Chinese Remainder Theorem

Theorem (S. Lang Algebra Revised Printing 1971 p. 63)

A is a commutative unital ring, $I_1, \ldots, I_n$ are ideals such that $I_i + I_j = A \quad \forall\, i \neq j$. $x_1, \ldots, x_n \in A$

$\Rightarrow \exists\ x \in A$ such that $x \equiv x_i \pmod{I_i} \quad \forall\, i = 1, \ldots, n.$
(i.e. $x - x_i \in I_i$)

Proof. $n = 2$ $\quad 1 = a_1 + a_2 \quad a_1 \in I_1,\ a_2 \in I_2$

Let $x := x_2 a_1 + x_1 a_2$ $\quad x - x_1 = x_2 a_1 + x_1 a_2 - x_1$

$= x_2 a_1 + x_1 (a_2 - 1)$

$= x_2 a_1 + x_1 (-a_1) \in I_1$

Is this used?

Assume true for $n-1$ ideals. For $i \geq 2$ $\exists\ a_i \in I_1,\ b_i \in I_i$

$a_i + b_i = 1$ so $1 = (a_2 + b_2)(a_3 + b_3) \cdots (a_n + b_n)$

$\in I_1 + I_2 \cdots I_n$ ← ideal

and $A = I_1 + I_2 \cdots I_n$

By the case $n = 2$, $\exists\ y_1 \in A$

$y_1 \equiv 1 \pmod{I_1}$

$y_1 \equiv 0 \pmod{I_2 \cdots I_n}$

Similarly $\exists\ y_2 \in A$ (since $I_2 + I_i = A \quad i \neq 2$)

$y_2 \equiv 1 \pmod{I_2}$

$y_2 \equiv 0 \pmod{I_i} \quad i \neq 2$

$\vdots$

$\exists\ y_2, y_3, \ldots, y_n \in A$

$y_j \equiv 1 \pmod{I_j}$

$y_j \equiv 0 \pmod{I_i} \quad i \neq j$

Let $x = x_1y_1 + x_2y_2 + \cdots + x_ny_n$

$$x - x_1 \pmod{I_1} = x_1(y_1 - 1) + x_2y_2 + \cdots + x_ny_n \pmod{I_1}$$
$$\equiv 0 \pmod{I_1}$$

$$x - x_2 \pmod{I_2} = x_1y_1 + x_2(y_2 - 1) + x_3y_3 + \cdots + x_ny_n \pmod{I_2}$$
$$\equiv 0 \pmod{I_2}$$

$$\vdots$$

$$x - x_n \pmod{I_n} = x_1y_1 + x_2y_2 + \cdots + x_n(y_n - 1) \pmod{I_n}$$
$$\equiv 0 \pmod{I_n}$$

Q.E.D.

Corollary 1 (Lang p. 64) A is a commutative unital ring with ideals $I_1, \ldots, I_n$ satisfying $I_i + I_j = A \quad \forall i \neq j$

Let $f : A \longrightarrow \bigoplus_{i=1}^{n} A/I_i \qquad f(a) = (a + I_1, a + I_2, \ldots, a + I_n)$

Then the kernel of f is $\bigcap_{i=1}^{n} I_i$ (obvious) and f is surjective; (from the theorem)

thus $$A/\bigcap_{i=1}^{n} I_i \simeq \bigoplus_{i=1}^{n} A/I_i$$

Corollary 2 (T. Hungerford, Algebra 1974 P. 132)

Let $m_1, m_2, \ldots, m_n$ be positive integers with $(m_i, m_j) = 1 \quad \forall i \neq j$ (relatively prime) If $b_1, \ldots, b_n \in \mathbb{Z}$ then the system of congruences $x \equiv b_1 \pmod{m_1}, x \equiv b_2 \pmod{m_2}, \ldots, x \equiv b_n \pmod{m_n}$ has an integral solution that is uniquely determined by $m = m_1m_2 \cdots m_n$

Let $A = \mathbb{Z} \quad I_i = \mathbb{Z}m_i$ = all integral multiples of m_i

The Euclidean algorithm says $\exists \alpha, \beta \in \mathbb{Z} \quad 1 = \alpha m_i + \beta m_j \quad i \neq j$

so $\mathbb{Z} = I_i + I_j$ for $i \neq j$ and the theorem applies ///