The Chinese Remainder Theorem

William Hua, Hillary Yang

Abstract

The Chinese remainder theorem (CRT) asserts a unique solution to a system of congruences with coprime moduli. In this paper, we first provide a brief history of the theorem. Then, we build up a rigorous foundation of the integers and their properties, which is used to prove the Chinese remainder theorem. Finally, we explore the possibility of extending this result to the Gaussian integers.

Contents

1. Introduction

The Chinese Remainder Theorem states that for k moduli n_i and k integers x_i with indices i from 1 to k, where all moduli are pairwise coprime, then the system of congruences

$$x \equiv x_i \pmod{n_i}$$

for all integer i with $1 \leq i \leq k$ results in a unique solution for x under modulo $n_1 n_2 \dots n_k$.

But what is a modulus? What does coprime mean? What are integers? We will define and prove a myriad of properties, most notably the Chinese remainder theorem, relating to the wonderful set of numbers we call integers.

2. History

As with many mathematical discoveries, the Chinese remainder theorem was conceived out of necessity. In the case of 2nd century Chinese astronomers, a method was needed to calculate a certain date based on the known dates of the winter solstice and the new moon.

The first recorded mention of the Chinese remainder theorem dates back to the 5th century, where Chinese mathematician Sunzi posed it as a problem in his book *Sunzi Suanjing*, which translates to *Master Sun's Mathematical Manual*. The original statement of the problem is as follows:

> There are certain things whose number is unknown. If we count them by threes, we have two left over; by fives, we have three left over; and by sevens, two are left over. How many things are there?[1]

This problem can be expressed as the system of congruences:

$$\begin{aligned} x &\equiv 2 \pmod{3} \\ x &\equiv 3 \pmod{5} \\ x &\equiv 2 \pmod{7} \end{aligned}$$

However, Sunzi's work lacked a proof, which was discovered by Qin Jiushao in his *Mathematical Treatise in Nine Sections*, published in 1247. Other mathematicians worked at the theorem between these years, including Aryabhata (6th century India), Brahmagupta (7th century India), and Fibonacci (13th century Italy).

In 1801, Gauss introduced the idea of modular congruences in his *Disquisitiones Arithmeticae*, and illustrated the Chinese remainder theorem with a problem involving the solar and lunar cycles.

3. Axioms

First, we need a definition of the integers. We will denote the set of integers as $\mathbb{Z}$, along with its two binary operations, addition ($+$) and multiplication ($\cdot$). To lay the framework for the integers, we start with what

[1] https://en.wikipedia.org/wiki/Chinese_remainder_theorem#History

are called the ring axioms.

3.1. Ring Axioms

Definition 1. The **ring axioms** are the following set of axioms:

- **Commutative**: $a + b = b + a$ and $ab = ba$.
- **Associative**: $a + (b + c) = (a + b) + c$.
- **Distributive**: $a(b + c) = ab + ac$.
- **Zero**: $\exists 0 \in \mathbb{Z}, \forall a \in \mathbb{Z}, a + 0 = a$.
- **Negatives**: $\forall a \in \mathbb{Z}, \exists x \in \mathbb{Z}, a + x = 0$.
- **One**: $\exists 1 \in \mathbb{Z}, \forall a \in \mathbb{Z}, a \cdot 1 = a$.

However, something is missing! The ring axioms don't give the integers a concept of "positivity" which is a critical property of the integers. This concept of "order" appears in a new set of axioms, aptly named the order axioms.

3.2. Order Axioms

Definition 2. The **order axioms** are the following set of axioms defined for a nonempty subset $\mathbb{Z}^+ \subseteq \mathbb{Z}$.

- **Additive closure**: $(\forall a, b \in \mathbb{Z}^+), a + b \in \mathbb{Z}^+$.
- **Multiplicative closure**: $(\forall a, b \in \mathbb{Z}^+), ab \in \mathbb{Z}^+$.
- **Nontriviality**: $0 \notin \mathbb{Z}^+$.
- **Trichotomy**: $(\forall a \in \mathbb{Z})$ exactly one of the following holds: $a \in \mathbb{Z}^+$, $a = 0$, or $-a \in \mathbb{Z}^+$.

Using the order axioms, we can define "greater/less than" and "greater/less than or equal to."

Definition 3. Suppose $a, b \in \mathbb{Z}$. Then,

- a is **less than b** (denoted as $a < b$) if there exists $x \in \mathbb{Z}^+$ such that $a + x = b$.
- a is **less than or equal to b** (denoted as $a \leq b$) if $a < b$ or $a = b$.
  - This is equivalent to saying there exists $x \in \mathbb{Z} \cup \{0\}$ such that $a + x = b$, since if $x = 0$, then $a + x = b \implies a = b$.
- a is **greater than b** (denoted as $a > b$) if $b < a$.
- a is **greater than or equal to b** (denoted as $a \geq b$) if $b \leq a$.

The final step in defining the integers is the **well-ordering principle**.

3.3. Well-Ordering Principle

Definition 4. The **well-ordering principle** (WOP for short) states that any nonempty subset S of $\mathbb{Z}^+$ has an element $m \in S$ such that for all $n \in S$, we have $m \leq n$.

Now, we can define the integers:

Definition 5. The ring of integers (denoted $\mathbb{Z}$) is the ordered ring that satisfies the well-ordering principle.

4. Math

4.1. More definitions

Definition 6. We say that $p \in \mathbb{Z}^+$ is **prime** if the only positive divisors of p are 1 and p. By definition, 1 is not prime.

For example: 17 is prime because the only positive divisors of 17 are 1 and 17.

Definition 7. Define

$$\prod_{i=1}^{1} a_i = a_i.$$

Then, for all positive integers n, we have the **product**

$$\prod_{i=1}^{n} a_i = a_n \cdot \prod_{i=1}^{n-1} a_i$$

Note: In this paper, we will also use $a_1 a_2 \cdots a_n$ to mean

$$\prod_{i=1}^{n} a_i.$$

Definition 8. The **absolute value** of an integer n is denoted as $|n|$, where:

$$|n| = \begin{cases} n & \text{if } n \in \mathbb{Z}^+ \cup \{0\} \\ -n & \text{if } -n \in \mathbb{Z}^+ \end{cases}$$

By trichotomy, exactly one of $n \in \mathbb{Z}^+$, $-n \in \mathbb{Z}^+$, or $n = 0$ is true. This means $|n| \in \mathbb{Z}^+ \cup \{0\}$.

4.2. Preliminary results

Armed with the ring axioms, the order axioms, and WOP, we can move on to exploring the numbers defined by these ground truths. Naturally, one of the first questions we ask is: Are zero and one, two of the most important integers, uniquely defined in $\mathbb{Z}$?

Lemma 1. *Zero is uniquely defined in $\mathbb{Z}$.*

Proof. For the sake of contradiction, assume that zero is not uniquely defined; in other words, there exist at least two distinct zeroes in $\mathbb{Z}$. Let two of these zeroes be 0_a and 0_b. From the zero axiom, we have $x + 0 = x \, \forall x \in \mathbb{Z}$. Since this axiom must hold for all zeroes, we have $x + 0_b = x$ for all $x \in \mathbb{Z}$. Furthermore, we can substitute $x = 0_a$ to obtain

$$0_a + 0_b = 0_a.$$

We can follow the same process for 0_a, so we have

$$0_b + 0_a = 0_b.$$

However, commutativity tells us that $0_a + 0_b = 0_b + 0_a$, and substituting, $0_a = 0_b$. This is absurd, since we assumed 0_a and 0_b were distinct. Therefore, any pair of zeroes must be the same, so all zeroes are the same. This means that zero is uniquely defined. □

Lemma 2. *One is uniquely defined in $\mathbb{Z}$.*

Proof. For contradiction, assume we have $1_a = 1_b \in \mathbb{Z}$. Then, by the one axiom, we have $x \cdot 1 = x \, \forall x \in \mathbb{Z}$. By substituting for x and 1, we have

$$1_a \cdot 1_b = 1_a$$
$$1_b \cdot 1_a = 1_b$$

But commutativity gives us $1_a \cdot 1_b = 1_b \cdot 1_a$, and substituting, $1_a = 1_b$, which is a contradiction. By similar reasoning as above, one must be uniquely defined. □

Now that we've established that 0 and 1 are unique and not equal to each other, we can move on to discussing an important property involving 0, which will help us prove that $0 \neq 1$.

Lemma 3. *Suppose $a \in \mathbb{Z}$. Then, $a \cdot 0 = 0$.*

Proof. Because $0 + 0 = 0$, we have $a(0 + 0) = a \cdot 0$ by substitution. However, by distributivity, $a(0 + 0) = a \cdot 0 + a \cdot 0$.

Hence, $a \cdot 0 + a \cdot 0 = a \cdot 0$. Add $-(a \cdot 0)$ to both sides to obtain $a \cdot 0 = 0$. □

We know that zero and one are both uniquely defined. But what if 0 and 1 are actually equal? While it seems absurd, it's not ruled out by anything we've proven so far.

Lemma 4. *Zero does not equal one in $\mathbb{Z}$.*

Proof. First, we prove that $\mathbb{Z}$ contains more than one element. For contradiction, assume 0 is the only element in $\mathbb{Z}$. By the order axioms and the definition of $\mathbb{Z}^+$, we know that $\mathbb{Z}^+ \subseteq \mathbb{Z}$. Furthermore, $0 \notin \mathbb{Z}^+$ by nontriviality, so $\mathbb{Z}^+$ must be empty since there are no other elements in $\mathbb{Z}$.

However, this contradicts the definition of $\mathbb{Z}^+$, which is defined as a nonempty subset of $\mathbb{Z}$. Therefore, 0 cannot be the only element in $\mathbb{Z}$, meaning that $\mathbb{Z}$ contains more than one element.

To prove that $0 \neq 1$, assume for contradiction that $0 = 1$ in $\mathbb{Z}$. Because there is more than one integer, there exists a nonzero element $a \in \mathbb{Z}$. Then, we have $a \cdot 0 = a \cdot 1$. By Lemma 3, $a \cdot 0 = 0$, and by the one property, we have $a \cdot 1 = a$. However, this means $0 = a$, which contradicts $a \neq 0$.

Hence, $0 \neq 1$. □

Knowing these important facts about 0 and 1, we can move on to exploring some properties of negatives.

Lemma 5. *Suppose $a \in \mathbb{Z}$. Then, $-(-a) = a$.*

Proof. Note that

$$0 = -a + (-(-a))$$

but

$$0 = a + (-a).$$

Hence, $-a + (-(-a)) = a + (-a)$. By commutativity and then adding a to both sides to cancel $-a$, we get $-(-a) = a$. □

Lemma 6. $-(ab) = (-a)b = a(-b)$.

Proof. We know $a(b + (-b)) = a \cdot 0$, but $a \cdot 0 = 0$ by Lemma 3. Thus, $a(b + (-b)) = 0$. By the distributive property, this means $ab + a(-b) = 0$. However, $ab + (-(ab)) = 0$. This means

$$ab + a(-b) = ab + (-(ab)).$$

Add $-(ab)$ to both sides to get $a(-b) = -(ab)$.

Similarly, $b(a + (-a)) = b \cdot 0 = 0$, so $ba + b(-a) = 0 \implies ab + (-a)b = 0 = ab + (-(ab))$. Add $-(ab)$ to both sides to get $-(ab) = (-a)b$. □

Lemma 7. *Suppose $a, b \in \mathbb{Z}$. Then, $(-a)(-b) = ab$.*

Proof. From Lemma 6, we have $(-x)y = x(-y)$ for $x, y \in \mathbb{Z}$. Then, let $x = a$ and $y = -b$. Substitute and get $(-a)(-b) = a(-(-b))$. Finally, use Lemma 5 to get $(-a)(-b) = ab$. □

After proving some results about negatives, we can move on to another fact about one:

Lemma 8. $-1 \notin \mathbb{Z}^+$ *and* $1 \in \mathbb{Z}^+$.

Proof. Say for the sake of contradiction that $-1 \in \mathbb{Z}^+$. Then, $(-1)(-1) = 1 \in \mathbb{Z}^+$ due to Lemma 7. However, by trichotomy, -1 and 1 cannot both be in $\mathbb{Z}^+$. Hence, $-1 \notin \mathbb{Z}^+$.

By trichotomy again, exactly one of the following is true:

- $-1 \in \mathbb{Z}^+$.
- $0 = 1$.
- $1 \in \mathbb{Z}^+$.

We know $-1 \notin \mathbb{Z}^+$. We also know $0 \neq 1$ because of Lemma 4. Hence, $1 \in \mathbb{Z}^+$. □

Now, let's transition to discussing the natural numbers.

Definition 9. Define the set of natural numbers, denoted $\mathbb{N}$, as $\mathbb{Z}^+ \cup \{0\}$.

There are two facts about $\mathbb{N}$ that we will prove and use, namely, that it is additively and multiplicatively closed.

Lemma 9. *$\mathbb{N}$ is additively closed.*

Proof. We want to show that $\forall a, b \in \mathbb{N}, a + b \in \mathbb{N}$. There are four cases:

- If $a = 0$ and $b = 0$, $a + b = 0 + 0 = 0 \in \mathbb{N}$.
- If $a = 0$ and $b \in \mathbb{Z}^+$, $a + b = 0 + b = b + 0 = b \in \mathbb{N}$.
- If $a \in \mathbb{Z}^+$ and $b = 0$, $a + b = a + 0 = a \in \mathbb{Z}^+$.
- If $a \in \mathbb{Z}^+$ and $b \in \mathbb{Z}^+$, then $a + b \in \mathbb{Z}^+$ because $\mathbb{Z}^+$ is additively closed.

Since all possible combinations of a and b give a value in $\mathbb{N}$, $\mathbb{N}$ is additively closed. □

Lemma 10. *$\mathbb{N}$ is multiplicatively closed*

Proof. We want to show that $\forall a, b \in \mathbb{N}, ab \in \mathbb{N}$.

- By Lemma 3, if either of a or b are zero, then $ab = 0$.
- If $a \in \mathbb{Z}^+$ and $b \in \mathbb{Z}^+$, then $ab \in \mathbb{Z}^+$ because $\mathbb{Z}^+$ is multiplicatively closed.

Since all possible combinations of a and b give a value in $\mathbb{N}$, $\mathbb{N}$ is additively closed. □

These lemmas help us prove some more interesting facts about the integers, such as:

Lemma 11. *If $ab = 0$ for $a, b \in \mathbb{Z}$, then $a = 0$ or $b = 0$.*

Proof. First, assume for contradiction that for $a \neq 0$ and $b \neq 0$, $ab = 0$. By trichotomy, this implies that $a \in \mathbb{Z}^+$ or $-a \in \mathbb{Z}^+$ and $b \in \mathbb{Z}^+$ or $-b \in \mathbb{Z}^+$.

There are four cases:

- If $a \in \mathbb{Z}^+$ and $b \in \mathbb{Z}^+$, then $ab \in \mathbb{Z}^+$, so $ab \neq 0$.
- If $a \in \mathbb{Z}^+$ and $-b \in \mathbb{Z}^+$, then $a(-b) \in \mathbb{Z}^+$. By Lemma 6, $a(-b) = -(ab)$, so $-(ab) \in \mathbb{Z}^+$. Then, by trichotomy, $ab \neq 0$.
- If $-a \in \mathbb{Z}^+$ and $b \in \mathbb{Z}^+$, then $(-a)b \in \mathbb{Z}^+$ and $-(ab) \in \mathbb{Z}^+$ by Lemma 6, so $ab \neq 0$.
- If $-a \in \mathbb{Z}^+$ and $-b \in \mathbb{Z}^+$, then $(-a)(-b) \in \mathbb{Z}^+$, so $ab \in \mathbb{Z}^+$ by Lemma 7 and $ab \neq 0$.

Since ab cannot equal zero in any case, our original assumption is false and at least one of a and b must be zero. □

This lemma helps us prove the next:

Lemma 12. *Suppose $a, b, b' \in \mathbb{Z}$ and $a \neq 0$. Then, if $ab = ab'$, we have $b = b'$.*

Proof. We have $ab + (-ab') = ab' + (-ab')$. By Lemma 6, $(-a)b' = -(ab')$, so $ab + (-ab') = ab' + (-(ab'))$. Substituting, $ab + (-ab') = 0$, and $a(b + (-b')) = 0$. Since $a \neq 0$, $b + (-b') = 0$ by Lemma 11, which tells us that $b = b'$ by adding b' on both sides. □

Now that we've established some basic facts involving equalities, we can move to discussing inequalities. The first lemma involves the adding two inequalities:

Lemma 13. *Suppose $a, b, x, y \in \mathbb{Z}$. If $a \leq b$ and $x \leq y$, then $a + x \leq b + y$.*

Proof. From $a \leq b$ and $x \leq y$, we have $a + m = b$ and $x + n = y$, where $m, n \in \mathbb{N}$ by the definition of $\leq$. Then, we can write $(b - a) + (y - x) = m + n$ so $(b + y) - (a + x) = m + n$, and $(a + x) + (m + n) = b + y$. Since $m + n \in \mathbb{N}$ by Lemma 9, the definition of $\leq$ tells us that $a + x \leq b + y$. □

A similar result involves multiplying the values in the two inequalities.

Lemma 14. *Suppose $a, b, x, y, \in \mathbb{Z}^+$. If $a < b$ and $x < y$, then $ax < by$.*

Proof. From $a < b$ and $x < y$, we have $b = a + m$ and $y = x + n$ where $m, n \in \mathbb{Z}^+$. Then,

$$by = ax + an + mx + mn.$$

However, $an, mx, mn \in \mathbb{Z}^+$ by the multiplicative closure of $\mathbb{Z}^+$. Then, $an + mx + mn \in \mathbb{Z}^+$ by the additive closure of $\mathbb{Z}^+$. Thus, $ax < by$ by the definition of $<$. □

With these lemmas, along with WOP, we can prove a very important fact: 1 is the smallest element of $\mathbb{Z}^+$.

Lemma 15. *The smallest element in $\mathbb{Z}^+$ is 1.*

Proof. By WOP, there is an element $m \in \mathbb{Z}^+$ such that $m \leq x$ for any $x \in \mathbb{Z}^+$.

Say for the sake of contradiction that $m < 1$. Then, because $m \in \mathbb{Z}^+$, and $1 \in \mathbb{Z}^+$ by Lemma 8, we have $m^2 < m$ by Lemma 14. However, $m^2 \in \mathbb{Z}^+$ by multiplicative closure, meaning we found a smaller element in $\mathbb{Z}^+$ than m, violating the minimality of m.

Hence, $m \geq 1$. Because $1 \in \mathbb{Z}^+$ by Lemma 8, we have $m = 1$. □

And we can show the discreteness quality of the integers:

Lemma 16. *Suppose n is an integer. There is never an integer strictly between n and $n + 1$.*

Proof. Say for the sake of contradiction that there exists an integer m such that $n < m < n + 1$.

Then, $m - n \in \mathbb{Z}^+$. By Lemma 15, we have $m - n \geq 1$. Similarly, we have $n + 1 - m \in \mathbb{Z}^+ \implies n + 1 - m \geq 1$.

Then, by Lemma 13, when we combine $m - n \geq 1$ and $n + 1 - m \geq 1$, we get

$$1 \geq 2$$

which is a contradiction.

Hence, there are no integers between n and $n+1$. □

4.3. Facts about division

Definition 10. For $a, b \in \mathbb{Z}$, a **divides** b, denoted $a \mid b$, if $b = ak$ for $k \in \mathbb{Z}$.

For example: We have $17 \mid 34$ since we can write $34 = 17 \cdot 2$.

Using this definition, we can establish many lemmas regarding division.

Lemma 17. *For every $a \in \mathbb{Z}$, $a \mid a$.*

Proof. By the one axiom, we have that $a \cdot 1 = a$ for all $a \in \mathbb{Z}$, so $a = a \cdot 1$. By Definition 10, we have $a \mid a$. □

Lemma 18. *For every $a \in \mathbb{Z}$, $a \mid |a|$.*

Proof. Recall that either $|a| = a$ or $|a| = -a$. If $|a| = a$, then use Lemma 17 to get $a \mid |a|$. Otherwise, by 6, we have $-a = -(a \cdot 1) = a \cdot (-1)$, which means $a \mid |a|$ as well. □

Lemma 19. *For all $a, b, c \in \mathbb{Z}$, if $a \mid b$ then $a \mid bc$.*

Proof. By the definition of $a \mid b$, we have $b = ak$ for some $k \in \mathbb{Z}$. Multiplying each side by $c \in \mathbb{Z}$, we have $bc = (ak)c = a(kc)$. Since $\mathbb{Z}$ is multiplicatively closed, $kc \in \mathbb{Z}$, so by Definition 10, we have $a \mid bc$. □

Lemma 20. *If $k \mid a$ and $k \mid b$, then $k \mid (a+b)$.*

Proof. By definition of $k \mid a$ and $k \mid b$, we get that $a = kx$ and $b = ky$ for some integers $x, y \in \mathbb{Z}$.

Thus, $a+b = kx+ky = k(x+y)$. Because $x+y \in \mathbb{Z}$ by additive closure, we have $k \mid (a+b)$ by the definition of k. □

Lemma 21. *If $d \mid a$ and $d \mid b$, then $d \mid (ar+bs)$ for $r, s \in \mathbb{Z}$.*

Proof. If $d \mid a$ and $d \mid b$, then by definition, we have $a = dm$ for $m \in \mathbb{Z}$ and $b = dn$ for $n \in \mathbb{Z}$. Then, we have $ar + bs = (dm)r + (dn)s$ by substitution.

By associativity and distributivity, we have

$$\begin{aligned}(dm)r + (dn)s &= d(mr) + d(ns) \\ &= d(mr + ns)\end{aligned}$$

By definition, d divides $d(mr+ns) = ar+bs$. Therefore, if $d \mid a$ and $d \mid b$, $d \mid (ar+bs)$ for every r and s in $\mathbb{Z}$. □

Lemma 22. *For all $a, b, c \in \mathbb{Z}$, if $a \mid b$ and $b \mid c$, then $a \mid c$.*

Proof. By Definition 10, $b = am$ for $m \in \mathbb{Z}$ and $c = bn$ for $n \in \mathbb{Z}$. Substituting, we have $c = (am)n = a(mn)$, which implies that $a \mid c$ since $mn \in \mathbb{Z}$. □

Lemma 23. *If $a, b \in \mathbb{Z}^+$ and $a \mid b$, then $a \leq b$.*

Proof. First, we prove that for all $a \in \mathbb{Z}^+$, $a - 1 \in \mathbb{N}$. Define $S \coloneqq \{a \in \mathbb{Z}^+ : a - 1 \notin \mathbb{N}\}$ and assume for contradiction that S is nonempty. By WOP, S contains a smallest element $m+1$, and $(m+1)-1 = m \notin \mathbb{N}$. Since $m \notin S$, $m - 1 \in \mathbb{N}$. However, by Lemma 9, $(m-1)+1 = m \in \mathbb{N}$, which is a contradiction. Therefore, S must be empty, and for all $a \in \mathbb{Z}^+$, $a - 1 \in \mathbb{N}$.

Next, we prove that for $a, b, k \in \mathbb{Z}^+$ and $b = ak$, $a \leq b$. We can rewrite $b = ak = a(k-1) + a$, so $b - a = a(k-1)$. By the proof above, we know that $k - 1 \in \mathbb{N}$ for all $k \in \mathbb{Z}^+$. By Lemma 10, $\mathbb{N}$ is multiplicatively closed, implying that $a(k-1) = x$ for $x \in \mathbb{N}$. Substituting, we have $b - a = x$, or $b = a + x$. Then, by definition, $a \leq b$. □

Lemma 24 (WOP on $\mathbb{N}$)**.** *Let S be a subset of $\mathbb{N}$. There, there is an element in S that is no greater than any other element in $\mathbb{N}$.*

Proof. If $0 \notin S$, then S is a subset of $\mathbb{Z}^+$, so we can apply WOP on $\mathbb{Z}^+$.

If $0 \in S$, then because the remaining elements in S will be positive integers, 0 will be less than all other elements in S. □

4.4. Modular arithmetic

Definition 11. We write $a \equiv b \pmod{m}$ for integers a, b if there exists an integer k such that $a = b + mk$.

For example: $3 \equiv 20 \pmod{17}$ since $3 = 20 + 17(-1)$

Definition 12. Let $\mathbb{Z}_n$ be the set of integers reduced modulo n, containing the integers between 0 and $n-1$.

Some examples of the usage of $\mathbb{Z}_n$:

- We have $17 = 3$ in $\mathbb{Z}_7$ because $17 \equiv 3 \pmod{7}$.
- In $\mathbb{Z}_5$, $1 + 4 = 1 + 9 = 10 = 0$, because the four numbers are congruent under modulo 5.

4.5. Greatest Common Divisor

Before we discuss the greatest common divisor, we first need to define the Euclidean Division Lemma, which discusses how many times a positive integer b can go into another integer a, and how much of a remains after several groups of b are taken out of it.

This is best represented with a word problem.

Problem 1. *Jared has 17 watermelons. He wants to split his watermelons into as many groups of 5 as possible. How many groups of 5 watermelons can he have, and how many watermelons will remain?*

Solution. If Jared makes one group of 5 watermelons, then there are still 12 watermelons remaining. Because $12 \geq 5$, this means Jared can create more groups of watermelons.

If Jared makes two groups of 5 watermelons, then there are still 7 watermelons remaining. Again, because $7 \geq 5$, Jared can still make more groups.

If Jared makes three groups of 5 watermelons, then there are 2 watermelons remaining. This time, because $2 < 5$, Jared cannot make any more groups of 5 watermelons.

Hence, Jared can make 3 groups of 5 watermelons, and there will be 2 watermelons remaining. ■

The Euclidean Division Lemma states that there is always a nonnegative remainder that is less than the size of the grouping:

Lemma 25. *Suppose a is an integer and b is a positive integer. Then, there exists $q, r \in \mathbb{Z}$ such that $0 \leq r < b$ and $a = bq + r$.*

Proof. If $b = 1$, then the result is clear: set $a = 1$, $q = 1$, and $r = 0$.

Otherwise, by Lemma 15, we have $b > 1$. Let S be the set of positive integers that cannot be expressed as $bq + r$ such that $0 \leq r < b$.

Say for the sake of contradiction that S is non-empty. Then, by WOP, there is an element m such that $m \leq n$ for all $n \in S$.

If $m = 1$, then since $b > 1$, we have $m = b(0) + 1$ works. Otherwise, by Lemma 15, we have $m > 1$. Then, $m - 1 \in \mathbb{Z}^+$ yet $m - 1 \notin S$. This means $m - 1 = bq_1 + r_1$ for some $q_1, r_1 \in \mathbb{Z}$ such that $0 \leq r_1 < b$.

Then, $m = bq_1 + (r_1 + 1)$. By Lemma 16, the only integer x such that $b - 1 \leq x < b$ is $b - 1$. There are now two cases:

Case 1: $r_1 = b - 1$. Then, $m = bq_1 + b = b(q_1 + 1) + 0$, meaning we can set $q = q_1 + 1$ and $r = 0$. This contradicts the fact that $m \in S$.

Case 2: $r_1 \neq b - 1$. Because the only integer between $b - 1 \leq x < b$ is $b - 1$, then $r_1 < b - 1$. Then, $r_1 + 1 < b$. Because $m = bq_1 + (r_1 + 1)$, we can set $q = q_1$ and $r = r_1 + 1$, and $r < b$. This contradicts the fact that $m \in S$.

Thus, S is empty, and all positive integers a can be expressed as $bq + r$ satisfying the conditions in the lemma.

If $a = 0$, then set $q = r = 0$, so the lemma is true for $a = 0$.

Finally, if a is negative, then $-a$ is positive, so $-a = bq' + r'$ for some $q', r' \in \mathbb{Z}$ and $0 \leq r' < b$. Then, $a = b(-q') + (-r')$, but $-b < r' \leq 0$. If $-r' = 0$, then set $r = -r'$. Otherwise, note that $a = b(-q' - 1) + (b - r')$, and since $-b < -r' < 0$, we have $0 < b - r' < b$, so we may set $q = -q' - 1$ and $r = b - r'$. Hence, the lemma is true for negative integer a.

Therefore, all integers a are expressible as $a = bq + r$ for $q, r \in \mathbb{Z}$, positive b, and $0 \leq r < b$. □

The numbers q and r in Lemma 25 are important, so we will give them names.

Definition 13. The number q in Lemma 25 is called the **quotient**. Note that it does not need to be a nonnegative integer.

The number r in Lemma 25 is called the **remainder**. This number will be a nonnegative integer.

Now, we can define the greatest common divisor of two numbers.

Definition 14. The **greatest common divisor (GCD)** of two integers a and b such that at least one of a or b is nonzero, denoted $\gcd(a, b)$, is equal to c for $c \in \mathbb{Z}^+$ if $c \mid a$ and $c \mid b$. Furthermore, for all $d \in \mathbb{Z}^+$ such that $d \mid a$ and $d \mid b$, $d \leq c$.

For example: The GCD of 34 and 85 is 17, since $17 \mid 34$ and $17 \mid 85$ and all other common divisors are less than 17.

Now that we've defined GCD, we must prove its existence and uniqueness, which is important for using the GCD in future results.

Lemma 26. *For any two integers a and b such that $a \neq 0$ or $b \neq 0$, there exists a greatest common divisor of a and b.*

Proof. To prove that the GCD exists, we must prove that there exists a common divisor of a and b. In other words, $d \in \mathbb{Z}^+$ such that $d \mid a$ and $d \mid b$. Then, we show that for all other common divisors c, $c \leq d$.

First, we show that there always exists a common divisor of a and b. In other words, there exists a positive integer d such that $d \mid a$ and $d \mid b$.

We define $S \coloneqq \{ax + by : x, y \in \mathbb{Z}, ax + by > 0\}$. If $a \neq 0$, then notice that $|a| \in S$ since $a \mid |a|$. Otherwise, $b \neq 0$, so $|b| \in S$ since $b \mid |b|$. Thus, S is nonempty.

Because S is nonempty, by WOP, S has a smallest element d, meaning we can write $d = ax + by$ for integers x and y.

For contradiction, assume that $d \nmid a$. Then, by Lemma 25, we can write $a = kd + r$ where $0 \leq r < d$. However, if $r = 0$, then we would have $d \mid a$, so we can further restrict the inequality to $0 < r < d$.

Then, we can write

$$\begin{aligned} r &= a - kd \\ &= a - k(ax + by) \\ &= a(1 - kx) - b(ky) \end{aligned}$$

and since r is positive, this means $r \in S$. However, as shown above, $r < d$, which contradicts the minimality of d. Therefore, $d \mid a$. By a similar argument, $d \mid b$. This implies the existence of a common divisor of a and b.

Next, we show that all other common divisors c of a and b are less than or equal to d. Since c is a common divisor of a and b, $c \mid a$ and $c \mid b$. By Lemma 21, $c \mid ax + by$ so $c \mid d$. By Lemma 23, $c \leq d$. Therefore, d is the largest of the common divisors.

Combining both parts, we know that a common divisor always exists, and that d, the GCD, is the largest of them, which by definition, implies the existence of a GCD. □

Now, we prove that the GCD of two numbers is unique.

Lemma 27. *For any two integers a and b such that $a \neq 0$ or $b \neq 0$, the GCD is uniquely defined.*

Proof. If there are two possible values of $\gcd(a, b)$, then call them g_1 and g_2. Then, by the definition of a greatest common divisor, we have $g_1 \geq g_2$. Again, by the definition of a greatest common divisor, we have $g_2 \geq g_1$. Hence, $g_1 = g_2$, meaning $\gcd(a, b)$ is unique. □

4.6. Bezout's Lemma

Consider the following problem:

Problem 2. *Ashlee plays a game where she starts with an empty pig sty. Every second, she does one of the following:*

1. *Add* 85 *pigs to the sty.*
2. *Remove* 85 *pigs from the sty.*
3. *Add* 34 *pigs to the sty.*
4. *Remove* 34 *pigs from the sty.*

What is the smallest positive number of pigs that could ever be in the sty at one time?

Solution. The problem boils down to finding possible values of c such that there exists two integers x, y satisfying $85x + 34y = c$.

Now, note that 17 is the greatest common divisor of 85 and 34. This means that if a positive integer c is a linear combination of 85 and 34, it must be a multiple of 17 by Lemma 21.

Thus, by Lemma 23, if $85x + 34y = c$ and c is positive, then $c \geq 17$. Note that $85(1) + 34(-2) = 17$, so the smallest positive integer number of pigs there could be in the sty is $\boxed{17}$. This occurs when Ashlee adds 85 pigs once and removes 34 pigs twice. ■

From an example like Problem 2, it appears that $\gcd(a, b)$ will always be a linear combination of a and b. This is called **Bezout's Lemma**.

Lemma 28 (Bezout's Lemma)**.** *For every $a, b \in \mathbb{Z}$ such that at least one of a, b is nonzero, then there exist $x, y \in \mathbb{Z}$ such that*

$$ax + by = \gcd(a, b).$$

Proof. Let $S \coloneqq \{ax + by \in \mathbb{Z}^+ : x, y \in \mathbb{Z}\}$. We know that S is nonempty because $|a| + |b|$ is positive since $a \neq 0$ or $b \neq 0$, and $|a| + |b| \in S$ since $a \mid |a|$ and $b \mid |b|$. Since S is nonempty, by WOP, S contains a smallest element m satisfying $m = ax + by$ for $x, y \in \mathbb{Z}$.

Using Euclidean division (Lemma 25), we can write $a = mk + r$ for $k \in \mathbb{Z}$ and $0 \leq r < m$, or

$$\begin{aligned} a &= (ax + by)k + r \\ a &= axk + byk + r \\ r &= a - axk - byk \\ &= a(1 - xk) - b(yk) \end{aligned}$$

However, Euclidean division is defined such that $0 \leq r < m$. Furthermore, as r cannot be less than the minimal element m, r can only satisfy the inequality if $r = 0$. This is because $r \notin S$, as S only considers positive integers. Therefore, we have $a = km$, and $m \mid a$.

Similarly, if we write $b = mk + r$, we obtain

$$\begin{aligned} b &= k(ax + by) + r \\ b &= kax + kby + r \\ r &= b - kax - kby \\ &= a(-kx) + b(1 - ky) \end{aligned}$$

which again implies $r = 0$, meaning that $b = mk$ so $m \mid b$ as well.

If we take some other common divisor e of a and b, we have that $e \mid a$ and $e \mid b$, so $e \mid (ax + by)$ by Lemma 21. Since $m = ax + by$ for some integers x and y, all other divisors e satisfy $e \mid m$. By Lemma 23, all common divisors e are less than or equal to m. By definition, this proves that m is the GCD, and that $ax + by = \gcd(a, b)$ has a solution for integers x, y. □

This lemma is incredibly significant, and we will use this lemma to prove many, many theorems in the future.

4.7. Linear Diophantine Equations

Problem 3. *Solve the system of congruences* $x \equiv 5 \pmod 7$ *and* $x \equiv 7 \pmod{11}$.

Solution. We can write $x = 7a + 5 = 11b + 7$ for some integers a and b. Hence,

$$7a - 11b = 2.$$

By Bezout's Lemma, there exist integers a', b' such that $7a' - 11b' = 1$. Then, let $a = 2a'$ and $b = 2b'$ to get $7a - 11b = 2$. The pair $(a, b) = (16, 10)$ is a solution. This gives $x = 7a + 5 = 117$.

We found one solution to (a, b), and we can then find x, but the Chinese Remainder Theorem emphasizes the uniqueness of a number x under a certain modulus (in this case, it is 77).

How do we prove that x is unique under mod 77?

We turn the two congruences into one linear Diophantine equation:

Definition 15. A **Diophantine equation** is an equation where we only look at integer solutions.

We found one solution to $7a - 11b = 2$, but are there any more solutions? If so, how do we parameterize them?

Consider our solution $(a_0, b_0) = (16, 10)$ again. Rewrite $7a-11b = 2$ as $11b = 7a-2$. Now, if we let $a = a_0+1$, notice that the right hand side will be $7 \pmod{11}$ and hence not a multiple of 11, so if $a = a_0 + 1$, then b is not an integer.

If we let $a = a_0 + 2$, then the right hand side will be $3 \pmod{11}$, meaning if $a = a_0 + 2$, then b is not an integer.

If we keep doing this, it seems like if $a \equiv a_0 \pmod{11}$, only then will b will be a multiple of 11, and then the Diophantine equation has a solution.

With this, it appears that all of our solutions are of the form $(a_0 + 11z, b_0 - 7z)$ for any integer z. Thus, $x = 7a + 5 = 7a_0 + 77z + 5$. This means x is unique under modulo 77, satisfying the Chinese remainder theorem. Why does this happen? ■

4.7.1. Coprime Condition

Recall that the Chinese Remainder Theorem has a condition stating that all the moduli are pairwise coprime.

Definition 16. Two integers a and b are **coprime** if $\gcd(a, b) = 1$. A set of k integers a_i for indices $1 \leq i \leq k$ is called **pairwise coprime** if $\gcd(a_i, a_j) = 1$ for all indices $1 \leq i \leq j$.

For example: 17 and 19 are coprime, as their GCD is 1. The set of integers $\{17, 19, 23\}$ are pairwise coprime, since $\gcd(17, 19) = \gcd(17, 23) = \gcd(19, 23) = 1$.

In our example, the moduli are 7 and 11. Those numbers are coprime. From our experiment, we tested different integer values of k to see when $a = a_0 + k$ yields an integer b.

Plugging this into $11b = 7a - 2$, we get $11b = 7a_0 + 7k - 2$. However, $7a_0 - 2 = 11b_0$, so $11b = 11b_0 + 7k$, and $7k = 11(b - b_0)$.

This means we need $7k$ to be a multiple of 11. We saw that k should then be a multiple of 11, but how do we go from $11 \mid 7k \implies 11 \mid k$?

This is where we utilize the coprime condition:

Theorem 29. *If $\gcd(a, n) = 1$, then there exists an integer a^{-1} such that $a \cdot a^{-1} \equiv 1 \pmod{n}$.*

Proof. By Bezout's Lemma, there exist integers x, y such that

$$ax + ny = \gcd(a, n) = 1.$$

Thus, $ax \equiv 1 \pmod{n}$. □

Numbers like a are important, so we will give them a name:

Definition 17. A integer a is a **unit** in $\mathbb{Z}_n$ if there exists an integer a^{-1} such that $a \cdot a^{-1} \equiv 1 \pmod{n}$.

With this, we can prove the **Fundamental Lemma**:

Lemma 30 (Fundamental Lemma)**.** *If $n \mid ab$ and $\gcd(a, n) = 1$, then we have $n \mid b$.*

Proof. Because $\gcd(a, n) = 1$, by Theorem 29, we get that a^{-1} exists. Then,

$$ab \equiv 0 \pmod{n} \implies ab \cdot a^{-1} \equiv 0 \cdot a^{-1} \equiv 0 \pmod{n} \implies b \equiv 0 \pmod{n}.$$

Hence, $n \mid b$. □

The Fundamental Lemma is how we get $11 \mid 7k \implies 11 \mid k$, since $\gcd(7, 11) = 1$. This proves that all solutions to (a, b) for our example earlier are of the form $(a_0 + 11z, b_0 - 7z)$.

4.7.2. Parametrizing Solutions

With the Fundamental Lemma, we can now parameterize solutions to Linear Diophantine equations:

Theorem 31. *Suppose a, b, c are integers. If $\gcd(a, b) = 1$, and (x_0, y_0) is an integer solution to $ax + by = c$, then all integer solutions are of the form $(x_0 + bz, y_0 - az)$ for some $z \in \mathbb{Z}$.*

Proof. Because $ax + by = c$, then $ax \equiv c \pmod{b}$. Since $\gcd(a, b) = 1$, by Theorem 29, we get that a^{-1} exists in $\mathbb{Z}_b$. This means

$$ax \equiv c \pmod{b} \implies x \equiv ca^{-1} \pmod{b}.$$

Hence, x is unique under modulo b. Because (x_0, y_0) is a solution, this means $x \equiv x_0 \pmod{b}$. This means $x = x_0 + bz$ for some integer z.

Thus, using the fact that $by_0 = c - ax_0$, we have

$$by = c - ax = c - ax_0 - abz = by_0 - abz = b(y_0 - az).$$

Hence, by Lemma 12, we get $y = y_0 - az$. □

4.8. Putting it all together

Theorem 31 is extremely imporant! This theorem is what we discovered from our experimentation with our example system of congruences, and it allows us to find all solutions to the system of congruences.

In fact, we can prove Chinese Remainder Theorem for two moduli right now:

Lemma 32 (Chinese Remainder Theorem for Two Moduli)**.** *Suppose x, x_1, x_2 are integers, and suppose n_1, n_2 are positive integers such that $\gcd(n_1, n_2) = 1$. If $x \equiv x_1 \pmod{n_1}$ and $x \equiv x_2 \pmod{n_2}$, then there is a unique solution for x under modulo $n_1 n_2$.*

Proof. The condition $x \equiv x_1 \pmod{n_1}$ means $x = n_1 q_1 + x_1$ for some integer q_1. Similarly, $x = n_2 q_2 + x_2$ for integer q_2.

This means

$$n_1 q_1 + x_1 = n_2 q_2 + x_2 \implies n_1 q_1 - n_2 q_2 = x_2 - x_1.$$

Because $\gcd(n_1, n_2) = 1$, Bezout's lemma tells us that there exist q_1', q_2' such that $n_1 q_1' - n_2 q_2' = 1$. Then, let $u = q_1' \cdot (x_2 - x_1)$ and $v = q_2' \cdot (x_2 - x_1)$ to get $n_1 u - n_2 v = x_2 - x_1$. Hence, $(q_1, q_2) = (u, v)$ is a valid solution.

Then, by Theorem 31, we get that all solutions (q_1, q_2) to $n_1 q_1 - n_2 q_2 = x_2 - x_1$ are of the form $(u - n_2 z, v - n_1 z)$ for some integer z.

Substitute q_1 into $x = n_1 q_1 + x_1$ to get $x = n_1 u - n_1 n_2 z + x_1$. This means $x \equiv n_1 u + x_1 \pmod{n_1 n_2}$, so x is unique under mod $n_1 n_2$. □

4.8.1. Lemmas About Primes

We need to prove the following two lemmas before proving the Chinese Remainder Theorem.

Lemma 33. *If x is a positive integer greater than 1, then x has a prime divisor.*

Proof. Let S be the set of positive integers greater than 1 that do not have a prime divisor. We wish to show that S is empty.

Say for the sake of contradiction that S is not empty. By WOP, we know that S has a minimum element m.

If m is prime, then it has a prime divisor m, which is a contradiction.

If m is not prime, then since $m \neq 1$ and thus has distinct divisors 1 and m, it will have another divisor d. By Lemma 23, we have $d \leq m$, and by Lemma 15, we have $d \geq 1$. However, $d \neq 1$ and $d \neq m$ so $1 < d < m$.

Because $d < m$ and $1 < d$, due to the minimality of m in S, we have that d has a prime divisor p.

However, because $m = dx$ for some integer x, and $d = py$ for some integer y, we get $m = pxy$, meaning $p \mid m$. This is a contradiction, so every positive integer greater than 1 has a prime divisor. □

Lemma 34. *Suppose p is a prime and a_i is an integer for all integers i between 1 and n, inclusive. If $p \mid a_1 a_2 \ldots a_n$, then $p \mid a_i$ for some integer i between 1 and n, inclusive.*

Proof. Let S be the set of positive integers n such that the given claim is not true. Then, by WOP, S has an element m that is no greater than other elements in S.

Note that $m \neq 1$, because $p \mid a_1 \implies p \mid a_1$ is true.

Hence, by Lemma 15, we get $m > 1$, so $m - 1$ is positive. However, $m - 1 < m$ so $m - 1 \notin S$, meaning that $n = m - 1$ satisfies the given claim.

There are now two cases. Either $p \mid a_m$, which contradicts $m \in S$, or $p \nmid a_m$. If $p \nmid a_m$, then $\gcd(p, a_m) = 1$, since the only positive divisor of p that is less than p is 1. Then, by Lemma 30, we get

$$p \mid \prod_{k=1}^{m-1} a_k$$

so $p \mid a_i$ for some index i with $1 \leq i \leq m - 1$, since $n = m - 1$ satisfies the given claim. This contradicts $m \in S$.

Hence, S is empty, and the result follows. □

And finally...

Theorem 35 (Chinese Remainder Theorem)**.** *Suppose we have k positive integer moduli n_i and k integers x_i for integers i such that the set of moduli are pairwise coprime. Then, the system of congruences*

$$x \equiv x_i \pmod{n_i}$$

for all integer i with $1 \leq i \leq k$ results in a unique solution for x under modulo $n_1 n_2 \dots n_k$.

Proof. Let S be the set of positive integer values of k such that the given claim is false. Say for the sake of contradiction that S is nonempty. By WOP, it has an element m that is no greater than any of the other elements in S.

Note that $m \neq 1$ because $x \equiv x_1 \pmod{n_1}$ yields a unique solution to x in mod $\prod_{j=1}^{k} a_j = a_1$.

Thus, by Lemma 15, we have $m > 1$. Then, $m-1$ is positive but not in S since $m-1 < m$. This means the given claim is true for $m-1$.

Let

$$J = \prod_{j=1}^{m-1} a_j.$$

Because the set of all moduli are pairwise coprime, this means the set of all moduli excluding n_m is also pairwise coprime. Then, since we have $x \equiv x_i \pmod{n_i}$ for all integer i between 1 and $m-1$, and the given claim is true for $k = m-1$, we have

$$x \equiv P \pmod{J}$$

for some integer P.

I claim $\gcd(J, n_m) = 1$. Say for the sake of contradiction that $\gcd(J, n_m) \neq 1$. Then, by Lemma 15, we have $d = \gcd(J, n_m) > 1$.

This means d has a prime divisor p by Lemma 33. Then, $d \mid J \implies p \mid J$. Then, by Lemma 34, we have that since $p \mid J$, we have $p \mid n_i$ for some integer i between 1 and $m-1$ inclusive.

However, then $\gcd(n_i, n_m) \geq p > 1$, which is a contradiction since $\gcd(n_i, n_m) = 1$, due to the set of moduli being pairwise coprime. Hence, $\gcd(J, n_m) = 1$.

Thus, we can use Lemma 32 to get that x has a unique solution under modulo Jn_m. Recalling the definition of J, we get that x has a unique solution under modulo $n_1 n_2 \dots n_m$. □

5. Conclusion

The Chinese Remainder Theorem is one of the most important results in number theory; yet, it is on the simpler end of theorems in the field. Still, the proof for this theorem utilizes many intermediate results.

This demonstrates how a few simple axioms, namely, the ring axioms, order axioms, and the well-ordering principle, lead us to discover many astonishing results about integers.

To prove the Chinese Remainder Theorem, we first proved properties that apply to all rings. Then, we introduced the concept of division and also proved the Euclidean Division Lemma. Using this, we proved Bezout's Lemma, a major result.

After proving Bezout's Lemma, we parameterized all solutions to a certain linear Diophantine equation. Solving this Diophantine equation is equivalent to solving a system of two modular congruences, which lead to the proof of the Chinese Remainder Theorem for two congruences.

Finally, we used the well-ordering principle of the integers to generalize the Chinese Remainder Theorem to a system of any number of congruences.

5.1. Chinese Remainder Theorem in Other Rings

Recall that we proved the Chinese Remainder Theorem from just the ring axioms, order axioms, and the well-ordering principle. Because we used the order axioms and well-ordering principle, which are not axioms that all rings have, the Chinese Remainder Theorem may not work for all rings.

While we could try to modify our proof of the Chinese Remainder Theorem to work in other rings, we cannot abandon the properties of the integers entirely. For example, we need the order axioms and the well-ordering principle to demonstrate that the Euclidean Division Lemma holds, which we used to prove Bezout's Lemma.

One way to get around this obstacle is to define a norm function $N\colon R \to \mathbb{N}$. The norm function measures the "size" of elements in a ring.

This concept of size is important, since the Euclidean Division Lemma states that given $a \in \mathbb{Z}$ and $b \in \mathbb{Z}^+$, there is an integer q and a "small enough" integer r such that $a = bq + r$. To determine if r is small enough, it must satisfy $0 \leq r < b$. In another ring, we could check if $N(r) < N(b)$.

For example, $\mathbb{Z}[i]$ is not an ordered ring. However, there does exist a norm function $N\colon \mathbb{Z}[i] \to \mathbb{N}$ in $\mathbb{Z}[i]$. If $a, b \in \mathbb{Z}$, then:

$$N(a + bi) = a^2 + b^2.$$

The norm function is useful because it can "convert" elements from any ring into natural numbers. Then, using 24, we could use WOP on the norms of the elements of $\mathbb{Z}[i]$ instead of the elements themselves.

Hence, we could use the Euclidean Division Lemma on ring R if we can find a good norm function for R. This opens the door to many other results; the Euclidean Division Lemma leads to Bezout's Lemma, which allows us to parameterize solutions to linear Diophantine equations. With this, we can prove the Chinese Remainder Theorem for R.