The Chinese Remainder Theorem!
What about it?

Sachin Kumar
University of Waterloo, Faculty of Mathematics

June 2023

This essay will talk about the famous Chinese remainder theorem and its proof, in both elementary number theory and ring theory.

Theorem 0.1 (The Chinese Remainder Theorem (Ring Theory vers.))**.** *Let $I_1, \dots, I_n$ be ideals in a ring R which satisfy $I_i + I_j = R$ for $i \neq j$. Then we have $I_1 \cap \cdots \cap I_n = I_1 \cdots I_n$ and the morphism of rings,*

$$R \to \bigoplus_{i=1}^{n} R/I_i$$

is an endomorphism with kernel $I_1 \cap \cdots \cap I_n$.

Proof. As a obvious proof method, we will use induction to prove the following theorem. First, note that for any two ideals I_1 and I_2, we have that $I_1 I_2 \subset I_1 \cap I_2$ and $(I_1 + I_2)(I_1 \cap I_2) \subset I_1 I_2$, because any element of $I_1 + I_2$ multiplied by any element of $I_1 \cap I_2$ will clearly be a sum of products of elements from both I_1 and I_2. Thus, if I_1 and I_2 are coprime, ie., $I_1 + I_2 = (1) = R$, then $(1)(I_1 \cap I_2) = (I_1 \cap I_2) \subset I_1 I_2 \subset I_1 \cap I_2$, so that $I_1 \cap I_2 = I_1 I_2$. Thus, we proved the result for $n = 2$.
If the ideals $I_1, \dots, I_n$ are pairwise coprime and the result holds for $n - 1$, then

$$\bigcap_{i=1}^{n-1} I_i = \prod_{i=1}^{n-1} I_i$$

Because $I_n + I_i = (1)$ for each $1 \leq i \leq n-1$, there must be $x_i \in I_n$ and $y_i \in I_i$, such that $x_i + y_i = 1$. Thus,

$$z_n = \prod_{i=1}^{n-1} y_i = \prod_{i=1}^{n-1} (1 - x_i) \in \prod_{i=1}^{n-1} I_i$$

clearly, $z_n + I_n = 1 + I_n$, since each $x_i \in I_n$. Thus,

$$I_n + \prod_{i=1}^{n-1} I_i = I_n + \bigcap_{i=1}^{n-1} I_i = (1)$$

and, we now can apply the case $n = 2$ case to conclude that,

$$\bigcap_{i=1}^{n} I_i = \prod_{i=1}^{n} I_i$$

Note that for any i, we can construct a z_i with $z_i \in I_j$ for $j \neq i$ and $z_i + I_i = 1 + I_i$, via the same procedure. Define $\phi : R \to \bigoplus R/I_i$ by $\phi(a) = (a + I_1, \ldots, a + I_n)$. The,

$$\ker \phi = \bigcap_{i=1}^{n} I_i$$

because $a + I_i = 0 + I_i$ if and only if $a \in I_i$, so $\phi(a) = (0 + I_1, \ldots, 0 + I_n)$ if and only if $a \in I_i$ for all i, ie.,

$$a \in \bigcap_{i=1}^{n} I_i$$

Combined with our previous result,

$$\ker \phi = \prod_{i=1}^{n} I_i$$

Finally, recall that we constructed $z_i \in R$ such that $z_i + I_i = 1 + I_i$, and $z + I_j = 0 + I_j$ for all $i \neq j$, so that $\phi(z_i) = (0 + I_1, \ldots, 1 + I_i, \ldots, 0 + I_n)$. Thus, $\phi(a_1 z_1 + \cdots + a_n z_n) = (a_1 + I_1, \ldots, a_n + I_n)$, for all $a_i \in R$, so that ϕ is onto. By the first, isomorphism theorem, we have that

$$R/I_1 \cdots I_n \simeq \bigoplus_{i=1}^{n} R/I_i$$

Hence, we have proved the result. $\square$

Theorem 0.2 (The Chinese Remainder Theorem (Number Theory vers.)). *For all $a_1, a_2 \in \mathbb{Z}$, and $m_1, m_2 \in \mathbb{Z}_+$, if $\gcd(m_1, m_2) = 1$, then the simultaneous linear congruences,*

$$\begin{aligned} n &\equiv a_1 \pmod{m_1} \\ n &\equiv a_2 \pmod{m_2} \end{aligned}$$

have a unique solution modulo $m_1 m_2$. Thus, if $n = n_0$ is one particular solution, then the solutions are given by the set of all $n \in \mathbb{Z}$ such that,

$$n \equiv n_0 \pmod{m_1 m_2}$$

Proof. Let a_1 and a_2 be arbitrary integers, and $m_1, m_2 \in \mathbb{Z}_+$. Assume that $\gcd(m_1, m_2) = 1$. From the definition of congruence and divisibility, the set of solutions to the congruence $n \equiv a_1 \pmod{m}_1$ is given by, $\{m_1 x + a_1 : x \in \mathbb{Z}\}$. An element of this set satisfies the congruence $n \equiv a_2 \pmod{m}_2$ if and only if there exists $x \in \mathbb{Z}$, satsifying the linear congruence, $m_1 x \equiv a_2 - a_1 \pmod{m}_2$. Now, we have that $\gcd(m_1, m_2) = 1$, and hence and hence from the Linear Congruence Theorem with $d = 1$ and the definitions of congruence and divisibility, the set of solutions to the above linear congruence is given by $\{m_2 y + x_0 : y \in \mathbb{Z}\}$, where x_0 is one particular solution, that there exists. Hence, replacing x by $m_2 y + x_0$, the set of solutions to the simultaneous congruences is given by $\{m_1(m_2 y + x_0) + a_1 : y \in \mathbb{Z}\} = \{m_1 m_2 y + (m_1 x_0 + a_1) : y \in \mathbb{Z}\}$, which is simply the congruence class $[n_0] \in \mathbb{Z}_{m_1 m_2}$, where $n_0 = m_1 x_0 + a_1$ is one particular solution. $\square$

Can this theorem be generalized?, ie., what if there are n simultaneous linear congruences? Will this theorem hold? Aparently, yes!

Theorem 0.3. *For all $k, m_1, m_2, \ldots, m_k \in \mathbb{Z}_+$ and $a_1, \ldots, a_k \in \mathbb{Z}$, if $\gcd(m_i, m_j) = 1$ for all $i \neq j$, the simultaneous linear congruences*

$$\begin{aligned} n &\equiv a_1 \pmod{m_1} \\ n &\equiv a_2 \pmod{m_2} \\ &\vdots \\ n &\equiv a_k \pmod{m_k} \end{aligned}$$

have a unique solution modulo $m_1 m_2 \cdots m_k$*. This, if* $n = n_0$ *is one particular solution, then the solutions are given by the set of all* $n \in \mathbb{Z}$ *such that,* $n \equiv n_0 \pmod{m_1 m_2 \cdots m_k}$*.*

What about the proof? It is trivial, by following the technique from previous theorem's proof.