Chinese Remainder Theorem

S. Kumaresan
School of Math. and Stat.
University of Hyderabad
Hyderabad 500046
kumaresa@gmail.com

Theorem 1 (Chinese Remainder Theorem)**.** *Let R be a principal ideal domain. Let $p_1, \ldots, p_n$ be pairwise relatively prime elements of R. Let x_i, $1 \leq i \leq n$ be arbitrary elements of R. Then there exists $x \in R$ such that $x \equiv x_i \pmod{p_i}$ for each i. If y also has this property then $x \equiv y \pmod{p_1 \cdots p_n}$.*

Proof. We claim that there exist elements y_i, $1 \leq i \leq n$, such that

$$y_i \equiv 1 \pmod{p_i}, \text{ and } y_i \equiv 0 \pmod{p_j} \text{ for } j \neq i.$$

If they exist, we let $x := x_1y_1 + \cdots + x_ny_n$, then x is as required.

As a first guess, we consider $q_i := p_1 \cdots \widehat{p_i} \cdots p_n$. Then p_i and q_i are relatively prime. Hence there exist $a_i, b_i \in R$ such that $a_iq_i + b_ip_i = 1$. If we take $y_i := a_iq_i$, then y_i is as required.

The last claim (concerning 'uniqueness') is easily seen. if x and y both satisfy the congruences, then each p_i divides $x - y$. Since p_i are pairwise relatively prime, the product $p_1 \cdots p_n$ divides $x - y$. □

Remark 2. Note that the proof is constructive in the sense it gives us an algorithm to solve the system of simultaneous congruences. See Examples below.

Example 3. A concrete example. What is the least positive integer n which leaves 2,3,2 respectively as remainders when divided by 3,5 and 7? This was a problem posed by Sun-Tsu in the first century.

We are required to solve the simultaneous congruences $x \equiv 2 \pmod{3}$, $x \equiv 3 \pmod{5}$ and $x \equiv 2 \pmod{7}$. We follow the method outlined in the proof of Theorem 1.

We have $p_1 = 3$, $p_2 = 5$ and $p_3 = 7$ and $q_1 = 35$, $q_2 = 21$ and $q_3 = 15$. We are looking for y_i such that $y_i \equiv 1 \pmod{p_i}$ and $y_i \equiv 0 \pmod{q_i}$, for $1 \leq i \leq 3$. We shall do this example in detail.

The congruences

$$y_1 \equiv 1 \pmod{3} \text{ and } y_1 \equiv 0 \pmod{35}$$

has 70 as a solution.

The congruences

$$y_2 \equiv 1 \pmod{5} \text{ and } y_2 \equiv 0 \pmod{21}$$

has 21 as a solution.

The congruences

$$y_3 \equiv 1 \pmod 7 \text{ and } y_1 \equiv 0 \pmod{15}$$

has 15 as a solution. Hence $x = x_1y_1 + x_2y_2 + x_3y_3 = 2 \times 70 + 3 \times 21 + 2 \times 15 = 233$ is a solution. Since $p_1p_2p_3 = 105$, we see that $23 = 233 - 2 \times 105$ is the smallest solution.

Example 4. This is due to Bhaskara in 6th century. A basket contains n eggs. If the eggs are removed 2,3,4,5, or 6 at a time, then the number of eggs that remain in the basket are 1,2,3,4 or 5 respectively. If the eggs are removed 7 at a time, then no eggs remain. What is the smallest number n of eggs that could have been in the basket at the start of this procedure?

We need to solve the simultaneous congruences

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 4 \\ x &\equiv 4 \pmod 5 \\ x &\equiv 5 \pmod 6. \end{aligned}$$

We cannot apply CRT directly here. (Why?) We may solve the system of the first three congruences as in the last example. We have $p_1 = 3$, $p_2 = 4$ and $p_3 = 5$ and $q_1 = 20$, $q_2 = 15$ and $q_3 = 12$. We are looking for y_i such that $y_i \equiv 1 \pmod{p_i}$ and $y_i \equiv 0 \pmod{q_i}$, for $1 \leq i \leq 3$.

We find that $y_1 = 40$, $y_2 = 45$ and $y_3 = 36$ are obvious solutions. We have $x = 359 \equiv 59 \pmod{60}$. Hence 59 is the smallest solution for the first 3 congruences. It turns out that it is also a solution of the fourth.

Ex. 5. Find all solutions of $x \equiv 2 \pmod 3$, $x \equiv 1 \pmod 4$ and $x \equiv 3 \pmod 5$.

A more general version is the following. We need a definition. We say that two ideals I and J of a ring R are *comaximal* if $I + J = R$. An obvious example is a pair of distinct maximal ideals or nonzero primes ideals in a PID.

Theorem 6. *Let R be a ring with identity. Let I_j, $1 \leq j \leq n$ be ideals of R such $I_i + I_j = R$ for $i \neq j$, that is, I_j's are pairwise comaximal ideals. Then the map*

$$f\colon R \to (R/I_1) \times \cdots \times (R/I_n) \text{ defined by } f(r) := (r + I_1, \ldots, r + I_n)$$

is an onto homomorphism with $\ker f = I_1 \cap \cdots \cap I_n$.

Proof. That the map is a ring homomorphism is trivial to check. So is the claim about the kernel. We need only establish that f is onto.

Thus, given r_i, $1 \leq i \leq n$, we need to find $r \in R$ such that $r \equiv r_i \pmod{I_i}$. We adapt the proof in the last theorem.

We find $s_i \in I_i$ such that $s_i \equiv 1 \pmod{I_i}$ and $s_i \equiv 0 \pmod{\cap_{j \neq i} I_j}$. Let us do this when $n = 2$ and reduce the general case to this.

Since $I_1 + I_2 = R$, there exist $a_1, a_2 \in I_1$ such that $a_1 + a_2 = 1$. We let $r = a_2 r_1 + a_1 r_2$. Then

$$\begin{aligned} r &\equiv a_2 r_1 \,(\mathrm{mod}\, I_1) \equiv r_1 \,(\mathrm{mod}\, I_1) \\ r &\equiv a_1 r_2 \,(\mathrm{mod}\, I_2) \equiv r21 \,(\mathrm{mod}\, I_2). \end{aligned}$$

In the above, we used the observation that since $a_2 \equiv 1 \,(\mathrm{mod}\, I_1)$, multiplying this congruence by r_1, we obtain $a_2 r_1 \equiv r_1 \,(\mathrm{mod}\, I_1)$.

Now we turn to $n \geq 3$. Since $I_i + I_k = 1$, for each $j \neq 1$, there exist $a_j \in I_1$ and $b_j \in I_j$ such that $a_j + b_j = 1$. Consider the product $1 = \prod_{j \neq i}(a_j + b_j)$. Except the term $b_2 \cdots b_n$, all other term involve some a_j and hence all these (other) terms lie in I_1. On the other hand, $b_2 \cdots b_n \in I_2 \cap \cdots \cap I_n$. We conclude that $1 \in I_1 + \cap_{j \neq 1} I_j$ and hence $I_1 + \cap_{j \neq 1} I_j = R$. From the $n = 2$ case above, there exists $s_1 \in I_1$ such that $s_1 \equiv 1 \,(\mathrm{mod}\, I_1)$ and $s_1 \equiv 0 \,(\mathrm{mod} \cap_{j \neq 1} I_j)$.

Since $I_i + I_j = 1$ for $j \neq i$, we can argue as in the case when $i = 1$ to obtain $s_i \in I_i$ such that

$$s_i \equiv 1 \,(\mathrm{mod}\, I_i) \quad \text{and} \quad s_i \equiv 0 \,(\mathrm{mod} \cap_{j \neq i} I_j).$$

> We can prove that $I_i + \cap_{j \neq i} I_j = R$ as follows. Let $J := \cap_{j \neq i} I_j$. If $I_i + J \neq R$, then there exists a maximal ideal P such that $I_i + J \subset P$. Since $I_1 \cdots \widehat{I_i} \cdots I_n \subset I_j$ for each $j \neq i$, it follows that $I_1 \cdots \widehat{I_i} \cdots I_n \subset J$. Hence the product of the ideals I_j, $j \neq i$, lies in the prime ideal P and hence at least one $I_j \subset P$. Since $j \neq i$, we have $R = I_j + I_i \subset P$, a contradiction.

If we let $r := r_1 s_1 + \cdots + r_n s_n$, then r is as required. □

We now give some examples of applications of CRT.

Example 7. Let $n = n_1 \cdots n_k$ be decomposition of $n \in \mathbb{N}$ into pairwise relatively prime integers n_i. Then as rings

$$\mathbb{Z}_n \simeq \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_k}.$$

We also have $U(\mathbb{Z}_n) = \oplus_{j=1}^{k} U(\mathbb{Z}_{n_j})$. □

Example 8. Let F be a field. Let $\alpha_i \in F$, $1 \leq i \leq n$ be distinct elements in F. Consider $f(x) := (x - \alpha_1) \cdots (x - \alpha_n)$. Then

$$F[x]/(f(x)) \simeq F^n, \text{ as } F[x]/((x - \alpha)) \simeq F.$$

Example 9. Let R be a PID. Let $a = u p_1^{m_1} \cdots p_n^{m_n}$ be the unique factorization of a nonzero nonunit element a (with u being a unit). Then we have ring isomorphism

$$R/(a) \simeq (R/(p_1^{m_1})) \times \cdots \times (R/(p_n^{m_n})).$$

Example 10. This is an application the Euler's totient function $\varphi \colon \mathbb{N} \to N$. Recall that, for any natural number n, the value of $\varphi(n)$ is the number of natural numbers k with $1 \leq k \leq n$ which are relatively prime to n.

Observe that in terms of algebra, $\varphi(n)$ is the number of elements in $U(\mathbb{Z}_n)$, the group of units in the ring $\mathbb{Z}_n$,

For example, if p is a prime, then $\varphi(p) = p - 1$. More generally, if $n = p^k$, then $\varphi(p^k) = p^{k-1}(p-1)$. For, if $1 \le k \le n$ is such that $\gcd(n,k) > 1$, then k must be a multiple of p: $p, 2p, \dots, p^k - p$. There are p^{k-1} of such numbers. So, $\varphi(p^k) = p^k - p^{k-1}$.

It follows (from Example 7) that $\varphi(mn) = \varphi(m)\varphi(n)$ if m and n are relatively prime.

If $n = p_1^{m_1} \cdots p_k^{m_k}$ is the prime decomposition, we arrive the following explicit formula for $\varphi(n)$:

$$\varphi(n) = \prod_{j=1}^{k} p_j^{m_j - 1}(p_j - 1) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

where the product is taken over all primes p dividing n.

Ex. 11. Let R be a commutative ring with 1. Assume that I_j, $1 \le j \le n$, are pairwise comaximal. Then we have

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

We prove this by induction. It is clear that $I_1 I_2 \subset I_1 \cap I_2$. To prove the reverse inclusion, let $x \in I_1 \cap I_2$. Write $1 = a_1 + a_2 \in I_1 + I_2 = R$. Then $x = xa_1 + xa_2 \in I_1.I_2$

Assume that $n \ge 3$ and let $J := I_1 \cdots I_{n-1} = I_1 \cap \cdots \cap I_{n-1}$. We have already seen (in the course of proof of Theorem 6 that $J + I_n = R$. Hence by $n = 2$ case, we have

$$I_1 \cap \cdots \cap I_{n-1} \cap I_n = J \cap I_n = JI_n = I_1 \cdots I_{n-1} I_n.$$

Ex. 12. This is CRT in the context of modules. Let N_j, $1 \le j \le k$ be submodules of an R-module M. Assume that

$$N_i + (N_1 \cap \cdots \cap N_{i-1} \cap N_{i+1} \cap \cdots \cap N_k) = R.$$

Prove that $M/\cap_{j=1}^{k} N_j \simeq (M/N_1) \oplus \cdots \oplus (M/N_k)$.

Remark 13. Some other concepts which are related to the Bezout type identity which we needed in the proofs above are partition of unity, resolution of identity, idempotent elements, projection maps relative to a direct sum and Lagrange interpolation. We explain the last one leaving the others for the exploration by the reader.

If we are given a self-adjoint linear map T over a finite dimensional inner product space V (over $\mathbb{R}$ or $\mathbb{C}$), the spectral theorem allows us to decompose V into an orthogonal direct sum of eigenspaces. If λ_j, $1 \le j \le k$ are the distinct (necessarily real) eigenvalues, the Lagrange interpolation gives rise to the polynomials

$$p_i(x) := \frac{\prod_{j \ne i}(x - \lambda_j)}{\prod_{j \ne i}(\lambda_i - \lambda_j)}.$$

Note that $p_i(\lambda_j) = \delta_{ij}$ and the operators $p_i(T)$ satisfy

$$I = p_1(T) + \cdots + p_k(T),$$

the so-called (spectral) resolution of the identity. Each $p_i(T)$ projects V onto the eigenspace of λ_i.