The Chinese Remainder Theorem

Kyle Miller

Feb 13, 2017

The Chinese Remainder Theorem says that systems of congruences always have a solution (assuming pairwise coprime moduli):

Theorem 1. *Let $n, m \in \mathbb{N}$ with $\gcd(n, m) = 1$. For any $a, b \in \mathbb{Z}$, there is a solution x to the system*

$$\begin{aligned} x &\equiv a \pmod{n} \\ x &\equiv b \pmod{m} \end{aligned}$$

In fact, the solution is unique modulo nm.

The key fact which lets us solve such a congruence is the following. Suppose we manage to find two numbers $\alpha, \beta \in \mathbb{Z}$ with the following four properties:

$$\begin{aligned} \alpha &\equiv 1 \pmod{n} & \qquad \alpha &\equiv 0 \pmod{m} \\ \beta &\equiv 0 \pmod{n} & \qquad \beta &\equiv 1 \pmod{m} \end{aligned}$$

Then, $x = \alpha a + \beta b$ is a solution to the system of congruences. This is because

$$\begin{aligned} \alpha a + \beta b \equiv_n 1a + 0b \equiv_n a \\ \alpha a + \beta b \equiv_m 0a + 1b \equiv_m b \end{aligned}$$

(where $x \equiv_n y$ is shorthand for $x \equiv n \pmod{n}$).

But, how do we find such a pair α and β? It turns out that Bézout's theorem gives us these. Since $\gcd(n, m) = 1$, there are two numbers $\nu, \mu \in \mathbb{Z}$ such that $1 = \nu n + \mu m$. This equation leads to the following congruences:

$$1 = \nu n + \mu m \equiv_n \nu 0 + \mu m \equiv_n \mu m$$

and

$$1 = \nu n + \mu m \equiv_m \nu n + \mu 0 \equiv_m \nu n$$

Thus,

$$\begin{aligned} \mu m &\equiv 1 \pmod{n} & \qquad \mu m &\equiv 0 \pmod{m} \\ \nu n &\equiv 0 \pmod{n} & \qquad \nu n &\equiv 1 \pmod{m} \end{aligned}$$

so $\alpha = \mu m$ and $\beta = \nu n$ are numbers which will do the job.

And, how do we calculate μ and ν? The extended Euclid's algorithm is able to compute them.

1 An extension

Suppose we have a system of three congruences:

$$\begin{aligned} x &\equiv a \pmod{n} \\ x &\equiv b \pmod{m} \\ x &\equiv c \pmod{\ell} \end{aligned}$$

such that $\gcd(n,m) = 1$, $\gcd(n,\ell) = 1$, and $\gcd(m,\ell) = 1$. One way to proceed is to solve the system consisting of only the first two congruences, which gives $x \equiv d \pmod{nm}$, and then solving the resulting system of two congruences.

Though, using similar logic to the two-congruence case, if we manage to find three numbers $\alpha, \beta, \gamma \in \mathbb{Z}$ with the following nine properties:

$$\begin{array}{lll} \alpha \equiv 1 \pmod{n} & \alpha \equiv 0 \pmod{m} & \alpha \equiv 0 \pmod{\ell} \\ \beta \equiv 0 \pmod{n} & \beta \equiv 1 \pmod{m} & \beta \equiv 0 \pmod{\ell} \\ \gamma \equiv 0 \pmod{n} & \gamma \equiv 0 \pmod{m} & \gamma \equiv 1 \pmod{\ell} \end{array}$$

then $x = \alpha a + \beta b + \gamma c$ is a solution to the system of congruences.

One way to produce such a trio of numbers is to compute many modulo inverses. To give some idea for how to come by this, for α, we want a number divisible by $m\ell$ but which leaves remainder 1 when divided by n. Since $\gcd(n, m\ell) = 1$, then $1 = \mu n + \nu m\ell$ for some $\mu, \nu \in \mathbb{Z}$, and thus $\alpha = \nu m\ell$ is a number with the correct property: $\nu m\ell = (1 - \mu n) \equiv_n 1 - 0 = 1$ and $\nu m\ell \equiv_{m\ell} \nu 0 = 0$.

In particular, if $\nu, \mu, \lambda \in \mathbb{Z}$ are numbers which are the following modulo inverses:

$$\begin{aligned} \nu &\equiv (m\ell)^{-1} \pmod{n} \\ \mu &\equiv (n\ell)^{-1} \pmod{m} \\ \lambda &\equiv (mn)^{-1} \pmod{\ell} \end{aligned}$$

(all of which exist because, for instance, $\gcd(m\ell, n) = 1$), then

$$\begin{aligned} \alpha &= \nu m\ell \\ \beta &= \mu n\ell \\ \gamma &= \lambda mn \end{aligned}$$

are three numbers with the required nine properties for being able to solve the system of congruences.

Example. Let us find $x \in \mathbb{Z}$ such that $x \equiv_2 1$, $x \equiv_3 2$, $x \equiv_5 4$. The first step is to find α, β, γ for $2, 3, 5$.

$$\begin{aligned} \nu &\equiv (3 \cdot 5)^{-1} \equiv 1^{-1} \equiv 1 \pmod{2} \\ \mu &\equiv (2 \cdot 5)^{-1} \equiv 1^{-1} \equiv 1 \pmod{3} \\ \lambda &\equiv (2 \cdot 3)^{-1} \equiv 1^{-1} \equiv 1 \pmod{5} \end{aligned}$$

(This was a total accident that ν, μ, λ were all 1.) Then,

$$\begin{aligned} \alpha &= 1 \cdot 3 \cdot 5 = 15 \\ \beta &= 1 \cdot 2 \cdot 5 = 10 \\ \gamma &= 1 \cdot 2 \cdot 3 = 6 \end{aligned}$$

Thus,

$$x \equiv 1 \cdot 15 + 2 \cdot 10 + 4 \cdot 6 \equiv 29 \pmod{30}$$

(In fact, the original system is $x \equiv_2 -1$, $x \equiv_3 -1$, and $x \equiv_5 -1$. Notice $x \equiv_{30} -1$.)

2 Polynomial interpolation

The problem of polynomial interpolation is suprisingly similar to the Chinese Remainder Theorem. Here is the problem: Given $x_1, \dots, x_n \in \mathbb{R}$, all distinct, and any values $y_1, \dots, y_n \in \mathbb{R}$, can we compute a polynomial p such that

$$\begin{aligned} p(x_1) &= y_1 \\ p(x_2) &= y_2 \\ &\vdots \\ p(x_n) &= y_n \end{aligned}$$

This is called interpolation because we can then use this polynomial p to compute intermediate values that aren't one of the $x_1, \dots, x_n$.

Suppose we found polynomials $g_1, \dots, g_n$ with the properties that $g_i(x_j) = \delta_{ij}$, where δ_{ij} is the Kronecker delta ($\delta_{ij} = 1$ if $i = j$ and $\delta_{ij} = 0$ if $i \neq j$; the i and j are not multiplied together, so try not to be confused by this notation!) That is to say, suppose the polynomials had the following properties:

$$\begin{array}{cccc} g_1(x_1) = 1 & g_1(x_2) = 0 & \cdots & g_1(x_n) = 0 \\ g_2(x_1) = 0 & g_1(x_2) = 1 & \cdots & g_2(x_n) = 0 \\ \vdots & \vdots & \ddots & \vdots \\ g_n(x_1) = 0 & g_n(x_2) = 0 & \cdots & g_n(x_n) = 1 \end{array}$$

Then, $p(x) = \sum_{i=1}^n y_i g_i(x)$ would be a polynomial which solves the system! That is because $p(x_j) = \sum_{i=1}^n y_i g_i(x_j) = \sum_{i=1}^n y_i \delta_{ij} = y_j$, to put it into symbols. Or,

$$\begin{aligned} p(x_j) &= y_1 g_1(x_j) + y_2 g_2(x_j) + \cdots + y_j g_j(x_j) + \cdots + y_n g_n(x_j) \\ &= y_1 0 + y_2 0 + \cdots + y_j 1 + \cdots + y_n 0 \\ &= y_j \end{aligned}$$

It turns out there is a rather easy way to come up with these polynomials. Let $h(x) = (x - x_1)(x - x_2) \cdots (x - x_n)$, which is a polynomial with $x_1, \dots, x_n$ as roots. Let $h_i(x) = h(x)/(x - x_i)$, which is the polynomial obtained by omitting the $(x - x_i)$ term from $h(x)$. This is to say,

$$h_i(x) = (x - x_1) \cdots (x - x_{i-1})(x - x_{i+1}) \cdots (x - x_n)$$

One thing is for certain, $h_i(x_i) \neq 0$ and $h_i(x_j) = 0$ when $j \neq i$. This is almost right except that $h_i(x_i)$ might not be 1. To remedy this, we just divide through by $h_i(x_i)$. Let

$$g_i(x) = \frac{h_i(x)}{h_i(x_i)}$$

which is a degree $n - 1$ polynomial.

For $n = 3$, these are the corresponding polynomials:

$$g_1(x) = \frac{(x - x_2)(x - x_3)}{(x_1 - x_2)(x_1 - x_3)} \qquad g_2(x) = \frac{(x - x_1)(x - x_3)}{(x_2 - x_1)(x_2 - x_3)} \qquad g_3(x) = \frac{(x - x_1)(x - x_2)}{(x_3 - x_1)(x_3 - x_2)}$$

The correspondence with the Chinese Remainder Theorem will take some time to develop, but here it is quickly, for $n = 3$ for notational simplicity. As polynomials, $x - x_1$, $x - x_2$, and $x - x_3$ are pairwise coprime, and we can instead think about solving the system of congruences

$$\begin{aligned} p(x) &\equiv y_1 \pmod{x - x_1} \\ p(x) &\equiv y_2 \pmod{x - x_2} \\ p(x) &\equiv y_3 \pmod{x - x_3} \end{aligned}$$

for a polynomial $p(x)$. Modulo a polynomial is defined the same: two polynomials are congruent modulo $g(x)$ if their difference is a multiple of $g(x)$. To understand modulo $x - x_i$, since $x \equiv x_i \pmod{x - x_i}$ we may replace all instances of x with x_i, so a fundamental fact is that $p(x) \equiv p(x_i) \pmod{x - x_i}$, and thus is in fact evaluation.

Equating terms with the Chinese Remainder Theorem, we see $n = x - x_1$, $m = x - x_2$, and $\ell = x - x_3$, with $\alpha = g_1$, $\beta = g_2$, and $\gamma = g_3$. When we calculated ν, we calculated $\nu \equiv (m\ell)^{-1} \pmod{n}$, which is $\nu \equiv ((x - x_2)(x - x_3))^{-1} \equiv ((x_1 - x_2)(x_1 - x_3))^{-1} \pmod{x - x_1}$, and then $\alpha = \nu m\ell = ((x_1 - x_2)(x_1 - x_3))^{-1}(x - x_2)(x - x_3)$, which is $g_1(x)$!

3 A deeper explanation

In this section, we will explore some of the algebra people came up with to explain the correspondence hinted at above. This will only be a *deeper* but not an *in-depth* explanation. Feel free to just read an actual textbook about abstract algebra instead (ring theory in particular).

Instead of congruence notation, a more modern (and in my opinion cleaner) way to go is to work with equivalence classes. Let $[a]_n$ denote the set of everything congruent to a modulo n. For $\mathbb{Z}$,

$$[a]_n = \{b \in \mathbb{Z} : a \equiv_n b\}$$

One may show that if $b \in [a]_n$, then $[a]_n = [b]_n$. Sometimes we may drop the sub-n if the modulus is clear from context.

We may define addition and multiplication by $[a]_n + [b]_n = [a + b]_n$ and $[a]_n[b]_n = [ab]_n$. For instance,

$$[2]_5 + [4]_5 = [2 + 4]_5 = [6]_5 = [1]_5$$

It follows from theorems about modulo arithmetic that if $[a]_n = [a']_n$ and $[b]_n = [b']_n$, then $[a+b]_n = [a'+b']_n$.

A more general point of view is the following. A subset $I \subseteq \mathbb{Z}$ is called an *ideal* of $\mathbb{Z}$ if the following properties hold:

1. $0 \in I$.
2. If $a, b \in I$, then $a + b \in I$.
3. If $n \in \mathbb{Z}$ and $a \in I$, then $na \in I$.

We may define an equivalence relation called *modulo I*. $a, b \in \mathbb{Z}$ are equivalent modulo I if $b - a \in I$. This is an equivalence relation because

- It is reflexive: $a \equiv a \pmod{I}$ since $a - a = 0 \in I$.
- It is symmetric: If $a \equiv b \pmod{I}$, then $b - a \in I$, so $a - b = -1(b - a) \in I$, too. Thus $b \equiv a \pmod{I}$.
- It is transitive: If $a \equiv b \pmod{I}$ and $b \equiv c \pmod{I}$, then $b - a \in I$ and $c - b \in I$, so $c - a = (c - b) + (b - a) \in I$. Thus $a \equiv c \pmod{I}$.

Whenever we have an equivalence relation, we may split a set into disjoint *equivalence classes*. The equivalence class containing $a \in \mathbb{Z}$ is $[a]_I = \{b \in \mathbb{Z} : b - a \in I\}$, and the set of equivalence classes is denoted $\mathbb{Z}/I$ (pronounced "zee mod eye"), which is the collection $\{[a]_I : a \in \mathbb{Z}\}$ of equivalence classes, and which is called a *quotient ring*.

The condition $b - a \in I$ is the same as saying $b \in a + I$, if we agree that $a + I = \{a + x : x \in I\}$. Thus, $[a]_I = a + I$, and in fact the latter notation is more common. With this notation, $\mathbb{Z}/I = \{a + I : a \in \mathbb{Z}\}$.

Just like for modulo, one can also show that $\mathbb{Z}/I$ has addition and multiplication operations, with $[0]_I$ the additive identity and $[1]_I$ the multiplicative identity.

(The even more general case is for a *ring* R, where an ideal of R is a subset with the same three properties, with R replacing $\mathbb{Z}$. Talking about rings in general will be taking us too far afield, though we will talk about the ring of polynomials later. We could also say that $\mathbb{Z}/I$ is a ring.)

Example. When $n \in \mathbb{Z}$, the set $n\mathbb{Z} = \{na : a \in \mathbb{Z}\}$ is an ideal. It is the ideal of multiples of n. When $n = 0$, $0\mathbb{Z} = \{0\}$, the *zero ideal*. When $n = 1$, $1\mathbb{Z} = \mathbb{Z}$, the entire set of integers.

Example. If $I \subseteq \mathbb{Z}$ is an ideal and $1 \in \mathbb{Z}$, then $I = \mathbb{Z}$. This is because for every $n \in \mathbb{Z}$, $n1 \in I$, too.

For $\mathbb{Z}$, these are in fact the only ideals, as the following theorem proves. Thus the only quotient rings of $\mathbb{Z}$ are $\mathbb{Z}/n\mathbb{Z}$ for some $n \in \mathbb{Z}$.

Theorem 2. *If $I \subseteq \mathbb{Z}$ is an ideal, then $I = n\mathbb{Z}$ for some $n \in \mathbb{Z}$.*

Proof. If $I = \{0\}$, then $I = 0\mathbb{Z}$. Otherwise, I contains a nonzero element n, which we may assume is positive since $-n = (-1)n \in I$, too. Furthermore, we may assume n is the least positive element in I. Since $na \in I$ for all $a \in \mathbb{Z}$, it is clear that $n\mathbb{Z} \subseteq I$. We will prove that $I \subseteq n\mathbb{Z}$.

Take an arbitrary element $x \in I$. By the division algorithm, there are integers q, r such that $x = qn + r$ with $0 \leq r < n$. Since $x \in I$ and $qn \in I$, $x - qn \in I$, so $r \in I$, too. Since n is the least positive element in I, and r is nonnegative and less than n, it must be the case that $r = 0$. Thus, $x = qn$, so $x \in n\mathbb{Z}$. This establishes the equality. □

Fact: if $I \subseteq \mathbb{Z}$ and $J \subseteq \mathbb{Z}$ are ideals, then

- $I + J = \{x + y : x \in I \text{ and } y \in J\}$ is an ideal. This is because of the following: $0 = 0 + 0 \in I + J$, for $x + y \in I + J$ and $x' + y' \in I + J$, $(x + y) + (x' + y') = (x + x') + (y + y') \in I + J$, and if $n \in \mathbb{Z}$, $n(x + y) = nx + ny \in I + J$.
- $I \cap J$ is an ideal. This ideal is equal to $IJ = \{xy : x \in I \text{ and } y \in J\}$. *Exercise.*

The *greatest common divisor* of n and m is the positive integer $d \in \mathbb{Z}$ such that $n\mathbb{Z} + m\mathbb{Z} = d\mathbb{Z}$. Such a number exists because $n\mathbb{Z} + m\mathbb{Z}$ is an ideal, and the theorem says every ideal is of the form $d\mathbb{Z}$ for some $d \in \mathbb{Z}$. Since $n = n + 0 \in n\mathbb{Z} + m\mathbb{Z}$, $n \in d\mathbb{Z}$, so there is an $a \in \mathbb{Z}$ such that $n = da$, hence $d|n$. Similarly $d|m$, so d is certainly a common divisor. If d' were also a common divisor, then $n \in d'\mathbb{Z}$ and $m \in d'\mathbb{Z}$, so $n\mathbb{Z} \subseteq d'\mathbb{Z}$ and $m\mathbb{Z} \subseteq d'\mathbb{Z}$, hence $n\mathbb{Z} + m\mathbb{Z} \subseteq d'\mathbb{Z}$, and so $d\mathbb{Z} \subset d'\mathbb{Z}$, which implies $d \in d'\mathbb{Z}$, so $d'|d$. Thus d is the *greatest* common divisor.

Notice that $n\mathbb{Z} + m\mathbb{Z} = d\mathbb{Z}$ implies Bézout's theorem since $d \in d\mathbb{Z}$, so $d \in n\mathbb{Z} + m\mathbb{Z}$, so there exist $a, b \in \mathbb{Z}$ such that $d = na + mb$.

Two numbers $n, m \in \mathbb{Z}$ are *coprime* if $n\mathbb{Z} + m\mathbb{Z} = \mathbb{Z}$. That is, if $\gcd(n, m) = 1$.

Theorem 3 (Chinese Remainder Theorem)**.** *If $I, J \subseteq \mathbb{Z}$ are ideals such that $I + J = \mathbb{Z}$, then the function*

$$f : \mathbb{Z} \to \mathbb{Z}/I \times \mathbb{Z}/J$$

defined by $f(n) = ([n]_I, [n]_J)$ is a surjection.

Proof. Since $I + J = \mathbb{Z}$, there is an $x \in I$ and $y \in J$ such that $x + y = 1$. Given an arbitrary $([a]_I, [b]_J) \in \mathbb{Z}/I \times \mathbb{Z}/J$, let $n = ay + bx$. We can calculate $[x]_I = 0$, $[x]_J = [1 - y]_J = [1]_J$, $[y]_I = [1 - x]_I = [1]_I$, and $[y]_J = [0]_J$, so $[ay + bx]_I = [a1 + b0] = [a]_I$ and $[ay + bx]_J = [a0 + b1]_J = [b]_J$. Therefore, $f(n) = ([a]_I, [b]_J)$, and since a, b were arbitrary, f is surjective.

In fact, one may prove that the kernel of f is $I \cap J$, so there is a bijection $\mathbb{Z}/(I \cap J) \to \mathbb{Z}/I \times \mathbb{Z}/J$. □

It should be said that f is what is called a *ring homomorphism*, which is a function with the extra properties that $f(x + y) = f(x) + f(y)$, $f(xy) = f(x)f(y)$, and $f(1) = 1$ (where each 1 is some multiplicative identity).

The theorem can be extended to any number of mutually coprime ideals. For instance, $I, J, K \subseteq \mathbb{Z}$ ideals such that $I + J = \mathbb{Z}$, $I + K = \mathbb{Z}$, and $J + K = \mathbb{Z}$ gives a surjection $f : \mathbb{Z} \to \mathbb{Z}/I \times \mathbb{Z}/J \times \mathbb{Z}/K$ (with kernel $I \cap J \cap K$).

3.1 To polynomials

A common notation for the set of polynomials with real coefficients with variable x is $\mathbb{R}[x]$. This is called the *ring of polynomials with real coefficients*. An ideal I of $\mathbb{R}[x]$ is defined similarly, except we replace $\mathbb{Z}$ with $\mathbb{R}[x]$ in the definition.

Polynomials also have a division algorithm theorem:

Theorem 4. *For $f, g \in \mathbb{R}[x]$ with $g \neq 0$, there are two polynomials $q, r \in \mathbb{R}[x]$ such that $f(x) = g(x)q(x) + r(x)$ and such that* $\deg r < \deg q$.

The only thing we needed in Theorem 2 was the division algorithm for $\mathbb{Z}$. From the same proof, replacing "least" with "least degree," it follows that every ideal $I \subset \mathbb{R}[x]$ is of the form $g\mathbb{R}[x]$ for some polynomial $g \in \mathbb{R}[x]$. Elements of $g\mathbb{R}[x]$ are those polynomials whose roots include all of the roots of g. (If we were talking about $\mathbb{C}[x]$ instead, ideals are in correspondence all possible finite sets of roots from $\mathbb{C}$.)

Theorem 5. *The function $\mathbb{R}[x] \to \mathbb{R}[x]/(x-a)$ defined by $p(x) \mapsto [p(x)]_{(x-a)}$ corresponds to the evaluation map $p(x) \mapsto p(a)$. In fact, $\mathbb{R}[x]/(x-a)$ is* isomorphic *to $\mathbb{R}$.*

Proof. Since $x \equiv a \pmod{x-a}$, it follows that $x^n \equiv a^n \pmod{x-a}$, so $\sum_n c_n x^n \equiv \sum_n c_n a^n \pmod{x-a}$. Thus, $p(x) \equiv p(a) \pmod{x-a}$ for every $p \in \mathbb{R}[x]$. In other words, $[p(x)]_{(x-a)} = [p(a)]_{(x-a)}$.

Since $p(a) \in \mathbb{R}$, $\mathbb{R}[x]/(x-a)$ is actually just $\mathbb{R}$. In particular, the isomorphism is defined by $[1]_{(x-a)} \mapsto 1$ and $[x]_{(x-a)} \mapsto a$. (I am being sketchy here.) □

The Chinese Remainder Theorem carries over to polynomials, too, since it was only a statement of abstract ideals. A specialization of the theorem to ideals of the form $(x-a)\mathbb{R}[x]$ is the following:

Theorem 6. *If $a_1, \dots, a_n \in \mathbb{R}$ are distinct, then the map $f : R[x] \to \mathbb{R}^n$ defined by $f(p) = (p(a_1), \dots, p(a_n))$ is a surjection.*

Proof. Fact: if $a_i \neq a_j$, then $(x-a_i)\mathbb{R}[x] + (x-a_j)\mathbb{R}[x] = \mathbb{R}[x]$. This is because $\frac{x-a_i}{a_j-a_i} + \frac{x-a_j}{a_i-a_j}$ is a linear polynomial which is 1 at a_i and at a_j, so it is equal to 1. Since $(x-a_i)\mathbb{R}[x] + (x-a_j)\mathbb{R}[x]$ is an ideal which contains 1, it is equal to $\mathbb{R}[x]$.

Thus, $(x-a_1)\mathbb{R}[x]$, $(x-a_2)\mathbb{R}[x]$, through $(x-a_n)\mathbb{R}[x]$ are ideals whose pairwise sums are $\mathbb{R}[x]$. This means the Chinese remainder theorem applies, saying $\mathbb{R}[x] \to (\mathbb{R}[x]/(x-a_1)\mathbb{R}[x]) \times \cdots \times (\mathbb{R}[x]/(x-a_n))$ is a surjection. Since $\mathbb{R}[x]/(x-a_i)$ is isomorphic to $\mathbb{R}$ and the corresponding map in the Chinese Remainder Theorem is evaluation of a polynomial at a_i, we have our result. □

3.2 Back to integers

A more advanced point of view is somewhat bizarre. Consider: the function $\mathbb{R}[x] \to \mathbb{R}[x]/(x-a)$ represents evaluation of a polynomial at a; and $x-a$ the polynomial is sort of like the point $a \in \mathbb{R}$ in that it has a root there. So: what if $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ represents "evaluating an integer" at the "point" n?

For sake of notation, for $a \in \mathbb{Z}$ let $a(n) = [a]_n$, representing this new concept of evaluating an integer a at n. Then, a system of congruences

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

can be written instead as

$$\begin{aligned} x(m_1) &= [a_1]_{m_1} \\ x(m_2) &= [a_2]_{m_2} \\ &\vdots \\ x(m_n) &= [a_n]_{m_n} \end{aligned}$$

While it is somewhat weird that each evaluation occurs in a different quotient ring (where in contrast for polynomial evaluation all the values ultimately were in $\mathbb{R}$, at least isomorphically), at least it looks somewhat like the polynomial interpolation problem.

I have ignored a particular issue: why for polynomials do we only evaluate a linear polynomial like $x-a$? The reason is that these are primes (and in $\mathbb{C}[x]$ these are *the* primes). One could evaluate at something like $x^2 - 2x + 3$ as well, but the value ends up being in $\mathbb{R}[x]/(x^2 - 2x + 3)$, which is a two-dimensional space of values! This is fine, but just something to be aware of. In algebraic geometry, there is a correspondence between primes (algebra) and points (geometry). The points for $\mathbb{Z}$ correspond to $2, 3, 5, 7, 11, \ldots$. Computing $[a]_n$ then gives the evaluation of a at the points which make up n, namely the prime factors of n.

The Chinese Remainder Theorem requires that each of the ideals be pairwise coprime. This is essentially saying that the sets of points each ideal corresponds to are pairwise disjoint. That is, the Chinese Remainder Theorem says, geometrically speaking, given values at a bunch of points in such a way that you are not giving different values to the same point, there exists some element which evaluates to those values at those points.

3.3 Books

If you got this far and want to know more, some books you might consider taking a look at:

1. Michael Artin's *Algebra* is the textbook from which I learned abstract algebra.
2. I've heard good things about Dummit and Foote's *Abstract Algebra*, though I've never opened it.
3. Once your mathematical maturity reaches a certain level you could attempt Serge Lang's *Algebra*. It's only clear, though, once the subject already makes sense.
4. Some number theory books include Rosen's *Elementary Number Theory* and Ireland and Rosen's *A Classical Introduction to Modern Number Theory.*
5. Bach and Shallit have *Algorithmic Number Theory* if you want to compute things, though they also have a good amount of underlying theory. (For instance, the convolution operator I mentioned and how it relates the totient to the "Möbius function" is in here.)
6. Shaferevich has an interesting book called *Algebra I*, if you want to learn more about algebraic geometry.