g holds because every system can be solved
- Injectivity of g holds because all soln's are congruent modulo $\bigcap_{i=1}^{n} I_i$.

Note: If R is a Euclidean domain, then the proof of the CRT is Constructive!

Specifically, use the Euclidean algorithm to write

$$c_k m_k + d_k \prod_{j \neq k} m_j = GCD\left(m_k, \prod_{j \neq k} m_j\right) = 1, \text{ where } I_j = (m_j).$$

Then set $s_k = d_k \prod_{j \neq k} m_j$ and $r = r_1 s_1 + \cdots + r_n s_n$ is the soln.

Example: $R = \mathbb{Z}$. If $I_1, \cdots, I_n$ are ideals, with $I_j = (m_j)$ and $(m_i, m_j) = 1$ $i \neq j$, then $I_1 \cap \cdots \cap I_n = (m_1, m_2 \cdots m_n)$ and $\mathbb{Z}_{m_1 m_2 \cdots m_n} \cong \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_n}$.

Cor: Let $n = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$ p_i's distinct primes. Then

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{a_1}} \oplus \cdots \oplus \mathbb{Z}_{p_n^{a_n}}.$$