Chinese Remainder Theorem

Jiya Dani, Henry Yao, Stephanie Yao

Contents

1. Introduction

The **Chinese Remainder Theorem (CRT)** is an ancient mathematical result credited to the Chinese mathematician *Sunzi* from the 3rd century AD. It is described in his work "*Sunzi Suanjing*." The theorem solves systems of linear congruences and has been widely studied and generalized by mathematicians worldwide. Its applications span various mathematical fields, contributing to the advancement of number theory and algebraic techniques. The name "**Chinese Remainder Theorem**" reflects its popularization in Chinese mathematical literature, although its development was influenced by mathematical advancements from different cultures.

The Chinese Remainder Theorem states that we can uniquely solve every pair of congruences under the condition that the divisors are pairwise coprime, which means no two divisors share a common factor greater than 1.

Theorem 1.1. ***2-variable Chinese Remainder Theorem.*** *Let $m, n \in \mathbb{Z}^+$ with $\gcd(m, n) = 1$. Given $a \in \mathbb{Z}_m$ and $b \in \mathbb{Z}_n$, there is an $x \in \mathbb{Z}$ such that x satisfies*

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

and x is unique mod mn.

Notice that here m, n must be relatively prime, while there are no restrictions on both a and b.

Theorem 1.1 states the Chinese Remainder Theorem when there are 2 congruences. We can also extend it to the general case.

Theorem 1.2. ***Chinese Remainder Theorem.*** *Let $n_1, n_2, \ldots, n_k \in \mathbb{Z}^+$, for each n_i with $i \in \{1, 2, \ldots, k\}$, if they are pairwise relatively prime, and if $a_1, a_2, \ldots, a_k \in \mathbb{Z}_{n_i}$, then the system of congruences*

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

has a solution, and any two solutions, say x_1 and x_2, are congruent modulo $n_1 n_2 \ldots n_k$, that is, $x_1 \equiv x_2 \pmod{n_1 n_2 \ldots n_k}$.

Chinese Remainder Theorem can help us solve numerical solutions of systems of congruences and also a pleasing number of number theory proofs. For example, the congruences $x \equiv 6 \mod 9$ and $x \equiv 4 \mod 11$ hold when $x = 15$, and more generally when $x \equiv 15 \mod 99$, and they do not hold for any other x.

We will prove the Chinese Remainder Theorem from the very beginning of integers, which are the axioms that integers satisfy, including the general case, and see some ways it is applied to study congruences.

2. Axioms

Axioms are those facts that you are not supposed to prove, they exist to prove other theorems. They are helpful to start with as the intuitive understanding of integers as whole numbers, including positive numbers, negative numbers, and zero. These axioms capture the essential properties of integers that we observe and use in everyday arithmetic.

2.1. The Ring Axioms

In $\mathbb{Z}$, addition and multiplication are binary operations. This means that for a,b $\in \mathbb{Z}$, the numbers $a + b$ and $a \cdot b$ are defined in $\mathbb{Z}$, which basically says that integers are closed under addition and multiplication. Additionally, $a \cdot b$ is sometimes written as just ab. Ring axioms contains following axioms:

Commutativity of addition: $a + b = b + a$

Associativity of addition: $a + (b + c) = (a + b) + c$

Distributivity: $a \cdot (b + c) = a \cdot b + a \cdot c$

Multiplicative Identity: There exists $1 \in \mathbb{Z}$ such that $a \cdot 1 = 1 \cdot a = a$ for all $a \in \mathbb{Z}$.

Commutativity of multiplication: $a \cdot b = b \cdot a$

Associativity of multiplication: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

Additive Identity: There exists $0 \in \mathbb{Z}$ such that $a + 0 = 0 + a = a$ for all elements $a \in \mathbb{Z}$.

Existence of **Additive Inverses**: For all $a \in \mathbb{Z}$ there is some $x \in \mathbb{Z}$ with $a + x = 0$.

Commutativity $\mathbb{Z}$ satisfies commutativity. Addition is commutative, when we add two integers up, the order of numbers doesn't affect the result. For example, $2 + 3 = 3 + 2$. Multiplication also satisfies commutativity, when we multiply two integers, the order of numbers doesn't affect the result. For example, $2 \cdot 3 = 3 \cdot 2$.

So for $a, b, c \in \mathbb{Z}$, we have

$$a + b = b + a,$$
$$a \cdot b = b \cdot a.$$

Associativity $\mathbb{Z}$ satisfies associativity. Addition is associative, when we add three integers up, the grouping of the numbers doesn't affect the result. For example, $(2 + 3) + 4$ is the same as $2 + (3 + 4)$. Multiplication also satisfy associativity, when we multiply three integers, the grouping of the numbers doesn't affect the result. For example, $(2 \cdot 3) \cdot 4 = 2 \cdot (3 \cdot 4)$.

For $a, b, c \in \mathbb{Z}$, we have

$$(a + b) + c = a + (b + c),$$
$$(a \cdot b) \cdot c = a \cdot (b \cdot c).$$

Distributivity The axiom distributivity connects addition and multiplication. For example, $(2 + 3) \cdot 4$ is a combination of both addition and multiplication. To compute this, there are two ways: first compute $2 + 3 = 5$, then substitute and compute $5 \cdot 4 = 20$; The other way is to separate

the parentheses and compute multiplication $2 \cdot 4 = 8$ and $3 \cdot 4 = 12$ first, then add $8 + 12 = 20$. Distributivity is a good way to eliminate the parentheses.

For $a, b, c \in \mathbb{Z}$, we have

$$a \cdot (b + c) = a \cdot b + a \cdot c.$$

Additive Identity In the set of integers $\mathbb{Z}$, there exists one number such that any numbers $a \in \mathbb{Z}$ add the number equals to a itself. We name this integer as 0.

There exists $0 \in \mathbb{Z}$ such that

$$a + 0 = 0 + a = a$$

for all $a \in \mathbb{Z}$.

Multiplicative Identity In the set of integers $\mathbb{Z}$, there exists one number such that any numbers $a \in \mathbb{Z}$ multiply the number equals to a itself. We name this integer as 1.

There exists $1 \in \mathbb{Z}$ such that

$$a \cdot 1 = 1 \cdot a = a$$

for all $a \in \mathbb{Z}$.

Existence of Additive Inverse The additive inverse give the concept of "cancellation" or "undoing" of operations. For example, if we have $a + b = a + a$, by intuition it is obvious that $b = a$, however, how can we rigorously prove that? The idea is to cancel one a on each side,

$$\begin{aligned} -a + (a + b) &= -a + (a + a) \\ (-a + a) + b &= (-a + a) + a \\ 0 + b &= a \\ b &= a \end{aligned}$$

For $a \in \mathbb{Z}$, there exists $x \in \mathbb{Z}$ such that

$$a + x = 0,$$

x is called the additive inverse of a.

Lemma 2.1. *In the set of integers, "zero" and "one" are uniquely defined.*

Proof. For the sake of contradiction, we first assume that 0 is not unique.

Suppose two 0_1 and 0_2 ($0_1 \neq 0_2$) are elements of $\mathbb{Z}$ with

$$a + 0_1 = a$$
$$a + 0_2 = a$$

for all $\mathbb{Z}$. Because $+$ is a binary operation, then $0_1 = 0_2$, contradicts with our assumption, then there is unique "zero" in $\mathbb{Z}$.

Similarly, apply multiplicative identity to two different 1_1 and 1_2, it contradicts the binary operation, so "one" is also unique in $\mathbb{Z}$. □

From the Ring Axioms, we can prove lemmas below.

Lemma 2.2. *For $a \in \mathbb{Z}$, $a \cdot 0 = 0$*

Proof. Let's start with $0 + 0 = 0$, which is true by the additive identity. Then, since multiplication is well-defined, we can multiply by a on both sides, giving $a \cdot (0+0) = a \cdot 0$. Then, by the distributive property, $a \cdot 0 + a \cdot 0 = a \cdot 0$. Then, since addition is well-defined, adding $-(a \cdot 0)$ to both sides gives us, $-(a \cdot 0) + (a \cdot 0 + a \cdot 0) = -(a \cdot 0) + a \cdot 0$. Then, by the additive inverse axiom, $-(a \cdot 0) + (a \cdot 0 + a \cdot 0) = 0$. Now using the associative property for addition, we get $(-(a \cdot 0) + a \cdot 0) + a \cdot 0 = 0$. Once again using the additive inverse axiom, we get that $0 + a \cdot 0 = 0$. Which is simply, $a \cdot 0 = 0$ by the additive identity axiom. □

Lemma 2.3. *For $0 \in \mathbb{Z}$, $0 = -0$.*

Proof. Start with $0 + 0 = 0$ from the additive identity axiom, then add -0 to both sides of the equation to give $(0+0)+(-0) = 0+(-0)$. Then, by the additive identity, $(0+0)+(-0) = -0$. From the associative property of addition, $0 + (0 + (-0)) = -0$. And by the additive inverse property, $0 + 0 = -0$, and finally using the additive identity property, we arrive at $0 = -0$ □

Lemma 2.4. *For $a \in \mathbb{Z}$, let $-a$ be the solution to $a + x = 0$ (the additive inverse of a), this solution is in fact unique.*

Proof. Let's assume that there are 2 x's, namely x_1 and x_2 such that $a + x_1 = 0$ and $a + x_2 = 0$. Then, by substitution, $a + x_1 = a + x_2$. Adding $-a$ to both sides of the equation gives, $(-a) + (a + x_1) = (-a) + (a + x_2)$. Then by the associative property of addition, we have that $((-a) + a) + x_1 = ((-a) + a) + x_2$. Now, using the commutative property of addition gives us $(a + (-a)) + x_1 = (a + (-a)) + x_2$, which by the additive inverse axiom turns into $0 + x_1 = 0 + x_2$. By the additive identity axiom, this just turns into $x_1 = x_2$. Since $x_1 = x_2$, this shows that x, the additive inverse is in fact unique. □

Lemma 2.5. $-ak = (-a)k = a(-k)$

Proof. $-ak = (-a)k$:

Let's take a look at $ak + (-a)k$. By the commutative property of multiplication, this equals $ka + k(-a)$. Then, by the distributive property, this equals $k(a + (-a))$, which by the additive inverse axiom, becomes $k(0)$ which from **Lemma 2.2** simply just equals 0. Since $ak + (-a)k = 0$ and $ak + (-ak) = 0$, then since we have shown that the additive inverse is unique in **Lemma 2.4**, this simply means that $(-ak) = (-a)k$.

$-ak = a(-k)$

Using a similar approach, let's once again take a look at $ak+a(-k)$. By the distributive property, this is equal to $a(k + (-k))$ which by the additive inverse axiom, just becomes $a(0)$ which then is just 0 from **Lemma 2.2**. Since $ak+a(-k) = 0$ and $ak+(-ak) = 0$, then since we have shown that the additive inverse is unique in **Lemma 2.4**, this simply means that $(-ak) = (-a)k = a(-k)$, completing our proof.

□

Lemma 2.6. $-a = (-1) \cdot a$

Proof. Let's start with the fact that $0 = a \cdot 0$ from **Lemma 2.2**. Then, using the fact that $1+(-1) = 0$ from the additive inverse axiom, substituting this in for 0 gives us that $0 = a(1+(-1))$. Now, using the distributive property, we can get that $0 = 1 \cdot a + ((-1) \cdot a)$. From the multiplicative identity, $0 = a + ((-1) \cdot a)$. Adding $-a$ to both sides gives us that $-a + 0 = -a + (a + (-1 \cdot a))$. Now from the additive identity axiom, $-a = -a + (a + (-1 \cdot a))$. Applying the associative property of addition, we get that $-a = ((-a) + a) + ((-1) \cdot a)$. From the commutative property of addition, this turns into $-a = (a + (-a)) + (-1 \cdot a)$, which by the additive inverse identity just turns into $-a = (0) + (-1 \cdot a)$. Applying the additive identity axiom, we get that $-a = (-1) \cdot a$, completing our proof. □

Lemma 2.7. $-(-a) = a$

Proof. Let's take a look at the two expressions $a+(-a)$ and $(-a)+(-(-a))$. By the additive inverse axiom, $a + (-a) = 0$ and $(-a) + (-(-a)) = 0$. Then, by substitution, $a + (-a) = (-a) + (-(-a))$. From the commutative property of addition, $(-a) + a = (-a) + (-(-a))$. Adding a to both sides gives us that $a+((-a)+a) = a+((-a)+(-(-a)))$. Then, from the associative property of addition, we have that $(a+(-a))+a = (a+(-a))+(-(-a))$. Which from the additive inverse axiom, becomes $0 + a = 0 + (-(-a))$, and by the additive identity axiom, we get that $a = -(-a)$. □

Lemma 2.8. $(-a)(-k) = ak$

Proof. From **Lemma 2.5**, we have that $-ak = a(-k)$. Multiplying both sides by (-1) gives us that $(-1) \cdot (-ak) = (-1) \cdot (a(-k))$. From the associative property of multiplication, we have that $(-1) \cdot (-ak) = ((-1) \cdot a)(-k))$. Then from **Lemma 2.6**, we have that $-(-ak) = (-a)(-k)$. This, from **Lemma 2.7** just becomes $ak = (-a)(-k)$, completing our proof. □

Definition 2.1. *Subtraction: Given a, b define $a - b$ to be the unique solution y to the equation $a = y + b$.*

Lemma 2.9. $a + (-b) = a - b$

Proof. From the definition of subtraction, we have that $a = y + b$ and $a - b = y$. Take the first of these 2 equations. Adding $-b$ to both sides of the equation gives us $a + (-b) = (y + b) + (-b)$. Then, by the associative property of addition, we have that $a + (-b) = y + (b + (-b))$, which by the additive inverse axiom just becomes $a + (-b) = y + 0$. Applying the additive identity axiom gives us that $a + (-b) = y$. Now, substituting the second equation in for y gives us that $a - b = a + (-b)$. □

Lemma 2.10. *If $ab = ab'$ and $a \neq 0$, then $b = b'$. And $ab = 0$ implies that $a = 0$ or $b = 0$*

Proof. Assume that $b \neq b'$, let k be the difference between b' and b. Then $b' - b = k$. Adding b to both sides gives us that $(b' - b) + b = k + b$. Then, by the associative property, $b' + ((-b) + b) = k + b$. And from the commutative property of addition, we have that $b' + (b + (-b)) = k + b$. Using the additive inverse axiom, this just gives us $b' + 0 = k + b$, or from the additive identity axiom, that $b' = k + b$. We know that $k \neq 0$, as otherwise:

$b' = 0 + b$, which just turns into $b' = b$ from the additive identity axiom, a violation to our assumption. So $k \neq 0$.

Then, ab' just turns into $a(k + b)$ which from the distributive property just turns into $ak + ab$. We know $ab = ab'$ from the problem statement, so substituting our expression in for b' gives us that $ab = a(k + b)$, which from the distributive property just turns into $ab = ak + ab$. Adding $(-ab)$ to both sides, gives us that $ab + (-ab) = (ak + ab) + (-ab)$. Which from the additive inverse axiom becomes $0 = (ak + ab) + (-ab)$. Then from the associative property of addition, $0 = ak + (ab + (-ab))$, which by the additive inverse axiom becomes $0 = ak + 0$, and from the additive identity axiom, becomes $0 = ak$, or $ak = 0$.

We know that $a \neq 0$ and we defined that $k \neq 0$, so by trichotomy, either $a \in \mathbb{Z}^+$ or $-a \in \mathbb{Z}^+$. And similarly, also from trichotomy, $k \in \mathbb{Z}^+$ or $-k \in \mathbb{Z}^+$.

Let's look at all of the 4 cases.

Case 1: If $a \in \mathbb{Z}^+$ and $k \in \mathbb{Z}^+$. Then, by multiplicative closure, $ak \in \mathbb{Z}^+$. So by trichotomy, since $ak \in \mathbb{Z}^+$, $ak \neq 0$.

Case 2: If $a \in \mathbb{Z}^+$ and $-k \in \mathbb{Z}^+$. Then, by multiplicative closure, $a(-k) \in \mathbb{Z}^+$ which from **Lemma 2.5**, just becomes $-(ak) \in \mathbb{Z}^+$. Then, once again, by trichotomy, since $-(ak) \in \mathbb{Z}^+$, $ak \neq 0/$

Case 3: If $-a \in \mathbb{Z}^+$ and $k \in \mathbb{Z}^+$. Then, by multiplicative closure, $(-a)k \in \mathbb{Z}^+$ which from **Lemma 2.5**, just becomes $-(ak) \in \mathbb{Z}^+$. Then, by trichotomy, since $-(ak) \in \mathbb{Z}^+$, $ak \neq 0/$.

Case 4: If $-a \in \mathbb{Z}^+$ and $-k \in \mathbb{Z}^+$. Then, by multiplicative closure, $(-a)(-k) \in \mathbb{Z}^+$. From **Lemma 2.8**, we have that, by substitution, $ak \in \mathbb{Z}^+$. Then, by trichotomy, since $ak \in \mathbb{Z}^+$, $ak \neq 0$.

In all four of these cases, $ak \neq 0$, so, it is required for one of $a = 0$ or $k = 0$ to be true for $ak = 0$. Then, since $a \neq 0$ is defined from the problem statement, this means that it is required for $k = 0$. Quickly checking, we see that $ak = a(0)$ by substitution, which equals 0 from **Lemma 2.2**. So this in fact works. (This proves the second part of our lemma, that $ak = 0$ implies that either $a = 0$ or $k = 0$).

Finally, substituting $k = 0$ into our derived equation $b' = k + b$ gives us $b' = 0 + b$, which from the additive identity axiom, just turns into $b' = b$. Completing our proof.

□

2.2. The Order Axioms

Why do we need Order Axioms? Order Axioms, as states in its name, enable us to compare elements and establish relationships such as "greater than" ($>$), "less than" ($<$), "greater than or equal to" ($\geq$), and "less than or equal to" ($\leq$) so that we can place all elements in order. This ordering relation is fundamental in mathematics and helps us understand the relative sizes, magnitudes, or positions of elements within a set. Also, Order Axioms establish the concept of positivity.

There is a nonempty subset $\mathbb{Z}^+ \subseteq \mathbb{Z}$ with the following properties:

Additive closure: For all $a, b \in \mathbb{Z}^+, a + b \in \mathbb{Z}^+$

Multiplicative closure: For all $a, b \in \mathbb{Z}^+, a \cdot b \in \mathbb{Z}^+$

Nontriviality: $0 \notin \mathbb{Z}^+$

Trichotomy : For all $a \in \mathbb{Z}$, exactly one of the following holds: $a \in \mathbb{Z}^+, a = 0,$ or $-a \in \mathbb{Z}^+$

Additive and Multiplicative Closure Positive integers are closed under addition and multiplication.

When two positive integers are added up, the result is always a positive integer. For example, adding 3 and 4 gives 7 which is also a positive integer. Also positive integers are closed under multiplication, when two positive integers are multiplied, the result is always a positive integer. For example, multiplying 2 and 5 gives 10 which is also a positive integer.

Therefore, for all $a, b \in \mathbb{Z}^+$

$$a + b \in \mathbb{Z}^+, ab \in \mathbb{Z}^+.$$

Trichotomy For all $a \in \mathbb{Z}$, exactly one of the following holds: $a \in \mathbb{Z}^+$, $a = 0$, or $-a \in \mathbb{Z}^+$

Trichotomy is very useful, we can define the inequalities.

Definition 2.2.

If $a > b$, then $a + (-b) \in \mathbb{Z}^+$.
If $a < b$, then $-(a + (-b)) \in \mathbb{Z}^+$.
If $a \geq b$, then either $a > b$ or $a = b$.
If $a \leq b$, then either $a < b$ or $a = b$.

Lemma 2.11. *For $a, b, x \in \mathbb{Z}$, if $a \leq b$, then $a + x \leq b + x$*

Proof. Let's try and prove this through a proof by cases. $a \leq b$ implies that $a = b$ or $a < b$.

Case 1: If $a = b$:

If $a = b$, then since addition is well-defined, we can simply add x to both sides and arrive at the equation $a + x = b + x$.

Case 2: If $a < b$:

If $a < b$, this means that $b + (-a) \in \mathbb{Z}^+$ by the definition of $<$. Now, let's take a look at $(b+x)+(-(a+x))$. Then since by **Lemma 2.6**, this expression is the same as $(b+x)+(-1(a+x))$. Then, using the distributive property, this just turns into $(b + x) + ((-1)a + (-1)x)$. This, using the same **Lemma 2.6**, gives us $(b+x)+((-a)+(-x))$. By the commutative property of addition, this expression turns into $(b + x) + ((-x) + (-a))$. Now, by general associativity, we get that $b + (x + (-x)) + (-a)$. Now from the additive inverse axiom, this expression is just $b + (0 + (-a))$ which by the additive identity axiom turns into $b+(-a)$. We know that $b+(-a) \in \mathbb{Z}^+$ from the fact that $a < b$. So, the expression $(b+x)+(-(a+x)) = b+(-a) \in \mathbb{Z}^+$, so $(b+x)+(-(a+x)) \in \mathbb{Z}^+$, which by the definition of $<$, says that $a + x < b + x$.

In the only two possible cases, we have shown that if $a \leq b$, then either $a + x = b + x$ or $a + x < b + x$. Combining these two inequalities into one encompassing inequality, just gives us that $a + x \leq b + x$, completing our proof.

□

Lemma 2.12. *For $a, b, x \in \mathbb{Z}$, if $a \leq b$ and $x \geq 0$, for $a, b \in \mathbb{Z}$, then $ax \leq bx$*

Proof. Let's try to do this through a proof by cases. $a \leq b$ implies that $a < b$ or $a = b$.

Case 1: If $a = b$, $x = 0$:

In this case, $ax = a \cdot 0$, and $bx = b \cdot 0$. Since $a, b \in \mathbb{Z}$, $a \cdot 0 = 0$ and $b \cdot 0 = 0$. So since $0 = 0$, by substitution, $ax = bx$

Case 2: If $a < b$, $x = 0$:

In this case, $ax = a \cdot 0$, and $bx = b \cdot 0$. Since $a, b \in \mathbb{Z}$, $a \cdot 0 = 0$ and $b \cdot 0 = 0$. So since $0 = 0$, by substitution, $ax = bx$

Case 3: If $a < b$, $x > 0$:

By the definition of $<$, $x + (-0) \in \mathbb{Z}^+$. By **Lemma 2.3**, substituting 0 for -0, we get that $x + 0 \in \mathbb{Z}^+$, or by the additive identity, we get $x \in \mathbb{Z}^+$. Similarly, by the definition of $<$, $b + (-a) \in \mathbb{Z}^+$. Let $b + (-a) = k$ for some $k \in \mathbb{Z}^+$. Then adding a to both sides of the equation gives, $(b + (-a)) + a = k + a$. Using the associative property of addition, we can arrive at $b + ((-a) + a) = k + a$. Now, using the commutative property of addition, we get that $b + (a + (-a)) = k + a$. Using the additive inverse axiom, $b + (0) = k + a$, and using the additive identity axiom, $b = k + a$. Then, $bx = xb$ by the commutative property of multiplication, and $xb = x(k + a)$ from substitution. Now, using the distributive property, we get $x(k + a) = xk + xa$, and from the commutative property of multiplication, $xk + ka = xk + ax$. If we want to show that $ax \leq bx$, we want to show that either $ax = bx$, or $ax < bx$ (would imply $(bx + (-ax)) \in \mathbb{Z}^+$ by the definition of $<$). Taking a look at this $(bx + (-ax))$ expression, substituting in $bx = xk + ax$, this expression turns into $(xk + ax) + (-ax)$. Using the associative property of addition, we get $xk + (ax + (-ax))$, and simplifying using the additive inverse axiom, we arrive at $xk + 0$ or simply just xk from the additive identity axiom. Now since $x \in \mathbb{Z}^+$ and $k \in \mathbb{Z}^+$, by multiplicative closure, $xk \in \mathbb{Z}^+$. So, we have shown that that $(bx + (-ax)) = xk \in \mathbb{Z}^+$. Or, by the definition of $<$, $ax < bx$.

Case 4: If $a = b, x > 0$:

Then, we simply have $a = b$, and multiplying by x on both sides simply gives us $ax = bx$.

Looking at the total four cases, three of them result in $ax = bx$ and one of them results in $ax < bx$. Combining these 4 inequalities into one encompassing inequality, we get that $ax \leq bx$. Which proves our lemma. □

Nontriviality Nontribiality states that 0 is not a positive integer, which can actually can be get from trichotomy because we have already proved **Lemma 2.3**.

Here, from the Order Axioms, we know that there will be positive, negative and 0 elements in $\mathbb{Z}$, but how do we know that which of them are positive and which of them are negative?

The enter point should be 1. And then the numbers larger than 1 defined as $(((1 + 1) + 1) + 1) + \cdots + 1$ should also be positive because of the additive closure, which make sense.

From common sense, we are clear that 1 is a positive integer, but how can we prove it rigorously?

Lemma 2.13. *For element* $0, 1 \in \mathbb{Z}$, $0 \neq 1$.

Proof. We can prove this by contradiction. Assume $0 = 1$, for all $a \in \mathbb{Z}$, $a \cdot 0 = a \cdot 1$ since $\cdot$ is well-defined. Then according to the additive and multiplicative identity, $0 = a$ for all $a \in \mathbb{Z}$. This shows $\mathbb{Z} = \{0\}$. However, according to Order Axioms, $0 \notin \mathbb{Z}^+$, then $\mathbb{Z}^+ = \emptyset$, contradicting $\mathbb{Z}^+$ is a nonempty set. Therefore, $0 \neq 1$. □

Lemma 2.14. *For element* $1 \in \mathbb{Z}$, $1 \in \mathbb{Z}^+$.

Proof. For the sake of contradiction, we first assume $1 \notin \mathbb{Z}^+$, then according to trichotomy, either $1 = 0$ or $-1 \in \mathbb{Z}^+$. In **Lemma 2.13**, we have proved that $1 \neq 0$, therefore, the only case is $-1 \in \mathbb{Z}^+$.

If $-1 \in \mathbb{Z}^+$, according to multiplicative closure, $(-1) \cdot (-1) = 1$, 1 should be in $\mathbb{Z}^+$, which contradicts trichotomy.

Therefore, $1 \in \mathbb{Z}^+$. □

Since we prove $1 \in \mathbb{Z}^+$, then a number a can be expressed as sum of 1s is a positive number by additive closure.

The other question is, how can we prove 1 is the smallest element in $\mathbb{Z}^+$ even though this seems to be something obvious?

To prove this, we need to introduce another axiom:

2.3. Well-Ordering Principle (WOP)

Well-Ordering Principle (WOP) says that for all nonempty subsets S of the positive integers, there exists a least element in S.

Theorem 2.1. *In $\mathbb{Z}^+$, 1 is the least element.*

Proof. Let $S = \mathbb{Z}^+$. Then S is nonempty (part of the Order Axioms for $\mathbb{Z}^+$). Then there exists a least element of $\mathbb{Z}^+$ by WOP. Let's prove this fact by contradiction. Assume there exists some $l \in \mathbb{Z}^+ where l < 1$ let there be some least element $l \in \mathbb{Z}^+$.

We have that since $l \in \mathbb{Z}^+$, then by the additive identity, $l + 0 \in \mathbb{Z}^+$, and from **Lemma 2.3** and substitution, $l + (-0) \in \mathbb{Z}^+$, which results in $l > 0$ by the definition of less than. Then, from case 3 in the proof of **Lemma 2.12**, since $l > 0$ and $l < 1$, then $l \cdot l < 1 \cdot l$. Which from the multiplicative identity results in, $l \cdot l < l$. But since $l \in \mathbb{Z}^+$, then $l \cdot l \in \mathbb{Z}^+$ by multiplicative closure. This is a contradiction as we claimed that l was the least element in Z^+, but $l * l$ is also in S and $l \cdot l < l$. So this proves that 1 is in fact the least element of $\mathbb{Z}^+$. □

Theorem 2.1 is also called **OLE**.

OLE helps to tell apart the integers from the real numbers and rational numbers since they both obey the Ring Axioms and the Order Axioms, but not OLE since there are smaller elements in $\mathbb{R}$ and $\mathbb{Q}$.

3. Modulo and Divisibility

Definition 3.1. *For $a, b \in \mathbb{Z}$, we say $a \mid b$ ("a divides b") if $b = aq$ for some $q \in \mathbb{Z}$.*

For example, $18 = 9 \cdot 2$, since 2 is an integer, we have $9 \mid 18$. However, does 9 also divides other numbers, take 22 as an example?

We know that we can express 22 as $9 \cdot 2 + 4$, we know that since $9 \mid 9 \cdot 2$, if $9 \mid 4$, then 9 can divide 22. This "$9 \mid 4, 9 \mid 9 \cdot 2$ implies $9 \mid 4 + 9 \cdot 2 = 22$" statement is actually by our intuition, but how to prove it rigorously?

Lemma 3.1. *For $a, b, d \in \mathbb{Z}$, if $d \mid a$ and $d \mid b$, then $d \mid (ar + bs)$ for every $r, s \in \mathbb{Z}$.*

Proof. If $d \mid a$, $a = dp$ for $p \in \mathbb{Z}$ and $d \mid b$ means $b = dq$ for $q \in \mathbb{Z}$.

Because $a = dp$, multiply r on both sides, we get $a \cdot r = (dp) \cdot r$. So $a \cdot r = (dp) \cdot r = d \cdot (pr)$ according to associativity.

Multiply s on both sides of $b = dq$, we get $b \cdot s = (dq) \cdot s$ and $b \cdot s = (dq) \cdot s = d \cdot (qs)$ due to associativity.

Add $b \cdot s$ on both sides of $a \cdot r = d \cdot (pr)$, we get $a \cdot r + b \cdot s = d \cdot (pr) + b \cdot s$. Then substitute $b \cdot s$ using $d \cdot (qs)$, we get $a \cdot r + b \cdot s = d \cdot (pr) + d \cdot (qs)$. From distributive axiom, we get $a \cdot r + b \cdot s = d \cdot (pr + qs)$.

$p, r \in \mathbb{Z}$, $pr \in \mathbb{Z}$ because of multiplicative closure. Similarly, $b, s \in \mathbb{Z}$, $bs \in \mathbb{Z}$. So $pr + bs \in \mathbb{Z}$ because of additive closure. Therefore, $d \mid (ar + bs)$. □

So if $9 \mid 4$, then $9 \mid 22$, but we know that actually 9 cannot divide 4, again the question is, how can we explain that 9 definitely cannot divide 4.

Lemma 3.2. *If $a \mid b$ and $a, b \in \mathbb{Z}^+$ then $a \leq b$.*

Proof. $a \mid b$ implies $a = bk$ for $k \in \mathbb{Z}$ by the definition of divisibility.

First, let's assume $k \notin \mathbb{Z}$, then by trichotomy, $k = 0$ or $-k \in \mathbb{Z}^+$

If $k = 0$: $b = ak$ turns into $b = a \cdot 0$. From **Lemma 2.2**, since a $\in \mathbb{Z}$, $a \cdot 0 = 0$. So by substitution, $b = 0$. This is a contradiction to the fact that $b \in \mathbb{Z}^+$, so $b \neq 0$ by trichotomy.

If $-k \in \mathbb{Z}^+$:

Taking, $b = ak$, since addition is well-defined, we can add $-b$ to both sides, which gives $b + (-b) = ak + (-b)$. Then by the additive inverse axiom, $0 = ak + (-b)$. Adding $-ak$ to both sides gives us, $0 + (-ak) = (-ak + (ak + (-b))$. Then by negativity, we have $(-ak) = (-ak + (ak + (-b)))$. And using the associative property for addition gives us $(-ak) = ((-ak + ak) + (-b))$. Simplifying this with negativity gives us, $(-ak) = (0 + (-b))$. Then, simplifying with the additive identity, axiom we get $-ak = -b$. Simplifying this using **Lemma 2.5**, we get $(a)(-k) = -b$. Since $a, (-k) \in \mathbb{Z}^+$, by multiplicative closure, $a(-k) \in \mathbb{Z}^+$, and by substitution, $-b \in \mathbb{Z}^+$. But this is a contradiction to the fact that $b \in \mathbb{Z}^+$ so $-b$ cannot be in $\mathbb{Z}+$ by trichotomy. So $-b \notin \mathbb{Z}^+$.

Then, k must be in $\mathbb{Z}^+$. We want to show $a \leq b$ or by substitution, $a \leq ak$. Using **Lemma 2.11**, we can add $-a$ to both sides of the inequality to get that $a + (-a) \leq ak + (-a)$. From the additive inverse axiom, this gives us $0 \leq ak + (-a)$, which from **Lemma 2.6** gives us $0 \leq ak + (-1)a$ which by the commutative property of multiplication is equivalent to $0 \leq ak + a(-1)$. By the distributive

property, this is simply $0 \leq a(k+(-1))$. We want to show this for k $\in \mathbb{Z}^+$. Since k $\in \mathbb{Z}^+$, by **Theorem 2.1**, we know that $k \geq 1$.

If $k = 1$: Then, $a(k+(-1)))$ by substitution is just $a(1+(-1))$. By the additive inverse axiom, this is equivalent to $a(0)$ which from **Lemma 2.2** is just equivalent to 0. We wanted to show that $0 \leq a(k+(-1))$, substituting $0 = a(k+(-1))$, we get that $0 \leq 0$. This is true as $0 = 0$, so if k=1, the inequality that we wanted to show holds.

If $k > 1$: Then, we know that $k+(-1) \in \mathbb{Z}^+$ by the definition of $<$. Since $a \in \mathbb{Z}^+, and k \in \mathbb{Z}^+$, then by multiplicative closure, $a(k+(-1)) \in \mathbb{Z}^+$. So $a(k+(-1))) + (0) \in \mathbb{Z}^+$ and from **Lemma 2.3**, $a(k+(-1))) + (0) \in \mathbb{Z}^+$ by substitution. Then, by the definition of $<$, $0 < a(k+(-1))$.

So, since we have shown that $0 \leq a(k+(-1))$ in both of the only 2 possible cases, we have equivalently proved that $a \leq ak$ or that $a \leq b$ if $a \mid b$. □

Lemma 3.2 is quite useful to acquire inequalities from statements involving the greatest common divisor that states in **§4**.

Therefore, since $9 - 4 = 5 \in \mathbb{Z}^+$, $9 > 4$, which implies $9 \nmid 4$, so $9 \nmid 22$.

For 23, it is similar, we know that $23 = 9 \cdot 2 + 5$ and $9 > 5$, which implies $9 \nmid 5$, so $9 \nmid 23$.

We compute 22 and 23 and find out we can only draw the conclusion that 9 cannot divide them, but how can we tell apart the difference between them? We observe that while $22 = 9 \cdot 2 + 4, 23 = 9 \cdot 2 + 5$ are different, 4 and 5 are also different, so we consider finding a way to tell the difference between 22 and 23, while we also want to say that 22, may have the similar property as $22 - 9 = 13$. That is why we come up with the concept of modulo.

Definition 3.2. *We define* $a \equiv r \pmod{b}$ *for* $a, r \in \mathbb{Z}$, $b \in \mathbb{Z}^+$ *if* $b \mid a - r$.

This definition help us to deal with a that m cannot divide. Take the same example, now we can express 22 when it is divided by 9: $22 \equiv 4 \pmod{9}$. To check, $22 - 4 = 18 = 9 \cdot 2$, this is true. Therefore, in $\mathbb{Z}_9$, 22 is equivalent to 4, while $23 \equiv 5 \pmod{9}$ and $13 \equiv 4 \pmod{9}$, meet our requirements.

However, there is a problem: not only $22 - 4 = 18$ is a multiple of 9, also if we have $22 - 13 = 9$ or $22 - 22 = 0 = 9 \cdot 9$, this is still true, while seems lose some meaning since it's not unique.

We want to add a limitation to r such that r is unique. By intuition, we know that when we limit r to be larger or equal to 0 and less than b, it will be unique. But how to prove it?

Theorem 3.1. ***Division Algorithm:*** *For* $a, b \in \mathbb{Z}$, $b \neq 0$, *there exists unique* q, r *such that* $a = bq + r$ *for* $0 \leq r < b$.

Proof. First, without loss of generality, assume $b > 0$ to make this simpler, the case $b < 0$ is nearly the same because just change it to $-b \in \mathbb{Z}^+$ does not affect the proof at all.

We define $S = \{r \in \mathbb{Z}^+ \cup \{0\} : r = a - bq \text{ for some } q \in \mathbb{Z}\}$, then $S \subseteq \mathbb{Z}^+ \cup \{0\}$.

If we can show that S is nonempty, then WOP will give us a least element of S and this will be the remainder r we are looking for. There are two cases.

Case 1: $a \geq 0$. In this case, we can set $q = 0$ and get the element $a - 0 \cdot b = a \geq 0$ of S.

Case 2: $a < 0$. In this case, set $q = a$. Then $a - bq = a - aq = a(1 - q)$. Since $a < 0$ and $q > 1$, $a(1 - q) > 0$, hence is an element of S.

Thus, S is not an empty set and so S has a least element $r = a - bq$ for some integer q. Thus, $a = bq + r$ and $r \geq 0$. What we need to prove is (i) $r < b$ and (ii) q and r are unique.

(i) Suppose $r \geq b$. Then $r = b + r'$, where $0 \leq r' < r$. Then $a = bq + r = bq + b + r' = b(q+1) + r'$, so that $r' = a - b(q + 1)$ is an element of S smaller than r. This contradicts the fact that r is the least element of S. Thus $r < b$.

(ii) Suppose integers q' and r' satisfy $a = bq' + r'$ and $0 \leq r' < b$. Assume $r' \geq r$, so that $0 \leq r - r' < b$. Since $a = bq' + r' = bq + r$,

$$r - r' = b(q' - q).$$

This means that d divides $r - r'$, which implies either $r - r' \geq b$ or $r - r' = 0$. But we know $0 \leq r - r' < d$. Thus, $r' = r$, which in turn implies $q' = q$. That is, q and r are unique.

So the full **division algorithm** is proved. □

Here let us explore more properties of modulos. For example, we have $22 \equiv 4 \pmod 9, 23 \equiv 5 \pmod 9$, we have $22 + 23 = 45 \equiv 0 \pmod 9$ and at the same time, $4 + 5 \equiv 0 \pmod 9$; Similarly, $22 \cdot 23 = 506 \equiv 2 \pmod 9$, and $4 \cdot 5 \equiv 2 \pmod 9$, are they coincidences?

Lemma 3.3. *If $a \equiv b \pmod m$ and $c \equiv d \pmod m$, then $a + c \equiv b + d \pmod m$ and $ac \equiv bd \pmod m$.*

Proof. According to definition of mod, we name $a = pm + b$ and $c = qm + d, p, q \in \mathbb{Z}$. Add them up together we get $a + c = (pm + b) + (qm + d) = (p + q)m + (b + d)$. Since $p, q \in \mathbb{Z}$, we get $p + q \in \mathbb{Z}$. So $(p + q)m + (b + d) \equiv (b + d) \pmod m$. Therefore, $a + c \equiv b + d \pmod m$.

Similarly, $a = pm + b, c = qm + d, p, q \in \mathbb{Z}$. $ac = (pm + b) \cdot (qm + d) = (pm) \cdot (qm) + (pm) \cdot d + b \cdot (qm) + b \cdot d = pqm^2 + pdm + bqm + bd = (pqm + pd + bq)m + bd$. Because $p, q, m, d, b \in \mathbb{Z}$ and the operation only includes addition and multiplication, $pqm + pd + bq \in \mathbb{Z}$. According to mod's definition, $(pqm + pd + bq)m + bd \equiv bd \pmod m$ and $ac \equiv bd \pmod m$. □

4. Greatest Common Divisor

Definition 4.1. *For $a, b, c, d \in \mathbb{Z}^+$, the greatest common divisor of a, b, $\gcd(a, b)$, is a number d such that $d \mid a$ and $d \mid b$. and for all c such that $c \mid a$ and $c \mid b$, $d \geq c$.*

For example, if we have two positive integers 12 and 18, the list of common divisors of 12 and 18 is $\{1, 2, 3, 6\}$. The greatest common divisor of 12 and 18 should be 6 because 6 is larger or equal to any of the elements in $\{1, 2, 3, 6\}$.

Theorem 4.1. ***Bezout's Identity:*** *For any two integers a, b with at least one of them nonzero, there exist integers m and n such that*

$$am + bn = \gcd(a, b)$$

Proof. Let a, b be any two integers in $\mathbb{Z}$. Let k be the smallest positive combination of a, b, meaning that for $m, n \in \mathbb{Z}$

$$am + bn = k \tag{4.1}$$

We need to prove that $k = \gcd(a, b)$. By division algorithm, there exists $q, r \in \mathbb{Z}$ such that

$$a = qk + r \tag{4.2}$$

where $0 \leq r < k$. Substitute (4.1) into (4.2) and we can get

$$\begin{aligned} a &= q(am + bn) + r \\ r &= a(1 - qm) + b(-n) \end{aligned}$$

Because we have $r < k$ and k is the smallest positive linear combination of a and b, we must have $r = 0$. Hence $a = qk + 0 = qk$. Therefore $k \mid a$. A symmetrical operation using Division Algorithm to rewrite b gives $k \mid b$. By definition of gcd, $k \leq \gcd(a, b) \mid a$ and $\gcd(a, b) \mid b$, $\gcd(a, b)$ divides any linear combination of a and b by **Lemma 3.1**.

Hence, $\gcd(a, b) \mid am + bn = k$. Thus, $\gcd(a, b) \mid k$. Since $\gcd(a, b), k \in \mathbb{Z}^+, \gcd(a, b) \leq k$. Now we have $k \leq \gcd(a, b)$ and $\gcd(a, b) \leq k$, we must have $k = \gcd(a, b)$ by trichotomy.

Therefore, for any two integers a, b with at least one is nonzero, then there exist $m, n \in \mathbb{Z}$ such that

$$\gcd(a, b) = am + bn$$

□

Corollary 4.1. *If $n \mid a$ and $n \mid b$, then $n \mid \gcd(a, b)$ for $a, b, n \in \mathbb{Z}$.*

Proof. $n \mid a$ and $n \mid b$ mean that $na_1 = a$ and $nb_1 = b$ for $a_1, b_1 \in \mathbb{Z}$ by the definition of divisibility. Let $d = \gcd(a, b)$, so $d \mid a$, $d \mid b$, and $da' = a$ and $db' = b$ for $a', b' \in \mathbb{Z}$ by the definition of divisibility and greatest common divisor.

Now, we use **Theorem 4.1 Bezout's Identity**. We know that there exist solutions $x, y \in Z$ to the equation $ax + by = \gcd(a, b) = d$, so substituting na_1 for a and na_2 for b, we get

$$(na_1)x + (nb_1)y = d$$

from which we get $n(a_1x + b_1y) = d$. From the definition of divisibility, we get that $n \mid d$, as desired. □

Lemma 4.1. $\gcd(a, b) \geq 1$ *for all* $a, b \in Z$.

Proof. We know that $1 \cdot a = a$ and $1 \cdot b = b$ by the multiplicative identity, so $1 \mid a$ and $1 \mid b$ by the definition of divisibility. By the definition of gcd, we must have $1 \leq \gcd(a, b)$, as desired. □

Lemma 4.2. *If* $ax + by = 1$ *for* $a, b, x, y \in \mathbb{Z}$, *then* $\gcd(a, b) = 1$.

Proof. By **Lemma 4.1**, we have that $\gcd(a, b) > 1$ or $\gcd(a, b) = 1$. If we assume that $\gcd(a, b) = 1$, then we're done, because that is the result we wanted to achieve.

Instead, if we assume $\gcd(a, b) = d > 1$, by the definition of gcd we get that $d \mid a$ and $d \mid b$, so $da' = d$, $db' = b$ for $a, b \in Z$ by the definition of divisibility. We then get

$$(a'd)x + (b'd)y = 1$$

giving us $d(a'x+b'y) = 1$, so $d \mid 1$. Since $d > 1$, we have $d-1 \in \mathbb{Z}^+$, so by closure $(d-1)+1 = d \in \mathbb{Z}^+$. Now since $d, 1 \in \mathbb{Z}^+$, by **Lemma 3.2**, we get $d \leq 1$, contradiction.

Therefore, we must have $\gcd(a, b) = 1$. □

The following lemmas and definitions will be very useful in our proof of the Chinese Remainder Theorem.

Lemma 4.3. *If* $\gcd(a_1, b) = 1$ *and* $\gcd(a_2, b) = 1$ *then* $\gcd(a_1a_2, b) = 1$ *for* $a_1, a_2, b \in \mathbb{Z}$.

Proof. Using **Theorem 4.1 Bezout's Identity**, since $\gcd(a_1, b) = 1$ and $\gcd(a_2, b) = 1$, we get that there exist $x_0, y_0, x_1, y_1 \in \mathbb{Z}$ such that

$$a_1x_1 + by_1 = 1$$

$$a_2x_2 + by_2 = 1$$

This motivates us to try to manipulate the equations into the form $(a_1a_2)x+by = 1$ where $x, y \in Z$, because using **Lemma 4.2**, we will be able to conclude that $\gcd(a_1a_2, b) = 1$.

Multiplying the first equation by a_2 and the second equation by a_1 gets us the equations

$$a_1a_2x_1 + ba_2y_1 = a_2$$

$$a_1a_2x_2 + ba_1y_2 = a_1$$

Now, since $\gcd(a_1, a_2) = 1$, we have that there exist $x_3, y_3 \in \mathbb{Z}$ such that $a_1x_3 + a_2y_3 = 1$. We substitute our equations we got for a_1 and a_2 to get

$$(a_1a_2x_2 + ba_1y_2)x_3 + (a_1a_2x_1 + ba_2y_1)y_3 = 1$$

We can rearrange the equation to get $(a_1a_2)(x_2x_3 + x_1y_3) + b(a_1x_3y_2 + a_2y_1y_3) = 1$, and set $x = x_2x_3 + x_1y_3, y = a_1x_3y_2 + a_2y_1y_3$ to get

$$(a_1a_2)x + by = 1,$$

From there, we use **Lemma 4.2** to get $\gcd(a_1a_2, b_1) = 1$, as desired. □

The definition of the product of multiple integers is needed to prove **Lemma 4.4**, so we will be defining it right here.

Definition 4.2. ***Product Definition.*** *For $a_i \in \mathbb{Z}$ with $1 \leq i \leq n$, we have that* $a_1a_2 \cdots a_n = \prod_{i=1}^{n} a_i = \begin{cases} a_n \cdot \prod_{i=1}^{n-1} a_i, & \text{if } n > 1 \\ a_1, & \text{if } n = 1 \end{cases}$

The definition of the sum of multiple integers will also be useful later on.

Definition 4.3. ***Sum Definition.*** *For $a_i \in \mathbb{Z}$ with $1 \leq i \leq n$, we have that* $a_1 + a_2 + \ldots + a_n = \sum_{i=1}^{n} a_i = \begin{cases} a_n + \sum_{i=1}^{n-1} a_i, & \text{if } n > 1 \\ a_1, & \text{if } n = 1 \end{cases}$

We will now prove the more general version of **Lemma 4.3**:

Lemma 4.4. *If $\gcd(a_i, b) = 1$ for all $1 \leq i \leq n$ then $\gcd(\prod_{i=1}^{n} a_i, b) = 1$ where all a_is and b are integers.*

Proof. For the sake of contradiction, let $S \subseteq \mathbb{Z}^+$ consist of all k such that $\gcd(a_i, b) = 1$ for all $1 \leq i \leq k$ but $\gcd(\prod_{i=1}^{k} a_i, b) \neq 1$. We want to show that there are no such elements in S. By WOP, S must have some least element, l.

If $k = 1$, we get that $\prod_{i=1}^{k} a_i = a_1$ by our definition of a product, and since we already have that $\gcd(a_1, b) = 1$, we have that $\gcd(\prod_{i=1}^{k} a_i, b) = 1$ for $k = 1$. Hence, $1 \notin S$. Since the least element of $\mathbb{Z}^+$ is 1 by OLE, **Theorem 2.1**, that means we must have $l > 1$. Hence, $l - 1 \in \mathbb{Z}^+$ but since l is the least element of S, we must have $l-1 \notin S$. Hence, we must have $\gcd(\prod_{i=1}^{l-1} a_i, b) = 1$.

Now, if $k = l$, we have that

$$\gcd(\prod_{i=1}^{l} a_i, b) = \gcd(a_l \cdot \prod_{i=1}^{l-1} a_i, b)$$

by our product definition. Since $\gcd(a_l, b) = 1$ by the given, and $\gcd(\prod_{i=1}^{l-1} a_i, b) = 1$, by **Lemma 4.3**, we get that $\gcd(a_l \cdot \prod_{i=1}^{l-1} a_i, b) = 1$, so $l \notin S$, contradiction. This shows that S must be empty, so we've proven our statement.

Here's an example: If we have $\gcd(4, 15) = 1$, $\gcd(7, 15) = 1$, and $\gcd(2, 15) = 1$, then we can indeed verify by ourselves that $\gcd(4 \cdot 7 \cdot 2, 15) = \gcd(56, 15)$ is indeed 1, and the gcd must be 1 because of the statement we just proved. □

To prove both **Theorem 1.1** and **Theorem 1.2** (2-variable and general Chinese Remainder Theorem), we will need the following lemma.

Lemma 4.5. *If $a \mid n$ and $b \mid n$ with $\gcd(a, b) = 1$, then $ab \mid n$ for $a, b, n \in \mathbb{Z}$.*

Proof. We will show that this holds for $n = 0$, and then $n \neq 0$.

If $n = 0$, then since $ab \in \mathbb{Z}$ by closure, we use **Lemma 2.2** to get that $(ab) \cdot 0 = 0 = n$, meaning $ab \mid n$ by the definition of divisibility.

Now we work on the case where $n \neq 0$. By the definition of divisibility, we can let $ak_1 = n$ and $bk_2 = n$ such that $k_1, k_2 \in \mathbb{Z}^+$. By **Theorem 4.1 Bezout's Identity**, there exist $x, y \in Z$ such that $ax + by = \gcd(a, b) = 1$, so we can multiply both sides by k_1k_2 to get

$$axk_1k_2 + byk_1k_2 = k_1k_2$$

which can be written as

$$(ak_1)(k_2x) + (bk_2)(k_1y) = n(k_2x) + n(k_1y) = n(k_2x + k_1y) = k_1k_2$$

Hence, by the definition of divisibility, we get $n \mid k_1k_2$, so we can let $nk_3 = k_1k_2$ for some $k_3 \in \mathbb{Z}$.

Now, notice that since $(ak_1)(bk_2) = n \cdot n$ and $nk_3 = k_1k_2$, we can rewrite the LHS of our equation as $ab(k_1k_2) = ab(nk_3)$, so our equation becomes

$$ab(nk_3) = n \cdot n$$

so by **Lemma 2.10**, since $n(abk_3) = n \cdot n$ where $abk_3 \in \mathbb{Z}$ by closure, and $n \neq 0$, we get that $abk_3 = n$, so $ab \mid n$, as desired.

Since for both $n = 0$ and $n \neq 0$ we have $ab \mid n$, we have proved our statement is true for all possible values of n, so we're done. □

We also need to prove the general version of **Lemma 4.5**, because we'll need it to prove general Chinese Remainder Theorem.

Lemma 4.6. *If $a_i \mid n$ for all $1 \leq i \leq k$ where $a_i, n \in \mathbb{Z}$, and $\gcd(a_i, a_j) = 1$ for all $1 \leq i, j \leq k$, $i \neq j$ then we have $\prod_{i=1}^{k} a_i \mid n$.*

Proof. For the sake of contradiction, let $S \subseteq \mathbb{Z}^+$ be the nonempty set of all positive integers k such that we have $\prod_{i=1}^{k} a_i \nmid n$ given the same conditions for all a_i and n. By WOP, we have that S must have some least element l.

When $k = 1$, we have that $a_1 \mid n$, so $\prod_{i=1}^{1} a_i = a_i$ by **Definition 4.2**, meaning we must have $1 \notin S$. Now, by OLE, we must have $l > 1$. Then, $l - 1 \in \mathbb{Z}^+$ but $l - 1 \notin S$ since l is the least element of S, which means our statement must hold for $k = l - 1$. Hence, $\prod_{i=1}^{l-1} a_i \mid n$.

Now we consider what happens when $k = l$. Since $\gcd(a_i, a_l) = 1$ for all $1 \leq i \leq l - 1$, we have that $\gcd(\prod_{i=1}^{l-1} a_i, a_l) = 1$ by **Lemma 4.4**. Now that we have

$$a_l \mid n, \quad \prod_{i=1}^{l-1} a_i \mid n, \quad \text{and} \quad \gcd(\prod_{i=1}^{l-1} a_i, a_l) = 1$$

by **Lemma 4.5**, we get that

$$a_l \cdot \prod_{i=1}^{l-1} a_i = \prod_{i=1}^{l} a_i \mid n$$

which means $l \notin S$, contradiction. Therefore, we must have that S is empty, so our statement is true for all k, as desired. □

Lemmas such as **Lemma 4.6** and **Lemma 4.4**, are not needed to prove the 2-variable case of the Chinese Remainder Theorem, **Theorem 1.1**, but are required for the general Chinese Remainder Theorem, **Theorem 1.2**. Since we have proven the lemmas required for proving the 2-variable Chinese Remainder Theorem, we will now prove it.

Proof. First we want to find a solution to both of those congruences. By **Theorem 4.1 Bezout's Identity**, since $\gcd(m, n) = 1$ there exist some integers X and Y such that $mX + nY = 1$. Now, we will show that $x = mXb + nYa$ satisfy both congruences.

$$x \equiv mXb + nYa \equiv nYa \equiv (1 - mX)a \equiv 1 \cdot a \equiv a \pmod{m}$$

Similarly,

$$x \equiv mXb + nYa \equiv mXb \equiv (1 - nY)b \equiv 1 \cdot b \equiv b \pmod{n}$$

Hence, $x = mXb + nYa$ satisfies both congruences.
Now we must show that $mXb + nYa$ is the only solution to these two congruences mod mn, or in other words, that solution is unique. For the sake of contradiction, assume that there are at least two distinct solutions to these congruences mod mn, so $x_1 \not\equiv x_2 \pmod{mn}$ but x_1 and x_2 still satisfy both congruences. We have

$$x_1 \equiv x_2 \equiv a \pmod{m}$$

$$x_1 \equiv x_2 \equiv b \pmod{n}$$

From this, we get $m \mid x_1 - x_2$ and $n \mid x_1 - x_2$. Since $\gcd(m, n) = 1$, by **Lemma 4.5** we get that $mn \mid x_1 - x_2$, so $x_1 \equiv x_2 \pmod{mn}$, contradiction. Hence, there can be only one solution to these congruences mod mn.

Since we have proven the existence and uniqueness of x, we're done. □

For the proof of **Theorem 1.2**, or the general case of the Chinese Remainder Theorem, we need one more lemma:

Lemma 4.7. *For any $a \in \mathbb{Z}$, $m \in \mathbb{Z}^+$ with $\gcd(a, m) = 1$, there exists some $x \in \mathbb{Z}$ such that $ax \equiv 1 \pmod{m}$.*

Proof. Since $\gcd(a, m) = 1$, by **Lemma 4.2**, we get that there exist $x, y \in \mathbb{Z}$ such that $ax+my = 1$. Hence, we have $ax+my-1 = 0$, so since $m \cdot 0 = 0$ by **Lemma 2.2**, we have that $m \mid 0 = ax+my-1$, so $ax + my - 1 \equiv 0 \pmod{m}$. We then get $ax + my \equiv 1 \pmod{m}$, but since $my \equiv 0 \pmod{m}$, we have $ax \equiv 1 \pmod{m}$, as desired. □

We have now acquired enough knowledge to prove **Theorem 1.2**, the general case of the Chinese Remainder Theorem.

Proof. We start with proving the existence of x, such that x satisfies all the congruences

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

To prove the existence of x, we will construct a solution that satisfies all those congruences. In the 2-variable case of the Chinese Remainder Theorem, notice that $x = mXb + nYa$ was congruent to mXb when taken mod n, and nYa when taken mod m. Also, we had an X such that $mXb \equiv b \pmod{n}$ and $nYa \equiv a \pmod{m}$.

So, the motivation for the following construction of x comes from these ideas we used to construct an x for the two-variable case.

First, let

$$N_i = n_1 \cdots n_{i-1} n_{i+1} \cdots n_k = \prod_{j=1}^{i-1} n_j \cdot \prod_{j=i+1}^{k} n_j$$

which is the product of all n_j for $1 \le j \le k$ except for $j = i$. Since for all $n_j \in \{n_1, n_2, \ldots, n_k\} \setminus \{n_i\}$ we have $\gcd(n_j, n_i) = 1$ by our given, we get

$$\gcd(\prod_{j=1}^{i-1} n_j \cdot \prod_{j=i+1}^{k} n_j, n_i) = \gcd(N_i, n_i) = 1$$

by **Lemma 4.4**. By **Lemma 4.7**, we get that there is some $M_i \in \mathbb{Z}$ such that

$$N_i M_i \equiv 1 \pmod{n_i}$$

because we had gotten that $\gcd(N_i, n_i) = 1$.

Now, consider

$$x = \sum_{i=1}^{k} a_i N_i M_i \pmod{n_j}$$

for all $1 \leq j \leq k$.

If $i \neq j$, then by definition of N_i, we have that N_i must have the divisor n_j, so since $n_j \mid a_i N_i M_i$ for all $i \neq j$, we have that $a_i N_i M_i \equiv 0 \pmod{n_j}$ for all $i \neq j$.

Otherwise, if $i = j$, then we have $a_i N_i M_i \equiv a_j N_j M_j \equiv a_j \pmod{n_j}$ because $N_j M_j \equiv 1 \pmod{n_j}$.

Hence,

$$x \equiv \sum_{i=1}^{k} a_i N_i M_i \equiv a_j \pmod{n_j}$$

for all $1 \leq j \leq k$, meaning that x satisfies all of our k congruences, showing the existence of an x.

Now we must prove that x is unique modulo $n_1 n_2 \cdots n_k = \prod_{i=1}^{k} n_i$, which is going be similar to proving uniqueness for two-variable Chinese Remainder Theorem.

For the sake of contradiction, we start with assuming that there are at least two solutions x_1 and x_2 that are different modulo $n_1 n_2 \cdots n_k$, but also satisfy all k congruences. Similar to the proof of 2-variable Chinese Remainder Theorem, we get that $x_1 \equiv x_2 \equiv a_i \pmod{n_i}$ for all $1 \leq i \leq k$, so from this, we get $n_i \mid x_1 - x_2$ for all $1 \leq i \leq k$. Since all n_i are pairwise relatively prime, which was given, we must have that

$$\prod_{i=1}^{k} n_i \mid x_1 - x_2$$

by **Lemma 4.6**, meaning $x_1 \equiv x_2 \pmod{\prod_{i=1}^{k} n_i}$, contradiction. Hence, there can't be some $x_1 \not\equiv x_2 \pmod{\prod_{i=1}^{k} n_i}$ that satisfy all k congruences.

Since we have proven both existence and uniqueness, we are done with the proof of the Chinese Remainder Theorem. □

5. Conclusion

The Chinese Remainder Theorem gives us a finite range for the values that we need to test and look at to find a solution for any amount of congruences. Having such a tool allows us to streamline and organize an otherwise difficult and chaotic computational mess.

The CRT's ability to solve systems of congruences efficiently, particularly when the moduli are pairwise coprime, has made it an invaluable tool in various fields. Its algorithmic approach, involving the computation of modular inverses and the Chinese remainder construction, allows for the determination of a unique solution that satisfies all the congruences.