Euclidean Algorithm, Bezout's Lemma, and the Chinese Remainder Theorem: These are a Few of My Favorite Things

Lola Huang, Max Yan

Contents

Abstract

In this paper, we present a comprehensive proof of the Chinese Remainder Theorem (CRT) by leveraging the axiomatic definition of the integers. Beginning with the fundamental properties of integers, we systematically develop the necessary tools, including ordering, subtraction, division, and modular arithmetic. The proof of the CRT is achieved by leveraging key corollaries, such as the Division Algorithm, Euclidean Algorithm, and Bezout's Lemma. Additionally, an alternative proof is explored in the Appendix, providing further insight into the versatility of the underlying mathematical structures.

1. Introduction

The Chinese Remainder Theorem (CRT) is a fundamental result in number theory and abstract algebra, providing a powerful tool for solving systems of linear congruence equations. This theorem describes the structure of the ring of integers modulo the product of pairwise coprime moduli, and has numerous applications in areas such as cryptography, coding theory, and computer science.

In this paper, we present a comprehensive proof of the CRT by meticulously building upon the axiomatic definition of the integers, denoted as $\mathbb{Z}$. Beginning with the ordered ring structure of the integers and the Well-Ordering Principle, we systematically develop the necessary concepts and tools required to establish the CRT.

Our approach starts with the fundamental properties of integers, including ordering, subtraction, and division. We then introduce modular arithmetic and establish key results such as the Division Algorithm, Euclidean Algorithm, and Bezout's

Lemma. These intermediate steps serve as essential building blocks for the final proof of the CRT.

In addition to the primary proof, we also explore an alternative proof of CRT in the Appendix. This comprehensive treatment aims to offer the reader a thorough understanding of the CRT and the elegant techniques employed in its proof.

2. History

The Chinese Remainder Theorem is a well-celebrated theorem originating from *Sunzi Suanjing* stated by the Chinese mathematician *Sunzi*. The original problem was stated as follows:

There is a collection of things, whose exact 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?

We can quickly check that 23 is a solution. But is it unique? Clearly not: so are $128, 233, 338$, and so on. These solutions seem to differ by multiples of 105. Is that always true? This type of problem is what the CRT, and the mathematicians who developed it, hoped to solve. Throughout the centuries as mathematicians axiomatized algebraic systems in an abstract algebra point of view, they have been able to generalize the CRT to any ring, with the formulation of two-sided ideals.

In this paper, we will focus on the early developments of the CRT from an axiomatic point of view.

3. The Very Beginning: Axioms

In this section we define the integers, $\mathbb{Z}$, using three sets of axioms, the ring axioms, the order axioms, and the Well-Ordering Principle. We delineate all defining characteristics of the integers so that we can derive corollaries and theorems solely using our axioms.

First, we capture an important characteristic of the operations we impose on the set of integers.

Definition 1. Binary Operation: A binary operation $\circ$ on a set S takes two elements, $a, b \in S$, and outputs a unique solution. Binary operations are closed; in other words, $(a \circ b) \in S$.

3.1. Ring Axioms

We begin by capturing the most important characteristic of the integers: two binary operations, addition and multiplication, together with a multiplicative identity one and an additive identity zero, define a ring. One could check from past experience in working with the integers that they do indeed satisfy the ring axioms.

Definition 2. Ring Axioms: A set R is a Ring if it is equipped with two binary operations $(+, \cdot)$ that satisfy the Ring Axioms.

(i) Additive Commutativity: $\forall\ a, b \in R : a + b = b + a$.

(ii) Additive Associativity: $\forall\ a, b, c \in R : (a + b) + c = a + (b + c)$.

(iii) Multiplicative Commutativity: $\forall\ a, b \in R : ab = ba$.

(iv) Multiplicative Associativity: $\forall\ a, b, c \in R : (ab)c = a(bc)$.

(v) Multiplicative Distribution: $\forall\ a, b, c \in R : a(b + c) = ab + ac$.

(vi) Zero: $\exists\ 0 \in R, \forall\ a \in R : a + 0 = a$.

(vii) One: $\exists\ 1 \in R, \forall\ a \in R : a \cdot 1 = a$.

(viii) Negatives: $\forall\ a \in R, \exists\ x \in R : a + x = 0$. Denote $x := -a$.

Now that we have established a few basic axioms, we explore the implications of such principles on general rings. Denote by R a ring satisfying the listed axioms. Although some of these corollaries might seem “trivial” given the readers’ prior experience, it is crucial for us to work our way through the corollaries carefully.

Corollary 1. *$\forall\ a \in R$, $(-a) + a = 0$.*

Proof. By additive commutativity, $(-a)+a = a+(-a)$. Since we have defined $(-a)$ to be the additive inverse of a, we have $(-a) + a = a + (-a) = 0$. □

The next corollary shows an important result for general rings R: the additive identity and the multiplicative identity are unique.

Corollary 2. *The additive identity* 0 *and the multiplicative identity* 1 *are unique.*

Proof. We first show that "0" is unique. Suppose there exists additive identities $0 \neq 0'$ such that $a + 0' = a$ and $a + 0 = a$ for all $a \in \mathbb{Z}$. We then have $a + 0 = a + 0'$. We add the negative of a to both sides and obtain $(-a) + (a+0) = (-a) + (a+0') \Rightarrow ((-a) + a) + 0 = ((-a) + a) + 0' \Rightarrow 0 + 0 = 0 + 0'$. Since $0 + 0 = 0$ and $0 + 0' = 0'$ (Zero Axiom), we must have $0 = 0'$.
Next, to show that "1" is unique, suppose there exists some $1 \neq 1'$ such that for all $a \in R$, $a \cdot 1' = a$. By the One Axiom on 1, we have $1' \cdot 1 = 1'$. By the One Axiom on $1'$, we have $1 \cdot 1' = 1 \Rightarrow 1' \cdot 1 = 1$. By transitivity of equality, we know that $1' = 1$. □

We next show the cancellation principle:

Corollary 3. *Given $a, b, b' \in R$, $a + b = a + b'$ must imply $b = b'$.*

Proof. We start by add $(-a)$ to both sides of the equation: $(-a) + (a + b) = (-a) + (a + b') \Rightarrow ((-a) + a) + b = ((-a) + a) + b' \Rightarrow 0 + b = 0 + b' \Rightarrow b = b'$. □

Recall that we have specified "left distributivity" $a(b+c) = ab+ac$ in our ring axioms. Note that by commutativity, we may easily conclude that $a(b + c) = (b + c)a = ab + ac = ba + bc$. The latter equation $(b + c)a = ba + ca$ is often regarded as "right distributivity."
Next, we show that negatives are unique.

Corollary 4. *There is a unique solution x to $a + x = 0$.*

Proof. Firstly, we know by the Negatives Axiom that there exists a solution to the equation, which we denote as $-a$. Now, if there is another solution, say x_1, we get $a + (-a) = 0$ and $a + x_2 = 0$. Thus, $a + (-a) = a + x_2$. We can now add $(-a)$ to both sides and apply additive associativity to get:

$$(-a) + (a + (-a)) = (-a) + (a + x_2),$$

$$\Rightarrow (-a + a) + (-a) = (-a + a) + x_2.$$

$$\Rightarrow 0 + (-a) = 0 + x_2,$$

$$\Rightarrow (-a) + 0 = x_2 + 0,$$

$$\Rightarrow (-a) = x_2.$$

Thus, $(-a)$ is unique. □

The next corollary proves to be important in later proofs.

Corollary 5. *For all $a, b \in R$, one must have $-(-a) = a$, $-ab = (-a)b = a(-b)$, and $ab = (-a)(-b)$. Furthermore, $-a = a \cdot (-1)$*

Proof. To prove the first claim, note that we could view $-(-a)$ as the negative of $-a$. Thus by the Negatives Axiom we have $(-a) + (-(-a)) = 0$. We add both sides of the equation by a and obtain $a + ((-a) + (-(-a))) = a \Rightarrow (a + (-a)) + (-(-a)) = a \Rightarrow 0 + (-(-a)) = a \Rightarrow -(-a) = a$.
To show that $-ab = (-a)b$, consider $ab + (-a)b = (a + (-a))b = 0 \cdot b = b \cdot 0 = 0 \Rightarrow ab + (-a)b = 0$. Thus, $-ab = (-a)b$. Note that the claim $-ab = a(-b)$ holds by symmetry: the proven claim $-ab = (-a)b$ implies that $-ab = -ba = (-b)a = a(-b)$ by commutativity.
The next claim $ab = (-a)(-b)$ could be shown using our previous results and a little algebraic manipulation: $(-a)(-b) = -(a)(-b) = -(-ab) = ab$.
Our last claim, $-a = a \cdot (-1)$ can be confirmed by taking our previous results: $(-ab) = a(-b)$. Take $b = 1$. Then, $(-ab) = (-a)$ and $a(-b) = a \cdot (-1)$. Thus, $-a = a \cdot (-1)$. □

The zero element has an important property that it *absorbs products*: we claim that the product of any element in the ring with the zero element is going to be zero.

Corollary 6. *For $a \in R$, $a \cdot 0 = 0$.*

Proof. By the negatives axiom, note that $a \cdot 0 + (-(a \cdot 0)) = 0$. Simultaneously, we have $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$. Therefore, $(a \cdot 0) + (-(a \cdot 0)) = 0 \Rightarrow (a \cdot 0 + a \cdot 0) + (-(a \cdot 0)) = 0 \Rightarrow a \cdot 0 + (a \cdot 0 + (-a \cdot 0)) = a \cdot 0 + 0 = 0$. Thus, $a \cdot 0 = 0$. □

We now define subtraction.

Definition 3. Subtraction: For $a, b \in R$, we define $a - b$ to be $a + (-b)$.

Note that subtraction is closed in R as $a, -b \in R$, and addition in R is a binary operation. Therefore, we claim the following:

Corollary 7. *Subtraction is closed in R.*

Although we are off to a good start, the Ring Axioms alone are not enough to define the integers. We have no sense of "positivity," "negativity," "less than," or any sense of "order." Thus, we introduce the Order Axioms below.

3.2. Order Axioms

Definition 4. Ordered Ring: A Ring R is an ordered Ring if there exists a nonempty subset $R^+ \subseteq R$ satisfying the Order Axioms.

(i) Additive Closure: $\forall\ a, b \in R^+ : a + b \in R^+$

(ii) Multiplicative Closure: $\forall\ a, b \in R^+ : ab \in R^+$

(iii) Nontriviality: $0 \notin R^+$

(iv) Trichotomy: $\forall\ a \in R$: exactly one of the following holds: $a \in R^+, a = 0,$ or, $-a \in R^+$

We now have some important properties to establish. From here on out, R now denotes an ordered Ring. Again, these facts may seem basic, but oftentimes we find that intuition can lead us astray; for example, one cannot prove that $0 \neq 1$ simply from the Ring Axioms alone, because $\{0\}$ is a Ring. Thus, we will go through these next proofs carefully.

Corollary 8. *In R, $0 \neq 1$.*

Proof. From Corollary 6, we see that $\forall a \in R$, $a \cdot 0 = 0$. For the sake of contradiction, assume that $0 = 1$. Then, we can substitute 1 into the equation:

$$a \cdot 1 = 0.$$

By the definition of 1, $a \cdot 1 = a$. Thus, $a = 0$. This implies that all elements of R are 0. By non-triviality, 0 is not in R^+. However, this must mean that R^+ is empty; this is a contradiction, because R^+ is defined to be nonempty. Thus, our original assumption must have been wrong and $0 \neq 1$. □

Although we have established R^+, we don't really know what is inside it. Let us try to determine if $1 \in R^+$:

Corollary 9. *$1 \in R^+$, $-1 \notin R^+$.*

Proof. Since $0 \neq 1$, we know that either $1 \in R^+$ or $-1 \in R^+$ by trichotomy. For the sake of contradiction, assume that $-1 \in R^+$. Then, we obtain: $(-1) \cdot (-1) = 1 \cdot 1 = 1$ after applying Corollary 5,. By multiplicative closure, we know that $1 \in R^+$. However, this implies that both -1 and 1 are in R^+, which is a contradiction of trichotomy. So, our original assumption must have been wrong. Thus, $1 \in R^+$ and $-1 \notin R^+$. □

Ordering is necessary in our path to establish the Chinese Remainder Theorem, but how should we order elements of R? These next definitions will help us establish methods to compare two elements.

Definition 5. Less Than: For $a, b \in R$, we define $a < b$ to mean that $(b - a) \in R^+$.

Definition 6. Less Than or Equal to: For $a, b \in R$, we define $a \leq b$ to mean that $(b - a) \in R^+ \cup \{0\}$.

Definition 7. Greater Than: For $a, b \in R$, we define $a > b$ to be equivalent to $b < a$.

Definition 8. Greater Than or Equal to: For integers a, b, we define $a \geq b$ to be equivalent to $b \leq a$.

We now establish an equivalence between $a \in R^+$ and $a > 0$.

Corollary 10. $a \in R^+ \iff a > 0$.

Proof. $(\Longrightarrow)$: We can see that $a = a - 0$, so because $a \in \mathbb{Z}^+$, we also have $(a - 0) \in R^+$. Therefore, $a > 0$. $(\Longleftarrow)$: If $a > 0$, then $(a - 0) \in R^+$. But we know that $a - 0 = a$, so $a \in R^+$. □

Next, we show a "trichotomy of relations" principle.

Corollary 11. ***Trichotomy of Relations****: For any two integers $a, b \in \mathbb{Z}$, exactly one of the following is true:*

$$\begin{cases} a > b \\ a = b \\ a < b \end{cases}$$

Proof. Consider $a - b$. If $a - b = 0$, we may add b to both sides, apply the additive associativity, apply Corollary 1, and apply the Zero Axiom to get

$$(a - b) + b = b,$$

$$a + ((-b) + b) = b,$$

$$a + 0 = b,$$

$$a = b.$$

If $a-b \neq 0$, then either $(a-b) \in \mathbb{Z}^+$ or $-(a-b) \in \mathbb{Z}$ by trichotomy. If $(a-b) \in \mathbb{Z}^+$, then $a > b$. If $-(a-b) \in \mathbb{Z}^+$, we see that $-(a-b) = -(a) - (-b) = -a + b = b - a$. Thus, $(b-a) \in \mathbb{Z}^+$ and so $a < b$. □

The next corollary establishes the transitivity of "lesser than" relations.

Corollary 12. *For integers a, b, c, if $a < b$ and $b < c$, then $a < c$.*

Proof. Because $a < b$, $(b-a) \in \mathbb{Z}^+$. Similarly, because $b < c$, $(c-b) \in \mathbb{Z}^+$. By additive closure, we have $((b-a)+(c-b)) \in \mathbb{Z}^+$. We may apply the Ring Axioms to find

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

Thus, $(c-a) \in \mathbb{Z}^+$, implying that $a < c$. □

Next, we develop a negation principle.

Corollary 13. *For $a, b \in R$, if $a < b$, then $-a > -b$. Similarly, if $a \leq b$, then $-a \geq -b$.*

Proof. Since $a < b$, we have $(b-a) \in R^+$. Now, we observe that $b - a = b + (-a) = (-a) + b = (-a) - (-b)$. Therefore, $((-a) - (-b)) \in R^+$. This implies that $-a > -b$.

For the second statement, note that $a \leq b$ implies that either $a > b$ or $a = b$. The first case implies that $-b < -a$. The second case implies that $-b = -a$. Therefore, $-b \leq -a$. □

Now, we prove that addition preserves order.

Corollary 14. *For $a, b, c \in R$, if $a < b$, then $a + c < b + c$. Similarly, $a \leq b$ implies $a + c \leq b + c$.*

Proof. Since $a < b$, we have $(b-a) \in R^+$. Through the Ring Axioms, we also know that $b - a = (b+c) - (a+c)$, implying that $(b+c) - (a+c) \in R^+$. Therefore, $a + c < b + c$.

Similarly, if $b - a \in R^+ \cup \{0\}$, then $(b+c) - (a+c) \in R^+ \cup \{0\}$. Therefore, $a + c \leq b + c$ □

Then, we establish a crucial corollary that will soon be in use in the "division" section.

Corollary 15. *For $a, b \in R^+$, if $a = bc$ for some $c \in R$, then $c \in R^+$.*

Proof. Firstly, if $c = 0$, then $a = bc = 0$. By non-triviality, a is not in R^+, which is a contradiction. If $c \notin R^+$, then $-c \in R^+$ by trichotomy. This implies that $b(-c) \in R^+$ by multiplicative closure. However, by trichotomy, $-(b(-c)) = bc = a$ is not positive, which is a contradiction. Thus, $c \in R^+$. □

Next, we prove a theorem that will help us distinguish ordered Rings from non-ordered Rings:

Definition 9. Zero Divisors: A Ring R is a Ring with *zero divisors* if there exist $a, b \in R\backslash\{0\}$ such that $ab = 0$. If $a, b \in R\backslash\{0\}$ and $ab = 0$, then a and b are said to be zero divisors.

Corollary 16. *An ordered Ring R is a Ring without zero divisors. That is, if $a, b \in R$, $ab = 0$, and $a \neq 0$, then we must have $b = 0$.*

Proof. Suppose for the sake of contradiction that neither a or b is equal to zero. If $a, b \in R^+$, then $ab \in R^+$ by multiplicative closure. Therefore, at least one of the following is true: $-a \in R^+$, $-b \in R^+$. Since $ab = ba$ by commutativity, we may suppose without loss of generality that $-a \in R^+$. If $b \in R^+$, we have $-ab = (-a)b \in R^+$. Thus, $ab \neq 0$. If $-b \in R^+$, then $ab = (-a)(-b) = ab \neq 0 \in R^+$. Therefore, at least one of a, b is zero when $ab = 0$. □

We will introduce one last definition to characterize ordered Rings:

Definition 10. Negatives: Inspired by the definition of positivity, we introduce a definition for negativitity: if $-a \in R^+$, then a is negative. Note that 0 is neither positive nor negative.

The integers seem to be almost completely defined, but we are still missing a key element. In particular, we have no method of distinguishing between $\mathbb{Z}$, $\mathbb{R}$, and $\mathbb{Q}$; all three are ordered Rings. Thus, we need one final axiom to distinguish the set of integers.

3.3. Well-Ordering Principle

The Well-Ordering Principle (WOP) is the final axiom we will use to define $\mathbb{Z}$. In essence, WOP captures the discrete nature of the integers and acts as a defining characteristic between $\mathbb{Z}$ and $\mathbb{R}$. In corollaries from now on, we will refer to the integers, an ordered ring satisfying WOP, as $\mathbb{Z}$.

Axiom 17. ***Well-Ordering Principle****: The Well-Ordering Principle states that for any $S \subseteq \mathbb{Z}^+$, S has a minimum element: that is, there exists an $s \in S$ such that for all $a \in S$, $s \leq a$.*

Next, we prove a profound result that is commonly taken for granted:

Corollary 18. 1 *is the least element of* $\mathbb{Z}^+$. *Equivalently, there does not exist any integer between* 0 *and* 1.

Proof. Let set $S := \{a \in \mathbb{Z}^+ : a < 1\}$. Then, by the Well-Ordering Principle, there exists a minimal element in S, say m. By multiplicative closure, $m^2 \in \mathbb{Z}^+$. But also, because $m < 1$, we have $(1 - m) \in \mathbb{Z}^+$. By multiplicative closure, $(1 - m)m \in \mathbb{Z}^+$, so $m - m^2 \in \mathbb{Z}^+$. That would mean that $m^2 < m$, but m is the minimal element of S. Thus, our original assumption must be wrong and S must be empty. Therefore, 1 is the least element of $\mathbb{Z}^+$. □

Using Corollary 18, we aim to show that there does not exist any integer between k and $k + 1$ where $k \in \mathbb{Z}$.

Corollary 19. *For every $k \in \mathbb{Z}$, there does not exist an integer m such that $k < m < k + 1$.*

Proof. If there exists some m, k such that $k < m < k + 1$, then we must have $0 < m - k < 1$ by the principles of ordering we have established in the former section. Given that subtraction is closed within the integers, we know that this is impossible as shown in Corollary 18. □

Although the Well-Ordering Principle is powerful on its own, we will often work with sets containing negative elements. Thus, we will extend the Well-Ordering Principle to help us in future proofs.

Definition 11. Lower Bound: A lower bound l of a set S is an integer such that $l \leq s$ for every element $s \in S$. Note that only finite integer sets have lower bounds.

Definition 12. Upper Bound: An upper bound g of a set S is an integer such that $g \geq s$ for every element $s \in S$.

Corollary 20. ***Extended Well-Ordering Principle Part 1****: If a set S of integers has a lower bound, then S has a minimum element.*

Proof. Since S has a lower bound, there exists an integer l such that $l \leq s$ for every element s of S. Thus, $(s-l) \in \mathbb{Z}^+ \cup \{0\}$. Consider $S' := \{s-l+1 : s \in S\}$. Based on the observation that $(s-l) \in \mathbb{Z}^+ \cup \{0\}$ for all $s \in S$, we know that $((s-l)+1) \in \mathbb{Z}^+$. Thus, S' is a subset of positive integers. We can apply the Well-Ordering Principle on S': let m be the minimum element of S'.
Now, we know that $m = n - l + 1$ for some element n in S. Consider an element $s \in S$. because m is minimal in S' and $(s - l + 1) \in S'$, we have:

$$s - l + 1 \geq m,$$

$$s - l + 1 \geq n - l + 1,$$

$$s \geq n.$$

Thus, n is the minimum element of S. □

Corollary 21. *Extended Well-Ordering Principle Part 2: If a set S of integers has an upper bound, then S has a maximal element.*

Proof. Since S has an upper bound, we know that there exists an integer g such that for every element s of S, $g \geq s$. By Corollary 13, we have $-g \leq -s$. Next, consider set $S' := \{-s : s \in S\}$. Because $-g \leq -s$ for all $s \in S$, $-g$ is a lower bound for

S'. By the Extended Well-Ordering Principle Part 1, we know that there exists a minimum element of S', say m. Now, observe that for any element s of S, we have $m \leq -s$. Therefore, $-m \geq s$ by Corollary 13. We also know that $-m \in S$ by how we have defined S'. Therefore, we have found the greatest element of S: $-m$. □

4. When You Read You begin with A-B-C: Preliminaries

4.1. Division

Now that we have familiarized ourselves with the integer ring and the implications of its operations, we encourage the readers to gaze on the corollaries we have established: we have defined subtraction, the negation of addition, yet an "inverse operation" of multiplication seems to be missing. In this section we explore division, a quasi-multiplicative inverse on the set of integers.

Definition 13. Division: For integers a, b, we say that a divides b (denoted $a \mid b$) if there exists an integer k such that $b = ak$. a is said to be a **divisor** of b if a divides b.

We establish basic properties of division. Firstly, any integer must divide itself.

Corollary 22. *For all $a \in \mathbb{Z}$, $a \mid a$.*

Proof. By the One Axiom, we know that $a \cdot 1 = a$. Thus, by our definition of divisors, $a \mid a$. □

Next, if an integer a divides b, then it must divide any multiple of b.

Corollary 23. *For $a, b, c \in \mathbb{Z}$, if $a \mid b$, then $a \mid bc$.*

Proof. Because $a \mid b$, there exists an integer k such that $b = ak$. Therefore, we can substitute for b: $bc = (ak)c = a(kc)$. This implies that $a \mid bc$. □

The following corollary accounts for the universality of the division of 0.

Corollary 24. $\forall\ a \in \mathbb{Z}, a \mid 0$.

Proof. Because $a \cdot 0 = 0$ for all $a \in \mathbb{Z}$, we know that $a \mid 0$. □

Next, we develop an implication of division:

Corollary 25. *For $a, b \in \mathbb{Z}^+$, if $a \mid b$, then $a \leq b$.*

Proof. Because $a \mid b$, there exists an integer k such that $ak = b$. By Corollary 15, $k \in \mathbb{Z}^+$. So, $k \geq 1$. If $k = 1$, then $a = b$, which satisfies the inequality. If $k \neq 1$, then $k > 1$. This implies that $k + (-1) > 1 + (-1)$ by Corollary 14. This simplifies to $k - 1 > 0$. By multiplicative closure, we have: $a \cdot (k-1) \in \mathbb{Z}^+$; in other words, $a(k-1) > 0$. We can distribute the a to get: $ak - a = b - a > 0$. Thus, in this case, $b > a$. Combining both cases gives us $b \geq a$. □

The following corollary ensures the preservation of division under linear combinations.

Corollary 26. $\forall\ a, b, d \in \mathbb{Z}$, *if $d \mid a$ and $d \mid b$ then $d \mid (ar + bs)$ for every r and s in $\mathbb{Z}$.*

Proof. Because $d \mid a$ and $d \mid b$, there exists some $p, q \in \mathbb{Z}$ such that $a = pd$ and $b = dq$. Then, $(ar + bs) = (pd)r + (dq)s = pdr + dqs = d(pr + qs)$. Thus, $d \mid (ar + bs)$. □

Additionally, we prove the transitivity of division.

Corollary 27. *For integers a, b, c, if $a \mid b$ and $b \mid c$, then $a \mid c$.*

Proof. Because $b \mid c$, there exists an integer k_1 such that $c = bk_1$. Because $a \mid b$, there exists an integer k_2 such that $b = ak_2$. Using substitution, we can find $c = bk_1 = (ak_2)k_1 = a(k_2k_1)$. Because multiplication is closed in $\mathbb{Z}$, k_2k_1 is an integer. Thus, $a \mid c$. □

4.2. Powers

Equipped with the armours of division, we define the notion of even and odd integers:

Definition 14. An integer m is called *even* if $m = 2k$ for some $k \in \mathbb{Z}$. It is called *odd* if $m = 2k + 1$ for some $k \in \mathbb{Z}$.

We define the integer closely-associated to the notion of parity:

Definition 15.

$$2 := 1 + 1.$$

Next we claim the following:

Lemma 28. *All even integers are divisible by* 2*, while all odd integers are not.*

Proof. The proof to the even case follows directly from the parity definition. Now given an odd integer $t = 2k + 1$ for $k \in \mathbb{Z}$, if $t = 2m$ for some $m \in \mathbb{Z}$, then this implies that $1 = 2(m - k)$. This is absurd given that $2 \nmid 1$: both 2 and 1 are positive, and $2 > 1$. □

Additionally, we justify the notion that even and odd integers partition the set of all integers:

Lemma 29. *For all* $n \in \mathbb{Z}$*, either* $2 \nmid n$ *or* $2 \mid n$*.*

Proof. Suppose there exists a nonempty set $S \subseteq \mathbb{Z}^+$ such that neither $2 \nmid n$ or $2 \mid n$ is true. Let $s = S_{\text{min}}$, the minimum element of S whose existence is guaranteed by WOP. Note that $1 \notin S$ because $1 = 1 \cdot 0 + 1$ is odd. If s is the smallest element, then $s - 1 \notin S$. If $s - 1 = 2k$ is even, then $s = 2k + 1$ is going to be odd. Similarly, if $s - 1 = 2k + 1$ is odd, then $s = 2k + 3 = 2(k + 1) + 1$ is going to be even. Therefore, S is empty and we have reached a contradiction. Thus, all $n \in \mathbb{Z}^+$ is either even or odd. Because $2 \mid n$ if and only if $2 \mid -n$, we can see that the statement holds true for all $n \in \mathbb{Z}$. □

Note that the notion of parity commonly comes into play in the realm of powers, especially the powers of (-1). Now, we will demonstrate the motivations behind the definitions of power.

Consider how the canonical representation of integers could be justified by our definitions:

Definition 16.

$$n := \begin{cases} 0, \, n = 0 \text{ defined.} \\ (n-1)+1, \, n > 0 \end{cases}.$$

This notion of "recursively" defining integers could be generalized to the definition of multiplication:

Definition 17.

$$m \cdot n := \begin{cases} n, \text{ if } m = 1 \\ (m-1)n + n, \text{ if } m > 1 \end{cases}.$$

What would happen if we move further up by one layer? That would give us **power**(s):

Definition 18. Given $m \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$, we define the n^{th} power of m as the following:

$$m^n := \begin{cases} 1, \text{ if } n = 0 \\ m \cdot m^{n-1}, \text{ if } n > 0 \end{cases}.$$

Equipped with these definitions, we claim the following:

Corollary 30. *For every $n \geq 0$, $n \in \mathbb{Z}$ we must have*

$$(-1)^n = \begin{cases} 1 \; \textit{if } n \textit{ is even} \\ -1 \; \textit{if } n \textit{ is odd} \end{cases}.$$

Proof. We WOP on the power of (-1). Before we start on the positive integers set, notice that by definition $(-1)^0 = 1$ for the even integer 0. Let $S \subseteq \mathbb{Z}^+$ denote the nonempty set of elements s for which

$$(-1)^n \neq \begin{cases} 1 \text{ if } n \text{ is even} \\ -1 \text{ if } n \text{ is odd} \end{cases}.$$

Note that $1 \notin S$ because $(-1)^1 = -1$ and 1 is odd. Let $s + 1 = S_{\min}$ be the minimal element of S. We then have $s \notin S$. Therefore,

$$(-1)^s = \begin{cases} 1 \text{ if } s \text{ is even} \\ -1 \text{ if } s \text{ is odd} \end{cases}.$$

If s is even, then $s+1$ must be odd. By definition, $(-1)^{s+1} = (-1)^s \cdot (-1) = 1 \cdot (-1) = -1$. Similarly, if s is odd, then $s + 1$ must be even. $(-1)^{s+1} = (-1)^s \cdot (-1) = (-1) \cdot (-1) = 1$. Thus, S is empty and we are done. □

That was indeed well-played, but where are we trying to get to? Bear with us; all the puzzles will be put together very soon.

4.3. Linear Diophantine Equations

Now that we have defined division, we hope that the readers have obtained a clearer grasp of the algebra on the set of integers. We now invite them to depart from the axiomatic world of $\mathbb{Z}$, and venture into the forest of integer lattices: consider the set of points (x_0, y_0) with $x_0, y_0 \in \mathbb{Z}$. These ordered pair of integers determine a lattice on a plane. Let $a, b, c \in \mathbb{Z}$, and we specify a line $ax + by = c$, which is essentially the trace left by ordered pairs of numbers (not necessarily integral) (x, y) satisfying the given equation. When does the line pass through at least one lattice point? That is equivalent to answering the question: given integers a, b, c, when does the equation

$$ax + by = c$$

have integer solutions (x, y)? Consider the case when one of the integers a, b is zero: if $a = 0$, then the equation has solutions if and only if $b \mid c$; if $b = 0$, then the equation has solutions if and only if $a \mid c$. We focus on the degenerate form of this equation, that is, equations $ax + by = c$ with $ab \neq 0$.

The aforementioned type of integral equations is called *Diophantine Equations.* Particularly, since all terms have degree one or less, we call the equations $ax - by = c$, $a, b, c \in \mathbb{Z}$ *Linear Diophantine Equations (LDE).* We might not have enough tools to answer that question yet, but we can be certain about one thing: *the equation $ax - by = c$ does not always have integer solutions.*

To see why, consider the equation $6x - 10y = 1 \Rightarrow 2(3x - 5y) = 1$. The left hand side of the equation is even, but the right hand side is odd. This is impossible; thus there is no integral solution to $6x - 10y = 1$.

5. When You Sing You Begin With Do-re-mi: Developments

The key to unlocking the solutions to LDE lies in the definition of greatest common divisors. Using that notion we will be able to determine which LDE has integral solutions. To find the solutions to solvable LDEs, we introduce the notion of a division algorithm (dividing an integer into unique quotients and remainders) and a powerful method (the Euclidean Algorithm) to locate the GCD of any two integers. Along the way, we will have found a generalized solution to any solvable LDE.

5.1. Greatest Common Divisors (GCD)

Definition 19. Greatest Common Divisor: If a and b are integers that are not simultaneously 0, define $d = \gcd(a, b)$ as the greatest integer that divides both a and b: that is, for $k \in \mathbb{Z}$ such that $k \mid a$ and $k \mid b$, we must have $k \leq d$. If $a = b = 0$, we define $\gcd(a, b) = \gcd(0, 0) = 0$.

Next, we state a corollary concerning the existence and uniqueness of greatest common factors.

Corollary 31. *The greatest common divisor of two integers always exists and is unique.*

Proof. Consider integers a, b which are not simultaneously 0. Let $S := \{s \in \mathbb{Z} : s \mid a, s \mid b\}$. Because 1 divides all elements in $\mathbb{Z}$, we know that $1 \in S$ and S is nonempty. Our goal now is to show that S must have an upper bound. Because 1 is greater than all negative numbers, we can ignore negative common divisors. Thus, consider $m \in \mathbb{Z}^+$, where $m \mid a$ and $m \mid b$. Because a and b are not simultaneously 0, one of them is non-zero. Assume without loss of generality that a is not 0. Then, if a is positive, we have $m \mid a \Rightarrow m \leq a$. Thus, S has an upper bound. If a is negative, then $m \mid -a \Rightarrow m \leq -a$. Therefore, this case also requires S to have an upper bound. Thus, S must have a maximum element, which we determine to be our gcd. □

Corollary 32. *Given $a, b \in \mathbb{Z}$ and a, b not simultaneously zero, we must have* $\gcd(a, b) \geq 1$.

Proof. Suppose for the sake of contradiction that $d = \gcd(a, b) \leq 0$. If $d = 0$ we must have $a = 0, b = 0$ because 0 never serves as a proper divisor. If $d < 0$, we have $a = (-k)d$ and $b = (-t)d$, but this implies that $a = k(-d)$, $b = t(-d)$. Notice that $-d \in \mathbb{Z}^+$, and $(-d) - d = 2(-d) \in \mathbb{Z}^+$. Thus, $d < -d$ and we have reached a contradiction since d is the greatest common divisor. □

To get an intuitive sense of how the greatest common divisor $d = \gcd(a, b)$ between two integers a, b with $a \leq b$ is constructed, imagine receiving a rectangular sheet of paper with length b and width a. Our goal is to find the largest square tile that could perfectly tile the rectangle. Now consider the new rectangle obtained by folding in the length of a: the largest tile that tiles an a by b grid must also be the largest tile that can tile a $b - a$, a grid. Can we generalize this first step by removing k copies of a such that $b - ak < b$? One may have to believe that they will be able to find the greatest common divisor of any two integers by recursively applying these steps. We will formalize our reasoning in the next sections.

5.2. Modular Arithmetic

What does it mean to say that $a \equiv b \pmod{m}$? Can this help us create classes of integers? Let's begin with some definitions:

Definition 20. Equivalence Relation: An equivalence relation on a set S, which we will denote R, relates two elements of a set. In particular, R must satisfy the following properties:

(i) Reflexivity: $\forall\ a \in S : a\ R\ a$

(ii) Symmetry: $\forall\ a, b \in S : a\ R\ b \Rightarrow b\ R\ a$

(iii) Transitivity: $\forall\ a, b, c \in S : a\ R\ b, b\ R\ c \Rightarrow a\ R\ c$

Now, let us define a specific equivalence relation:

Definition 21. Equivalence mod m: $a \equiv b \pmod{m}$ if and only if $m \mid (a - b)$.

Although it may seem obvious that congruence modulo m is an equivalence relation, let us confirm this fact:

Corollary 33. *Equivalence modulo m is an equivalence relation.*

Proof. First, let us prove that it satisfies the reflexive property. Since $a - a = 0$ and all integers divide 0, we have $m \mid 0$. Thus, $a \equiv a \pmod{m}$. Next, let us prove that equivalence satisfies symmetry. Because $m \mid (a - b)$, m also divides $(a - b) \cdot (-1) = b - a$. Thus, $b \equiv a \pmod{m}$. Lastly, we need to check the transitive property: since $m \mid (b - a)$ and $m \mid (c - b)$, m also divides $(b - a) + (c - b) = c - a$. Thus, $a \equiv c \pmod{m}$. □

Now, by our definition of equivalence modulo m , we can see that many of the corollaries we have established related to divisors can also be applied to equivalence relationships. We will list these properties without proofs, as they are identical to the properties established about divisors.

Corollary 34. *For $a, b, c \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$, if $a \equiv b \pmod{m}$, then $ac \equiv bc \pmod{m}$. In addition, $a + c \equiv b + c \pmod{m}$.*

5.3. The Division Algorithm

As remarked in the last section, we aim to justify the notion that given any integers $a \leq b$, we may always reduce the larger integer b to an integer closer to a. We carefully analyze the concept of division in this section. Notice that we have primarily been dealing with positive integers, but generally, division could be applied to all $a, b \in \mathbb{Z}$. To do so, we define an *absolute value function*.

Definition 22. Absolute Value: Define the *absolute value* of an integer a to be the following function:

$$|a| := \begin{cases} a, \text{ if } a \in \mathbb{Z}^+ \cup \{0\} \\ -a, \text{ if } -a \in \mathbb{Z}^+ \end{cases} .$$

Next, we state a generalized claim commonly referred to as the *division algorithm*:

Corollary 35. ***Division Algorithm***: *Given any $a, b \in \mathbb{Z}$ and $b \neq 0$, there exist unique integers q, r such that $a = bq + r$ and $0 \leq r < |a|$.*

Proof. Suppose we are given some fixed integers $a, b \in \mathbb{Z}$ and $b \neq 0$. Let Q range over $\mathbb{Z}$ and let R satisfy $R = a - bQ$. We use WOP on R. Let $S := \{R : R = a - bQ\}$ for every fixed $a, b \in \mathbb{Z}$, $b \neq 0$, and for all $Q \in \mathbb{Z}$. The proof consists of two parts: showing that there exists non-negative elements in S, and showing that there exists non-negative elements in S with absolute value lesser than $|a|$.
Let $S^* \subseteq \mathbb{Z}^+$ be the largest subset of S contained in $\mathbb{Z}^+ \cup \{0\}$. We aim to show that S^* is nonempty. By WOP, we either have $b \leq a$ or $a < b$. If $b \leq a$, we can pick $Q = 1$. Then we must have $r = a - b \cdot 1 \geq 0$ by definition.

Otherwise suppose $a < b \Leftrightarrow a - b < 0$. For the sake of contradiction, suppose in this case $R < 0$ regardless of our choice of Q. Thus for all $r \in S$, we must have $-r \in \mathbb{Z}^+$. Let $S^- \subseteq \mathbb{Z}^+$ denote the set of negatives of r. Then by WOP there exists a minimum element $-r' \in S^-$ such that there does not exist a $-t \in S^-$ satisfying $-t < -r'$. Equivalently, there exists an $r' \in S$ such that $t \leq r'$ for all $t \in S$. Suppose $r' = a - bQ_0$. By our assumption, we know that $r' < 0$. But consider the integer

$\alpha = r' + |a|$: we claim that $\alpha \in S$, but $\alpha \geq 0$. To see why, note that the expression

$$s + |a| = \begin{cases} a + (1 - Q_0)b, \text{ if } b > 0 \\ a - (1 - Q_0)b, \text{ if } b < 0 \end{cases} .$$

produces a totally valid value of Q. Therefore, $\alpha \in S$ and $r' < \alpha$, falsifying our conjecture. Therefore, there exists $R \in S$ such that $R \geq 0$.
Next we show that there exists an R such that $0 \leq R < |a|$. Recall that $S^* \subseteq \mathbb{Z}^+ \cup \{0\}$ is the subset of S for which every element in S^* is nonnegative. By Lemma 20, -1 is a lower bound to S^*. Thus, S^* must have a minimum element s_1. If $s_1 = 0 < |a|$, then $0 \leq r = s_1 < |a|$ is a valid remainder. Otherwise, suppose for the sake of contradiction that $r_1 = a - Q_0 b \geq |a|$. But then there exists $r_1 > r_0 = r_1 - |a| \geq 0$, a contradiction. Therefore there exists an r with $0 \leq r < |a|$ in S.

Now, to prove that such r is unique. For the sake of contradiction, assume that there exist two such r_1, r_2 where $a = bq_1 + r_1$ and $a = bq_2 + r_2$ where $0 \leq r_1, r_2 < |b|$. Because $bq_1 + r_1 = bq_2 + r_2 \Rightarrow b(q_1 - q_2) = r_2 - r_1$, we have $r_1 \equiv r_2 \pmod{|b|}$. Without loss of generality, assume that $r_1 > r_2$. We can see that because $0 \leq r_1, r_2 < |b|$, we have $0 < r_1 - r_2 < |b|$. However, no integer multiples of b are between 0 and $|b|$ non-inclusive, leading us to a contradiction. □

Lemma 36. *For $a \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$, there exists a unique solution x such that $0 \leq x < m$ for $a \equiv x \mod m$.*

Proof. As justified by Corollary 35, we may apply the division algorithm on a, m to obtain $a = mq + r$. Since $mq = a - r$, we have $m \mid (a - r)$. Thus $a \equiv r \mod m$. Now, our proof of Corollary 35 demonstrates that r is unique. □

5.4. Euclidean Algorithm

Having established the division algorithm on integers a, b, we formalize our iterative process of folding squares by the Euclidean Algorithm on positive integers in this section. We will account for negative integers shortly after we have defined the Euclidean Algorithm on positive integers.

Definition 23. The *Euclidean Algorithm* is an iterative process that takes in $(r_{-1}, r_0) = (a, b) \in \mathbb{Z}^+ \times \mathbb{Z}^+$ and runs according to the expression

$$r_i = r_{i+1}q_{i+2} + r_{i+2}$$

for $0 < r_{i+2} < r_{i+1}$ and $0 \leq i \leq n-2$ until $r_n = 0$.

We begin by proving that the Euclidean Algorithm always terminates:

Lemma 37. *For any two positive integers a, b, the Euclidean algorithm eventually terminates.*

Proof. Consider $a, b \in \mathbb{Z}^+$. Then, apply the Euclidean algorithm. Take S, the set of remainders. S must be nonempty because there is always at least one step to the Euclidean algorithm by Corollary 35. We know that every element of S must be non-negative based on the definition of how we find r_k. By the Extended Well-Ordering Principle, S must have a minimum, say r_m.

For the sake of contradiction, assume that $r_m \neq 0$. Then, consider the equation $r_{m-1} = r_m q_{m+1} + r_{m+1}$. By Corollary 35, because $r_m \neq 0$, we can find an integer solution to this equation where $0 \leq r_{m+1} < r_m$. This is a contradiction, because r_m is the minimum element of S. Thus, the minimum element of S must be 0 and the Euclidean algorithm must terminate. □

Next, we claim that the last nonzero remainder of the Euclidean Algorithm on two positive integers must be the greatest common divisor of a, b.

Theorem 38. *For any two positive integers a, b, the last non-zero remainder of the Euclidean algorithm is* $\gcd(a, b)$.

To prove Theorem 38, consider the following lemma:

Lemma 39. *Given positive integers a, b, let $r_{-1} = a$, $r_0 = b$. Run the Euclidean Algorithm once and let $r_1 = r$. We claim that* $\gcd(a, b) = \gcd(b, r)$.

Proof. Let $a = bq + r$, and $d = \gcd(a, b)$. Since $d \mid a$, $d \mid b$, we must have $d \mid r$ by $a = bq + r$. Therefore, $d \leq \gcd(b, r)$. If $d < d' = \gcd(b, r)$, suppose $b = b_0 d'$, $r = r_0 d'$. We have $a = (b_0 q + r_0)d'$. Therefore, $d' \mid a$. But note that $d' \mid a$, $d' \mid b$ while $d' > d = \gcd(a, b)$: that is a contradiction to the maximality of greatest common divisors (between a, b). Note too, that this proof implies $\gcd(a, b) = \gcd(b, a - bq)$ for any integer q. □

Equipped with Lemma 39, we are ready to prove Theorem 38.

Proof. Essentially, we want to prove that $\gcd(a, b) = \gcd(r_i, r_{i+1})$ for every $-1 \leq i \leq n - 1$, $n \in \mathbb{Z}^+$. When $i = -1$, since we have defined $r_{-1} = a$ and $r_0 = b$, we know directly that $\gcd(r_{-1}, r_0) = \gcd(a, b)$. Lemma 39 also tells us that $\gcd(a, b) = \gcd(r_0, r_1)$. Now let $S \subseteq \mathbb{Z}^+$ be the nonempty set of positive integers such that for all $\alpha \in S$, $\gcd(a, b) \neq \gcd(r_\alpha, r_{\alpha+1})$. Now let $s = S_{\text{min}}$. We then have $(s - 1) \notin S$, and since $s - 1 \geq 0$ we must have $\gcd(a, b) = \gcd(r_{s-1}, r_s)$. But the steps

$$r_{s-1} = r_s q_{s+1} + r_{s+1},$$

$$r_s = r_{s+1} q_{s+2} + r_{s+2}$$

implies that $\gcd(r_{s-1}, r_s) = \gcd(r_s, r_{s+1}) = \gcd(a, b)$. Therefore, $s \notin S$ and we have reached a contradiction. □

We have now established a sophisticated algorithm to calculate the greatest common divisors between to positive integers a, b. How can we transform the general problem of calculating the greatest common divisor between two arbitrary integers to the task of performing a Euclidean Algorithm? We claim the following:

Corollary 40. *For every $a, b \in \mathbb{Z}$, $\gcd(a, b) = \gcd(|a|, |a|)$.*

Proof. It suffices to show that given any $t \in \mathbb{Z}^+ \cup \{0\}$, if we define $D(n) := \{d : d \in \mathbb{Z} \land d \mid n\}$, we must have $D(t) = D(-t)$. For the sake of contradiction there exists some $d \in D(t)$ but $d \notin D(-t)$. We then have $t = kd$ for some $k \in \mathbb{Z}$. Note that $-t = (-k)d$, so $d \in D(-t)$, a contradiction. Thus $D(t) \subseteq D(-t)$. We could show by a similar argument that $D(-t) \subseteq D(t)$. Thus, $D(t) = D(-t)$. □

We have therefore been able to find the greatest common divisor between any two integers. Next, we introduce an important identity related to the results in a Euclidean Algorithm.

Definition 24. Magic Table: Recall that the Euclidean Algorithm takes in positive integers $r_0 = a$,$r_1 = b$, and produces a sequence of quotients (q_i) and remainders (r_i) according to the expression $r_i = r_{i+1}q_{i+1} + r_{i+2}$. We define two other sequences (x_i) and (y_i) according to the following rule:

$$x_{-1} = 0,\ x_0 = 1,\ x_{i+1} = q_{i+1}x_i + x_{i-1},$$

$$y_{-1} = 1,\ y_0 = 0,\ y_{i+1} = q_{i+1}y_i + y_{i-1}.$$

We claim that the two sequences (x_i) and (y_i) define the remainders sequence.

Lemma 41. *The Euclidean Algorithm on positive integers a, b with quotients q_k and remainders r_k as described in 38 and 24 satisfy*

$$r_k = (-1)^k \begin{vmatrix} x_k & a \\ y_k & b \end{vmatrix}, \textit{ for every index } k \leq n+1.$$

Note that each remainder r_k is a linear combination of a and b.

Proof. When $k = 1$, LHS $= r_1$ and

$$\text{RHS} = -\begin{vmatrix} x_1 & a \\ y_1 & b \end{vmatrix} = -\begin{vmatrix} q_1 & a \\ 1 & b \end{vmatrix} = a - q_1 b = r_1 = \text{LHS}.$$

When $k = 2$, $r_2 = b - r_1q_2 = b - a + bq_1q_2$, $x_2 = 1 + q_1q_2$ and $y_2 = q_2$. We plug in the values and verify that $1 \cdot (x_2b - y_2a) = r_2$.
Suppose the claim does not hold for a nonempty set of positive integers S, that is, for all $k \in S$,

$$r_k \neq (-1)^k \begin{vmatrix} x_k & a \\ y_k & b \end{vmatrix}.$$

Let $k = S_{min}$. We then have the theorem holds for $k-1$:

$$r_{k-1} = (-1)^{k-1} \begin{vmatrix} x_{k-1} & a \\ y_{k-1} & b \end{vmatrix}.$$

Therefore, by definition ($r_{k-2} = r_{k-1}q_k + r_k$, $x_k = x_{k-2} + x_{k-1}q_k$),

$$r_k = r_{k-2} - q_k r_{k-1} = r_{k-2} - (-1)^{k-1} q_k \begin{vmatrix} x_{k-1} & a \\ y_{k-1} & b \end{vmatrix} = (-1)^{k-2} \begin{vmatrix} x_{k-2} & a \\ y_{k-2} & b \end{vmatrix} + (-1)^k q_k \begin{vmatrix} x_{k-1} & a \\ y_{k-1} & b \end{vmatrix},$$

$$\Rightarrow r_k = (-1)^{k-2}(bx_{k-2} - ay_{k-2} + q_k bx_{k-1} - q_k ay_{k-1}),$$

$$\Rightarrow r_k = (-1)^{k-2}(b(x_{k-2} + q_k x_{k-1}) - a(y_{k-2} + q_k y_{k-1})) = (-1)^{k-2} \begin{vmatrix} x_k & a \\ y_k & b \end{vmatrix}.$$

Since $(-1)^{k-2} = (-1)^k$, we then have

$$r_k = (-1)^k \begin{vmatrix} x_k & a \\ y_k & b \end{vmatrix}.$$

□

5.5. Bezout's Lemma

In this section, we introduce Bezout's Lemma, an important result for determining the solvability of LDEs.

Lemma 42. ***Bezout's Lemma**: Given integers a, b, n, where a and b are not simultaneously zero, there exists $x, y \in \mathbb{Z}$ such that $ax + by = n$ if and only if $d = \gcd(a, b) \mid n$.*

Proof. If one of a, b is zero, by the commutative nature of addition we could suppose without loss of generality that $a = 0 \wedge b \neq 0$; we have $0 \cdot x + b \cdot y = n \Rightarrow b \cdot y = n$. Note that $\gcd(a, b) = \gcd(0, b) = b$. Thus, if $d = b \mid n$, there must exist an y such that $by = n$. Reversely, if $by = n$, by definition we have $b = d \mid n$.

Next, suppose both a and b are nonzero integers. Then we must have $|a|, |a| \in \mathbb{Z}^+$. To show the forward direction of the theorem, we perform the Euclidean Algorithm on the integers $|a|$ and $|a|$. Let r_n be the last nonzero remainder of the Euclidean Algorithm on $|a|, |a|$. By Theorem 38, we know that $r_n = \gcd(|a|, |a|)$. Now consider the result we proved in Lemma 41:

$$r_n = (-1)^n \begin{vmatrix} x_n & |a| \\ y_n & |a| \end{vmatrix}.$$

If we equate both equations, we have $\gcd(|a|, |a|) = (-1)^n |a| x_n + (-1)^{n+1} |a| y_n$. By Corollary 40, we know that $\gcd(a, b) = \gcd(|a|, |a|) = (-1)^n x_n |a| + (-1)^{n+1} y_n |a|$. If $a > 0, b > 0$, we have $\gcd(a, b) = ((-1)^n x_n) b + ((-1)^{n+1} y_n) a$. If $a > 0, b < 0$ we have $\gcd(a, b) = ((-1)^{n+1} x_n) b + ((-1)^{n+1} y_n) a$. If $a < 0, b > 0$ we have $\gcd(a, b) = ((-1)^n x_n) b + ((-1)^n y_n) a$. If $a > 0, b < 0$ we have $\gcd(a, b) = ((-1)^{n+1} x_n) b + ((-1)^n y_n) a$. Thus, if $\gcd(a, b) \mid n$ and $n = \gcd(a, b) \cdot k$, we could scale the coefficients in front of a and b and obtain a solution.

To show that there exists $x, y \in \mathbb{Z}$ such that $ax + by = n$ only if $\gcd(a, b) \mid n$, note that $d = \gcd(a, b) \mid (ax + by)$. Therefore, we must have $d \mid n$.

Thus, we conclude that $ax + by = n$ if and only if $\gcd(a, b) \mid n$. □

Note that as we complete our proof to Bezout's Lemma, we have not only been able to determine whether an LDE is solvable, but have also developed a procedure to solve all solvable LDEs, which, although not strongly relevant to the Chinese Remainder Theorem, serves a vital role in completing our delineation of integer arithmetic.

5.6. Solving Linear Diophantine Equations

We aim to generate all solutions to Linear Diophantine Equations. Before that, we prove the *Fundamental Lemma*, a lemma justifying our deduction that $m \mid ab$ implies $m \mid a$ in specified situations.

Lemma 43. ***The Fundamental Lemma***: *For all $a, b, c \in \mathbb{Z}$, if $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.*

Proof. Since $\gcd(a, b) = 1$, there exists $x, y \in \mathbb{Z}$ such that $ax + by = 1$. We could multiply both sides of the equation by c and obtain $(ac)x + (bc)y = c$. Since $a \mid bc$, let $bc = at$ Since LHS $= a(cx + ty)$, we must have $a \mid$ LHS $=$ RHS $= c$. □

The following lemma allows us to build all solutions from a pair of special solution (x_0, y_0):

Lemma 44. *The Linear Diophantine Equation $ax+by = c$ for $a, b, c \in \mathbb{Z}$ has general solutions $x = x_0 + b_0t$, $y = y_0 - a_0t$ for $t \in \mathbb{Z}$ when (x_0, y_0) is a particular solution to the equation, and $(a, b) = (a_0 \cdot \gcd(a, b), b_0 \cdot \gcd(a, b))$.*

Proof. Suppose $x = x_0 + m$, $y = y_0 - n$ is a pair of solution to the given equation for $m, n \in \mathbb{Z}$. Note that x, y represents all integer pairs by the arbitrary nature of m, n. We substitute $(x, y) = (x_0 + m, y_0 - n)$ into the equation and obtain the following: $a(x_0 + m) + b(y_0 - n) = c \Rightarrow am = bn \Rightarrow a_0m = b_0n$. Let $d = \gcd(a, b)$. Note that $\gcd(a_0, b_0) = 1$, since if $d_0 = \gcd(a_0, b_0) > 1$, the greatest common divisor of a, b will then have to be d_0d, a contradiction. Thus, $b_0 \mid m$. Let $m = b_0u$. Similarly, let $n = a_0v$. We then have $a_0b_0u = b_0a_0v \Rightarrow u = v$. Therefore, we conclude that $(m, n) = t(b_0, a_0)$. □

How are we to find a special solution to a given Linear Diophantine Equation?

Given an LDE $ax + by = c$, consider its *base equation* $ax + by = d$, where $d = \gcd(a, b)$. We know that there exists integer solutions to the equation $ax+by = c$ if and only if $d \mid c$. For the sake of convenience, let $a, b \in \mathbb{Z}^+$. Note that this manipulation does not affect the generalizability of our method, since we have the identity $ax = (-a)(-x)$: that is, if we negate a negative element a to make it positive, we could always solve for the negative of the solution x (that is $(-x)$), and let $x = -(-x)$.

We perform the Euclidean Algorithm on positive integers a, b. By Lemma 41, we directly obtain a solution to the LDE $ax + by = d$:

$$d = r_{n-1} = (-1)^{n-1}x_{n-1}b + (-1)^n y_{n-1}a.$$

Since $(x_i), (y_i)$ are defined iteratively, we know from the properties of Euclidean Algorithms that we could always reach the solution $(x_0, y_0) = ((-1)^n y_{n-1}, (-1)^{n-1}x_{n-1})$. If we let $c = kd$, we then have a special solution to $ax + by = c$: $(X_0, Y_0) = (kx_0, ky_0) = k(x_0, y_0)$. By Lemma 44, we conclude that the general solution to $ax+by = c$ has to be of the form $(X, Y) = (X_0+b_0t, Y_0-a_0t)$, where $(a, b) = (a_0d, b_0d)$.

6. Do-re-mi-fa-so-la-ti: A Proof to the CRT

Armed with all necessary lemmas and definitions, we are ready to welcome the ultimate guest of the day: the Chinese Remainder Theorem. We first state the theorem for two integers, and prove the generalized result using the former theorem as a base case.

Theorem 45. ***Chinese Remainder Theorem on Two Integers**: If $a, b \in \mathbb{Z}$ and $m, n \in \mathbb{Z}^+$ with $\gcd(m, n) = 1$, then there exists a unique integer solution x such that $0 \leq x < mn$ to the system*

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}.$$

Proof. Given that

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases},$$

consider $x = a + k_1m$, $x = b + k_2n$ for $k_1, k_2 \in \mathbb{Z}$: we equate both sides and obtain the Linear Diophantine Equation with unknowns (k_2, k_1): $k_2n - k_1m = a - b$. Since $\gcd(m, n) = 1$ and $a - b \in \mathbb{Z}$, we know that the linear Diophantine equation has at least one solution by Lemma 42 (Bezout's Lemma). If there is a special solution (x_0, y_0) to the equation then the general solution could be written out as $(k_2, k_1) = (x_0 - mt, y_0 - nt)$ for some $m, n \in \mathbb{Z}$ by Lemma 44. Thus $x = (a + y_0 m) - (mn)t$. Let $\alpha = a + y_0 m$ and $mn = \kappa$. By the division algorithm on α and κ we know that there exists some t such that $\alpha = \kappa t + x$ for $0 \leq x < \kappa$. Thus, we have found a solution x with $0 \leq x < mn$. By Corollary 35, we conclude that such x is unique. □

What if we are modding out by more than two integers? We claim that the theorem still holds in a nice way in Theorem 49. Before proceeding to prove it, we first fiddle with a few preliminary lemmas.

Lemma 46. *If $a, b \in \mathbb{Z}$ and $m, n \in \mathbb{Z}^+$ with $\gcd(m, n) = 1$, then for any two solutions x, y to the system*

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases} .$$

we have: $x \equiv y \mod mn$.

Proof. By Theorem 45, we see that x is unique for $0 \leq x < mn$. We claim that all solutions to the system are of the form $X = x + k(mn)$ for $k \in \mathbb{Z}$. To prove this, first note that X is a solution to the system because $X \equiv a \pmod{m}$, $X \equiv b \pmod{n}$. Next, suppose for the sake of contradiction that $X = x + k(mn) + t$ for $0 < t < mn$ is a solution to the system. We then have $X \equiv a + t \equiv a \pmod{m}$, $X \equiv b + t \equiv b \pmod{n}$. Thus, $t \equiv 0 \pmod{m} \wedge t \equiv 0 \pmod{n}$. Thus, $mn \mid t$ and we have reached a contradiction. Thus, all solutions to the system are of the form $X = x + k(mn)$, $k \in \mathbb{Z}$, and for any two solutions x, y, we must have $x \equiv y \pmod{mn}$. □

Recall that we have deduced the Fundamental Lemma before solving LDEs. Note that we could generalize our argument made in the Fundamental Lemma as given below.

Lemma 47. *Given integers $m_1, m_2, \ldots, m_k$ and an integer n satisfying $\gcd(n, m_i) = 1$ for all $1 \leq i \leq k$, $k \in \mathbb{Z}$, we must have $d = \gcd\left(\prod_{i=1}^{k} m_i, n\right) = 1$.*

Proof. We use WOP on the number of terms in the product $P(k) := \prod_{i=1}^{k} m_i$. Define $S \subseteq \mathbb{Z}^+$ as the set of all k for which $\gcd(n, m_i) = 1$ does not imply $d = 1$. Note that $k = 1 \notin S$ because the conditions explicitly state that $\gcd(n, m_1) = 1$. Suppose $t + 1 = S_{\text{min}}$. We then have $t \in \mathbb{Z}^+$ but $t \notin S$. That is, if $\gcd(n, m_i) = 1$ is true for all $1 \leq i \leq t$, then we have $\gcd(n, P(t)) = 1$. Now consider $P(t+1) = P(t) \cdot m_{t+1}$. Suppose for the sake of contradiction that $\gcd(n, P(t+1)) = d > 1$. We then have $d \mid n$ and $d \mid P(t+1)$. That is, $d \mid m_{t+1}P(t)$. Since $\gcd(n, P(k)) = 1$, we must have $d \mid m_{t+1}$. Recall that d also divides n: thus, $\gcd(n, m_{t+1}) > 1$, which is a contradiction. □

Lemma 48. *Consider $a, b \in \mathbb{Z}$ and $m, n \in \mathbb{Z}^+$. If $a \equiv b \pmod{mn}$, then $a \equiv b \mod m$ and $a \equiv b \mod n$.*

Proof. Since $a \equiv b \pmod{mn}$, we have $a - b = k(mn)$ for $k \in \mathbb{Z}$. If we take mod$m$ on both sides of the equation, we get $a - b \equiv 0 \pmod{m} \Rightarrow a \equiv b \pmod{m}$. Similarly, we could obtain $a - b \equiv 0 \pmod{n} \Rightarrow a \equiv b \pmod{n}$. □

Definition 25. Relatively Prime: Two integers are said to be *relatively prime* if their GCD is 1. A set of integers is said to be pairwise relatively prime if the GCD of any two elements is always 1.

Next, we state and prove the generalized CRT.

Theorem 49. ***Generalized Chinese Remainder Theorem**: If $a_1, a_2, \ldots a_k \in \mathbb{Z}$ and $m_1, m_2, \ldots m_k$ are pairwise relatively prime positive integers, there exists a unique solution $0 \leq x < \prod_{i=1}^{k} m_i$ such that $x \equiv a_i \pmod{m_i}$ for $1 \leq i \leq k$.*

Proof. Let S be the set of indices s $(1 \leq s \leq k)$ where the solution to the system $x \equiv a_i \pmod{m_i}$, $0 \leq x < \prod_{i=1}^{s} m_i$ is not unique. First note that $1 \notin S$ because there only exists one such x where $0 \leq x < m_1$ and $x \equiv a_1 \mod m_1$. Now, for the sake of contradiction, assume that S is nonempty. Then, S must have a minimum, say p. We know that $p \neq 1$, so we also have: $1 \leq p-1 \leq k$. Since $p-1$ cannot be in S, there must exist a unique solution $0 \leq x < \prod_{i=1}^{p-1} m_i, x \equiv a_i \pmod{m_i}$ for $1 \leq i \leq p-1$.

Now, by Lemma 47, we have $\gcd\left(\prod_{i=1}^{p-1} m_i, m_p\right) = 1$, which allows us to apply the Chinese Remainder Theorem for Two Integers. Thus, there exists a unique solution to

$$0 \leq y < \left(\prod_{i=1}^{p-1} m_i\right) m_p = \prod_{i=1}^{p} m_i,$$

$$\begin{cases} y \equiv x \pmod{\prod_{i=1}^{p-1} m_i} \\ y \equiv a_p \pmod{m_p} \end{cases}. \tag{1}$$

Since $\gcd\left(\prod_{i=1}^{p-1} m_i, m_p\right) = 1$, we know that there is a unique solution to Equation 1 for $0 \leq y < \prod_{i=1}^{p} m_i$. By Lemma 48, we see that $y \equiv x \equiv a_i \pmod{m_i}$ for $1 \leq i \leq p-1$. Thus, y satisfies

$$0 \leq y < \prod_{i=1}^{p} m_i,$$

$$y \equiv a_i \pmod{m_i} \text{ for } 1 \leq i \leq p.$$

In addition, y is unique modulo $\prod_{i=1}^{p} m_i$ by Lemma 6. Therefore, our set S is empty by the division algorithm and the uniqueness of the remainder, since there is a unique solution y such that $0 \leq y < \prod_{i=1}^{p} m_i$.

□

7. Back to Do: Conclusion

Having traveled a long way from the definition of integers to a proof of the Chinese Remainder Theorem, we cordially invite our readers to marvel at the power of an axiomatic definition of the integers $\mathbb{Z}$. Utilizing the definition of integers as an ordered ring satisfying the Well-Ordering Principle, we have been able to reveal profound characteristics of the so-called "whole numbers", a concept that may seem familiar, but is now imbued with deeper mathematical significance.

From the axiomatic definition of integers, we gained insight to define ordering and subtraction. Inspired by the natural concept of subtraction, we defined division to stand as a quasi-inverse of multiplication. Next, as we worked our way through the recursive definition of integers and multiplication, we extended our recursive definition to powers. A we probed into the world of integral lattices, the natural question of LDEs arose. To investigate this problem, we introduced essential tools as the division algorithm, the Euclidean Algorithm, and Bezout's Lemma. Along the way, we developed modular arithmetic, a prompt to the statement of the CRT. Finally, we proved the CRT using the corollaries we have developed. In the Appendix, we will investigate an alternative path to the proof of CRT without the use of the Euclidean Algorithm.

As a closing remark, we invite our readers to reflect on the profound insights that can be unlocked by rigorously examining even the most elementary mathematical concepts. The journey from integers to the Chinese Remainder Theorem stands as a testament to the ROSS motto, "think deeply about simple things."

8. Appendix

8.1. An Alternative Path: Units

In this section, we will side-step the Euclidean Algorithm with the help of units, but we will still use other basic properties that we have established, such as the division algorithm and the Fundamental Lemma. Note that our proof to the Fundamental Lemma in the previous sections requires Bezout's Lemma, which was proven using the Euclidean Algorithm. Thus, we will provide an alternative proof to Bezout's Lemma (Lemma 42); before we prove Bezout's, we will first need some important properties about GCD:

Definition 26. Least Common Multiple: The lcm of two non-zero integers is the least positive integer that is a multiple of both. $\forall\, a \in \mathbb{Z}, \operatorname{lcm}(a, 0) = \operatorname{lcm}(0, a) = 0$.

Corollary 50. *The Least Common Multiple always exists and is unique*

Proof. Let S be the set of all positive integer multiplies of non-zero integers a and b. We know that S is nonempty because $|a| \cdot |b|$ is a positive integer that is divisible by both a and b. Thus, S must have a minimum by WOP. This is our lcm. □

In our proof of Bezout's Lemma, we will use the fact that all common divisors of a and b divide $\gcd(a, b)$. This fact is commonly proven using Bezout's, which would result in circular reasoning. Thus, we will provide an alternate proof:

Corollary 51. *$\forall\, a, b, c \in \mathbb{Z}$, if $a \mid c$ and $b \mid c$, then $\operatorname{lcm}(a, b) \mid c$.*

Proof. If either $a = 0$ or $b = 0$, we are done: c must be 0 too. Thus, we will consider non-zero integers. Let S be the set of positive common multiples of non-zero integers a and b that are not divisible by $d = \operatorname{lcm}(a, b)$. If there exist no positive common multiples of a and b that are divisible by d, then there also don't exist negative common multiples of a and b that are divisible by d. Thus, it is sufficient to prove that S is empty.

For the sake of contradiction, assume that S is nonempty. Then, by the Well Ordering Principle, S must have a minimum say m. By the definition of lcm, we know that $m \geq d$. Furthermore, $m \neq d$ because then $d \mid m$. Thus, $m > d$. Because $a \mid m$ and $a \mid d$, then $a \mid (m - d)$. In addition, because $d \nmid m$, $d \nmid (m - d)$. However, $m - d > 0$. Thus, $m - d$ is in S, which is a contradiction because m is the minimum element of S. Thus, our original assumption must be wrong and S must be empty. So, $\operatorname{lcm}(a, b)$ divides all common multiples of a and b. □

Corollary 52. *$\forall\, a, b, e \in \mathbb{Z}$, let $d = \gcd(a, b)$. If $e \mid a$ and $e \mid b$, then $e \mid d$.*

Proof. If either $a = b = 0$, then $\gcd(a, b) = 0$. Thus, all divisors of a and b must divide $\gcd(a, b)$ too. So, let us consider a, b which are not simultaneously 0.

Let S be the set of all positive integers e such that $e \mid a$ and $e \mid b$ but $e \nmid d$. If there doesn't exist any positive common divisor of a and b that doesn't divide d, then all negative common divisors must divide d too. Thus, it is sufficient to prove that S is empty. For the sake of contradiction, assume that S is nonempty.

By WOP Extended, because S has an upper bound of d, we have a maximum element, say m. Consider $\operatorname{lcm}(m, d)$. By Corollary 51, we have: $\operatorname{lcm}(m, d) \mid a$ and $\operatorname{lcm}(m, d) \mid b$. Note that because $m \mid \operatorname{lcm}(m, d)$ and $m \nmid d$, $\operatorname{lcm}(m, d) \nmid d$. However, $\operatorname{lcm}(m, d) \geq d$ (because d and m are positive). We know that $\operatorname{lcm}(m, d) \neq d$, because that would imply that $m \mid d$. Thus, $\operatorname{lcm}(m, d) > d$. However, this is a contradiction, because d is the greatest common divisor of a and b. □

We will need one last tool for Bezout's Lemma:

Corollary 53. *For positive integers a, b, if $a \mid b$ and $b \mid a$, then $a = b$.*

Proof. Because $a \mid b$, $a \leq b$. But because $b \mid a$, $b \leq a$. This implies that $a = b$. □

Lemma 54. *Bezout's Lemma: revisted. For $a, b \in \mathbb{Z}$, there exists integral solutions to $ax + by = \gcd(a, b)$.*

Proof. If $a = b = 0$, we are done, because $0x + 0y = \gcd(0, 0) = 0$ certainly has integral solutions. Thus, let a and b not be simultaneously 0. Let $S := \{ax + by : x, y \in \mathbb{Z}, ax + by > 0\} \subseteq \mathbb{Z}^+$. Because a and b are not both 0, S is nonempty. By WOP, we know that there exists a $d = S_{\text{min}} = as + bt$ for some $s, t \in \mathbb{Z}$. We want to prove that $d = \gcd(a, b)$. By the division algorithm, we know that $a = dq + r$ for some $0 \leq r < d$. Next note that $r = a - dq = a - q(as + bt) = (1 - qs)a - (qt)b$; thus $r \in S \cup \{0\}$. Since $r < d$ and d is the minimum element in S, we must have $r \notin S$ so $r = 0$. That is, $d \mid a$. By a similar argument, we could see that $d \mid b$. Therefore, $d \mid \gcd(a, b)$. It remains for us to show that for any $c \in \mathbb{Z}^+$, $c \mid a$, $c \mid b$, we must have $c \mid d$. Suppose $a = cm$, $b = cn$ for $m, n \in \mathbb{Z}$. We then have $d = c(ms + nt)$. Therefore, $c \mid d$, implying that $\gcd(a, b) \mid d$. Because $\gcd(a, b) \mid d$ and $d \mid \gcd(a, b)$, both of which are positive, $d = \gcd(a, b)$. □

Next, we proceed by defining modular spaces.

Definition 27. Equivalence class: If we have a definition for "equivalence" in a set, such as equivalence modulo m, we can split a set up into "equivalence classes," subsets of the original set such that any two elements within a subset are equivalent.

Definition 28. $\mathbb{Z}_m$: We define $\mathbb{Z}_m$, where $m \geq 1$, to be the Ring with elements $\{0, 1, \ldots m{-}1\}$. Note, however, that the elements of $\mathbb{Z}_m$ are not numbers; rather, they are equivalence classes, defined by equivalence modulo m. By the Division Algorithm, we know that every integer is uniquely represented by one of these equivalence classes. Because of the way that $\mathbb{Z}_m$ is constructed, working in $\mathbb{Z}_m$ is equivalent to working in $\pmod{m}$. Thus, we will use these interchangeably.

Now that we have defined $\mathbb{Z}_m$, let us consider some properties about that space. Firstly, we can see that $\mathbb{Z}_m$ may or may not have zero-divisors. For example, we can quickly check that $\mathbb{Z}_2$ has no zero-divisors. However, $\mathbb{Z}_4$ has the property that $2 \cdot 2 \equiv 0$, even though $2 \not\equiv 0$ in $\mathbb{Z}_4$.

What's also strange, in comparison to $\mathbb{Z}$, are multiplicative inverses in $\mathbb{Z}_m$. For example, $2 \cdot 3 \equiv 1$ in $\mathbb{Z}_5$. But not all numbers have multiplicative inverses modulo m. For example, 2 has no multiplicative inverse in $\mathbb{Z}_4$, because $2k \not\equiv 1 \pmod{4}$ for any integer k. Let us try to characterize the elements that have multiplicative inverses:

Definition 29. Units: A element $u \in \mathbb{Z}_m$ is a unit if there exists $x \in \mathbb{Z}_m$ such that $ux \equiv 1$ in $\mathbb{Z}_m$. We use $\mathbb{U}_m$ to denote the set of units in $\mathbb{Z}_m$.

Next, we will prove an important property about units:

Lemma 55. *If $a \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$ then: a represents a unit (mod m) $\iff$ $\gcd(a, m) = 1$.*

Proof. $\Longrightarrow$: If a is a unit in $\mathbf{Z}_m$, there must exist $x \in \mathbf{Z}_m$ such that $ax \equiv 1 \mod m$. Thus, $m \mid ax - 1$. This means that $ax - 1 = my$ for some integer y. We can rearrange terms to find $ax - my = 1$. Thus, there needs to exist an integer solution to this equation. Because $\gcd(a, m) \mid a$ and $\gcd(a, m) \mid m$, then $\gcd(a, m) \mid (ax - my) = 1$. The only divisors of 1 are 1 and -1, so $\gcd(a, m)$ must be 1.

$\Longleftarrow$ If $\gcd(a, m) = 1$, then by Bezout's, there exists an integral solution to $ax + my = \gcd(a, b) = 1$. If we take $\mod m$ of both sides, we see that $ax \equiv 1 \mod m$ for some integer x. Thus, a represents a unit. □

Because we have established Bezout's Lemma, we also have the Fundamental Lemma. The proof is identical to that which we have already presented, so we will omit it in this section.

Lemma 56. *If a is a unit $\pmod m$, then there exists a unique solution x modulo m to $ax \equiv 1 \mod m$.*

Proof. Consider two solutions, x_1, x_2, to $ax \equiv 1 \pmod m$. We can see that $ax_1 \equiv ax_2 \pmod m$. Thus, $m \mid (ax_1 - ax_2)$. But a is a unit, so $\gcd(a, m) = 1$. By the Fundamental Lemma, we have $m \mid (x_1 - x_2)$ so $x_1 \equiv x_2 \pmod m$. □

Theorem 57. ***Chinese Remainder Theorem on Two Integers**: If $a, b \in \mathbb{Z}$ and $m, n \in \mathbb{Z}^+$ with $\gcd(m, n) = 1$, then there exists a unique integer solution x such that $0 \leq x < mn$ to the system*

$$\begin{cases} x \equiv a \pmod m \\ x \equiv b \pmod n \end{cases}.$$

Proof. If $x \equiv a \pmod m$, then $x = a + mk$ for some integer k. Now, we plug into the second equation: $a + mk \equiv b \pmod n$. This must mean that $mk \equiv b - a \pmod n$. Consider $m^{-1} \pmod n$. We know this must exist because $\gcd(m, n) = 1$ and must be unique $\pmod n$. Thus, let $m^{-1} = c \pmod n$ where $0 \leq c < n$; we know that c is unique. Now, we can do some equation manipulation:

$$mk \equiv (b - a) \pmod n,$$

$$cmk \equiv c(b - a) \pmod n,$$

$$k \equiv c(b - a) \pmod n,$$

$$k = c(b - a) + nk' \text{ for some integer } k'.$$

Plugging into the original equation, we get

$$x = a + mk = a + m(c(b - a) + nk')$$

$$x = a + mk = a + mc(b - a) + mnk'$$

Because $a + mc(b - a)$ are fixed already, and k' is the only non-fixed variable, we know that any two solutions x_1, x_2 will be equivalent mod mn. Thus, we can apply the division algorithm and find a unique $0 \leq x < mn$. □

The proof for the Generalized Chinese Remainder Theorem is very similar to that presented in the original section, so we will omit it.

In this proof, we used the axiomatic descriptions of the integers, division, GCD, modular arithmetic, and the division algorithm from our main text. However, instead of travelling through the Euclidean Algorithm, we continued with modular arithmetic to prove the Chinese Remainder Theorem. Firstly, we introduced the concept of lcm to prove that common divisors divide the gcd of a pair of integers. Then, using that fact, we proved Bezout's Lemma. From there, we proved that units in $\mathbb{Z}_m$ must be relatively prime to m and that inverses are unique modulo m. With all those tools, we were able to prove the Chinese Remainder Theorem.

8.2. Authors' Last Note

We will leave the readers with these "wise" words.

In the beginning, all was complex. The world consisted of the complex plane with the real axis removed, and thus nothing could be perceived.

But one day, Ross, having awakened from his complex sleep, said to the world: "Thou shalt be real."

And then the world was real.

On the second day, using reverse Dedekind cuts, Ross created the rational numbers. And on the third day, he invented the right-hand rule, thus creating the positive numbers. On the fourth day, He realized that all rational numbers were ratios of integers, and thus created the integers.

On the fifth day, Ross combined the work of his previous days, creating the positive integers. And on the sixth day, he presented the Well-Ordering Principle and the Axiom of Choice.

Satisfied with his work, Ross rested on the seventh day and proclaimed it a day of the Pursuit of Trivial Results. Thereafter, every seventh day, two hours shall be set aside to proving $0 \neq 1$*.*

The above text has been repurposed from a joke made in Max's school Math Team. Although not meant to be taken seriously, it reflects an important

Interestingly, our section naming system pays tribute to *The Sound of Music*, a musical drama film centered around the undoubted power of rhythms and artistry. This beloved classic has been a constant presence in Lola's life, ever since she sang the iconic lyrics ”do, a deer, a female deer” at her kindergarten graduation.

Just as how the stirring melodies and captivating story of the von Trapp family have left an indelible mark, we regard this paper with the same sense of reverence and artistry.

9. References

1. Shen, Kangshen. ”Mathematical Problems on Surveying in Ancient China.” *Historia Mathematica*, vol. 16, no. 3, 1989, pp. 203–218. JSTOR, www.jstor.org/stable/41133792.

2. Plofker, Kim. *Mathematics in India.* Princeton University Press/Oxford University Press, 2009.

3. Pei, Dingyi, Arto Salomaa, and Cunsheng Ding. *Chinese Remainder Theorem: Applications In Computing, Coding, Cryptography.* World Scientific, 2016.