An Exploration of the Chinese Remainder Theorem

William M. Faucette

University of West Georgia

Summer 2021

Outline

The Chinese Remainder Theorem

We start with a standard result in number theory:

Theorem (Chinese Remainder Theorem)

Let $n_1, n_2, \ldots, n_r$ be positive integers such that $\gcd(n_i, n_j) = 1$ for $i \neq j$. Then the system of linear congruences

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \qquad\quad \vdots \\ x &\equiv a_r \pmod{n_r} \end{aligned}$$

has a simultaneous solution, which is unique modulo $N = n_1 n_2 \cdots n_r$.

The Chinese Remainder Theorem

The solution is found following this process.
Let $N = n_1 \cdots n_r$ and $N_i = N/n_i$. Since the n_i's are relatively prime, the greatest common divisor of N_i and n_i is 1. So, there exists a multiplicative inverse x_i so that $x_i N_i \equiv 1 \,(\text{mod } \mathrm{n_i})$. So, we have

$$x_i N_i \equiv \begin{cases} 1 \,(\text{mod } \mathrm{n_i}) \\ 0 \,(\text{mod } \mathrm{n_j}) \ \text{ for } j \neq i. \end{cases}$$

The solution to the system of congruences is then

$$x = a_1 x_1 N_1 + \cdots + a_r x_r N_r.$$

Example 1

Example

Find all solutions of the system of congruences

$$x \equiv 2 \pmod{3}$$
$$x \equiv 3 \pmod{5}$$
$$x \equiv 2 \pmod{7}.$$

Example 1

Solution

Here, $n_1 = 3$, $n_2 = 5$, *and* $n_3 = 7$.
Let $N = 3 \cdot 5 \cdot 7 = 105$.
Let

$$N_1 = \frac{N}{n_1} = 5 \cdot 7 = 35$$
$$N_2 = \frac{N}{n_2} = 3 \cdot 7 = 21$$
$$N_3 = \frac{N}{n_3} = 3 \cdot 5 = 15.$$

Note that N_i *and* n_i *are relatively prime for each* i.

Example 1

Solution

We compute

$$N_1 \cdot x_1 = 35 \cdot 2 = 70 \equiv 1 \pmod 3$$
$$N_2 \cdot x_2 = 21 \cdot 1 = 21 \equiv 1 \pmod 5$$
$$N_3 \cdot x_3 = 15 \cdot 1 = 15 \equiv 1 \pmod 7 .$$

So,

$$x_1 = 2$$
$$x_2 = 1$$
$$x_3 = 1.$$

Example 1

Solution

Our solution is then

$$\begin{aligned} x &\equiv a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3 \pmod{\mathrm{N}} \\ &\equiv 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 \pmod{105} \\ &\equiv 140 + 63 + 30 \pmod{105} \\ &\equiv 233 \pmod{105} \\ &\equiv 23 \pmod{105}. \end{aligned}$$

Notice that $23 \equiv 2 \pmod{3}$, $23 \equiv 3 \pmod{5}$, $23 \equiv 2 \pmod{7}$, *so this is a solution of the system of congruences.*

All other solutions are $23 + 105k$ *for* $k \in \mathbb{Z}$.

A Closer Look

Let's look at this a bit more closely.

The number n_i corresponds to a principal ideal (n_i) in the ring $\mathbb{Z}$.

Since n_i and n_j are relatively prime, there exists integers $a, b \in \mathbb{Z}$ so that $an_i + bn_j = 1$.

Hence the sum of the ideals (n_i) and (n_j) is the entire ring $\mathbb{Z}$.

$$(n_i) + (n_j) = \mathbb{Z}.$$

A Closer Look

$$(n_i) + (n_j) = \mathbb{Z}.$$

Further, the intersection of these ideals (n_i) is the principal ideal (N) generated by $N = \text{lcm}(\text{n}_\text{i})$, which is the product $\prod_i n_i$ if these factors are pairwise relatively prime.

$$(N) = \bigcap_{i=1}^{r} (n_i) = \prod_{i=1}^{r} (n_i) = \left(\prod_{i=1}^{r} n_i \right).$$

Coprime Ideals

Generalizing this property, we define ideals $\mathfrak{a}$ and $\mathfrak{b}$ in a (commutative) ring R to be **coprime** (or **comaximal**) if

$$\mathfrak{a} + \mathfrak{b} = R.$$

The map from R to $\prod_i R/\mathfrak{a}_i$

For ideals $\mathfrak{a}_i$ in a ring R we have natural quotient maps $\varphi_i : R \to R/\mathfrak{a}_i$, which we can put together to give a ring homomorphism

$$\varphi : R \to \prod_i R/\mathfrak{a}_i$$
$$\varphi(x) = (\varphi_i(x))_i$$

The kernel of this map is easily seen to be the intersection $\bigcap_i \mathfrak{a}_i$.

The map from R to $\prod_i R/\mathfrak{a}_i$

If the ideals $\mathfrak{a}_i$ in a ring R are pairwise coprime, then the homomorphism $\varphi : R \to \prod_i R/\mathfrak{a}_i$ is surjective.

Let's see that.

The map from R to $\prod_i R/\mathfrak{a}_i$

Fix i. For each $j \neq i$, there exist $x_j \in \mathfrak{a}_i$ and $y_j \in \mathfrak{a}_j$ so that $x_j + y_j = 1$. Then $y_j = 1 - x_j \equiv 1 \pmod{\mathfrak{a}_i}$ and $y_j \equiv 0 \pmod{\mathfrak{a}_j}$ for $j \neq i$. Letting $e_i = \prod_{j \neq i} y_j$ satisfies

$$e_i \equiv 1 \pmod{\mathfrak{a}_i} \quad \text{and} \quad e_i \equiv 0 \pmod{\mathfrak{a}_j} \quad \text{for } j \neq i.$$

That is, e_i maps to $(0, \ldots, 0, 1, 0, \ldots, 0) \in \prod_i R/\mathfrak{a}_i$, where 1 is in the i^{th} place.

Then the element $x = \sum_i a_i e_i$ maps to $(a_1, a_2, \ldots, a_n)$.

Example 2

As a second example, let $\mathbb{Z}$ be the ring of integers and let (r) and (s) be ideals in $\mathbb{Z}$ with $\gcd(r, s) = 1$.

We have the natural quotient homomorphisms

$$\varphi_r : \mathbb{Z} \to \mathbb{Z}/(r),$$
$$\varphi_s : \mathbb{Z} \to \mathbb{Z}/(s).$$

We can put together these homomorphisms to give us a homomorphism into the product:

$$\varphi : \mathbb{Z} \to \mathbb{Z}/(r) \times \mathbb{Z}/(s).$$

Example 2

Since r and s are relatively prime, the ideals (r) and (s) are coprime, so the Chinese Remainder Theorem gives us an epimorphism

$$\mathbb{Z} \to \mathbb{Z}/(r) \times \mathbb{Z}/(s)$$

with kernel (rs), so this gives us an isomorphism

$$\mathbb{Z}/(rs) \to \mathbb{Z}/(r) \times \mathbb{Z}/(s).$$

This is a special case of the theorem on the classification of finite abelian groups.

Example 2

As concrete examples . . .

Example

1. $\mathbb{Z}/(15) = \mathbb{Z}/(3 \cdot 5) \cong \mathbb{Z}/(3) \times \mathbb{Z}/(5)$
2. $\mathbb{Z}/(21) = \mathbb{Z}/(3 \cdot 7) \cong \mathbb{Z}/(3) \times \mathbb{Z}/(7)$
3. $\mathbb{Z}/(187) = \mathbb{Z}/(11 \cdot 17) \cong \mathbb{Z}/(11) \times \mathbb{Z}/(17)$

Example 3

As a third example, let $\mathbb{Q}[x]$ be a polynomial ring over the rational numbers. Let $p(x) \in \mathbb{Q}[x]$ be a monic irreducible polynomial of degree at least 2.

Then $K = \mathbb{Q}[x]/(p(x))$ is a finite extension field of $\mathbb{Q}$.

A finite extension field of the field of rational numbers is called a **number field**.

Irreducible Polynomials Have Distinct Roots

We remark that all the roots of $p(x)$ in any number field must be distinct.

Suppose $p(x)$ has a root α of multiplicity at least 2. Then over some field $p(x) = q(x)(x-\alpha)^n$, with $n \geq 2$. Taking the derivative, we get

$$\begin{aligned} p'(x) &= q'(x)(x-\alpha)^n + q(x) \cdot n(x-\alpha)^{n-1} \\ &= [q'(x)(x-\alpha) + nq(x)](x-\alpha)^{n-1}. \end{aligned}$$

Since $n \geq 2$, $p'(\alpha) = 0$.

Irreducible Polynomials Have Distinct Roots

We have just shown that α is a root of both $p(x)$ and $p'(x)$.

Since $p(x)$ and $p'(x)$ are polynomials with rational coefficients which have a common root, they must have a common factor.

Since p is irreducible and p' has smaller degree than p, this is a contradiction.

Example 3

The natural inclusion of the field of rational numbers into the field of complex numbers (or any other algebraically closed field containing $\mathbb{Q}$), induces a ring homomorphism

$$\varphi : \mathbb{Q}[x]/(p(x)) \to \mathbb{C}[x]/(p(x)).$$

Since $p(x)$ is irreducible over $\mathbb{Q}$, $\mathbb{Q}[x]/(p(x))$ is our number field K.

However, $p(x)$ is no longer irreducible in $\mathbb{C}[x]$, so $\mathbb{C}[x]/(p(x))$ is not a field.

We will use the Chinese Remainder Theorem to see what it is.

Example 3

Since the field of complex numbers is algebraically closed, $p(x)$ factors into linear factors in $\mathbb{C}[x]$: $p(x) = \prod_i (x - r_i)$ with $r_i \in \mathbb{C}$ being the complex roots of p.

Since p is irreducible these roots are distinct. This means the ideals $(x - r_i)$ are pairwise coprime. That means we can use the Chinese Remainder Theorem.

Example 3

The Chinese Remainder Theorem gives us an isomorphism

$$\mathbb{C}[x]/\prod_{i=1}^{n}(x-r_i) \cong \prod_{i=1}^{n}\mathbb{C}[x]/(x-r_i) \cong \mathbb{C}^n,$$

where this last map is given by sending $f(x) \in \mathbb{C}[x]$ to $(f(r_i))_i$.

Example 3

Composing this isomorphism with our original map of K into $\mathbb{C}[x]/(p(x))$, we get a homomorphism

$$K \to \mathbb{C}[x]/\prod_i (x - r_i) \cong \prod_{i=1}^{n} \mathbb{C}[x]/(x - r_i) \cong \mathbb{C}^n,$$

where this last map is given by sending $f(x) \in \mathbb{Q}[x]$ to $(f(r_i))_i \in \mathbb{C}^n$.

Let $\sigma_i : K \to \mathbb{C}$ be the projection of this last map onto the ith coordinate. This gives n embeddings of the number field K into the field of complex numbers.

The Trace and Norm

Let $\sigma_i : K \to \mathbb{C}$ be the n embeddings of the number field K into the field of complex numbers constructed in the last frame.

Definition

The **trace** of an element α in the number field K is the sum

$$T(\alpha) = \sigma_1(\alpha) + \sigma_2(\alpha) + \cdots + \sigma_n(\alpha).$$

The **norm** of an element α in the number field K is the product

$$N(\alpha) = \sigma_1(\alpha)\sigma_2(\alpha)\cdots\sigma_n(\alpha).$$

The Trace and Norm

For any $\alpha \in K$, $T(\alpha)$ and $N(\alpha)$ lie in $\mathbb{Q}$.

If $\alpha \in K$ is an algebraic integer, that is, the root of a monic polynomial with coefficients in K, then $T(\alpha)$ and $N(\alpha)$ lie in $\mathbb{Z}$.

Further, the trace function is additive and the norm function is multiplicative:

$$T(\alpha + \beta) = T(\alpha) + T(\beta)$$
$$N(\alpha\beta) = N(\alpha)N(\beta).$$

Example 4

Let $p(x) = x^2 - q$ where q be a square-free a rational number. Then $p(x)$ is irreducible in $\mathbb{Q}$. The field

$$K = \mathbb{Q}[x]/(x^2 - q) \cong \mathbb{Q}[\sqrt{q}] = \{a + b\sqrt{q} \mid a, b \in \mathbb{Q}\}.$$

There are two embeddings of K in $\mathbb{C}$:

$$\sigma_1 : \mathbb{Q}[\sqrt{q}] \to \mathbb{C} \qquad \sigma_2 : \mathbb{Q}[\sqrt{q}] \to \mathbb{C}$$
$$\sigma_1(a + b\sqrt{q}) = a + b\sqrt{q} \qquad \sigma_2(a + b\sqrt{q}) = a - b\sqrt{q}$$

Example 4

$$\sigma_1 : Q[\sqrt{q}] \to \mathbb{C} \qquad \sigma_2 : Q[\sqrt{q}] \to \mathbb{C}$$
$$\sigma_1(a + b\sqrt{q}) = a + b\sqrt{q} \qquad \sigma_2(a + b\sqrt{q}) = a - b\sqrt{q}$$

Then

$$T(a + b\sqrt{q}) = (a + b\sqrt{q}) + (a - b\sqrt{q}) = 2a$$
$$N(a + b\sqrt{q}) = (a + b\sqrt{q})(a - b\sqrt{q}) = a^2 - qb^2$$

Notice both these numbers are rational numbers.

Example 5

Let $p(x) = x^3 - 2$. Then $p(x)$ is irreducible in $\mathbb{Q}$. The field

$$K = \mathbb{Q}[x]/(x^3 - 2) \cong \mathbb{Q}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} \mid a, b \in \mathbb{Q}\}.$$

There are three embeddings of K in $\mathbb{C}$:

$$\begin{aligned}
\sigma_1 &: Q[\sqrt[3]{2}] \to \mathbb{C} \\
\sigma_1(a + b\sqrt[3]{2}) &= a + b\sqrt[3]{2} \\
\sigma_2 &: Q[\sqrt[3]{2}] \to \mathbb{C} \\
\sigma_2(a + b\sqrt[3]{2}) &= a + b\omega\sqrt[3]{2} \\
\sigma_3 &: Q[\sqrt[3]{2}] \to \mathbb{C} \\
\sigma_3(a + b\sqrt[3]{2}) &= a + b\omega^2\sqrt[3]{2}
\end{aligned}$$

where ω is a primitive cube root of 1. We note that $\omega^2 + \omega + 1 = 0$.

Example 5

Then

$$\begin{aligned} T(a+b\sqrt[3]{2}) &= (a+b\sqrt[3]{2})+(a+b\omega\sqrt[3]{2})+(a+b\omega^2\sqrt[3]{2}) \\ &= 3a+b\sqrt[3]{2}\left(1+\omega+\omega^2\right) \\ &= 3a \\ N(a+b\sqrt[3]{2}) &= (a+b\sqrt[3]{2})(a+b\omega\sqrt[3]{2})(a+b\omega^2\sqrt[3]{2}) \\ &= (a^3+2b^3)+a^2b\sqrt[3]{2}(\omega^2+\omega+1)+ab^2\sqrt[3]{4}(\omega^2+\omega+1) \\ &= a^3+2b^3 \end{aligned}$$

Notice both these numbers are rational numbers.

Using the Norm

If α is an algebraic integer in some number field, then the norm of α, $N(\alpha)$, is an integer.

This is because the norm of α is always a rational number. And if the rational number is an algebraic integer, it must be a rational integer. That is, it must lie in $\mathbb{Z}$.

The same is true for the trace of α, $T(\alpha)$.

Using the Norm

Since the norm function is multiplicative, for any unit α in the ring of algebraic integers, there exists an algebraic integer β so that $\alpha\beta = 1$. Then

$$N(\alpha)N(\beta) = N(\alpha\beta) = N(1) = 1.$$

So, if α is a unit and an algebraic integer, its norm must be ± 1. The converse of this is also true.
This implies that the norms of associates in the ring of algebraic integers must be the same up to sign.

Using the Norm

Example

The norm and trace on the number field $\mathbb{Q}[\sqrt{-5}]$ is given by

$$N(a + b\sqrt{-5}) = a^2 + 5b^2$$
$$T(a + b\sqrt{-5}) = 2a.$$

The ring of algebraic integers is the set of all elements of $\mathbb{Q}[\sqrt{-5}]$ where both these numbers are integers. This forces a and b to be integers. So, the ring of algebraic integers in $\mathbb{Q}[\sqrt{-5}]$ is $\mathbb{Z}[\sqrt{-5}]$.

Using the Norm

Example

First, we compute

$$N(2) = 2^2 + 5 \cdot 0^2 = 4$$
$$N(3) = 3^2 + 5 \cdot 0^2 = 9$$
$$N(1 \pm \sqrt{-5}) = 1^2 + 5 \cdot 1^2 = 6.$$

Since associates must have the same norm, we see that neither 2 nor 3 is an associate of $1 \pm \sqrt{-5}$.

Using the Norm

Example

Suppose $N(a + b\sqrt{-5}) = 2$. Then the integers a and b must satisfy

$$a^2 + 5b^2 = 2.$$

This is not possible, so there is no element of norm 2 in $\mathbb{Z}[\sqrt{-5}]$.

Similarly, there is no element of norm 3 in $\mathbb{Z}[\sqrt{-5}]$.

Using the Norm

Example

It follows that 2, 3, and $1 \pm \sqrt{-5}$ are irreducible, since the only proper divisors of their norms are 2, 3, or both.

Since

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}),$$

we see that $\mathbb{Z}[\sqrt{-5}]$ is not a unique factorization domain.

Using the Norm

So, the norm and trace can be used to determine if a ring of algebraic integers is a unique factorization domain.

This is a central problem in number theory that sparked a great deal of development in commutative algebra in the late nineteenth century.

A Note of Thanks

Thank you for attending.