Number Theory

Jason Sass

July 3, 2023

Natural number system

Peano Axioms for natural number system

Proposition 1. *The successor of a natural number is unique.*

Proof. Let $n \in \mathbb{N}$.

Each natural number has a successor, by the axiom for $\mathbb{N}$, so n has a successor.

Suppose $a' \in \mathbb{N}$ and $b' \in \mathbb{N}$ are successors of n.

Then a' is the concatenation of n and 1 and b' is the concatenation of n and 1.

The concatenation of 1 to n is n followed by 1 and this occurs in exactly one way.

So, any concatenation of n by 1 must be the same.

Therefore, $a' = b'$, so the successor is unique. □

Theorem 2. ***Laws of addition***

Let k, m, n be natural numbers.

1. $m + n = n + m$. (addition is commutative)

2. $(k + m) + n = k + (m + n)$. (addition is associative)

3. Let s be the successor operation on a natural number n.

Then $s(n) = n + 1$.

Proof. We prove 1.

If we combine m ones and n ones, then the order in which we combine doesn't matter if we're interested in just the total number of ones.

Therefore, $m + n = n + m$. □

Proof. We prove 2.

The total number of ones is the same whether we concatenate the ones of the first two numbers and then concatenate the ones from the third number, or whether we concatenate the ones of the second two numbers and then concatenate the ones from the first number.

Therefore, $(k + m) + n = k + (m + n)$. □

Proof. We prove 3.

The successor of n is the natural number formed by the concatenation of n with $|$.

Therefore, $s(n) = n + 1$. □

Theorem 3. ***Laws of multiplication***

Let k, m, n be natural numbers.

1. $mn = nm$. (multiplication is commutative)

2. $(km)n = k(mn)$. (multiplication is associative)

3. $n \times 1 = n$ (multiplicative identity)

Proof. We prove 1.

TODO □

Proposition 4. ***relation $<$ over $\mathbb{N}$ is transitive***

Let $a, b, c \in \mathbb{N}$.

If $a < b$ and $b < c$, then $a < c$.

Proof. Suppose $a < b$ and $b < c$.

Then there exists $x \in \mathbb{N}$ such that $a + x = b$ and there exists $y \in \mathbb{N}$ such that $b + y = c$.

Thus, $c = b + y = (a + x) + y = a + (x + y)$.

Since $\mathbb{N}$ is closed under $+$ and $x, y \in \mathbb{N}$ then $x + y \in \mathbb{N}$.

Hence $a < c$, by definition of $<$.

Therefore, $<$ is transitive. □

Construction of $\mathbb{Z}$

Theorem 5. ***Algebraic properties of addition and multiplication in $\mathbb{Z}$***

1. For all $a, b, c \in \mathbb{Z}$, $(a + b) + c = a + (b + c)$. Addition is associative.

2. For all $a, b \in \mathbb{Z}$, $a + b = b + a$. Addition is commutative.

3. For all $a, b, c \in \mathbb{Z}$, $(ab)c = a(bc)$. Multiplication is associative.

4. For all $a, b \in \mathbb{Z}$, $ab = ba$. Multiplication is commutative.

5. For all $a, b, c \in \mathbb{Z}$, $a(b + c) = ab + ac$. Multiplication is distributive over addition.

Proof. TODO □

Proposition 6. ***Zero is additive identity in $\mathbb{Z}$***

For all $a \in \mathbb{Z}$, $a + 0 = a$.

Proof. TODO □

Proposition 7. ***One is multiplicative identity in $\mathbb{Z}$***

For all $a \in \mathbb{Z}$, $1 \cdot a = a$.

Proof. TODO □

Proposition 8. ***Additive inverse of*** a ***is*** $-a$ ***in*** $\mathbb{Z}$
Let $a \in \mathbb{Z}$.
Then there exists $-a \in \mathbb{Z}$ *such that* $a + (-a) = 0$.

Proof. TODO ☐

Proposition 9. ***The only integers whose product is one are one and negative one.***
Let $a, b \in \mathbb{Z}$.
If $ab = 1$, *then either* $a = b = 1$ *or* $a = b = -1$.

Proof. TODO ☐

Proposition 10. ***Cancellation law for*** $\mathbb{Z}$
Let $a, b, c \in \mathbb{Z}$.
If $c \neq 0$ *and* $ac = bc$, *then* $a = b$.

Proof. TODO ☐

Proposition 11. *For all* $a, b \in \mathbb{Z}$
1. $a > 0$ *iff* $a \in \mathbb{Z}^+$
2. $a < 0$ *iff* $-a \in \mathbb{Z}^+$.
3. $a < b$ *iff* $b - a > 0$.

Proof. We prove 1.
Let $a \in \mathbb{Z}$.
Observe that

$$\begin{aligned} a > 0 &\Leftrightarrow 0 < a \\ &\Leftrightarrow a - 0 \in \mathbb{Z}^+ \\ &\Leftrightarrow a + (-0) \in \mathbb{Z}^+ \\ &\Leftrightarrow a + 0 \in \mathbb{Z}^+ \\ &\Leftrightarrow a \in \mathbb{Z}^+. \end{aligned}$$

Therefore, $a > 0$ iff $a \in \mathbb{Z}^+$. ☐

Proof. We prove 2.
Let $a \in \mathbb{Z}$.
Observe that $a < 0$ iff $0 - a \in \mathbb{Z}^+$ iff $0 + (-a) \in \mathbb{Z}^+$ iff $-a \in \mathbb{Z}^+$.
Therefore, $a < 0$ iff $-a \in \mathbb{Z}^+$. ☐

Proof. We prove 3.
Let $a \in \mathbb{Z}$.
Observe that $a < b$ iff $b - a \in \mathbb{Z}^+$ iff $b - a > 0$.
Therefore, $a < b$ iff $b - a > 0$. ☐

Theorem 12. *$\mathbb{Z}$ **satisfies transitivity and trichotomy laws***

1. $a < a$ is false for all $a \in \mathbb{Z}$. (Therefore, $<$ is not reflexive.)
2. For all $a, b, c \in \mathbb{Z}$, if $a < b$ and $b < c$, then $a < c$. ($<$ is transitive)
3. For every $a \in \mathbb{Z}$, exactly one of the following is true (trichotomy):
i. $a > 0$
ii. $a = 0$
iii. $a < 0$
4. For every $a, b \in \mathbb{Z}$, exactly one of the following is true (trichotomy):
i. $a > b$
ii. $a = b$
iii. $a < b$

Proof. We prove 1.
Let $a \in \mathbb{Z}$.
By the trichotomy axiom for $\mathbb{Z}^+$, $0 \notin \mathbb{Z}^+$, so $a - a \notin \mathbb{Z}^+$.
Therefore, $a \not< a$, by definition of $<$. □

Proof. We prove 2.
Suppose $a < b$ and $b < c$.
Then $b - a \in \mathbb{Z}^+$ and $c - b \in \mathbb{Z}^+$.
Since the sum of positive integers is positive, then $(c - b) + (b - a) \in \mathbb{Z}^+$.
Observe that

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

Therefore, $c - a \in \mathbb{Z}^+$, so $a < c$. □

Proof. We prove 3.
Let $a \in \mathbb{Z}$.
By trichotomy, exactly one of the following is true: $a \in \mathbb{Z}^+$, $a = 0$, $-a \in \mathbb{Z}^+$.
Observe that $a \in \mathbb{Z}^+$ iff $a > 0$ and $-a \in \mathbb{Z}^+$ iff $a < 0$.
Therefore, exactly one of the following is true: $a > 0$, $a = 0$, $a < 0$. □

Proof. We prove 4.
Let $a, b \in \mathbb{Z}$.
Since $\mathbb{Z}$ is a ring, then $\mathbb{Z}$ is closed under subtraction, so $a - b \in \mathbb{Z}$.
By the trichotomy law for axioms of $\mathbb{Z}^+$, exactly one of the following is true: $a - b \in \mathbb{Z}^+$, $a - b = 0$, $-(a - b) \in \mathbb{Z}^+$.
Observe that $a - b \in \mathbb{Z}^+$ iff $b < a$ iff $a > b$.
Observe that $a - b = 0$ iff $a = b$.
Observe that $-(a - b) \in \mathbb{Z}^+$ iff $-a + b \in \mathbb{Z}^+$ iff $b - a \in \mathbb{Z}^+$ iff $a < b$.
Therefore, exactly one of the following is true: $a > b$, $a = b$, $a < b$. □

Theorem 13. ***order is preserved by the ring operations in*** $\mathbb{Z}$

Let $a, b, c \in \mathbb{Z}$.

1. If $a < b$, *then* $a + c < b + c$. *(preserves order for addition)*

2. If $a < b$, *then* $a - c < b - c$. *(preserves order for subtraction)*

3. If $a < b$ *and* $c > 0$, *then* $ac < bc$. *(preserves order for multiplication by a positive integer)*

4. If $a < b$ *and* $c < 0$, *then* $ac > bc$. *(reverses order for multiplication by a negative integer)*

Proof. We prove 1.

Suppose $a < b$.

Then $b - a \in \mathbb{Z}^+$.

Let $c \in \mathbb{Z}$.

Observe that

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

Therefore, $(b + c) - (a + c) \in \mathbb{Z}^+$, so $a + c < b + c$. □

Proof. We prove 2.

Suppose $a < b$.

Then $b - a \in \mathbb{Z}^+$.

Let $c \in \mathbb{Z}$.

Observe that

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

Therefore, $(b - c) - (a - c) \in \mathbb{Z}^+$, so $a - c < b - c$. □

Proof. We prove 3.

Suppose $a < b$ and $c > 0$.

Then $b - a \in \mathbb{Z}^+$ and $c \in \mathbb{Z}^+$.

Since the product of positive integers is a positive integer, then $(b-a)c \in \mathbb{Z}^+$.

Therefore, $(b - a)c = bc - ac \in \mathbb{Z}^+$, so $ac < bc$. □

Proof. We prove 4.

Suppose $a < b$ and $c < 0$.

Then $b - a \in \mathbb{Z}^+$ and $-c \in \mathbb{Z}^+$.

Since the product of positive integers is a positive integer, then $(b-a)(-c) \in \mathbb{Z}^+$.

Observe that

$$\begin{aligned} (b-a)(-c) &= (b+(-a))(-c) \\ &= b(-c)+(-a)(-c) \\ &= -bc+ac \\ &= ac-bc. \end{aligned}$$

Hence, $ac - bc \in \mathbb{Z}^+$, so $bc < ac$.

Therefore, $ac > bc$. ☐

Theorem 14. ***Principle of Mathematical Induction***

Let S be a subset of $\mathbb{Z}^+$ such that

1. $1 \in S$ (basis)

2. for all $k \in \mathbb{Z}^+$, if $k \in S$, then $k+1 \in S$. (induction hypothesis)

Then $S = \mathbb{Z}^+$.

Proof. We prove by contradiction.

Assume $\mathbb{Z}^+ - S \neq \emptyset$.

Since $\mathbb{Z}^+ - S \neq \emptyset$ and $\mathbb{Z}^+ - S \subset \mathbb{Z}^+$, then by the well ordering property of $\mathbb{Z}^+$, the set $\mathbb{Z}^+ - S$ has a least element m, so $m \in \mathbb{Z}^+ - S$ and $m \leq x$ for each $x \in \mathbb{Z}^+ - S$.

Since $m \in \mathbb{Z}^+ - S$, then $m \in \mathbb{Z}^+$ and $m \notin S$.

Since $m \in \mathbb{Z}^+$, then $m \in \mathbb{Z}$ and $m \geq 1$.

Since $1 \in S$ and $m \notin S$, then $m \neq 1$.

Since $m \geq 1$ and $m \neq 1$, then $m > 1$, so $m - 1 > 0$.

Since $m \in \mathbb{Z}$, then $m - 1 \in \mathbb{Z}$.

Since $m - 1 \in \mathbb{Z}$ and $m - 1 > 0$, then $m - 1 \in \mathbb{Z}^+$.

By hypothesis, if $m - 1 \in S$, then $m \in S$, so if $m \notin S$, then $m - 1 \notin S$.

Since $m \notin S$, then we conclude $m - 1 \notin S$.

Since $m - 1 \in \mathbb{Z}^+$ and $m - 1 \notin S$, then $m - 1 \in \mathbb{Z}^+ - S$.

Since $m - m = 0 < 1$, then $m < m + 1$, so $m - 1 < m$.

Thus, there exists $m - 1 \in \mathbb{Z}^+ - S$ such that $m - 1 < m$.

This contradicts the assumption that m is the least element of $\mathbb{Z}^+ - S$.

Hence, $\mathbb{Z}^+ - S = \emptyset$.

Since $\mathbb{Z}^+ = S \cup (\mathbb{Z}^+ - S) = S \cup \emptyset = S$, then $S = \mathbb{Z}^+$, as desired. ☐

Theorem 15. ***Principle of Mathematical Induction(strong)***

Let S be a subset of $\mathbb{Z}^+$ such that

1. $1 \in S$ (basis)

2. for all $k \in \mathbb{Z}^+$, if $1, 2, ..., k \in S$, then $k + 1 \in S$. (strong induction hypothesis)

Then $S = \mathbb{Z}^+$.

Proof. We prove by contradiction.

Assume $\mathbb{Z}^+ - S \neq \emptyset$.

Since $\mathbb{Z}^+ - S \neq \emptyset$ and $\mathbb{Z}^+ - S \subset \mathbb{Z}^+$, then by the well ordering property of $\mathbb{Z}^+$, the set $\mathbb{Z}^+ - S$ has a least element m, so $m \in \mathbb{Z}^+ - S$ and $m \leq x$ for all $x \in \mathbb{Z}^+ - S$.

Since $m \in \mathbb{Z}^+ - S$, then $m \in \mathbb{Z}^+$ and $m \notin S$.

Since $m \in \mathbb{Z}^+$, then $m \in \mathbb{Z}$ and $m \geq 1$.

Since $1 \in S$ and $m \notin S$, then $m \neq 1$.

Since $m \geq 1$ and $m \neq 1$, then $m > 1$, so $m - 1 > 0$.

Since $m \in \mathbb{Z}$, then $m - 1 \in \mathbb{Z}$.

Since $m - 1 \in \mathbb{Z}$ and $m - 1 > 0$, then $m - 1 \in \mathbb{Z}^+$.

Since $m \leq x$ for all $x \in \mathbb{Z}^+ - S$, then if $x \in \mathbb{Z}^+ - S$, then $m \leq x$, so if $x < m$, then $x \notin \mathbb{Z}^+ - S$.

Since $x \in \mathbb{Z}^+ - S$ iff $x \in \mathbb{Z}^+$ and $x \notin S$, then $x \notin \mathbb{Z}^+ - S$ iff either $x \notin \mathbb{Z}^+$ or $x \in S$.

Thus, if $x \notin \mathbb{Z}^+ - S$, then either $x \notin \mathbb{Z}^+$ or $x \in S$.

Hence, if $x \in \mathbb{Z}^+$ and $x \notin \mathbb{Z}^+ - S$, then $x \in S$.

Since $1, 2, ..., m - 1$ are positive integers, then $1, 2, ..., m - 1 \in \mathbb{Z}^+$.

Since $1 < m$ and $2 < m$ and ... and $m-1 < m$, then $1, 2, ..., m-1 \notin \mathbb{Z}^+ - S$.

Thus, $1, 2, ..., m - 1 \in S$.

Since $m - 1 \in \mathbb{Z}^+$, then by hypothesis, if $1, 2, ..., m - 1 \in S$, then $m \in S$.

Therefore, $m \in S$.

Thus, we have $m \in S$ and $m \notin S$, a contradiction

Hence, $\mathbb{Z}^+ - S - \emptyset$.

Since $\mathbb{Z}^+ = S \cup (\mathbb{Z}^+ - S) = S \cup \emptyset = S$, then $S = \mathbb{Z}^+$, as desired. □

Theorem 16. ***Archimedean Property of*** $\mathbb{Z}^+$

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

Then there exists $n \in \mathbb{Z}^+$ such that $nb \geq a$.

Proof. We prove by contradiction.

Suppose $nb < a$ for all $n \in \mathbb{Z}^+$.

Let $S = \{a - nb : n \in \mathbb{Z}^+\}$.

Since $1 \in \mathbb{Z}^+$, then $a - (1)b = a - b \in S$, so $S \neq \emptyset$.

We prove $S \subset \mathbb{Z}^+$.

Let $x \in S$.

Then $x = a - nb$ for some $n \in \mathbb{Z}^+$.

Since $n \in \mathbb{Z}^+$, then $nb < a$, so $a > nb$.

Hence, $a - nb > 0$.

Since $a, b, n \in \mathbb{Z}$ and $\mathbb{Z}$ is closed under subtraction and multiplication, then $a - nb \in \mathbb{Z}$.

Since $a - nb \in \mathbb{Z}$ and $a - nb > 0$, then $a - nb \in \mathbb{Z}^+$, so $x \in \mathbb{Z}^+$.
Therefore, $S \subset \mathbb{Z}^+$.

Since $S \subset \mathbb{Z}^+$ and $S \neq \emptyset$, then by WOP, S has a least element m.
Thus, $m \in S$ and $m \leq x$ for all $x \in S$.

Since $m \in S$, then $m = a - kb$ for some $k \in \mathbb{Z}^+$.
Since $k \in \mathbb{Z}^+$, then $k + 1 \in \mathbb{Z}^+$, so $a - (k + 1)b \in S$.
Since $b \in \mathbb{Z}^+$, then $b \in \mathbb{Z}$ and $b > 0$, so $-b < 0$.
Hence, $a - (k + 1)b = a - kb - b < a - kb = m$, so $a - (k + 1)b < m$.
Thus, there exists $a - (k + 1)b \in S$ such that $a - (k + 1)b < m$.
This contradicts the fact that $m \leq x$ for all $x \in S$.
Therefore, the assumption is false, so there exists $n \in \mathbb{Z}^+$ such that $nb \geq a$. □

Proposition 17. *For all $n \in \mathbb{N}$, $n \geq 1$.*

Proof. We prove the statement $n \geq 1$ for all $n \in \mathbb{N}$ by induction on n.
Let $S = \{n \in \mathbb{N} : n \geq 1\}$.
Basis:
Since $1 \in \mathbb{N}$ and $1 = 1$, then $1 \in S$.
Induction:
Suppose $k \in S$.
Then $k \in \mathbb{N}$ and $k \geq 1$.
The successor of k is $k + 1 \in \mathbb{N}$.
Since $1, k \in \mathbb{N}$ and $1 + k = k + 1$ then $1 < k + 1$ by definition of $<$.
Since $k + 1 \in \mathbb{N}$ and $k + 1 > 1$ then $k + 1 \in S$.
Hence, $k \in S$ implies $k + 1 \in S$.
Since $1 \in S$ and $k \in S$ implies $k + 1 \in S$ for any $k \in S$, then $n \in S$ for any $n \in \mathbb{N}$ by induction.
Therefore, by PMI, $n \geq 1$ for all $n \in \mathbb{N}$. □

Proposition 18. *There is no greatest natural number.*

Proof. Suppose $g \in \mathbb{N}$ is a greatest natural number.
Then $g + 1 \in \mathbb{N}$ is the unique successor of g.
Since $1 \in \mathbb{N}$ and $g + 1 = g + 1$ then $g < g + 1$ by definition of $<$.
Therefore $g + 1 > g$.
Hence there exists a natural number that is larger than a greatest natural number, a contradiction.
Therefore there is no greatest natural number. □

Proposition 19. *Let $a, b, c, d \in \mathbb{Z}^+$.*
If $a < b$ and $c < d$, then $ac < bd$.

Proof. Suppose $a < b$ and $c < d$.

Then there exists $a' \in \mathbb{Z}^+$ such that $a + a' = b$ and there exists $c' \in \mathbb{Z}^+$ such that $c + c' = d$.

Let $e = ac' + a'c + a'c'$.

Since a, a', c, c' are positive integers and $\mathbb{Z}^+$ is closed under addition and multiplication, then e is a positive integer.

Observe that

$$\begin{aligned} ac + e &= ac + (ac' + a'c + a'c') \\ &= (ac + ac') + (a'c + a'c') \\ &= a(c + c') + a'(c + c') \\ &= (a + a')(c + c') \\ &= bd. \end{aligned}$$

Since there exists a positive integer e such that $ac+e = bd$, then $ac < bd$. □

Lemma 20. *Let $a, b \in \mathbb{N}$.*

If $a < b$ then $b \not\leq a$.

Proof. Suppose for the sake of contradiction $b \leq a$.

Then either $b < a$ or $b = a$ by defn of $\leq$.

We consider these cases separately.

Case 1: Suppose $b < a$.

Then $\exists c \in \mathbb{N}$ such that $b + c = a$, by defn of $<$.

Since $a < b$ then $\exists d \in \mathbb{N}$ such that $a + d = b$, by defn of $<$.

Choose $c, d \in \mathbb{N}$ such that $b + c = a$ and $a + d = b$.

Then $b + c + d = b$.

Set $m = c + d$.

Then $b + m = b$.

Since $\mathbb{N}$ is closed under $+$ and $c, d \in \mathbb{N}$ then $c + d \in \mathbb{N}$, so $m \in \mathbb{N}$.

The only solution to $b + m = b$ is $m = 0$.

But $0 \notin \mathbb{N}$, so $m \notin \mathbb{N}$.

Thus we have $m \in \mathbb{N}$ and $m \notin \mathbb{N}$, a contradiction.

Hence, $b \not< a$.

Case 2: Suppose $b = a$.

Since $a < b$ then $\exists c \in \mathbb{N}$ such that $a + c = b$.

Choose $c \in \mathbb{N}$ such that $a + c = b$.

Since $b = a$ then $a + c = a$.

The only solution to $a + c = a$ is $c = 0$.

But, $0 \notin \mathbb{N}$ so $c \notin \mathbb{N}$.

Thus we have $c \in \mathbb{N}$ and $c \notin \mathbb{N}$, a contradiction.

Hence, $b \neq a$.

Both cases show that $b \not< a$ and $b \neq a$.

Thus neither $b < a$ nor $b = a$, so $b \not\leq a$. □

Theorem 21. *$\leq$ is a partial order on $\mathbb{Z}$*

1. *For all $a \in \mathbb{Z}$, $a \leq a$. (Reflexive)*
2. *For all $a, b \in \mathbb{Z}$, if $a \leq b$ and $b \leq a$, then $a = b$. (Anti-symmetric)*
3. *For all $a, b, c \in \mathbb{Z}$, if $a \leq b$ and $b \leq c$, then $a \leq c$. (Transitive)*

Proof. To prove $\leq$ is reflexive, let $a \in \mathbb{Z}$.

Then $a = a$, so either $a = a$ or $a < a$.

Hence, either $a < a$ or $a = a$, so $a \leq a$.

Therefore, $\leq$ is reflexive. □

Proof. To prove $\leq$ is anti-symmetric, we must prove $a \leq b$ and $b \leq a$ implies $a = b$ for all $a, b \in \mathbb{Z}$.

We shall prove the logically equivalent statement $a \leq b$ and $a \neq b$ implies $b \not\leq a$ for all $a, b \in \mathbb{Z}$.

Let $a, b \in \mathbb{Z}$ such that $a \leq b$ and $a \neq b$.

Since $a \leq b$, then either $a < b$ or $a = b$.

Since $a \neq b$, then we conclude $a < b$.

By trichotomy of $\mathbb{Z}$, we have $a \neq b$ and $a \not> b$, so $b \not< a$ and $b \neq a$.

Therefore, $b \not\leq a$, so $\leq$ is anti-symmetric. □

Proof. To prove $\leq$ is transitive, let $a, b, c \in \mathbb{Z}$ such that $a \leq b$ and $b \leq c$.

Then

$$\begin{aligned}
(a \leq b) \wedge (b \leq c) &\rightarrow \\
(a \leq b) \wedge (b < c \vee b = c) &\rightarrow \\
(a \leq b \wedge b < c) \vee (a \leq b \wedge b = c) &\rightarrow \\
((a < b \vee a = b) \wedge b < c) \vee ((a < b \vee a = b) \wedge b = c) &\rightarrow \\
((a < b \wedge b < c) \vee (a = b \wedge b < c)) \vee ((a < b \wedge b = c) \vee (a = b \wedge b = c)) &\rightarrow \\
((a < c) \vee (a < c)) \vee ((a < c) \vee (a = c)) &\rightarrow \\
(a < c) \vee (a < c) \vee (a = c) &\rightarrow \\
(a < c) \vee (a = c) &\rightarrow \\
a \leq c &
\end{aligned}$$

Therefore, $\leq$ is transitive.

Since $\leq$ is reflexive, anti-symmetric, and transitive, then $\leq$ is a partial order. □

Proposition 22. ***No natural number exists between two consecutive natural numbers.***

Let n be a natural number.

There is no $m \in \mathbb{N}$ such that $n < m < n + 1$.

Proof. Suppose there is $m \in \mathbb{N}$ such that $n < m < n + 1$.

Then $n < m$ and $m < n + 1$.

Since $n < m$, then there exists $p \in \mathbb{N}$ such that $n + p = m$.

Thus, $p = m - n$, so $m - n \in \mathbb{N}$.
Since every natural number is greater than or equal to one, then $m - n \geq 1$.
Since $m < n + 1$, then $m - n < 1$.
Since $m - n \in \mathbb{N}$ and $m - n < 1$ and $m - n \geq 1$, then we have a violation of trichotomy.
Therefore, there is no $m \in \mathbb{N}$ such that $n < m < n + 1$. □

Elementary Aspects of Integers

Lemma 23. *Every positive integer is either even or odd.*

Proof. We prove by induction on n.
Let $S = \{n \in \mathbb{Z}^+ : n \text{ is even or } n \text{ is odd}\}$.
Basis:
Since $1 = 2 \cdot 0 + 1$ and 0 is an integer, then 1 is odd.
Since $1 \in \mathbb{Z}^+$ and 1 is odd, then $1 \in S$.
Induction:
Suppose $k \in S$.
Then $k \in \mathbb{Z}^+$ and k is even or k is odd.
Since $k \in \mathbb{Z}^+$, then $k + 1 \in \mathbb{Z}^+$.
Since k is either even or odd, we consider these cases separately.
Case 1: Suppose k is even.
Then $k = 2a$ for some integer a.
Thus, $k + 1 = 2a + 1$, so $k + 1$ is odd.
Case 2: Suppose k is odd.
Then $k = 2b + 1$ for some integer b.
Thus, $k + 1 = (2b + 1) + 1 = 2b + 2 = 2(b + 2)$.
Since $b + 2$ is an integer, then this implies $k + 1$ is even.
Hence, in all cases, either $k + 1$ is even or $k + 1$ is odd.
Since $k + 1 \in \mathbb{Z}^+$ and $k + 1$ is either even or odd, then $k + 1 \in S$.
Therefore, by PMI, $S = \mathbb{Z}^+$. □

Lemma 24. *An integer is not both even and odd.*

Proof. Let n be an integer.
We prove by contradiction.
Suppose n is both even and odd.
Then n is even and n is odd.
Since n is even, then $n = 2k$ for some integer k.
Since n is odd, then $n = 2m + 1$ for some integer m.
Thus, $2k = n = 2m + 1$, so $2k = 2m + 1$.
Hence, $1 = 2k - 2m = 2(k - m)$, so $k - m = \frac{1}{2}$.
Since k and m are integers, then $k - m$ is an integer.
Thus, $\frac{1}{2}$ is an integer, a contradiction.
Therefore, n is not both even and odd. □

Proposition 25. *A positive integer is either even or odd, but not both.*

Proof. Let n be a positive integer.

Then either n is even or n is odd.

Since n is an integer, then n is not both even and odd.

Therefore, n is either even or odd, but not both. □

Proposition 26. ***A product of two consecutive integers is even.***
If $n \in \mathbb{Z}$, then $n(n+1)$ is even.

Proof. Let $n \in \mathbb{Z}$ be given.

Either n is even or n is not even.

We consider these cases separately.

Case 1: Suppose n is even.

Then there exists $m \in \mathbb{Z}$ such that $n = 2m$.

Thus, $n(n+1) = 2m(n+1)$.

Since $m \in \mathbb{Z}$ and $n+1 \in \mathbb{Z}$, then $m(n+1) \in \mathbb{Z}$.

Therefore, $n(n+1)$ is even.

Case 2: Suppose n is not even.

Then n is odd, so there exists $m \in \mathbb{Z}$ such that $n = 2m+1$.

Thus, $n(n+1) = (2m+1)(2m+2) = (2m+1)(2)(m+1) = 2(2m+1)(m+1)$.

Since $m \in \mathbb{Z}$, then $2m+1 \in \mathbb{Z}$ and $m+1 \in \mathbb{Z}$, so $(2m+1)(m+1) \in \mathbb{Z}$.

Therefore, $n(n+1)$ is even.

Hence, in all cases, $n(n+1)$ is even, as desired. □

Natural Number Formulae

Proposition 27. *The sum of the first n natural numbers is $\frac{n(n+1)}{2}$.*

Solution. We let $S_n = 1 + 2 + 3 + ... + n$.

We can reverse the sum of terms and add each pair of corresponding terms of the equation.

Each pair of terms add up to $n+1$. Since we have a total of n terms, then the sum is $n(n+1)$ if we add both equations as below

$$\begin{aligned} S_n &= 1 + 2 + 3 + \cdots + (n) \\ S_n &= n + (n-1) + (n-2) + \cdots + 1 \end{aligned}$$

Thus we get

$$\begin{aligned} 2S_n &= (n+1)n \\ S_n &= \frac{n(n+1)}{2} \end{aligned}$$

So, we've shown that the sum is $\frac{n(n+1)}{2}$. □

Proof. We prove $(\forall n \in \mathbb{N})(\sum_{k=1}^{n} k = \frac{n(n+1)}{2})$ by induction on n.

Let $S = \{n \in \mathbb{N} : \sum_{k=1}^{n} k = \frac{n(n+1)}{2}\}$.

Basis:

Since $1 \in \mathbb{N}$ and $\sum_{k=1}^{1} k = 1 = \frac{1(1+1)}{2}$, then $1 \in S$.
Induction:
Suppose $m \in S$.
Then $m \in \mathbb{N}$ and $\sum_{k=1}^{m} k = \frac{m(m+1)}{2}$.
Since $m \in \mathbb{N}$, then $m + 1 \in \mathbb{N}$.
Observe that

$$\begin{aligned}
\sum_{k=1}^{m+1} k &= \sum_{k=1}^{m} k + (m+1) \\
&= \frac{m(m+1)}{2} + (m+1) \\
&= (m+1)(\frac{m}{2} + 1) \\
&= (m+1)\frac{(m+2)}{2} \\
&= \frac{(m+1)[(m+1)+1]}{2}.
\end{aligned}$$

Since $m + 1 \in \mathbb{N}$ and $\sum_{k=1}^{m+1} = \frac{(m+1)[(m+1)+1]}{2}$, then $m + 1 \in S$.
Therefore, by PMI, $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$ for all $n \in \mathbb{N}$. □

Proposition 28. *The sum of the first n odd natural numbers is n^2.*

Solution. Let S_{odd} = the set of odd natural numbers = $\{1, 3, 5, 7, 9, ...\}$.

The first odd number 1 occurs for $n = 1$, the second odd number 3 occurs for $n = 2$, the third odd number 5 occurs for $n = 3$, the fourth odd number 7 occurs for $n = 4$.

So we see a pattern in which the n^{th} odd number is simply $2n - 1$ using inductive reasoning.

Therefore we really have a sequence $(1, 3, 5, 7, ..., 2n - 1)$ whose n^{th} term is $2n - 1$.

Let (a_n) be the sequence in $\mathbb{R}$ defined by $a_n = 2n - 1$ for all $n \in \mathbb{Z}^+$.

We can make a table of values by plugging in various values to determine if a pattern emerges.

n	sum of first n odd natural numbers
1	$1 = 1^2$
2	$1 + 3 = 4 = 2^2$
3	$1 + 3 + 5 = 9 = 3^2$
4	$1 + 3 + 5 + 7 = 16 = 4^2$
5	$1 + 3 + 5 + 7 + 9 = 25 = 5^2$
...	...
n	$1 + 3 + 5 + 7 + 9 + ... + (2n - 1) = \sum_{i=1}^{n}(2i - 1) = n^2$

Thus our proposition is really asserting that

$$\forall (n \in \mathbb{N}), \sum_{i=1}^{n} (2i - 1) = n^2.$$

Let

$$S_n = \sum_{i=1}^{n}(2i-1).$$

We expand this sum to show the terms

$$S_n = \sum_{i=1}^{n}(2i-1) = 1+3+5+7+\cdots+(2n-1) \qquad (1)$$

We can reverse the sum of terms and add each pair of corresponding terms of Equation 1. Each pair of terms add up to $2n$. Since we have a total of n terms, then the sum is $2n(n)$ if we add both equations as below

$$\begin{aligned} S_n &= 1+3+5+7+\cdots+(2n-1) \\ S_n &= (2n-1)+(2n-3)+(2n-5)+(2n-7)+\cdots+1 \end{aligned}$$

Thus we get

$$\begin{aligned} 2S_n &= 2n(n) \\ S_n &= n^2 \end{aligned}$$

So, we've shown that the sum is n^2. Now we will prove this result using mathematical induction since we have an infinite set of statements to prove (since we're asserting the sum holds true for all natural numbers).

Note that the universally quantified statement $\forall(n \in \mathbb{N}), \sum_{i=1}^{n}(2i-1) = n^2$ is logically equivalent to the conditional implication if $n \in \mathbb{N}$, then $\sum_{i=1}^{n}(2i-1) = n^2$. □

Proof. We must prove $\sum_{k=1}^{n}(2k-1) = n^2$ for all $n \in \mathbb{N}$.

We prove $\sum_{k=1}^{n}(2k-1) = n^2$ for all $n \in \mathbb{N}$ by induction on n.

Let $S = \{n \in \mathbb{N} : \sum_{k=1}^{n}(2k-1) = n^2\}$.

Basis:

Since $1 \in \mathbb{N}$ and $\sum_{k=1}^{1}(2k-1) = 2\cdot 1 - 1 = 2-1 = 1 = 1^2$, then $1 \in S$.

Induction:

Suppose $m \in S$.

Then $m \in \mathbb{N}$ and $\sum_{k=1}^{m}(2k-1) = m^2$.

Since $m \in \mathbb{N}$, then $m+1 \in \mathbb{N}$.

To prove $m+1 \in S$, we must prove $\sum_{k=1}^{m+1}(2k-1) = (m+1)^2$.

Observe that

$$\begin{aligned} \sum_{k=1}^{m+1}(2k-1) &= \sum_{k=1}^{m}(2k-1) + [2(m+1)-1] \\ &= m^2 + (2m+2-1) \\ &= m^2 + (2m+1) \\ &= (m+1)^2, \text{ as desired.} \end{aligned}$$

□

Proposition 29. *The sum of the squares of the first n natural numbers is* $\frac{n(n+1)(2n+1)}{6}$.

Proof. We must prove $\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$ for all $n \in \mathbb{N}$.
We prove by induction on n.
Let $S = \{n \in \mathbb{N} : \sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}\}$.
Basis:
Since $1 \in \mathbb{N}$ and $\sum_{k=1}^{1} k^2 = 1^2 = 1 = \frac{1(1+1)(2\cdot 1+1)}{6}$, then $1 \in S$.
Induction:
Suppose $m \in S$.
Then $m \in \mathbb{N}$ and $\sum_{k=1}^{m} k^2 = \frac{m(m+1)(2m+1)}{6}$.
Since $m \in \mathbb{N}$, then $m+1 \in \mathbb{N}$.
To prove $m+1 \in S$, we must prove $\sum_{k=1}^{m+1} k^2 = \frac{(m+1)[(m+1)+1][2(m+1)+1]}{6}$.
Observe that

$$\begin{aligned}
\sum_{k=1}^{m+1} k^2 &= \sum_{k=1}^{m} k^2 + (m+1)^2 \\
&= \frac{m(m+1)(2m+1)}{6} + (m+1)^2 \\
&= (m+1) \cdot [\frac{m(2m+1)}{6} + (m+1)] \\
&= (m+1) \cdot \frac{(2m^2 + m + 6m + 6)}{6} \\
&= (m+1) \cdot \frac{(2m^2 + 7m + 6)}{6} \\
&= (m+1) \cdot \frac{(m+2)(2m+3)}{6} \\
&= \frac{(m+1)[(m+1)+1][2(m+1)+1]}{6} \text{, as desired.}
\end{aligned}$$

□

Proposition 30. *The sum of the cubes of the first n natural numbers is* $(\frac{n(n+1)}{2})^2$.

Proof. We must prove $\sum_{k=1}^{n} k^3 = \frac{n^2(n+1)^2}{4}$ for all $n \in \mathbb{N}$.
We prove by induction on n.
Let $S = \{n \in \mathbb{N} : \sum_{k=1}^{n} k^3 = \frac{n^2(n+1)^2}{4}\}$.
Basis:
Since $1 \in \mathbb{N}$ and $\sum_{k=1}^{1} k^3 = 1^3 = 1 = \frac{1^2(1+1)^2}{4}$, then $1 \in S$.
Induction:
Suppose $m \in S$.
Then $m \in \mathbb{N}$ and $\sum_{k=1}^{m} k^3 = \frac{m^2(m+1)^2}{4}$.
Since $m \in \mathbb{N}$, then $m+1 \in \mathbb{N}$.
To prove $m+1 \in S$, we must prove $\sum_{k=1}^{m+1} k^3 = \frac{(m+1)^2([m+1)+1]^2}{4}$.

Observe that

$$\begin{aligned}
\sum_{k=1}^{m+1} k^3 &= \sum_{k=1}^{m} k^3 + (m+1)^3 \\
&= \frac{m^2(m+1)^2}{4} + (m+1)^3 \\
&= (m+1)^2 \cdot [\frac{m^2}{4} + (m+1)] \\
&= (m+1)^2 \cdot \frac{(m^2+4m+4)}{4} \\
&= (m+1)^2 \cdot \frac{(m+2)^2}{4} \\
&= \frac{(m+1)^2[(m+1)+1]^2}{4} \text{, as desired.}
\end{aligned}$$

□

Divisibility and greatest common divisor

Proposition 31. *Every integer divides zero.* $(\forall n \in \mathbb{Z})(n|0)$.

Proof. Let n be an arbitrary integer.
Since 0 is an integer and $0 = n \cdot 0$, then $n|0$. □

Proposition 32. *The number 1 divides every integer.* $(\forall n \in \mathbb{Z})(1|n)$.

Proof. Let n be an arbitrary integer.
Since n is an integer and $n = 1 \cdot n$, then $1|n$. □

Proposition 33. *Every integer divides itself.* $(\forall n \in \mathbb{Z})(n|n)$.

Proof. Let n be an arbitrary integer.
Since 1 is an integer and $n = n \cdot 1$, then $n|n$. □

Proposition 34. *Let* $a, b, c, d \in \mathbb{Z}$.
If $a|b$ *and* $c|d$, *then* $ac|bd$.

Proof. Suppose $a|b$ and $c|d$.
Then $b = am$ and $d = cn$ for some integers m and n.
We multiply to obtain $bd = (am)(cn) = a(mc)n = a(cm)n = (ac)(mn)$.
Since mn is an integer, then $ac|bd$. □

Proposition 35. $(\forall a, b \in \mathbb{Z}^*)(a|b \wedge b|a \to a = \pm b)$.

Proof. Let a and b be arbitrary nonzero integers such that $a|b$ and $b|a$.
Since $a|b$, then $b = an_1$ for some integer n_1.
Since $b|a$, then $a = bn_2$ for some integer n_2.
Since $a = bn_2 = (an_1)n_2 = a(n_1n_2)$, then $0 = a(n_1n_2) - a = a(n_1n_2 - 1)$.

Thus, either $a = 0$ or $n_1 n_2 - 1 = 0$.
Since $a \neq 0$, then $n_1 n_2 - 1 = 0$, so $n_1 n_2 = 1$.
The only integers whose product is one are one and negative one.
Therefore, either $n_1 = n_2 = 1$ or $n_1 = n_2 = -1$.
We consider these cases separately.
Case 1: Suppose $n_1 = n_2 = 1$.
Then $a = bn_2 = b(1) = b$.
Case 2: Suppose $n_1 = n_2 = -1$.
Then $a = bn_2 = b(-1) = -b$.
Therefore, in all cases, either $a = b$ or $a = -b$, so $a = \pm b$. □

Theorem 36. ***divides relation is transitive***
For any integers a, b and c, if $a|b$ and $b|c$, then $a|c$.

Proof. Let a, b, and c be arbitrary integers such that $a|b$ and $b|c$.
Then $b = am$ and $c = bn$ for some integers m and n.
Thus, $c = (am)n = a(mn)$.
Since mn is an integer, then $a|c$. □

Theorem 37. *The divides relation defined on $\mathbb{Z}^+$ is a partial order.*

Proof. To prove the divides relation is reflexive, we must prove $a|a$.
Let $a \in \mathbb{Z}^+$ be arbitrary.
Since $a \in \mathbb{Z}^+$ and $\mathbb{Z}^+ \subset \mathbb{Z}$, then $a \in \mathbb{Z}$.
By proposition 33, every integer divides itself, so $a|a$.
Therefore, $|$ is reflexive. □

Proof. To prove the divides relation is antisymmetric, we must prove $a|b$ and $b|a$ implies $a = b$.
Let $a, b \in \mathbb{Z}^+$.
Then $a > 0$ and $b > 0$.
Suppose $a|b$ and $b|a$.
Then there exist integers k_1 and k_2 such that $b = ak_1$ and $a = bk_2$.
Hence, $a = (ak_1)k_2 = a(k_1 k_2)$.
Since $a > 0$, then $a \neq 0$, so we divide by a to get $1 = k_1 k_2$.
The only integers whose product is one are one and negative one.
Therefore, either $k_1 = k_2 = 1$ or $k_1 = k_2 = -1$.

Since $a > 0$ and $b > 0$ and $b = ak_1$, then $k_1 > 0$.
Since $a > 0$ and $b > 0$ and $a = bk_2$, then $k_2 > 0$.
Hence, $k_1 = k_2 = 1$.
Therefore, $a = b(1) = b$, so $a = b$. □

Proof. To prove the divides relation is transitive, we must prove $a|b$ and $b|c$ implies $a|c$.
Let $a, b, c \in \mathbb{Z}^+$.
The divides relation defined on $\mathbb{Z}$ is transitive.
Hence, $x|y$ and $y|z$ implies $x|z$ for all integers x, y, z.

Since $a, b, c \in \mathbb{Z}^+$ and $\mathbb{Z}^+ \subset \mathbb{Z}$, then $a, b, c \in \mathbb{Z}$.
Therefore, $a|b$ and $b|c$ implies $a|c$.

Since the divides relation is reflexive, antisymmetric, and transitive on $\mathbb{Z}^+$, then the divides relation $|$ is a partial order over $\mathbb{Z}^+$. □

Proposition 38. *Let $a, b \in \mathbb{Z}^+$.*
If $a|b$, then $a \leq b$.

Proof. Suppose $a|b$.
Then $b = an$ for some integer n.
Since $a, b \in \mathbb{Z}^+$, then $a > 0$ and $b > 0$.
Since $b = an$ and $a > 0$ and $b > 0$, then $n > 0$.
Since $n \in \mathbb{Z}$ and $n > 0$, then $n \geq 1$, so either $n > 1$ or $n = 1$.
We consider these cases separately.
Case 1: Suppose $n = 1$.
Then $a = a \cdot 1 = an = b$, so $a = b$.
Case 2: Suppose $n > 1$.
Then $0 > 1 - n$.
Since $a > 0$ and $1 - n < 0$, then $a(1 - n) < 0$.
Since $a - b = a - an = a(1 - n) < 0$, then $a - b < 0$, so $a < b$.
Therefore, in all cases, $a \leq b$. □

Proposition 39. *Let $a, d \in \mathbb{Z}$.*
If $d \mid a$, then $d \mid ma$ for all $m \in \mathbb{Z}$.

Proof. Let $m \in \mathbb{Z}$ be arbitrary.
Suppose $d \mid a$.
Then $a = dk$ for some integer k.
Thus, $ma = m(dk) = (md)k = (dm)k = d(mk)$.
Since $m, k \in \mathbb{Z}$ and $\mathbb{Z}$ is closed under multiplication, then $mk \in \mathbb{Z}$.
Therefore, $d \mid ma$. □

Proposition 40. *Let $a, b, n \in \mathbb{Z}$.*
1. *If $a|b$, then $na|nb$.*
2. *If $n \neq 0$, then $na|nb$ implies $a|b$.*

Proof. We prove 1.
Suppose $a|b$.
Then $b = ak$ for some integer k.
Thus, $nb = n(ak) = (na)k$.
Since k is an integer, then $na|nb$. □

Proof. We prove 2.
Suppose $n \neq 0$ and $na|nb$.
Since $na|nb$, then $nb = (na)m$ for some integer m.
Thus, $0 = nb - (na)m = nb - n(am) = n(b - am)$, so either $n = 0$ or $b - am = 0$.

Since $n \neq 0$, then $b - am = 0$, so $b = am$.
Since $m \in \mathbb{Z}$, then $a|b$. □

Theorem 41. ***Division Algorithm***
Let $a, b \in \mathbb{Z}$ with $b > 0$.
Then there exist unique integers q and r such that $a = bq+r$, with $0 \leq r < b$.

Solution. We must prove the statement:
$(\forall a, b \in \mathbb{Z}, b > 0)(\exists! q, r \in \mathbb{Z})(a = bq + r \wedge 0 \leq r < b)$.
Let $a, b \in \mathbb{Z}$ be arbitrary with $b > 0$.
We must prove $(\exists! q, r \in \mathbb{Z})(a = bq + r \wedge 0 \leq r < b)$.
To prove existence we can think about a set of integers for which r could be an element of; ie, let $r = a - bq$. Thus, let us define a set $S = \{a - bk : k \in \mathbb{Z}\}$. If we drew a number line of this sequence of integers: ...,$a - 3b, a - 2b, a - b, a, a + b, a + 2b, a + 3b$,..., then we would see that we would want r to be such that r is non-negative(ie, $r \geq 0$) and we want r to be the smallest such number in this subset of integers. The well ordered principle says that any subset of natural numbers has a smallest element.

The set S is really an arithmetic sequence of integers whose common difference is b; ie, the next element in order from smallest to largest is always the previous element plus b. Thus, any subset can be arranged from smallest to largest. Thus we can apply the Well Ordering Principle to set S if we can show that $S \subset \mathbb{N}$.

Then we let r be the least integer in S.

Note that there exists non-negative integers in set S because we can choose $k \in \mathbb{Z}$ such that $a \geq kb$ which causes $a - kb \geq 0$.

Note that $q + 1 > q$, so if we multiply by $b > 0$, we get $(q + 1)b > qb$. If we then multiply by -1 we get $-(q + 1)b < -qb$.

If we then add a to both sides we get $a - (q + 1)b < a - qb$. This simply shows that $a - qb$ is the next element in the sequence following the element $a - (q + 1)b$. We easily see that this is the case by simply drawing the number line and it becomes obvious that the element $a - (q + 1)b$ is to the left of the element $a - qb$. □

Proof. **Existence:**
Let a and b be arbitrary integers and $b > 0$.
We must prove there exist integers q and r such that $a = bq+r$ and $0 \leq r < b$.
Let $S = \{a - bk : (\exists k \in \mathbb{Z})(a - bk \geq 0)\}$.
Suppose there exists $k \in \mathbb{Z}$ such that $a - bk \geq 0$.
Since $a, b, k \in \mathbb{Z}$, then $a - bk \in \mathbb{Z}$.
Since $a - bk \in \mathbb{Z}$ and $a - bk \geq 0$, then $a - bk$ is a non-negative integer, so S is a subset of non-negative integers.
Either $0 \in S$ or $0 \notin S$.
We consider these cases separately.
Case 1: Suppose $0 \in S$.
Then there is some integer q such that $a - bq = 0$, so $a = bq$.
Let $r = 0$.

Then q and r are integers and $a = bq = bq + 0 = bq + r$, so $a = bq + r$.
Since $r = 0$ and $0 < b$, then $r = 0 < b$, so $0 = r < b$.
Case 2: Suppose $0 \notin S$.
We show that S is not empty.
By the trichotomy property of $\mathbb{Z}$, either $a > 0$ or $a = 0$ or $a < 0$.
We consider these cases separately.
Let $x = a - bk$ for some integer k.
Case 2a: Suppose $a = 0$.
Let $k = -1$.
Then $x = a - bk = 0 - b(-1) = 0 + b = b > 0$.
Since $x = a - bk$ and $x > 0$, then $x \in S$, so $S \neq \emptyset$.
Case 2b: Suppose $a > 0$.
Let $k = 0$.
Then $x = a - bk = a - b(0) = a - 0 = a > 0$.
Since $x = a - bk$ and $x > 0$, then $x \in S$, so $S \neq \emptyset$.
Case 2c: Suppose $a < 0$.
Let $k = 2a$.
Since $a \in \mathbb{Z}$, then $k \in \mathbb{Z}$.
Observe that $x = a - bk = a - b(2a) = a(1 - 2b)$.
Since $b \in \mathbb{Z}$ and $b > 0$, then $b \geq 1$.
Hence, $-2b \leq -2$, so $1 - 2b \leq -1 < 0$.
Since $a < 0$ and $1 - 2b < 0$, then $x = a(1 - 2b) > 0$.
Since $x = a - bk$ and $x > 0$, then $x \in S$, so $S \neq \emptyset$.

Hence, in all cases there is an integer k such that $S \neq \emptyset$.

Since S is a set of non-negative integers and $0 \notin S$, then S is a set of positive integers, so $S \subset \mathbb{Z}^+$.
Since $S \neq \emptyset$ and $S \subset \mathbb{Z}^+$, then by the well ordering principle of $\mathbb{Z}^+$, S has a least element r.
Therefore, $r \in S$ and $r \leq x$ for all $x \in S$.
Since $r \in S$, then there is some integer q such that $r = a - bq$ and $r \geq 0$.
Since $r \geq 0$, then either $r > 0$ or $r = 0$.
Since $0 \notin S$ and $r \in S$, then $r \neq 0$, so $r > 0$.
Since $r = a - bq$, then $a = bq + r$.

Suppose $r \geq b$.
Observe that $a - b(q + 1) = a - bq - b = r - b$.
Since $r \geq b$, then $r - b \geq 0$, so $a - b(q + 1) \geq 0$.
Since $q \in \mathbb{Z}$, then $q + 1 \in \mathbb{Z}$.
Since $q + 1 \in \mathbb{Z}$ and $a - b(q + 1) \geq 0$, then $a - b(q + 1) \in S$.
Since $b > 0$, then $-b < 0$, so $a - bq - b < a - bq$.
Thus, $a - b(q + 1) < a - bq$, so $a - b(q + 1) < r$.
Hence, $a - b(q + 1)$ is an element of S that is smaller than the least element $r \in S$, a contradiction.

Therefore, r cannot be greater than or equal to b, so $r < b$.
Since $0 < r$ and $r < b$, then $0 < r < b$.

Hence, in all cases we have shown the existence of integers q and r such that $a = bq + r$ and $0 \leq r < b$. ☐

Proof. **Uniqueness:**
Suppose there are integers q_1, q_2, r_1, and r_2 such that $a = bq_1 + r_1$ and $a = bq_2 + r_2$ and $0 \leq r_1 < b$ and $0 \leq r_2 < b$.
Since $a = bq_1 + r_1$ and $a = bq_2 + r_2$, then $bq_1 + r_1 = bq_2 + r_2$, so $b(q_1 - q_2) = r_2 - r_1$.
Thus, b divides $r_2 - r_1$, so $r_2 - r_1$ is a multiple of b.

Since $r_2 < b$ and $0 \leq r_1$, then by adding these inequalities we obtain $r_2 < b + r_1$, so $r_2 - r_1 < b$.
Since $r_1 < b$ and $0 \leq r_2$, then by adding these inequalities we obtain $r_1 < b + r_2$, so $-b < r_2 - r_1$.
Thus, $-b < r_2 - r_1 < b$.
The only multiple of b between $-b$ and b is zero, so $r_2 - r_1 = 0$.
Therefore, $r_1 = r_2$.

Observe that $b(q_1 - q_2) = r_2 - r_1 = 0$, so $b(q_1 - q_2) = 0$.
Since $\mathbb{Z}$ is an integral domain, then either $b = 0$ or $q_1 - q_2 = 0$.
Since $b > 0$, then $b \neq 0$.
Thus, $q_1 - q_2 = 0$, so $q_1 = q_2$.
Therefore, r is unique and q is unique. ☐

Theorem 42. ***Any common divisor of*** a ***and*** b ***divides any linear combination of*** a ***and*** b.
Let $a, b, d \in \mathbb{Z}$.
If $d|a$ *and* $d|b$, *then* $d|(ma + nb)$ *for all integers* m *and* n.

Proof. Suppose $d|a$ and $d|b$.
Then there exist integers x and y such that $a = dx$ and $b = dy$.
Let m and n be arbitrary integers.
Then $ma + nb = m(dx) + n(dy) = m(xd) + n(yd) = (mx)d + (ny)d = (mx + ny)d = d(mx + ny)$.
Since $mx + ny$ is an integer, then $d|(ma + nb)$, as desired. ☐

Corollary 43. *Let* $a, b, d \in \mathbb{Z}$.
If $d|a$ *and* $d|b$, *then* $d|(a + b)$ *and* $d|(a - b)$.

Proof. Suppose $d|a$ and $d|b$.
Then d is a common divisor of a and b, so d divides any linear combination of a and b.
Hence, $d|(ma + nb)$ for all integers m and n.
In particular, if $m = 1$ and $n = 1$, then $d|(1 \cdot a + 1 \cdot b)$, so $d|(a + b)$.
If $m = 1$ and $n = -1$, then $d|(1 \cdot a + (-1)b)$, so $d|(a - b)$. ☐

Corollary 44. ***Any common divisor of a finite number of integers divides any linear combination of those integers.***

Let $a_1, a_2, ..., a_n, d \in \mathbb{Z}$.

If $d|a_1$, $d|a_2$, ..., $d|a_n$, *then* $d|(c_1a_1 + c_2a_2 + ... + c_na_n)$ *for any integers* $c_1, c_2, ..., c_n$.

Proof. Suppose $d|a_1$ and $d|a_2$ and ... $d|a_n$.

Since $d|a_1$, then d divides any multiple of a_1, so $d|c_1a_1$ for any integer c_1.

By similar reasoning, $d|c_2a_2$ for any integer c_2 and ... and $d|c_na_n$ for any integer c_n.

Since $d|c_1a_1$, then $c_1a_1 = dk_1$ for some integer k_1.

By similar reasoning, $c_2a_2 = dk_2$ for some integer k_2 and ... and $c_na_n = dk_n$ for some integer k_n.

Observe that

$$\begin{aligned} c_1a_1 + c_2a_2 + ... + c_na_n &= dk_1 + dk_2 + ... + dk_n \\ &= d(k_1 + k_2 + ... + k_n). \end{aligned}$$

Since $k_1 + k_2 + ... + k_n$ is an integer, then this implies d divides $c_1a_1 + c_2a_2 + ... + c_na_n$. □

Theorem 45. ***existence and uniqueness of greatest common divisor***

Let $a, b \in \mathbb{Z}^*$.

Then $\gcd(a, b)$ *exists and is unique.*

Moreover, $\gcd(a, b)$ *is the least positive linear combination of* a *and* b.

Proof. **Existence:**

Let $a, b \in \mathbb{Z}^*$.

We prove there exists a positive integer d such that $d|a$ and $d|b$.

Let S be the set of all positive linear combinations of a and b.

Then $S = \{ma + nb : ma + nb > 0, m, n \in \mathbb{Z}\}$.

Let $m = a$ and $n = 0$.

Then $ma + nb = a^2 + 0 = a^2$.

Since $a \neq 0$, then $a^2 > 0$.

Thus, $a^2 \in S$, so $S \neq \emptyset$.

Since $S \subset \mathbb{Z}^+$ and $S \neq \emptyset$, then by the well ordering principle of $\mathbb{Z}^+$, S contains a least element.

Let d be the least element of S.

Then there exist integers m_0, n_0 such that $d = m_0a + n_0b$ and $d > 0$ and for every $x \in S, d \leq x$.

We prove $d|a$ and $d|b$.

By the Division Algorithm there exist unique integers q and r such that $a = dq + r$ and $0 \leq r < d$.

Either $r > 0$ or $r = 0$.

Suppose $r > 0$.

Then $r = a - dq = a - (m_0a + n_0b)q = a - m_0aq - n_0bq = a(1 - m_0q) + b(-n_0q)$.

Since $1 - m_0 q$ and $-n_0 q$ are integers, then r is a linear combination of a and b.

Hence, $r \in S$.

Thus, $d \leq r$, so $r \geq d$.

Consequently, we have $r < d$ and $r \geq d$, a contradiction.

Therefore, r cannot be greater than zero.

Since either $r > 0$ or $r = 0$, and $r \not> 0$, then $r = 0$.

Therefore, $a = dq$, so $d|a$.

By similar reasoning, $d|b$.

Hence $d|a$ and $d|b$, so d is a common divisor of a and b.

Suppose c is an arbitrary common divisor of a and b.

Then $c|a$ and $c|b$.

Thus there are integers k_1 and k_2 such that $a = ck_1$ and $b = ck_2$.

Hence $d = m_0(ck_1) + n_0(ck_2) = c(m_0k_1) + c(n_0k_2) = c(m_0k_1 + n_0k_2)$.

Since $m_0k_1 + n_0k_2$ is an integer, then $c|d$.

Thus, any common divisor of a and b divides d.

Since d is a common divisor of a and b and any common divisor of a and b divides d, then d is a greatest common divisor of a and b.

Hence, a greatest common divisor of a and b exists. □

Proof. **Uniqueness:**

Suppose $d_1 = \gcd(a, b)$ and $d_2 = \gcd(a, b)$.

Any common divisor of a and b divides a greatest common divisor of a and b.

Since d_1 is a common divisor of a and b and d_2 is a greatest common divisor of a and b, then $d_1|d_2$.

Since d_2 is a common divisor of a and b and d_1 is a greatest common divisor of a and b, then $d_2|d_1$.

Since d_1 and d_2 are positive integers and $d_1|d_2$ and $d_2|d_1$, then by the anti-symmetric property of divisibility, $d_1 = d_2$.

Therefore, a greatest common divisor of a and b is unique. □

Proposition 46. ***Properties of gcd***

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

Then

1. $\gcd(a, 0) = a$.
2. $\gcd(a, 1) = 1$.
3. $\gcd(a, a) = a$.
4. $\gcd(a, b) = \gcd(b, a)$.
5. $\gcd(a, b) = \gcd(-a, b) = \gcd(a, -b) = \gcd(-a, -b)$.
6. $\gcd(ka, kb) = k\gcd(a, b)$ *for all* $k \in \mathbb{Z}^+$.

Proof. We prove 1.

Since $a \in \mathbb{Z}^+$ and $\mathbb{Z}^+ \subset \mathbb{Z}$, then $a \in \mathbb{Z}$.

By proposition 33, every integer divides itself, so $a|a$.

By proposition 31, every integer divides zero, so $a|0$.

Hence, $a|a$ and $a|0$, so a is a common divisor of a and 0.

Suppose c is an arbitrary common divisor of a and 0.

Then $c|a$ and $c|0$, so $c|a$.

Hence, any common divisor of a and 0 divides a.

Since $a \in \mathbb{Z}^+$ and a is a common divisor of a and 0 and any common divisor of a and 0 divides a, then $a = \gcd(a, 0)$. □

Proof. We prove 2.

Since $a \in \mathbb{Z}^+$ and $\mathbb{Z}^+ \subset \mathbb{Z}$, then $a \in \mathbb{Z}$.

By proposition 32, one divides every integer, so $1|a$.

Since $1|a$ and $1|1$, then 1 is a common divisor of a and 1.

Suppose c is an arbitrary common divisor of a and 1.

Then $c|a$ and $c|1$, so $c|1$.

Hence, any common divisor of a and 1 divides 1.

Since $1 \in \mathbb{Z}^+$ and 1 is a common divisor of a and 1 and any common divisor of a and 1 divides 1, then $1 = \gcd(a, 1)$. □

Proof. We prove 3.

Since $a \in \mathbb{Z}^+$ and $\mathbb{Z}^+ \subset \mathbb{Z}$, then $a \in \mathbb{Z}$.

By proposition 33, every integer divides itself, so $a|a$.

Since $a|a$ and $a|a$, then a is a common divisor of a and a.

Suppose c is an arbitrary common divisor of a and a.

Then $c|a$ and $c|a$, so $c|a$.

Hence, any common divisor of a and a divides a.

Since $a \in \mathbb{Z}^+$ and a is a common divisor of a and a and any common divisor of a and a divides a, then $a = \gcd(a, a)$. □

Proof. We prove 4.

Since $a, b \in \mathbb{Z}^+$, then $\gcd(a, b)$ exists and is unique.

Let $d = \gcd(a, b)$.

Then $d \in \mathbb{Z}^+$ and $d|a$ and $d|b$ and if c is any integer such that $c|a$ and $c|b$, then $c|d$.

We prove $\gcd(a, b) = \gcd(b, a)$.

Since $d|a$ and $d|b$, then $d|b$ and $d|a$, so d is a common divisor of b and a.

Suppose c is an arbitrary divisor of b and a.

Then $c|b$ and $c|a$, so $c|a$ and $c|b$.

Hence, $c|d$.

Thus, any common divisor of b and a divides d.

Since $d \in \mathbb{Z}^+$ and d is a common divisor of b and a and any common divisor of b and a divides d, then $d = \gcd(b, a)$. □

Proof. We prove 5.

Since $a, b \in \mathbb{Z}^+$, then $\gcd(a, b)$ exists and is unique.

Let $d = \gcd(a, b)$.

Then $d \in \mathbb{Z}^+$ and $d|a$ and $d|b$ and if c is any integer such that $c|a$ and $c|b$, then $c|d$.

We prove $\gcd(a, b) = \gcd(-a, b)$.
Since $d|a$, then d divides any multiple of a, so d divides $(-1)a = -a$.
Hence, $d|(-a)$.
Since $d|(-a)$ and $d|b$, then d is a common divisor of $-a$ and b.
Suppose c is an arbitrary common divisor of $-a$ and b.
Then $c|(-a)$ and $c|b$.
Since $c|(-a)$, then c divides any multiple of $-a$, so c divides $(-1)(-a) = a$.
Hence, $c|a$.
Since $c|a$ and $c|b$, then $c|d$.
Hence, any common divisor of $-a$ and b divides d.
Since $d \in \mathbb{Z}^+$ and d is a common divisor of $-a$ and b and any common divisor of $-a$ and b divides d, then $d = \gcd(-a, b)$.

We prove $\gcd(a, b) = \gcd(a, -b)$.
Since $d|b$, then d divides any multiple of b, so d divides $(-1)b = -b$.
Hence, $d|(-b)$.
Since $d|a$ and $d|(-b)$, then d is a common divisor of a and $-b$.
Suppose c is an arbitrary common divisor of a and $-b$.
Then $c|a$ and $c|(-b)$.
Since $c|(-b)$, then c divides any multiple of $-b$, so c divides $(-1)(-b) = b$.
Hence, $c|b$.
Since $c|a$ and $c|b$, then $c|d$.
Hence, any common divisor of a and $-b$ divides d.
Since $d \in \mathbb{Z}^+$ and d is a common divisor of a and $-b$ and any common divisor of a and $-b$ divides d, then $d = \gcd(a, -b)$.

We prove $\gcd(a, b) = \gcd(-a, -b)$.
Since $d|a$, then d divides any multiple of a, so d divides $(-1)a = -a$.
Since $d|b$, then d divides any multiple of b, so d divides $(-1)b = -b$.
Hence, $d|(-a)$ and $d|(-b)$, so d is a common divisor of $-a$ and $-b$.
Suppose c is an arbitrary common divisor of $-a$ and $-b$.
Then $c|(-a)$ and $c|(-b)$.
Since $c|(-a)$, then c divides any multiple of $-a$, so c divides $(-1)(-a) = a$.
Hence, $c|a$
Since $c|(-b)$, then c divides any multiple of $-b$, so c divides $(-1)(-b) = b$.
Hence, $c|b$.
Since $c|a$ and $c|b$, then $c|d$.
Hence, any common divisor of $-a$ and $-b$ divides d.
Since $d \in \mathbb{Z}^+$ and d is a common divisor of $-a$ and $-b$ and any common divisor of $-a$ and $-b$ divides d, then $d = \gcd(-a, -b)$. $\square$

Proof. We prove 6.

Let $k \in \mathbb{Z}^+$.

Let $d = \gcd(a, b)$.

Then $d \in \mathbb{Z}^+$ and $d|a$ and $d|b$.

Since $k \in \mathbb{Z}^+$ and $d \in \mathbb{Z}^+$, then $kd \in \mathbb{Z}^+$.

Since $d|a$ and $d|b$, then $kd|ka$ and $kd|kb$.

Therefore, kd is a common divisor of ka and kb.

Suppose c is an arbitrary common divisor of ka and kb.

Then $c|ka$ and $c|kb$.

Since $d = \gcd(a, b)$, then there exist integers m and n such that $d = ma + nb$.

Thus, $kd = k(ma + nb) = kma + knb = mka + nkb$, so kd is a linear combination of ka and kb.

Since $c|ka$ and $c|kb$, then c divides any linear combination of ka and kb, so $c|kd$.

Thus, any common divisor of ka and kb divides kd.

Since $kd \in \mathbb{Z}^+$ and kd is a common divisor of ka and kb and any common divisor of ka and kb divides kd, then $kd = \gcd(ka, kb)$.

Therefore, $\gcd(ka, kb) = kd = k \gcd(a, b)$. ☐

Theorem 47. *Let $a, b \in \mathbb{Z}^*$.*

Let $c \in \mathbb{Z}$.

Then c is a linear combination of a and b iff c is a multiple of $\gcd(a, b)$.

Proof. We prove if c is a linear combination of a and b, then c is a multiple of $\gcd(a, b)$.

Suppose c is a linear combination of a and b.

By theorem 42, any common divisor of a and b divides any linear combination of a and b.

Since $\gcd(a, b)$ is a common divisor of a and b, then $\gcd(a, b)$ divides any linear combination of a and b.

Hence, $\gcd(a, b)$ divides c, so c is a multiple of $\gcd(a, b)$.

Conversely, we prove if c is a multiple of $\gcd(a, b)$, then c is a linear combination of a and b.

Suppose c is a multiple of $\gcd(a, b)$.

Then there exists an integer k such that $c = k \gcd(a, b)$.

Since $\gcd(a, b)$ is the least positive linear combination of a and b, then there exist integers m and n such that $\gcd(a, b) = ma + nb$.

Thus, $c = k(ma + nb) = kma + knb = (km)a + (kn)b$.

Since km and kn are integers, then c is a linear combination of a and b. ☐

Corollary 48. *Let $a, b \in \mathbb{Z}^*$.*

Then $\gcd(a, b) = 1$ iff there exist $m, n \in \mathbb{Z}$ such that $ma + nb = 1$.

Proof. Suppose $\gcd(a, b) = 1$.
Then 1 is the least positive linear combination of a and b.
Hence, there exist integers m and n such that $1 = ma + nb$, as desired.

Conversely, suppose there exist integers m and n such that $ma + nb = 1$.
Then 1 is a linear combination of a and b.
Since 1 is a linear combination of a and b iff 1 is a multiple of $\gcd(a, b)$, then 1 is a multiple of $\gcd(a, b)$.
Therefore, $\gcd(a, b)|1$.
The only positive integer that divides 1 is 1, so $\gcd(a, b) = 1$, as desired. ☐

Corollary 49. *Let $a, b \in \mathbb{Z}^*$ and $d \in \mathbb{Z}^+$.*
If $\gcd(a, b) = d$, then $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$.

Proof. Suppose $\gcd(a, b) = d$.
Then $d \in \mathbb{Z}^+$ and $d|a$ and $d|b$.
Since $d \in \mathbb{Z}^+$, then $d > 0$, so $d \neq 0$.
Since $d|a$ and $d|b$, then $a = dr$ and $b = ds$ for some integers r and s.
Since $\frac{a}{d} = r$ and $\frac{b}{d} = s$, then $\frac{a}{d} \in \mathbb{Z}$ and $\frac{b}{d} \in \mathbb{Z}$.
Since d is the least positive linear combination of a and b, then there exist integers m and n such that $ma + nb = d$.
Since $d \neq 0$, we divide by d to get $m(\frac{a}{d}) + n(\frac{b}{d}) = 1$.
Since $\frac{a}{d} \in \mathbb{Z}$ and $\frac{b}{d} \in \mathbb{Z}$ and $m(\frac{a}{d}) + n(\frac{b}{d}) = 1$, then $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$. ☐

Theorem 50. *Let $a, b, d \in \mathbb{Z}$.*
If $d|ab$ and $(d, a) = 1$, then $d|b$.

Proof. Suppose $d|ab$ and $\gcd(d, a) = 1$.
Since $\gcd(d, a) = 1$, then there exist integers k and m such that $kd + ma = 1$.
Thus, $b = b \cdot 1 = b(kd + ma) = bkd + bma = (bk)d + m(ab)$ is a linear combination of d and ab.
Since $d|d$ and $d|ab$, then d divides any linear combination of d and ab, so $d|b$. ☐

Proposition 51. *Let $a, b, m \in \mathbb{Z}$.*
If $a|m$ and $b|m$ and $\gcd(a, b) = 1$, then $ab|m$.

Proof. Suppose $a|m$ and $b|m$ and $\gcd(a, b) = 1$.
Since $a|m$, then $m = ak_1$ for some $k_1 \in \mathbb{Z}$.
Since $b|m$, then $m = bk_2$ for some $k_2 \in \mathbb{Z}$.
Since $\gcd(a, b) = 1$, then $1 = xa + yb$ for some $x, y \in \mathbb{Z}$.
Observe that

$$
\begin{aligned}
m &= m \cdot 1 \\
&= m(xa + yb) \\
&= mxa + myb \\
&= (bk_2)xa + (ak_1)yb \\
&= ab(k_2x) + ab(k_1y) \\
&= ab(k_2x + k_1y).
\end{aligned}
$$

Since $x, y, k_1, k_2 \in \mathbb{Z}$, then $k_2x + k_1y \in \mathbb{Z}$, so $ab|m$. □

Proof. Suppose $a|m$ and $b|m$ and $\gcd(a, b) = 1$.
Since $b|m$, then there exists an integer k such that $m = bk$.
Since $a|m$, then $a|bk$.
Since $a|bk$ and $\gcd(a, b) = 1$, then $a|k$.
Hence, $ab|kb$, so $ab|bk$.
Therefore, $ab|m$. □

Euclidean Algorithm

Lemma 52. *Let $a, b \in \mathbb{Z}$ and $b > 0$.*
If a is divided by b with remainder r, then $\gcd(a, b) = \gcd(b, r)$.

Proof. Suppose a is divided by b.
By the division algorithm, there exist unique integers q and r such that $a = bq + r$ and $0 \leq r < b$.
Let $d = \gcd(b, r)$.

Then $d \in \mathbb{Z}^+$ and $d|b$ and $d|r$ and if c is any integer such that $c|b$ and $c|r$, then $c|d$.
Since $d|b$ and $d|r$, then d divides any linear combination of b and r.
Since $a = bq + r$ is a linear combination of b and r, then $d|a$.
Since $d|a$ and $d|b$, then d is a common divisor of a and b.

Let c be an arbitrary common divisor of a and b.
Then $c|a$ and $c|b$, so c divides any linear combination of a and b.
Since $r = a - bq$ is a linear combination of a and b, then $c|r$.
Since $c|b$ and $c|r$, then $c|d$, so any common divisor of a and b divides d.

Since $d \in \mathbb{Z}^+$ and d is a common divisor of a and b and any common divisor of a and b divides d, then $d = \gcd(a, b)$.
Therefore, $\gcd(a, b) = d = \gcd(b, r)$. □

Theorem 53. ***Euclidean Algorithm***

Let $a, b \in \mathbb{Z}$ and $b > 0$.

Let n be the number of iterative steps and

$$\begin{aligned} a &= bq_1 + r_1, \text{ where } 0 < r_1 < b \\ b &= r_1 q_2 + r_2, \text{ where } 0 < r_2 < r_1 \\ r_1 &= r_2 q_3 + r_3, \text{ where } 0 < r_3 < r_2 \\ \ldots & \\ r_{k-2} &= r_{k-1} q_k + r_k, \text{ where } 0 < r_k < r_{k-1} \\ \ldots & \\ r_{n-3} &= r_{n-2} q_{n-1} + r_{n-1}, \text{ where } 0 < r_{n-1} < r_{n-2} \\ r_{n-2} &= r_{n-1} q_n + 0. \end{aligned}$$

Then $\gcd(a, b) = r_{n-1}$.

Solution. By the division algorithm, $a = bq_1 + r_1$ and $0 < r_1 < b$, so $\gcd(a, b) = \gcd(b, r_1)$ by lemma 52.

By the division algorithm, $b = r_1 q_2 + r_2$ and $0 < r_2 < r_1$, so $\gcd(b, r_1) = \gcd(r_1, r_2)$ by lemma 52.

We repeat this process a finite number of times.

By the division algorithm, $r_{n-2} = r_{n-1} q_n + r_n$ and $r_n = 0$, so $\gcd(r_{n-2}, r_{n-1}) = \gcd(r_{n-1}, r_n) = \gcd(r_{n-1}, 0) = r_{n-1}$. □

Proof. Let $a, b \in \mathbb{Z}^*$.

On the n^{th} step, the remainder $r_n = 0$, so $r_{n-2} = r_{n-1} q_n$.

Hence $r_{n-1} | r_{n-2}$.

On the $(n-1)$ step $r_{n-3} = r_{n-2} q_{n-1} + r_{n-1}$.

Since $r_{n-1} | r_{n-1}$ and $r_{n-1} | r_{n-2}$, then r_{n-1} divides any linear combination of r_{n-1} and r_{n-2}, so $r_{n-1} | r_{n-3}$.

Similarly, $r_{n-1} | r_{n-4}$ since $r_{n-4} = r_{n-3} q_{n-2} + r_{n-2}$ and $r_{n-1} | r_{n-2}$ and $r_{n-1} | r_{n-3}$.

This continues all the way back to $b = r_1 q_2 + r_2$ and $a = bq_1 + r_1$, so $r_{n-1} | b$ and $r_{n-1} | a$.

Thus r_{n-1} is a common divisor of a and b.

Let d be any common divisor of a and b.

Then $d | a$ and $d | b$, so d divides any linear combination of a and b.

In particular, $d | (a - bq_1)$.

Since $r_1 = a - bq_1$, then this implies $d | r_1$.

Since $d | b$ and $d | r_1$, then d divides any linear combination of b and r_1.

Since $r_2 = b - r_1 q_2$, then this implies $d | r_2$.

Similarly, $r_3 = r_1 - r_2 q_3$, so $d | r_3$.

This continues all the way to r_{n-1} since $r_n = 0$.

Therefore, $d | r_{n-1}$, so any common divisor of a and b divides r_{n-1}.

Since $r_{n-1} \in \mathbb{Z}^+$ and r_{n-1} is a common divisor of a and b and any common divisor of a and b divides r_{n-1}, then by definition of gcd, $r_{n-1} = \gcd(a, b)$.

TODO

We prove the algorithm terminates by induction on the number of remaining steps to finish the computation. □

Least common multiple

Theorem 54. ***existence and uniqueness of least common multiple***

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

The least common multiple of a and b exists and is unique.

Moreover, $lcm(a, b) \cdot \gcd(a, b) = ab$.

Proof. **Existence:**

Since $a \neq 0$ and $b \neq 0$, then $\gcd(a, b)$ exists.

Let $d = \gcd(a, b)$.

Then $d \in \mathbb{Z}^+$ and $d|a$ and $d|b$, so $a = dr$ and $b = ds$ for some integers r and s.

Let $m = \frac{ab}{d}$.

Then $as = a(\frac{b}{d}) = m = (\frac{a}{d})b = rb$.

Since there exist integers s and r such that $m = as$ and $m = rb$, then m is a common multiple of a and b.

Let $c \in \mathbb{Z}$ be any common multiple of a and b.

Then $a|c$ and $b|c$, so $c = au$ and $c = bv$ for some integers u and v.

Since $\gcd(a, b) = d$, then there exist integers x and y such that $d = xa + yb$.

Since $m = \frac{ab}{d}$ and $d \neq 0$, then $dm = ab$.

Since $a \neq 0$ and $b \neq 0$, then $\frac{dm}{ab} = 1$.

Observe that

$$\begin{aligned} c &= c \cdot 1 \\ &= c(\frac{dm}{ab}) \\ &= \frac{c}{ab}(dm) \\ &= \frac{c}{ab}(xa + yb)m \\ &= (\frac{cx}{b} + \frac{cy}{a})m \\ &= (vx + uy)m. \end{aligned}$$

Since $v, x, u, y \in \mathbb{Z}$, then $vx + uy \in \mathbb{Z}$, so $m|c$.

Thus, any common multiple of a and b is a multiple of m.

Since m is a common multiple of a and b and any common multiple of a and b is a multiple of m, then $m = lcm(a, b)$.

Observe that $\gcd(a, b) * lcm(a, b) = dm = ab$. ☐

Proof. **Uniqueness:**

Let m_1 and m_2 be least common multiples of a and b.

Since m_1 is a least common multiple of a and b, then m_1 is a positive integer and $a|m_1$ and $b|m_1$ and for every integer c, if $a|c$ and $b|c$, then $m_1|c$.

Since m_2 is a least common multiple of a and b, then m_2 is a positive integer and $a|m_2$ and $b|m_2$ and for every integer c, if $a|c$ and $b|c$, then $m_2|c$.

If $c = m_1$, then we have $a|m_1$ and $b|m_1$ implies $m_2|m_1$.

Since $a|m_1$ and $b|m_1$, then $m_2|m_1$.

If $c = m_2$, then we have $a|m_2$ and $b|m_2$ implies $m_1|m_2$.

Since $a|m_2$ and $b|m_2$, then $m_1|m_2$.

Since m_1 and m_2 are positive integers and $m_1|m_2$ and $m_2|m_1$, then $m_1 = m_2$ by the antisymmetric property of the divides relation over $\mathbb{Z}^+$.

Therefore, a least common multiple of a and b is unique. ☐

Corollary 55. *Let $a, b \in \mathbb{Z}^+$.*

Then $lcm(a, b) = ab$ iff $\gcd(a, b) = 1$.

Proof. Suppose $lcm(a, b) = ab$.

Since $\gcd(a, b) \cdot lcm(a, b) = ab$, then $\gcd(a, b) = \frac{ab}{lcm(a,b)}$.

Observe that

$$\begin{aligned} \gcd(a, b) &= \frac{ab}{lcm(a, b)} \\ &= \frac{ab}{ab} \\ &= 1. \end{aligned}$$

Therefore, $\gcd(a, b) = 1$, as desired.

Conversely, suppose $\gcd(a, b) = 1$.

Since $\gcd(a, b) \cdot lcm(a, b) = ab$, then $lcm(a, b) = \frac{ab}{\gcd(a,b)}$.

Observe that

$$\begin{aligned} lcm(a, b) &= \frac{ab}{\gcd(a, b)} \\ &= \frac{ab}{1} \\ &= ab. \end{aligned}$$

Therefore, $lcm(a, b) = ab$, as desired. ☐

Proposition 56. ***Properties of lcm***

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

Then

1. $lcm(a, 0) = 0$.
2. $lcm(a, 1) = a$.
3. $lcm(a, a) = a$.
4. $lcm(a, b) = lcm(b, a)$.
5. $lcm(ka, kb) = k \cdot lcm(a, b)$ *for all* $k \in \mathbb{Z}^+$.
6. $\gcd(a, b) \mid lcm(a, b)$.
7. $\gcd(a, b) = lcm(a, b)$ *iff* $a = b$.
8. $a|b$ *iff* $\gcd(a, b) = a$ *iff* $lcm(a, b) = b$.

Proof. We prove 1.

Since every integer divides zero, then $a|0$.

Since every integer divides itself, then $0|0$.

Thus, $a|0$ and $0|0$, so 0 is a multiple of a and 0.

Let $m \in \mathbb{Z}$ such that $a|m$ and $0|m$.

Then $0|m$, so any multiple of a and 0 is a multiple of 0.

Since 0 is a multiple of a and 0 and any multiple of a and 0 is a multiple of 0, then $0 = lcm(a, 0)$. □

Proof. We prove 2.

Since every integer divides itself, then $a|a$.

Since one divides every integer, then $1|a$.

Thus, $a|a$ and $1|a$, so a is a multiple of a and 1.

Let $m \in \mathbb{Z}$ such that $a|m$ and $1|m$.

Then $a|m$, so any multiple of a and 1 is a multiple of a.

Since a is a multiple of a and 1 and any multiple of a and 1 is a multiple of a, then $a = lcm(a, 1)$. □

Proof. We prove 3.

Since every integer divides itself, then $a|a$.

Since $a|a$ and $a|a$, then a is a multiple of a and a.

Let $m \in \mathbb{Z}$ such that $a|m$ and $a|m$.

Then $a|m$, so any multiple of a and a is a multiple of a.

Since a is a multiple of a and a and any multiple of a and a is a multiple of a, then $a = lcm(a, a)$. □

Proof. We prove 4.

Let $m = lcm(a, b)$.

Since $m = lcm(a, b)$, then $a|m$ and $b|m$ and for every $c \in \mathbb{Z}$, if $a|c$ and $b|c$, then $m|c$.

Since $a|m$ and $b|m$, then $b|m$ and $a|m$, so m is a multiple of b and a.

Let c be any multiple of b and a.

Then $b|c$ and $a|c$, so $a|c$ and $b|c$.

Hence, $m|c$.

Thus, any multiple of b and a is a multiple of m.

Therefore, $m = lcm(b, a)$. □

Proof. We prove 5.

Let $k \in \mathbb{Z}^+$.

Observe that

$$\begin{aligned} lcm(ka, kb) &= \frac{(ka)(kb)}{\gcd(ka, kb)} \\ &= \frac{kakb}{k \gcd(a, b)} \\ &= \frac{akb}{\gcd(a, b)} \\ &= \frac{kab}{\gcd(a, b)} \\ &= k \cdot lcm(a, b). \end{aligned}$$

Therefore, $lcm(ka, kb) = k \cdot lcm(a, b)$. ☐

Proof. We prove 6.

Let $d = \gcd(a, b)$.

Let $m = lcm(a, b)$.

We must prove $d \mid m$.

Since $d = \gcd(a, b)$, then d is a common divisor of a and b, so d is a divisor of a.

Thus, $d|a$.

Since $m = lcm(a, b)$, then m is a multiple of a and b, so m is a multiple of a.

Hence, $a|m$.

Since $d|a$ and $a|m$, then $d|m$, as desired. ☐

Proof. We prove 7.

We prove if $a = b$, then $\gcd(a, b) = lcm(a, b)$.

Suppose $a = b$.

Then

$$\begin{aligned} \gcd(a, b) &= \gcd(a, a) \\ &= a \\ &= lcm(a, a) \\ &= lcm(a, b). \end{aligned}$$

Therefore, $\gcd(a, b) = lcm(a, b)$.

Conversely, we prove if $\gcd(a, b) = lcm(a, b)$, then $a = b$.

Suppose $\gcd(a, b) = lcm(a, b)$.

Let $d = \gcd(a, b)$.

Then $d = lcm(a, b)$.

Since $d = \gcd(a, b)$, then d is a common divisor of a and b, so $d|a$ and $d|b$.

Since $d = lcm(a, b)$, then d is a common multiple of a and b, so $a|d$ and $b|d$.

Since $a, d \in \mathbb{Z}^+$ and $a|d$ and $d|a$, then by the antisymmetric property of $|$, $a = d$.

Since $b, d \in \mathbb{Z}^+$ and $b|d$ and $d|b$, then by the antisymmetric property of $|$, $b = d$.

Therefore, $a = d = b$, so $a = b$. □

Proof. We prove 8.

We prove $a|b$ iff $\gcd(a, b) = a$.

Suppose $a|b$.

Since every integer divides itself, then $a|a$.

Since $a|a$ and $a|b$, then a is a common divisor of a and b.

Let c be an arbitrary common divisor of a and b.

Then $c|a$ and $c|b$, so $c|a$.

Hence, any common divisor of a and b divides a.

Since $a \in \mathbb{Z}^+$ and a is a common divisor of a and b and any common divisor of a and b divides a, then $a = \gcd(a, b)$.

Conversely, suppose $\gcd(a, b) = a$.

Then a is a common divisor of a and b, so a is a divisor of b.

Therefore, $a|b$.

We prove $\gcd(a, b) = a$ iff $lcm(a, b) = b$.

Suppose $\gcd(a, b) = a$.

Then

$$\begin{aligned} lcm(a, b) &= \frac{ab}{\gcd(a, b)} \\ &= \frac{ab}{a} \\ &= b. \end{aligned}$$

Therefore, $lcm(a, b) = b$.

Conversely, suppose $lcm(a, b) = b$.

Then

$$\begin{aligned} \gcd(a, b) &= \frac{ab}{lcm(a, b)} \\ &= \frac{ab}{b} \\ &= a. \end{aligned}$$

Therefore, $\gcd(a, b) = a$.

We prove $a|b$ iff $lcm(a,b) = b$.

Since $a|b$ iff $\gcd(a,b) = a$ and $\gcd(a,b) = a$ iff $lcm(a,b) = b$, then $a|b$ iff $lcm(a,b) = b$. ☐

Prime Numbers and Fundamental Theorem of Arithmetic

Lemma 57. ***A composite number has a positive divisor other than 1 or itself.***

Let $n \in \mathbb{Z}^+$.

Then n is composite iff there exists $d \in \mathbb{Z}^+$ with $1 < d < n$ such that $d|n$.

Proof. Suppose n is composite.

Then $n \neq 1$ and n is not prime.

Since n is not prime, then there is some positive divisor of n other than 1 or n.

Hence, there exists $d \in \mathbb{Z}^+$ such that $d|n$ and $d \neq 1$ and $d \neq n$.

Since $d \in \mathbb{Z}^+$ and $d \neq 1$, then $d > 1$.

Since $d, n \in \mathbb{Z}^+$ and $d|n$, then $d \leq n$ by proposition 38.

Since $d \leq n$ and $d \neq n$, then $d < n$.

Since $1 < d$ and $d < n$, then $1 < d < n$.

Therefore, there exists $d \in \mathbb{Z}^+$ with $1 < d < n$ such that $d|n$. ☐

Proof. Conversely, suppose there exists $d \in \mathbb{Z}^+$ with $1 < d < n$ such that $d|n$.

Since $0 < 1 < d < n$, then $1 < d$ and $d < n$ and $1 < n$ and $0 < d$.

Since $d > 1$, then $d \neq 1$.

Since $d < n$, then $d \neq n$.

Since $n > 1$, then $n \neq 1$.

Since $n \in \mathbb{Z}^+$ and $n \neq 1$, then n is a positive integer other than 1.

Since $d \in \mathbb{Z}^+$ and $d|n$ and $d \neq 1$ and $d \neq n$, then there is a positive divisor of n other than 1 or n.

Since n is a positive integer other than 1 and there is a positive divisor of n other than 1 or n, then n is not prime.

Since n is a positive integer other than 1 and n is not prime, then n is composite. ☐

Proposition 58. ***A composite number is composed of smaller positive factors.***

Let $n \in \mathbb{Z}^+$.

Then n is composite iff there exist $a, b \in \mathbb{Z}^+$ with $1 < a < n$ and $1 < b < n$ such that $n = ab$.

Proof. Suppose n is composite.

Then there exists $a \in \mathbb{Z}^+$ with $1 < a < n$ such that $a|n$ by lemma 57.

Since $0 < 1 < a < n$, then $1 < a$ and $a < n$ and $1 < n$ and $0 < a$ and $0 < n$.

Since $a|n$, then there exists $b \in \mathbb{Z}$ such that $n = ab$.

Since $n > 0$ and $a > 0$, then $b > 0$.
Since $b \in \mathbb{Z}$ and $b > 0$, then $b \in \mathbb{Z}^+$.

Since $a > 1$ and $b > 0$, then $n = ab > b$, so $n > b$.
Since $ab = n > a$, then $ab > a$.
Since $a > 0$, then we divide to obtain $b > 1$.

Since $1 < b$ and $b < n$, then $1 < b < n$.
Therefore, there exist $a, b \in \mathbb{Z}^+$ with $1 < a < n$ and $1 < b < n$ such that $n = ab$. □

Proof. Conversely, suppose there exists $a, b \in \mathbb{Z}^+$ with $1 < a < n$ and $1 < b < n$ such that $n = ab$.
Since $b \in \mathbb{Z}^+$ and $\mathbb{Z}^+ \subset \mathbb{Z}$, then $b \in \mathbb{Z}$.
Since $b \in \mathbb{Z}$ and $n = ab$, then $a|n$.
Since $a \in \mathbb{Z}^+$ and $1 < a < n$ and $a|n$, then n is composite by lemma 57. □

Proposition 59. *Every integer greater than 1 has a prime factor.*

Proof. Let $n \in \mathbb{Z}$ and $n > 1$.
We must prove n has a prime factor.
Either n is prime or n is not prime.
We consider these cases separately.
Case 1: Suppose n is prime.
Since n is prime and $n|n$, then n is a prime factor of n.
Case 2: Suppose n is not prime.
Since $n \in \mathbb{Z}$ and $n > 1$ and n is not prime, then n is composite.
Thus, there exists $d \in \mathbb{Z}^+$ with $1 < d < n$ and $d|n$ by lemma 57.

Let $S = \{s \in \mathbb{Z}^+ : 1 < s < n, s|n\}$.
Since $d \in \mathbb{Z}^+$ and $1 < d < n$ and $d|n$, then $d \in S$, so $S \neq \emptyset$.
Since $S \subset \mathbb{Z}^+$ and $S \neq \emptyset$, then by the well-ordering principle of $\mathbb{Z}^+$, S has a least element p.
Thus, $p \in S$ and $p \leq s$ for all $s \in S$.
Since $p \in S$, then $p \in \mathbb{Z}^+$ and $1 < p < n$ and $p|n$.
Since $1 < p < n$, then $1 < p$ and $p < n$.
Since $p > 1$, then $p \neq 1$.
Since $p \in \mathbb{Z}^+$ and $p \neq 1$, then p is either prime or not prime.

Suppose p is not prime.
Since $p \in \mathbb{Z}^+$ and $p \neq 1$ and p is not prime, then p must be composite.
Therefore, there exists $a \in \mathbb{Z}^+$ with $1 < a < p$ and $a|p$ by lemma 57.
Since $1 < a < p$, then $1 < a$ and $a < p$.
Since $a|p$ and $p|n$, then $a|n$.
Since $1 < a$ and $a < p$ and $p < n$, then $1 < a < p < n$, so $1 < a < n$.
Since $a \in \mathbb{Z}^+$ and $1 < a < n$ and $a|n$, then $a \in S$.

Hence, $a \in S$ and $a < p$.
But, this contradicts the fact that p is the least element of S.
Therefore, p must be prime.

Since p is prime and $p|n$, then p is a prime factor of n. □

Proof. Let $p(n)$ be the predicate n has a prime factor and $n > 1$ defined over $\mathbb{Z}^+$.
We prove $p(n)$ is true for all integers $n > 1$ by strong induction on n.
Basis:
Since $2|2$ and 2 is prime, then 2 is a prime factor of 2, so 2 has a prime factor.
Since $2 \in \mathbb{Z}^+$ and $2 > 1$ and 2 has a prime factor, then $p(2)$ is true.
Induction:
For any integer $k \geq 3$, assume $p(n)$ is true for $n = 2, 3, ..., k-1$.
Then $p(m)$ is true for any integer m such that $2 \leq m \leq k-1$.
Thus, $p(m)$ is true for any integer m such that $1 < m < k$.
Since $k - 1 \in \mathbb{Z}$, then $k \in \mathbb{Z}$.
Since $k \geq 3 > 1$, then $k > 1$.
To prove $p(k)$ is true, we must prove k has a prime factor.
Since $k \in \mathbb{Z}^+$ and $k > 1$, then either k is prime or k is composite.
We consider these cases separately.
Case 1: Suppose k is prime.
Since k is prime and $k|k$, then k is a prime factor of k, so k has a prime factor.
Case 2: Suppose k is composite.
Then there exists $d \in \mathbb{Z}^+$ such that $d|k$ and $1 < d < k$ by lemma 57.
Since $d \in \mathbb{Z}$ and $1 < d < k$, then by the induction hypothesis, $p(d)$ is true, so d has a prime factor.
Therefore, there exists a prime q such that $q|d$.
Since $q|d$ and $d|k$, then $q|k$.
Since q is prime and $q|k$, then q is a prime factor of k, so k has a prime factor. □

Theorem 60. ***Euclid's Theorem***
There are infinitely many prime numbers.

Proof. Suppose there are finitely many prime numbers.
Let $p_1, p_2, ..., p_s$ be these prime numbers.
Let $n = p_1 p_2 \cdots p_s + 1$.
Since each prime is positive, then $p_1 p_2 \cdots p_s > 0$, so $n = p_1 p_2 \cdots p_s + 1 > 0 + 1 = 1$.
Hence, $n > 1$, so the integer n has a prime factor p by proposition 59.
This prime factor p must be one of $p_1, p_2, ..., p_s$.
Since p is a factor of n, then $p|n$.
Since p is one of the factors of the product $p_1 p_2 \cdots p_s$, then p divides $p_1 p_2 \cdots p_s$.

Since $p|n$ and $p|(p_1p_2\cdots p_s)$, then p divides any linear combination of n and $p_1p_2\cdots p_s$.

Since $1 = n - p_1p_2\cdots p_s$ is a linear combination of n and $p_1p_2\cdots p_s$, then p must divide 1.

But, there is no prime that divides 1, since each prime is greater than 1.

Therefore, there are not finitely many prime numbers, so there are infinitely many prime numbers. ☐

Proof. Let $S = \{p_1, p_2, ..., p_n\}$ be a finite set of primes.

We show that there exist primes that are not in S.

Let $p = p_1 * p_2 * ... * p_n$.

Let $q = p + 1$.

Either q is prime or not.

We consider these cases separately.

We consider two cases.

Case 1: Suppose q is prime.

Then q is greater than each of the primes in S, so q is not one of the primes in S.

Hence, there exists some prime that is not in S.

Case 2: Suppose q is not prime.

Then q has some prime factor, say r.

Thus, $r|q$.

Suppose for the sake of contradiction that $r \in S$.

Then r is one of the factors of p, so $r|p$.

Since $r|p$ and $r|q$, then r divides any linear combination of p and q.

Thus, since $1 = q - p$, then $r|1$.

Hence, $r = 1$.

But, r is prime so $r \neq 1$.

Therefore, $r \notin S$.

Hence, there exists some prime that is not in S.

Both cases show that for any finite set of primes, there exists some prime number that is not contained in it.

Therefore, there must be infinitely many prime numbers. ☐

Proof. Suppose for the sake of contradiction that there are only finitely many prime numbers.

Then we can list all the prime numbers as $p_1, p_2, p_3, ...p_n$, where $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7$, and so on.

Thus p_n is the nth and largest prime number.

Now consider the number $a = (p_1p_2p_3\cdots p_n) + 1$, that is a is the product of all prime numbers, plus 1.

Now a, like any natural number greater than 1, has at least one prime divisor (by proposition 59) and that means $p_k \mid a$ for at least one of our n prime numbers p_k.

Thus there is an integer c for which $a = cp_k$, which is to say

$$(p_1p_2p_3\cdots p_{k-1}p_kp_{k+1}\cdots p_n) + 1 = cp_k.$$

Dividing both sides of this by p_k gives us

$$(p_1p_2p_3 \cdots p_{k-1}p_{k+1} \cdots p_n) + \frac{1}{p_k} = c,$$

so

$$\frac{1}{p_k} = c - (p_1p_2p_3 \cdots p_{k-1}p_{k+1} \cdots p_n).$$

The expression on the right is an integer, while the expression on the left is not an integer. These numbers can't be equal, so this is a contradiction. □

Proof. Suppose for the sake of contradiction that there exist finitely many primes.

Then we could list all the primes.

Let $p_1, p_2, ..., p_n$ be a listing where each p_i is prime.

To derive at a contradiction we construct a number which is not in the list and which must be prime.

Let $p = p_1p_2 * * * p_n + 1$.

Clearly, p is not in the list and each p_i divides the product $p_1p_2 * * * p_n$.

Therefore, none of the p_i can divide p.

For if a certain p_i divided both p and $p_1p_2 * * * p_n$, then p_i would divide their difference $p - p_1p_2 * * * p_n = 1$.

Hence, $p_i|1$ which implies $p_i = 1$.

But, 1 is not prime contradicting the assumption p_i is prime.

Hence, p is not divisible by any prime, so p itself must be prime. □

Lemma 61. *Let $p, n \in \mathbb{Z}^+$.*

If p is prime, then either $p|n$ or $\gcd(p, n) = 1$.

Proof. Suppose p is prime and $p \nmid n$.

We prove $\gcd(p, n) = 1$.

Since p is prime, then $p \neq 1$ and the only positive divisors of p are 1 and p.

Since $p, n \in \mathbb{Z}$ and 1 divides every integer, then $1|p$ and $1|n$, so 1 is a common divisor of p and n.

Let c be any positive common divisor of p and n.

Then $c \in \mathbb{Z}^+$ and $c|p$ and $c|n$.

Since the only positive divisors of p are 1 and p and c is a positive divisor of p, then either $c = 1$ or $c = p$.

Since $p \nmid n$ and $c|n$, then $c \neq p$, so $c = 1$.

Since $1|1$ and $c = 1$, then $c|1$, so any common positive divisor of p and n divides 1.

Since 1 is a common divisor of p and n and any common positive divisor of p and n divides 1, then $\gcd(p, n) = 1$, as desired. □

Lemma 62. ***Euclid's Lemma***

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

If p is prime and $p|ab$, then either $p|a$ or $p|b$.

Proof. Suppose p is prime and $p|ab$.

Either $\gcd(p, a) = 1$ or $\gcd(p, a) \neq 1$.

We consider these cases separately.

Case 1: Suppose $\gcd(p, a) = 1$.

Since $p|ab$ and $\gcd(p, a) = 1$, then $p|b$, by proposition 50.

Case 2: Suppose $\gcd(p, a) \neq 1$.

Let $d = \gcd(p, a)$.

Then $d \neq 1$, so $d > 1$.

Since d is a common divisor of p and a, then $d|p$ and $d|a$.

Since p is prime, then the only positive divisors of p are 1 and p.

Since $d|p$ and $d \neq 1$, then this implies $d = p$.

Since $d|a$, then this implies $p|a$. □

Proof. Suppose p is prime and $p|ab$ and $p \nmid a$.

We prove $p|b$.

If p is prime, then either $p|a$ or $\gcd(p, a) = 1$ by lemma 61.

Thus, if p is prime and $p \nmid a$, then $\gcd(p, a) = 1$.

Since p is prime and $p \nmid a$, then we conclude $\gcd(p, a) = 1$.

Since $p|ab$ and $\gcd(p, a) = 1$, then $p|b$, by proposition 50. □

Corollary 63. *Let $p, a_1, a_2, ..., a_n \in \mathbb{Z}^+$.*

If p is prime and $p|a_1a_2...a_n$, then $p|a_k$ for some integer k with $1 \leq k \leq n$.

Proof. We prove by induction on n, the number of factors in the product $a_1a_2...a_n$.

Let $S = \{n \in \mathbb{Z}^+ :$ if p is prime and $p|a_1a_2...a_n$, then $p|a_k$ for some integer k with $1 \leq k \leq n\}$.

Basis:

If p is prime and $p|a_1$, then $p|a_1$, so $p|a_k$ for integer $k = 1$ with $1 \leq k \leq 1$.

Therefore, $1 \in S$.

If p is prime and $p|a_1a_2$, then by Euclid's lemma, either $p|a_1$ or $p|a_2$, so $p|a_k$ for some integer k with $1 \leq k \leq 2$.

Therefore, $2 \in S$.

Induction:

Suppose $m \in S$.

Then $m \in \mathbb{Z}^+$ and if p is prime and $p|a_1a_2...a_m$, then $p|a_k$ for some integer k with $1 \leq k \leq m$.

Since $m \in \mathbb{Z}^+$, then $m + 1 \in \mathbb{Z}^+$.

Suppose p is prime and $p|a_1a_2...a_ma_{m+1}$.

Since p is prime and $p|(a_1a_2...a_m)a_{m+1}$, then by Euclid's lemma, either $p|a_1a_2...a_m$ or $p|a_{m+1}$.

We consider each case separately.

Case 1: Suppose $p|a_{m+1}$.

Let $k = m + 1$.

Then $k \in \mathbb{Z}$ and $1 \leq k = m + 1$.

Case 2: Suppose $p|a_1a_2...a_m$.

Since p is prime and $p|a_1a_2...a_m$, then by the induction hypothesis, $p|a_k$ for some integer k with $1 \leq k \leq m$.

Hence, in either case, if p is prime and $p|(a_1a_2...a_m)a_{m+1}$, then $p|a_k$ for some integer k with $1 \leq k \leq m+1$, so $m+1 \in S$.

Since $m \in S$ implies $m+1 \in S$, then by PMI, if p is prime and $p|a_1a_2...a_n$, then $p|a_k$ for some integer k with $1 \leq k \leq n$ for all $n \in \mathbb{Z}^+$. □

Corollary 64. *Let $p, q_1, q_2, ..., q_n \in \mathbb{Z}^+$.*

If $p, q_1, q_2, ..., q_n$ are all prime and $p|q_1q_2...q_n$, then $p = q_k$ for some integer k with $1 \leq k \leq n$.

Proof. Suppose $p, q_1, q_2, ..., q_n$ are all prime and $p|q_1q_2...q_n$.

Since $p, q_1, q_2, ..., q_n$ are all prime, then p is prime and $q_1, q_2, ..., q_n$ are all prime.

Since p is prime and $p|q_1q_2...q_n$, then $p|q_k$ for some integer k with $1 \leq k \leq n$, by corollary 63.

Since $q_1, q_2, ..., q_n$ are all prime and $1 \leq k \leq n$, then q_k is prime, so the only positive divisors of q_k are 1 and q_k.

Since $p \in \mathbb{Z}^+$ and $p|q_k$, then this implies either $p = 1$ or $p = q_k$.

Since p is prime, then $p > 1$, so $p \neq 1$.

Therefore, $p = q_k$. □

Theorem 65. ***Fundamental Theorem of Arithmetic(Existence)***

Every integer greater than one can be represented as a product of one or more primes.

Proof. Let $n \in \mathbb{Z}^+$ and $n > 1$.

Then either n is prime or n is composite.

We consider these cases separately.

Case 1: Suppose n is prime.

Then n is a product of one prime(itself).

Case 2: Suppose n is composite.

Then there exists $d \in \mathbb{Z}^+$ with $1 < d < n$ such that $d|n$, by lemma 57.

Let $S = \{d \in \mathbb{Z}^+ : d > 1 \wedge d|n\}$.

Then $S \subset \mathbb{Z}^+$ and $S \neq \emptyset$, so S has a least element $p_1 \in S$, by the well ordering principle of $\mathbb{Z}^+$.

We claim p_1 must be prime.

Suppose p_1 is not prime.

Since $p_1 \in S$, then $p_1 > 1$ and $p_1|n$.

Since p_1 is not prime and $p_1 \neq 1$, then p_1 is composite, so there exists $q \in \mathbb{Z}^+$ with $1 < q < p_1$ such that $q|p_1$, by lemma 57.

Since $q|p_1$ and $p_1|n$, then $q|n$.

Since $q \in \mathbb{Z}^+$ and $q > 1$ and $q|n$, then $q \in S$.

But $q \in S$ and $q < p_1$ contradicts the fact that p_1 is the least element of S.

Therefore, p_1 is prime.

Since n is composite and $p_1|n$ and a composite number has smaller positive factors by proposition 58, then there exists $n_1 \in \mathbb{Z}^+$ such that $n = p_1 n_1$ with $1 < n_1 < n$.

Since $n_1 > 1$, then either n_1 is prime or n_1 is composite.

If n_1 is prime, then $n = p_1 n_1$ is a product of primes.

If n_1 is composite, we repeat the same argument to produce another prime number p_2 such that $n_1 = p_2 n_2$ with $1 < n_2 < n_1$ for some $n_2 \in \mathbb{Z}^+$.

Since $n_2 > 1$, then either n_2 is prime or n_2 is composite.

If n_2 is prime, then $n = p_1 n_1 = p_1(p_2 n_2) = p_1 p_2 n_2$ is a product of primes.

If n_2 is composite, then we repeat the same argument to produce another prime number p_3 such that $n_2 = p_3 n_3$ with $1 < n_3 < n_2$ for some $n_3 \in \mathbb{Z}^+$.

Since $n_3 > 1$, then either n_3 is prime or n_3 is composite.

If n_3 is prime, then $n = p_1 n_1 = p_1(p_2 n_2) = p_1 p_2(p_3 n_3) = p_1 p_2 p_3 n_3$ is a product of primes.

If n_3 is composite, then we repeat the same argument.

Eventually this process must end, since the decreasing sequence $n > n_1 > n_2 > ... > 1$ cannot continue indefinitely.

Hence, after a finite number of steps, n_{k-1} is prime, say p_k.

Therefore, $n = p_1 p_2 \cdots p_k$ is a product of primes. □

Proof. **Existence:**

We prove every integer greater than one can be represented as a product of one or more primes.

Let $p(n)$ be the predicate n is a product of one or more primes and $n > 1$ defined over $\mathbb{Z}^+$.

To prove n is a product of one or more primes, we prove $p(n)$ is true for all positive integers $n > 1$ by strong induction on n.

Basis:

Since 2 is prime, then 2 is product of one prime(itself).

Since $2 \in \mathbb{Z}^+$ and $2 > 1$ and 2 is a product of one prime, then $p(2)$ is true.

Induction:

For an integer $k \geq 3$, assume $p(n)$ is true for $n = 2, 3, ..., k-1$.

Then $p(m)$ is true for any integer m such that $2 \leq m \leq k-1$.

Hence, $p(m)$ is true for any integer m such that $1 < m < k$.

Since $k - 1 \in \mathbb{Z}$, then $k \in \mathbb{Z}$.

Since $k \geq 3 > 1$, then $k > 1$.

To prove $p(k)$ is true, we must prove k is a product of one or more primes.

Since $k \in \mathbb{Z}^+$ and $k > 1$, then either k is prime or k is composite.

We consider these cases separately.

Case 1: Suppose k is prime.

Then k is a product of one prime(itself).

Case 2: Suppose k is composite.

Then there exists $a, b \in \mathbb{Z}^+$ such that $k = ab$ and $1 < a < k$ and $1 < b < k$ by lemma 58.

Since $a \in \mathbb{Z}$ and $1 < a < k$, then by the induction hypothesis, $p(a)$ is true.

Thus, a is a product of one or more primes, so there exist primes $p_1, p_2, ..., p_s$ such that $a = p_1 p_2 ... p_s$.

Since $b \in \mathbb{Z}$ and $1 < b < k$, then by the induction hypothesis, $p(b)$ is true.

Thus, b is a product of one or more primes, so there exist primes $q_1, q_2, ..., q_t$ such that $b = q_1 q_2 ... q_t$.

Therefore, $k = ab = (p_1 p_2 ... p_s)(q_1 q_2 ... q_t)$ is a product of primes. □

Theorem 66. ***Fundamental Theorem of Arithmetic(Unique Factorization)***

The representation of any integer greater than one as a product of primes is unique up to the order of the factors.

Proof. **Uniqueness:**

Let $n \in \mathbb{Z}^+$ and $n > 1$.

Then n can be represented as a product of primes.

Suppose n is represented as a product of primes in two ways.

Let $n = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$, where p_i and q_j are all primes and $p_1 \leq p_2 \leq \dots \leq p_r$ and $q_1 \leq q_2 \dots \leq q_s$ and $r \leq s$.

Since p_1 divides $n = q_1 q_2 \dots q_s$ and p_1 and all q_j are primes, then by corollary 64, $p_1 = q_k$ for some integer k with $1 \leq k \leq s$.

Since $q_k \geq q_1$ and $p_1 = q_k$, then $p_1 \geq q_1$.

Since q_1 divides $n = p_1 p_2 \dots p_r$ and q_1 and all p_i are primes, then by corollary 64, $q_1 = p_m$ for some integer m with $1 \leq m \leq r$.

Since $p_m \geq p_1$ and $q_1 = p_m$, then $q_1 \geq p_1$.

Since $p_1 \leq q_1$ and $q_1 \leq p_1$, then $p_1 = q_1$, by the anti-symmetric property of $\leq$ on $\mathbb{Z}^+$.

Thus, we may cancel the factor $p_1 = q_1$ to obtain $p_2 p_3 \dots p_r = q_2 q_3 \dots q_s$.

We repeat this process to obtain $p_2 = q_2$, and thus $p_3 p_4 \dots p_r = q_3 q_4 \dots q_s$.

We continue this process.

Since $r \leq s$, then either $r < s$ or $r = s$.

Suppose $r < s$.

Then eventually we will reach $1 = q_{r+1} q_{r+2} \dots q_s$.

Since each q_j is prime, then each q_j is greater than one, so the product $q_{r+1} q_{r+2} \dots q_s$ must be greater than one.

This contradicts $q_{r+1} q_{r+2} \dots q_s = 1$.

Hence, r cannot be less than s, so $r = s$.

Therefore, $p_1 = q_1$ and $p_2 = q_2$ and ... and $p_r = q_s = q_r$, so n is represented as a product of primes in only one way. □

Proof. **Uniqueness:**

Let $a \in \mathbb{Z}$ and $a > 1$.

Then a can be represented as a product of primes, by FTA existence theorem 65.

Let $a = p_1p_2...p_{n_1}$ and $a = q_1q_2...q_{n_2}$ be two such representations where $p_1, p_2, ..., p_{n-1}$ and $q_1, q_2, ..., q_{n_2}$ are all primes and $p_1 \leq p_2 \leq ... \leq p_{n_1}$ and $q_1 \leq q_2 \leq ... \leq q_{n_2}$.

To prove the prime factorization of a is unique, we must prove $n_1 = n_2$ and $p_m = q_m$ for each integer m such that $1 \leq m \leq n_1$.

We prove by strong induction on a.

Let $x(a)$ be the predicate over $\mathbb{Z}^+$ defined by:

If $p_1, p_2, ..., p_{n_1}$ and $q_1, q_2, ..., q_{n_2}$ are all primes and $p_1 \leq p_2 \leq ... \leq p_{n_1}$ and $q_1 \leq q_2 \leq ... \leq q_{n_2}$ and $a = p_1p_2...p_{n_1}$ and $a = q_1q_2...q_{n_2}$, then $n_1 = n_2$ and $p_m = q_m$ for each integer m such that $1 \leq m \leq n_1$.

Basis:

Since 2 is prime, then the only prime factor of 2 is 2 itself, so $1 = n_1 = n_2$ and $2 = p_1 = q_1$.

Since p_1 and q_1 are prime and $2 = p_1$ and $2 = q_1$ and $n_1 = n_2$ and $p_1 = q_1$, then $x(2)$ is true.

Induction:

For an integer $a \geq 3$, assume $x(n)$ is true for $n = 2, 3, ..., a - 1$.

Then $x(m)$ is true for any integer m such that $2 \leq m \leq a - 1$.

Hence, $x(m)$ is true for any integer m such that $1 < m < a$.

Since $a - 1 \in \mathbb{Z}$, then $a \in \mathbb{Z}$.

To prove $x(a)$ is true, we must prove:

If $p_1, p_2, ..., p_{n_1}$ and $q_1, q_2, ..., q_{n_2}$ are all primes and $p_1 \leq p_2 \leq ... \leq p_{n_1}$ and $q_1 \leq q_2 \leq ... \leq q_{n_2}$ and $a = p_1p_2...p_{n_1}$ and $a = q_1q_2...q_{n_2}$, then $n_1 = n_2$ and $p_m = q_m$ for each integer m such that $1 \leq m \leq n_1$.

Suppose $p_1, p_2, ..., p_{n_1}$ and $q_1, q_2, ..., q_{n_2}$ are all primes and $p_1 \leq p_2 \leq ... \leq p_{n_1}$ and $q_1 \leq q_2 \leq ... \leq q_{n_2}$ and $a = p_1p_2...p_{n_1}$ and $a = q_1q_2...q_{n_2}$.

Either a is prime or not.

We consider these cases separately.

Case 1: Suppose a is prime.

Then the only prime factor of a is a itself, so $1 = n_1 = n_2$ and $a = p_1 = q_1$.

Since p_1 and q_1 are prime and $a = p_1$ and $a = q_1$ and $n_1 = n_2$ and $p_1 = q_1$, then $x(a)$ is true.

Case 2: Suppose a is not prime.

We must prove $n_1 = n_2$ and $p_m = q_m$ for each integer m such that $1 \leq m \leq n_1$.

Since a is not prime, then a has at least two prime factors, so $n_1 > 1$ and $n_2 > 1$.

Since $q_1 | q_1q_2...q_{n_2}$ and $q_1q_2...q_{n_2} = a = p_1p_2...p_{n_1}$, then $q_1 | p_1p_2...p_{n_1}$.

Since q_1 and $p_1, p_2, ..., p_{n-1}$ are all prime and $q_1 | p_1p_2...p_{n_1}$, then by Euclid's corollary, $q_1 = p_r$ for some integer r with $1 \leq r \leq n_1$.

Since $a = p_1p_2...p_{n_1}$, then $p_1 | a$.

Since $p_1 | a$ and $a = q_1q_2...q_{n_2}$, then $p_1 | q_1q_2...q_{n_2}$.

Since p_1 and $q_1, q_2, ..., q_{n_2}$ are all prime and $p_1 | q_1q_2...q_{n_2}$, then by Euclid's corollary, $p_1 = q_s$ for some integer s with $1 \leq s \leq n_2$.

Since $p_1 \leq p_2 \leq ... \leq p_{n_1}$ and $1 \leq r \leq n_1$, then $p_1 \leq p_r$.
Since $q_1 \leq q_2 \leq ... \leq q_{n_2}$ and $1 \leq s \leq n_2$, then $q_1 \leq q_s$.
Since $p_1 \leq p_r$ and $p_r = q_1$, then $p_1 \leq q_1$.
Since $q_1 \leq q_s$ and $q_s = p_1$, then $q_1 \leq p_1$.
Since $p_1 \leq q_1$ and $q_1 \leq p_1$, then by the antisymmetric property of $\leq$, we have $p_1 = q_1$.

Since $p_1, a \in \mathbb{Z}^+$ and $p_1|a$, then $p_1 \leq a$.
Since p_1 is prime and a is not prime, then $p_1 \neq a$.
Since $p_1 \leq a$ and $p_1 \neq a$, then $p_1 < a$.
Since p_1 is prime, then $p_1 > 1$.
Since $p_1|a$, then $\frac{a}{p_1} \in \mathbb{Z}$.
Since $p_1 < a$ and $p_1 > 0$, then $1 < \frac{a}{p_1}$.
Since $p_1 > 1$ and $a > 0$, then $ap_1 > a$, so $a > \frac{a}{p_1}$.
Since $1 < \frac{a}{p_1} < a$ and $\frac{a}{p_1} = p_2p_3...p_{n_1} = q_2q_3...q_{n_2}$, then $1 < \frac{a}{p_1} = (p_2p_3...p_{n_1}) = (q_2q_3...q_{n_2}) < a$.
Thus, the products $p_2p_3...p_{n_1}$ and $q_2q_3...q_{n_2}$ are prime decompositions of the same integer $\frac{a}{p_1}$.
Since $1 < \frac{a}{p_1} < a$, then by the induction hypothesis, the integer $\frac{a}{p_1}$ has a unique factorization, so $n_1 = n_2$ and $p_m = q_m$ for each integer m with $2 \leq m \leq n_1$.
Since $p_1 = q_1$ and $p_m = q_m$ for each integer m with $2 \leq m \leq n_1$, then $p_m = q_m$ for each integer m such that $1 \leq m \leq n_1$.
Therefore, $n_1 = n_2$ and $p_m = q_m$ for each integer m such that $1 \leq m \leq n_1$, as desired. □

Corollary 67. ***Every integer greater than one has a unique canonical prime factorization***

Every integer $n > 1$ can be written uniquely in a canonical form $n = p_1^{e_1}p_2^{e_2}...p_k^{e_k}$, where for each $i = 1, 2, ..., k$, each exponent e_i is a positive integer and each p_i is a prime with $p_1 < p_2 < ... < p_k$.

Proof. Let $n \in \mathbb{Z}$ and $n > 1$.
By FTA, n can be represented as a product of primes unique up to the order of the factors of n.
Let S be the set of distinct primes in the prime factorization of n.
Then $S = \{p_1, p_2, ..., p_k\}$, where each p_i is a distinct prime factor in the prime factorization of n.
Let these distinct prime factors be ordered such that $p_1 < p_2 < ... < p_k$.
Let e_i be the number of occurrences of prime p_i in the prime factorization of n.
Then e_i is a positive integer and $n = p_1^{e_1}p_2^{e_2}...p_k^{e_k}$. □

Linear Diophantine Equations

Theorem 68. ***Existence of a solution to linear Diophantine equation***

Let $a, b, c \in \mathbb{Z}$ with $a \neq 0$ and $b \neq 0$.

A solution $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ to the linear diophantine equation $ax + by = c$ exists if and only if $\gcd(a, b) \mid c$.

Proof. Let $d = \gcd(a, b)$.

Suppose $d|c$.

Since c is a linear combination of a and b if and only if $d|c$, then c is a linear combination of a and b.

Hence, there exist integers x_0 and y_0 such that $ax_0 + by_0 = c$, as desired.

Conversely, suppose there exist integers x_0 and y_0 such that $ax_0 + by_0 = c$.

Then c is a linear combination of a and b.

Since $d|c$ if and only if c is a linear combination of a and b, then $d|c$.

Therefore, $\gcd(a, b) \mid c$, as desired. □

Corollary 69. ***Characterization of solution to linear Diophantine equation***

Let $a, b, c \in \mathbb{Z}$ with $a \neq 0$ and $b \neq 0$.

If $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$ is a particular solution to the linear Diophantine equation $ax + by = c$, then a general solution is given by $x = x_0 + (\frac{b}{d})t$ and $y = y_0 - (\frac{a}{d})t$ for $t \in \mathbb{Z}$, where $d = \gcd(a, b)$.

Proof. Suppose (x_0, y_0) is a particular solution to the linear diophantine equation $ax + by = c$.

Then $x_0 \in \mathbb{Z}$ and $y_0 \in \mathbb{Z}$ and $ax_0 + by_0 = c$.

Let (x', y') be another solution to the equation.

Then $x' \in \mathbb{Z}$ and $y' \in \mathbb{Z}$ and $ax' + by' = c$.

Thus, $ax' + by' = c = ax_0 + by_0$, so $ax' + by' = ax_0 + by_0$.

Hence, $a(x' - x_0) = ax' - ax_0 = by_0 - by' = b(y_0 - y')$, so $a(x' - x_0) = b(y_0 - y')$.

Let $d = \gcd(a, b)$.

Then $d \in \mathbb{Z}^+$ and $d|a$ and $d|b$, so $a = dr$ and $b = ds$ for some integers r and s.

Thus, $(dr)(x' - x_0) = (ds)(y_0 - y')$.

Since $d \neq 0$, then we divide to obtain $r(x' - x_0) = s(y_0 - y')$, so $r|s(y_0 - y')$.

Since $d = \gcd(a, b)$, then $1 = \gcd(\frac{a}{d}, \frac{b}{d}) = \gcd(r, s)$.

Since $r|s(y_0 - y')$ and $\gcd(r, s) = 1$, then $r|(y_0 - y')$, so $y_0 - y' = rt$ for some integer t.

Hence, $y' = y_0 - rt = y_0 - (\frac{a}{d})t$.

Thus, $r(x' - x_0) = s(y_0 - y') = srt$.

Since $d > 0$ and $a > 0$ and $a = dr$, then $r > 0$, so $r \neq 0$.

Hence, we divide by r to obtain $x' - x_0 = st$, so $x' = x_0 + st = x_0 + (\frac{b}{d})t$.

Therefore, $x' = x_0 + (\frac{b}{d})t$ and $y' = y_0 - (\frac{a}{d})t$.

We verify x' and y' satisfy the equation.
Observe that

$$\begin{aligned}
ax' + by' &= a[x_0 + (\frac{b}{d})t] + b[y_0 - (\frac{a}{d})t] \\
&= ax_0 + (\frac{ab}{d})t + by_0 - (\frac{ab}{d})t \\
&= (ax_0 + by_0) + (\frac{ab}{d})t - (\frac{ab}{d})t \\
&= (ax_0 + by_0) + (\frac{ab}{d} - \frac{ab}{d})t \\
&= c + 0 \cdot t \\
&= c.
\end{aligned}$$

□

Congruences

Theorem 70. *Let $n \in \mathbb{Z}^+$.*
Let $a, b \in \mathbb{Z}$.
Then $a \equiv b \pmod{n}$ if and only if a and b leave the same remainder when divided by n.

Proof. We first prove if a and b leave the same remainder when divided by n then $a \equiv b \pmod{n}$.
By the division algorithm there exist unique integers q_1, q_2, r_1, r_2 such that $a = nq_1 + r_1$ and $0 \leq r_1 < n$ and $b = nq_2 + r_2$ and $0 \leq r_2 < n$.
Suppose $r_1 = r_2$.
Then $a - nq_1 = b - nq_2$, so $a - b = nq_1 - nq_2 = n(q_1 - q_2)$.
Since $q_1 - q_2 \in \mathbb{Z}$, then $n|(a - b)$, so $a \equiv b \pmod{n}$. □

Proof. Conversely, we prove if $a \equiv b \pmod{n}$ then a and b leave the same remainder when divided by n.
Suppose $a \equiv b \pmod{n}$.
Then $n|(a - b)$, so $a - b = nk$ for some integer k.
Thus, $a = nk + b$.
By the division algorithm there exist unique integers q, r such that $b = nq+r$.
Thus, r is the remainder when b is divided by n.
Hence, $a = nk + (nq + r) = nk + nq + r = n(q + k) + r$.
Since $a = n(q + k) + r$, then by the division algorithm, r is the unique remainder when a is divided by n.
Thus, r is the remainder when each of a and b is divided by n.
Therefore, a and b leave the same remainder when divided by n. □

Theorem 71. *The congruence modulo relation is an equivalence relation over $\mathbb{Z}$.*

Proof. Let $n \in \mathbb{Z}^+$ and $a, b, c \in \mathbb{Z}$.

Let $R = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : n|(a - b)\}$.

Since $R \subset \mathbb{Z} \times \mathbb{Z}$, then R is the congruence modulo n relation over $\mathbb{Z}$.

Since every integer divides zero, then in particular, $n|0$.

Hence, $n|a - a$, so $a \equiv a \pmod{n}$.

Therefore, R is reflexive.

Suppose $a \equiv b \pmod{n}$.

Then $n|(a - b)$, so $a - b = nk$ for some integer k.

Thus, $b - a = -(nk) = n(-k)$.

Since $-k$ is an integer, then $n|(b - a)$, so $b \equiv a \pmod{n}$.

Hence, $a \equiv b \pmod{n}$ implies $b \equiv a \pmod{n}$, so R is symmetric.

Suppose $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$.

Then $n|a-b$ and $n|b-c$, so there exist integers k_1 and k_2 such that $a-b = nk_1$ and $b - c = nk_2$.

Adding these equations we obtain $a - c = (a - b) + (b - c) = nk_1 + nk_2 = n(k_1 + k_2)$.

Since $k_1 + k_2 \in \mathbb{Z}$, then this implies $n|a - c$, so $a \equiv c \pmod{n}$.

Therefore, $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ imply $a \equiv c \pmod{n}$, so R is transitive.

Since R is reflexive, symmetric, and transitive, then R is an equivalence relation over $\mathbb{Z}$. ☐

Theorem 72. *Let $n \in \mathbb{Z}^+$.*

Let $a, b, c, d \in \mathbb{Z}$.

If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then

1. $a + c \equiv b + d \pmod{n}$ (addition)

2. $a - c \equiv b - d \pmod{n}$ (subtraction)

3. $ac \equiv bd \pmod{n}$. (multiplication)

Proof. Suppose $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$.

Then $n|a - b$ and $n|c - d$.

Thus, there exist integers k_1 and k_2 such that

$$a - b = nk_1 \quad (2)$$

$$c - d = nk_2 \quad (3)$$

Adding these equations we get $(a + c) - (b + d) = n(k_1 + k_2)$.

Since $k_1 + k_2$ is an integer, then $n|(a + c) - (b + d)$.

Therefore, $a + c \equiv b + d \pmod{n}$.

Subtracting these equations we get $(a - c) - (b - d) = n(k_1 - k_2)$.

Since $k_1 - k_2$ is an integer, then $n|(a - c) - (b - d)$.

Therefore, $a - c \equiv b - d \pmod{n}$.

Multiplying the first equation by c we get $ac - bc = nk_1c$.

Multiplying the second equation by b we get $bc - bd = bnk_2$.

We add these equations to get $ac - bd = nk_1c + bnk_2 = n(k_1c + bk_2)$.
Since $k_1c + bk_2$ is an integer, then $n|ac - bd$.
Therefore, $ac \equiv bd \pmod{n}$. □

Theorem 73. *Let $n \in \mathbb{Z}^+$.*
Let $a, b \in \mathbb{Z}$.
1. If $a \equiv b \pmod{n}$, then $a + c \equiv b + c \pmod{n}$ for all $c \in \mathbb{Z}$. (addition preserves congruence)
2. If $a \equiv b \pmod{n}$, then $ac \equiv bc \pmod{n}$ for all $c \in \mathbb{Z}$. (multiplication preserves congruence)
3. If $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$ for all $k \in \mathbb{Z}^+$. (exponentiation preserves congruence)

Proof. We prove 1.
Suppose $a \equiv b \pmod{n}$.
Let $c \in \mathbb{Z}$.
Since $a \equiv b \pmod{n}$, then $n|a - b$.
Since $a - b = a - c + c - b = a + c - c - b = a + c - b - c = (a + c) - (b + c)$, then $n|(a + c) - (b + c)$.
Therefore, $a + c \equiv b + c \pmod{n}$. □

Proof. We prove 2.
Suppose $a \equiv b \pmod{n}$.
Let $c \in \mathbb{Z}$.
Since $a \equiv b \pmod{n}$, then $n|a - b$, so n divides any multiple of $a - b$.
Thus, $n|(a - b)c$, so $n|(ac - bc)$.
Therefore, $ac \equiv bc \pmod{n}$. □

Proof. We prove 3.
Suppose $a \equiv b \pmod{n}$.
We prove $a^k \equiv b^k \pmod{n}$ for all $k \in \mathbb{Z}^+$ by induction on k.
Let $p(k)$: be the predicate $a^k \equiv b^k \pmod{n}$ defined over $\mathbb{Z}^+$.
Basis:
Since $a \equiv b \pmod{n}$, then $a^1 \equiv b^1 \pmod{n}$, so $p(1)$ is true.
Induction:
Let $k \in \mathbb{Z}^+$ such that $p(k)$ is true.
Then $a^k \equiv b^k \pmod{n}$.
Since $a \equiv b \pmod{n}$, then $a^k a \equiv b^k b \pmod{n}$, so $a^{k+1} \equiv b^{k+1} \pmod{n}$.
Thus, $p(k + 1)$ is true, so $p(k)$ implies $p(k + 1)$ for all $k \in \mathbb{Z}^+$.
By induction, we conclude $p(k)$ is true for all $k \in \mathbb{Z}^+$.
Therefore, $a^k \equiv b^k \pmod{n}$ for all $k \in \mathbb{Z}^+$. □

Theorem 74. *Let $n \in \mathbb{Z}^+$.*
Let $a, b, c \in \mathbb{Z}$.
1. If $a + c \equiv b + c \pmod{n}$, then $a \equiv b \pmod{n}$. (cancellation addition)
2. If $ac \equiv bc \pmod{n}$ and $d = \gcd(n, c)$, then $a \equiv b \pmod{\frac{n}{d}}$. (cancellation multiplication)

Proof. We prove 1.

Suppose $a + c \equiv b + c \pmod{n}$.

Then $n|(a + c) - (b + c)$, so $n|a - b$.

Therefore, $a \equiv b \pmod{n}$. □

Proof. We prove 2.

Suppose $ac \equiv bc \pmod{n}$ and $d = \gcd(n, c)$.

Since $ac \equiv bc \pmod{n}$, then $n|ac - bc$, so $ac - bc = nk$ for some integer k.

Thus, $nk = (a - b)c$.

Since $\gcd(n, c) = d$, then $\gcd(\frac{n}{d}, \frac{c}{d}) = 1$, by corollary 49.

Since $\frac{(a-b)c}{d} = \frac{nk}{d}$, then $\frac{n}{d}$ divides $\frac{(a-b)c}{d}$.

Since $\frac{n}{d}$ divides $\frac{(a-b)c}{d}$ and $\gcd(\frac{n}{d}, \frac{c}{d}) = 1$, then $\frac{n}{d}$ divides $a - b$, by theorem 50.

Therefore, $a \equiv b \pmod{\frac{n}{d}}$. □

Corollary 75. *Let $n \in \mathbb{Z}^+$.*

Let $a, b, c \in \mathbb{Z}$.

If $ac \equiv bc \pmod{n}$ and $\gcd(n, c) = 1$, then $a \equiv b \pmod{n}$. (cancellation multiplication relatively prime)

Proof. Suppose $ac \equiv bc \pmod{n}$ and $\gcd(n, c) = 1$.

By the previous theorem, part 2, if $ac \equiv bc \pmod{n}$ and $\gcd(n, c) = 1$, then $a \equiv b \pmod{\frac{n}{1}}$.

Therefore, if $ac \equiv bc \pmod{n}$ and $\gcd(n, c) = 1$, then $a \equiv b \pmod{n}$. □

Proof. Suppose $ac \equiv bc \pmod{n}$ and $\gcd(n, c) = 1$.

Since $ac \equiv bc \pmod{n}$, then $n|ac - bc$, so $n|c(a - b)$.

Since $n|c(a - b)$ and $\gcd(n, c) = 1$, then $n|a - b$, by theorem 50.

Therefore, $a \equiv b \pmod{n}$. □

Corollary 76. *Let $p \in \mathbb{Z}^+$.*

Let $a, b, c \in \mathbb{Z}$.

If $ac \equiv bc \pmod{p}$ and p is prime and $p \nmid c$, then $a \equiv b \pmod{p}$. (cancellation multiplication prime modulus)

Proof. Suppose $ac \equiv bc \pmod{p}$ and p is prime and $p \nmid c$.

Let $d = \gcd(p, c)$.

Then $d|p$ and $d|c$.

Suppose $d \neq 1$.

Since p is prime, then the only positive divisors of p are 1 and p.

Since $d|p$, then either $d = 1$ or $d = p$.

Since $d \neq 1$, then $d = p$, so $p|c$.

But, this contradicts $p \nmid c$.

Therefore, $d = 1$.

Hence, $1 = \gcd(p, c)$.

Since $ac \equiv bc \pmod p$ and $\gcd(p, c) = 1$, then by the previous corollary, $a \equiv b \pmod p$. ☐

Proposition 77. *Let $n \in \mathbb{Z}^+$.*

Let $a, b, c \in \mathbb{Z}$.

If $c \neq 0$, then $ac \equiv bc \pmod{nc}$ iff $a \equiv b \pmod n$.

Proof. Let $c \neq 0$.

Suppose $ac \equiv bc \pmod{nc}$.

Then $nc|(ac - bc)$, so $cn|c(a - b)$.

Since $c \neq 0$ and $cn|c(a - b)$, then $n|(a - b)$, by proposition 40.

Therefore, $a \equiv b \pmod n$.

Conversely, suppose $a \equiv b \pmod n$.

Then $n|(a - b)$, so $cn|c(a - b)$, by proposition 40.

Hence, $nc|(a - b)c$, so $nc|ac - bc$.

Therefore, $ac \equiv bc \pmod{nc}$. ☐

Proposition 78. *Let $n \in \mathbb{Z}^+$.*

Let $a \in \mathbb{Z}^+$.

Then a is invertible modulo n iff $\gcd(a, n) = 1$.

Proof. Suppose $\gcd(a, n) = 1$.

Since gcd is the least positive linear combination of a and n and $\gcd(a, n) = 1$, then there exist integers r and s such that $ra + sn = 1$.

Thus, $ra - 1 = -sn$, so $ar - 1 = n(-s)$.

Since $s \in \mathbb{Z}$, then $-s \in \mathbb{Z}$, so n divides $ar - 1$.

Therefore, $ar \equiv 1 \pmod n$.

Since $r \in \mathbb{Z}$ and $ar \equiv 1 \pmod n$, then r is a multiplicative inverse of a, so a is invertible. ☐

Proof. Suppose a is invertible.

Then there is an integer b such that $ab \equiv 1 \pmod n$, so n divides $ab - 1$.

Thus, $ab - 1 = nk$ for some integer k.

Hence, $1 = ab - nk = ba + (-k)n$ is a linear combination of a and n.

Thus, 1 is a multiple of $\gcd(a, n)$, so $\gcd(a, n)$ divides 1.

Therefore, $\gcd(a, n)$ must be 1, so $\gcd(a, n) = 1$. ☐

Linear Congruences

Proposition 79. *Let $a, b, x, x_0 \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$.*

If x_0 is a solution to $ax \equiv b \pmod n$, then so is $x_0 + nk$ for any integer k.

Proof. Let k be an arbitrary integer.

Suppose x_0 is a solution to $ax \equiv b \pmod{n}$.

Then $ax_0 \equiv b \pmod{n}$.

Since $ank \equiv ank \pmod{n}$, we add these equations to get $ax_0 + ank \equiv (b + ank) \pmod{n}$.

Thus, $a(x_0 + nk) \equiv (b + ank) \pmod{n}$.

For any integer m, $n|nm - 0$, so $nm \equiv 0 \pmod{n}$.

Hence, in particular, $n(ak) \equiv 0 \pmod{n}$, so $ank \equiv 0 \pmod{n}$.

Since $ank \equiv 0 \pmod{n}$ and $b \equiv b \pmod{n}$, then by adding these equations we get $b + ank \equiv b \pmod{n}$.

Since $a(x_0 + nk) \equiv (b + ank) \pmod{n}$ and $b + ank \equiv b \pmod{n}$, then we conclude $a(x_0 + nk) \equiv b \pmod{n}$, as desired. □

Proof. Let k be an arbitrary integer.

Suppose x_0 is a solution to $ax \equiv b \pmod{n}$.

Then $ax_0 \equiv b \pmod{n}$.

Observe that

$$\begin{aligned} n|nk &\Rightarrow n|(x_0 + nk) - x_0 \\ &\Rightarrow x_0 + nk \equiv x_0 \pmod{n} \\ &\Rightarrow a(x_0 + nk) \equiv ax_0 \pmod{n} \\ &\Rightarrow a(x_0 + nk) \equiv b \pmod{n}. \end{aligned}$$

□

Theorem 80. ***Existence of solution to linear congruence***

Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$.

A solution exists to the linear congruence $ax \equiv b \pmod{n}$ if and only if $d|b$, where $d = \gcd(a, n)$.

Moreover, if a solution exists, then there are d distinct solutions modulo n and these solutions are congruent modulo $\frac{n}{d}$.

Solution. We must prove:

1. if a solution exists, then $\gcd(a, n)|b$.
2. if $\gcd(a, n)|b$, then a solution exists. □

Proof. Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$.

Suppose a solution exists to the linear congruence $ax \equiv b \pmod{n}$.

Then there exists an integer x_0 such that $ax_0 \equiv b \pmod{n}$, so $n|(ax_0 - b)$.

Hence, there exists an integer k such that $ax_0 - b = nk$.

Thus, $ax_0 - nk = b$, so $ax_0 + n(-k) = b$.

Since $-k$ is an integer, then b is a linear combination of a and n.

Now, b is a multiple of $\gcd(a, n)$ if and only if b is a linear combination of a and n.

Hence, b is a multiple of $\gcd(a, n)$, so $\gcd(a, n)|b$.

Conversely, suppose $\gcd(a,n)|b$.

To prove a solution exists we must prove there exists an integer x_0 such that $ax_0 \equiv b \pmod{n}$.

Let $d = \gcd(a,n)$.

Then $d|b$, so there exists some integer k such that $b = dk$.

Since d is the least positive linear combination of a and n, then there exist integers r and s such that $ra + sn = d$.

We multiply this equation by k to obtain $rak + snk = dk = b$.

Hence, $rak - b = -snk$, so $a(rk) - b = n(-sk)$.

Let $x_0 = rk$.

Then x_0 is an integer and $ax_0 - b = n(-sk)$.

Since $-sk$ is an integer, then $n|(ax_0 - b)$, so $ax_0 \equiv b \pmod{n}$.

Suppose a solution exists to the linear congruence $ax \equiv b \pmod{n}$.

Then $\gcd(a,n)|b$.

Since $ax \equiv b \pmod{n}$, then $n|(ax - b)$, so there exists an integer k such that $ax - b = nk$.

Hence, $ax - nk = b$.

Let $y = -k$.

Then $ax + ny = b$.

The equation $ax + ny = b$ is a linear diophantine equation.

Since $\gcd(a,n)|b$, then a solution exists to the diophantine equation.

Let (x_0, y_0) be a particular solution to $ax + ny = b$.

Then the solution set has the form $(x_0 + t\frac{n}{d}, y_0 - t\frac{a}{d})$ where $d = \gcd(a,n)$ and t is any integer, by corollary 69.

Suppose $0 \leq t < d$.

Then x is one of $x_0, x_0 + \frac{n}{d}, x_0 + 2\frac{n}{d}, x_0 + 3\frac{n}{d}, ..., x_0 + (d-1)\frac{n}{d}$.

To prove each of these d solutions is a distinct element modulo n, suppose for the sake of contradiction that there exist a pair of these solutions that are not distinct modulo n.

Then there exist a pair of these solutions that are congruent modulo n.

Let x', x'' be a pair of these solutions such that $x' \equiv x'' \pmod{n}$, where $x' = x_0 + t_1\frac{n}{d}$ and $x'' = x_0 + t_2\frac{n}{d}$ and $0 \leq t_1 < d$ and $0 \leq t_2 < d$.

Then $n|(x' - x'')$, so $n|(x_0 + t_1\frac{n}{d}) - (x_0 + t_2\frac{n}{d})$.

Hence, $n|(t_1\frac{n}{d} - t_2\frac{n}{d})$, so $n|\frac{n}{d}(t_1 - t_2)$.

Thus, $n|\frac{n}{d}(|t_1 - t_2|)$, so $n \leq \frac{n}{d}|t_1 - t_2|$.

Hence, $1 \leq \frac{|t_1 - t_2|}{d}$, so $d \leq |t_1 - t_2|$.

Since $0 \leq t_1 < d$ and $0 \leq t_2 < d$, then $0 \leq |t_1 - t_2| < d$, so $|t_1 - t_2| < d$.

Thus, we have $d \leq |t_1 - t_2|$ and $|t_1 - t_2| < d$, a contradiction.

Therefore, no such pair exists, so each of these d solutions is a distinct element modulo n.

To prove each of these d solutions is congruent modulo $\frac{n}{d}$, let x' and x'' be arbitrary solutions such that $x' = x_0 + t'\frac{n}{d}$ and $x'' = x_0 + t''\frac{n}{d}$ where $0 \leq t' < d$ and $0 \leq t'' < d$.

Observe that

$$\begin{aligned}
\frac{n}{d} &\mid \frac{n}{d} \\
&\mid \frac{n}{d}(t' - t'') \\
&\mid (t'\frac{n}{d} - t''\frac{n}{d}) \\
&\mid (x_0 + t'\frac{n}{d}) - (x_0 + t''\frac{n}{d}) \\
&\mid (x' - x'').
\end{aligned}$$

Hence, $x' \equiv x'' \pmod{\frac{n}{d}}$.

Since x and x' are arbitrary, then each of the d solutions is congruent modulo $\frac{n}{d}$. ☐

Corollary 81. *Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$.*

There exists an integer b such that $ab \equiv 1 \pmod{n}$ if and only if $\gcd(a, n) = 1$.

Moreover, b is the inverse of a and the inverse of a is unique modulo n.

Proof. **Existence:**

Suppose there exists an integer b such that $ab \equiv 1 \pmod{n}$.

Then b is a solution to the linear congruence $ax \equiv 1 \pmod{n}$.

A solution to the linear congruence $ax \equiv 1 \pmod{n}$ exists iff $\gcd(a, n)|1$.

Hence, $\gcd(a, n)|1$. Therefore, $\gcd(a, n) = 1$.

Conversely, suppose $\gcd(a, n) = 1$.

Since $\gcd(a, n)|1$, then there exists a solution to the linear congruence $ax \equiv 1 \pmod{n}$.

Let b be a solution.

Then b is an integer such that $ab \equiv 1 \pmod{n}$.

Therefore, b is an inverse of a.

Uniqueness:

Let b and b' be inverses of a modulo n.

Since b is an inverse of a, then $ab \equiv 1 \pmod{n}$.

Since b' is an inverse of a, then $ab' \equiv 1 \pmod{n}$.

Hence, b and b' are solutions to the linear congruence $ax \equiv 1 \pmod{n}$.

Therefore, $\gcd(a, n) = 1$.

Since $ab \equiv 1 \pmod{n}$, then $1 \equiv ab \pmod{n}$.

Since $ab' \equiv 1 \pmod{n}$ and $1 \equiv ab \pmod{n}$, then $ab' \equiv ab \pmod{n}$.

Since $\gcd(a, n) = 1$, then we may cancel to obtain $b' \equiv b \pmod{n}$, by corollary 75.

Therefore, the inverse is unique modulo n. ☐

Integers Modulo n

Lemma 82. ***addition modulo n is well-defined***

Let $[a], [b] \in \mathbb{Z}_n$.

Let $x, x' \in [a]_n$ and $y, y' \in [b]_n$.

Then $[x + y] = [x' + y']$.

Proof. Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$.

Suppose $x, x' \in [a]_n$ and $y, y' \in [b]_n$.

Then $[a]_n = \{x \in \mathbb{Z} : x \equiv a \pmod{n}\}$ and $[b]_n = \{x \in \mathbb{Z} : x \equiv b \pmod{n}\}$.

Since $x, x' \in [a]$, then $x, x' \in \mathbb{Z}$ and $x \equiv a \pmod{n}$ and $x' \equiv a \pmod{n}$.

Since $y, y' \in [b]$, then $y, y' \in \mathbb{Z}$ and $y \equiv b \pmod{n}$ and $y' \equiv b \pmod{n}$.

Since $x' \equiv a \pmod{n}$, then $a \equiv x' \pmod{n}$.

Since $x \equiv a \pmod{n}$ and $a \equiv x' \pmod{n}$, then $x \equiv x' \pmod{n}$.

Since $y' \equiv b \pmod{n}$, then $b \equiv y' \pmod{n}$.

Since $y \equiv b \pmod{n}$ and $b \equiv y' \pmod{n}$, then $y \equiv y' \pmod{n}$.

Adding the congruences $x \equiv x' \pmod{n}$ and $y \equiv y' \pmod{n}$, we obtain $x + x' \equiv (y + y') \pmod{n}$.

Therefore, $[x + x'] = [y + y']$.

Notes:

We observe that if $x, x' \in [a]$ and $y, y' \in [b]$, then $[x + y] = [x' + y']$. ☐

Proposition 83. ***Addition modulo n is a binary operation.***

Let $+_n : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ be a binary relation defined by $[a] + [b] = [a + b]$ for all $[a], [b] \in \mathbb{Z}_n$.

Then $+_n$ is a binary operation on $\mathbb{Z}_n$.

Solution. To prove $+_n$ is a binary operation on $\mathbb{Z}_n$, we must prove:

1. Closure: $(\forall [a], [b] \in \mathbb{Z}_n)([a] + [b] \in \mathbb{Z}_n)$.
2. Uniqueness: $(\forall [a], [b] \in \mathbb{Z}_n)([a] + [b])$ is unique.

To prove $[a] + [b]$ is unique, we must prove:

if $([a], [b]), ([a'], [b']) \in \mathbb{Z}_n \times \mathbb{Z}_n$ such that $([a], [b]) = ([a'], [b'])$, then $[a] + [b] = [a'] + [b']$.

Thus, assume $([a], [b]) = ([a'], [b'])$. Prove $[a] + [b] = [a'] + [b']$.

Suppose $([a], [b]) = ([a'], [b'])$.

Then $[a] = [a']$ and $[b] = [b']$.

Thus, $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$.

Thus, we must prove the result does not depend on the choice of a particular representative of the equivalence class. ☐

Proof. Let $[x], [y] \in \mathbb{Z}_n$.

Then x and y are integers.

Since $x + y$ is an integer, then $[x + y] \in \mathbb{Z}_n$.

Observe that $[x + y] = [x] + [y]$.

Hence, $[x] + [y] \in \mathbb{Z}_n$.

Therefore, $\mathbb{Z}_n$ is closed under addition modulo n.

We prove addition modulo n is well defined.

Let $([a], [b]), ([a'], [b']) \in \mathbb{Z}_n \times \mathbb{Z}_n$ such that $([a], [b]) = ([a'], [b'])$.

Then $[a] = [a']$ and $[b] = [b']$.

Hence, $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$.

Adding these congruences, we obtain $a + b \equiv (a' + b') \pmod{n}$.

Hence, $[a + b] = [a' + b']$.

Therefore,

$$\begin{aligned} [a] + [b] &= [a + b] \\ &= [a' + b'] \\ &= [a'] + [b']. \end{aligned}$$

Hence, $[a] + [b] = [a'] + [b']$, so addition modulo n is well defined. $\square$

Theorem 84. ***algebraic properties of addition modulo*** n

1. $[a] + ([b] + [c]) = ([a] + [b]) + [c]$ *for all* $[a], [b], [c] \in \mathbb{Z}_n$.*(associative)*
2. $[a] + [b] = [b] + [a]$ *for all* $[a], [b] \in \mathbb{Z}_n$.*(commutative)*
3. $[a] + [0] = [0] + [a] = [a]$ *for all* $[a] \in \mathbb{Z}_n$. *(additive identity)*
4. $[a] + [-a] = [-a] + [a] = [0]$ *for all* $[a] \in \mathbb{Z}_n$. *(additive inverses)*

Proof. We prove 1.

Let $[a], [b], [c] \in \mathbb{Z}_n$.

Then $[a]+([b]+[c]) = [a]+[b+c] = [a+(b+c)] = [(a+b)+c] = [a+b]+[c] = ([a] + [b]) + [c]$. $\square$

Proof. We prove 2.

Let $[a], [b] \in \mathbb{Z}_n$.

Then $[a] + [b] = [a + b] = [b + a] = [b] + [a]$. $\square$

Proof. We prove 3.

Let $[a] \in \mathbb{Z}_n$.

Then $[a] + [0] = [a + 0] = [a] = [0 + a] = [0] + [a]$. $\square$

Proof. We prove 4.

Let $[a] \in \mathbb{Z}_n$.

Then $[a] + [-a] = [a + (-a)] = [0] = [-a + a] = [-a] + [a]$. $\square$

Proposition 85. ***Multiplication modulo*** n ***is a binary operation.***

Let $*_n : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ *be a binary relation defined by* $[a][b] = [ab]$ *for all* $[a], [b] \in \mathbb{Z}_n$.

Then $*_n$ *is a binary operation on* $\mathbb{Z}_n$.

Solution. To prove $*_n$ is a binary operation on $\mathbb{Z}_n$, we must prove:

1. Closure: $(\forall [a], [b] \in \mathbb{Z}_n)([a][b] \in \mathbb{Z}_n)$.
2. Uniqueness: $(\forall [a], [b] \in \mathbb{Z}_n)([a][b])$ is unique.

To prove $[a][b]$ is unique, we must prove:

if $([a], [b]), ([a'], [b']) \in \mathbb{Z}_n \times \mathbb{Z}_n$ such that $([a], [b]) = ([a'], [b'])$, then $[a][b] = [a'][b']$.

Thus, assume $([a],[b]) = ([a'],[b'])$. Prove $[a][b] = [a'][b']$.
Suppose $([a],[b]) = ([a'],[b'])$.
Then $[a] = [a']$ and $[b] = [b']$.
Thus, $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$.
Thus, we must prove the result does not depend on the choice of a particular representative of the equivalence class. $\square$

Proof. Let $[x],[y] \in \mathbb{Z}_n$.
Then x and y are integers.
Since xy is an integer, then $[xy] \in \mathbb{Z}_n$.
Observe that $[xy] = [x][y]$.
Hence, $[x][y] \in \mathbb{Z}_n$.
Therefore, $\mathbb{Z}_n$ is closed under multiplication modulo n.
We prove multiplication modulo n is well defined.
Let $([a],[b]), ([a'],[b']) \in \mathbb{Z}_n \times \mathbb{Z}_n$ such that $([a],[b]) = ([a'],[b'])$.
Then $[a] = [a']$ and $[b] = [b']$.
Hence, $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$.
Multiplying these congruences, we obtain $ab \equiv a'b' \pmod{n}$.
Hence, $[ab] = [a'b']$.
Therefore,

$$\begin{aligned} [a][b] &= [ab] \\ &= [a'b'] \\ &= [a'][b']. \end{aligned}$$

Hence, $[a][b] = [a'][b']$, so multiplication modulo n is well defined. $\square$

Theorem 86. ***algebraic properties of multiplication modulo*** n

1. $[a]([b][c]) = ([a][b])[c]$ *for all* $[a],[b],[c] \in \mathbb{Z}_n$. *(associative)*
2. $[a][b] = [b][a]$ *for all* $[a],[b] \in \mathbb{Z}_n$. *(commutative)*
3. $[a][1] = [1][a] = [a]$ *for all* $[a] \in \mathbb{Z}_n$. *(multiplicative identity)*
4. $[a][0] = [0][a] = [0]$ *for all* $[a] \in \mathbb{Z}_n$.
5. $[a]([b]+[c]) = [a][b] + [a][c]$ *for all* $[a],[b],[c] \in \mathbb{Z}_n$. *(left distributive)*
6. $([a]+[b])[c] = [a][c] + [b][c]$ *for all* $[a],[b],[c] \in \mathbb{Z}_n$. *(right distributive)*

Proof. We prove 1.
Let $[a],[b],[c] \in \mathbb{Z}_n$.
Then $[a]([b][c]) = [a][bc] = [a(bc)] = [(ab)c] = [ab][c] = ([a][b])[c]$. $\square$

Proof. We prove 2.
Let $[a],[b] \in \mathbb{Z}_n$.
Then $[a][b] = [ab] = [ba] = [b][a]$. $\square$

Proof. We prove 3.
Let $[a] \in \mathbb{Z}_n$.
Then $[a][1] = [a1] = [a] = [1a] = [1][a]$. $\square$

Proof. We prove 4.
Let $[a] \in \mathbb{Z}_n$.
Then $[a][0] = [a0] = [0] = [0a] = [0][a]$. ☐

Proof. We prove 5.
Let $[a], [b], [c] \in \mathbb{Z}_n$.
Then $[a]([b] + [c]) = [a][b + c] = [a(b + c)] = [ab + ac] = [ab] + [ac] = [a][b] + [a][c]$. ☐

Proof. We prove 6.
Let $[a], [b], [c] \in \mathbb{Z}_n$.
Then $([a] + [b])[c] = [a + b][c] = [(a + b)c] = [ac + bc] = [ac] + [bc] = [a][c] + [b][c]$. ☐

Theorem 87. ***Existence of multiplicative inverse of*** $[a]$ ***modulo*** n
Let $n \in \mathbb{Z}^+$.
Let $[a] \in \mathbb{Z}_n$.
Then $[a]$ *has a multiplicative inverse in* $\mathbb{Z}_n$ *iff* $\gcd(a, n) = 1$.

Proof. Let n be a positive integer.
Let $[a] \in \mathbb{Z}_n$.
Suppose $[a]$ has a multiplicative inverse.
Then there exists $[b] \in \mathbb{Z}_n$ such that $[a][b] = [1]$, so $[ab] = [1]$.
Hence, $ab \equiv 1 \pmod{n}$, so $n|(ab - 1)$.
Thus, $ab - 1 = nk$ for some integer k.
Consequently, $1 = ab - nk = ba - nk = ba - kn = ba + (-k)n$ is a linear combination of a and n.
Let $d = \gcd(a, n)$.
Any common divisor of a and n divides any linear combination of a and n.
Hence, d divides any linear combination of a and n, so d divides 1.
Since $d \in \mathbb{Z}^+$ and $d|1$, then $d = 1$, so $\gcd(a, n) = 1$.

Conversely, suppose $\gcd(a, n) = 1$.
Then there exists $x, y \in \mathbb{Z}$ such that $xa + yn = 1$, so $xa - 1 = -yn$.
Since $-y \in \mathbb{Z}$, then this implies n divides $xa - 1$, so $xa \equiv 1 \pmod{n}$.
Thus, $1 \equiv xa$, so $[1] = [xa] = [x][a] = [a][x]$.
Since $[x] \in \mathbb{Z}_n$ and $[a][x] = [1]$, then $[a]$ has a multiplicative inverse. ☐

Corollary 88. *The inverse of* $[0]$ *in* $\mathbb{Z}_1$ *is* $[0]$.
Let $n \in \mathbb{Z}^+$.
If $n > 1$, *then* $[0]$ *has no multiplicative inverse.*

Proof. Let $n \in \mathbb{Z}^+$.
Then either $n = 1$ or $n > 1$.
We consider these cases separately.
Case 1: Suppose $n = 1$.
Then $\mathbb{Z}_1 = \{[0]\}$.
Since $0 \equiv 1 \pmod{1}$, then $[0] = [1]$.

Hence, $[1] \in \mathbb{Z}_1$.

Since $[1] = [0] = [0 * 0] = [0][0]$, then there exists $[0] \in \mathbb{Z}_1$ such that $[0][0] = [1]$.

Therefore, $[0]$ has a multiplicative inverse in $\mathbb{Z}_1$ and $[0]^{-1} = [0]$.

Case 2: Suppose $n > 1$.

Then $\gcd(0, n) = n > 1$, so $\gcd(0, n) > 1$.

Thus, $\gcd(0, n) \neq 1$.

Since $[0]$ has a multiplicative inverse in $\mathbb{Z}_n$ iff $\gcd(0, n) = 1$, then $[0]$ does not have a multiplicative inverse in $\mathbb{Z}_n$. □

Theorem 89. *Let $n \in \mathbb{Z}^+$.*

A nonzero element of $\mathbb{Z}_n$ either has a multiplicative inverse or is a divisor of zero.

Solution. Let $[a] \in \mathbb{Z}_n, [a] \neq [0]$.

We must prove: Either $[a]$ has a multiplicative inverse or $[a]$ is a divisor of zero.

Either a and n are relatively prime or not. □

Proof. Let n be a positive integer.

Let $[a] \in \mathbb{Z}_n$ and $[a] \neq [0]$.

Since $[a] \in \mathbb{Z}_n$, then a is an integer.

Either a and n are relatively prime or not.

We consider these cases separately.

Case 1: Suppose a and n are relatively prime.

Then $\gcd(a, n) = 1$.

The element $[a]$ has a multiplicative inverse in $\mathbb{Z}_n$ iff $\gcd(a, n) = 1$.

Hence, $[a]$ has a multiplicative inverse in $\mathbb{Z}_n$.

Case 2: Suppose a and n are not relatively prime.

Then $\gcd(a, n) \neq 1$, so $\gcd(a, n) > 1$.

Let $d = \gcd(a, n)$.

Then $d > 1$.

Consider the equation $[a][x] = [0]$.

Observe that $[a][x] = [ax] = [0]$.

Hence, $ax \equiv 0 \pmod{n}$.

The linear congruence has a solution iff $\gcd(a, n)|0$.

Hence, a solution exists iff $d|0$.

Any integer divides zero, so $d|0$.

Hence, a solution exists and there are d distinct solutions modulo n.

Zero is a solution since $a * 0 \equiv 0 \pmod{n}$.

Thus, there are $d - 1$ distinct nonzero solutions modulo n.

Since $d > 1$, then $d - 1 > 0$, so $d - 1 \geq 1$.

Hence, there exists at least one nonzero solution modulo n, say b.

Thus, b is a nonzero positive integer that is less than n and is a solution to $ax \equiv 0 \pmod{n}$.

Hence, $[b] \in \mathbb{Z}_n$ and $[b] \neq [0]$ and $ab \equiv 0 \pmod{n}$.

Since $ab \equiv 0 \pmod{n}$, then $[ab] = [0]$, so $[a][b] = [0]$.

Since $[b] \in \mathbb{Z}_n$ and $[b] \neq [0]$ and $[a][b] = [0]$, then $[a]$ is a divisor of zero. $\square$

Proposition 90. *If p is prime, then $\phi(p) = p - 1$.*

Proof. Suppose p is a prime number.
Then p is a positive integer and $p > 1$.
Let $S = \{1, 2, ..., p - 1, p\}$.
Let $a \in S$.
Since $a \in S$ and $S \subset \mathbb{Z}^+$, then $a \in \mathbb{Z}^+$.
Either $a < p$ or $a = p$.
We consider these cases separately.
Case 1: Suppose $a < p$.
Since a and p are positive integers and $a < p$, then $p \not| a$.
Since p is prime, then either $p|a$ or $\gcd(p, a) = 1$.
Since $p \not| a$, then $\gcd(p, a) = 1$.
Hence, a is relatively prime to p.
Thus, there are $p - 1$ positive integers less than p that are relatively prime to p.
Case 2: Suppose $a = p$.
Then $\gcd(p, a) = \gcd(p, p) = p > 1$.
Thus, $\gcd(p, a) \neq 1$, so p and a are not relatively prime.
Hence, in all cases, there are exactly $p-1$ positive integers less than or equal to p that are relatively prime to p.
Therefore, $\phi(p) = p - 1$. $\square$

Fermat's Theorem

Theorem 91. ***Fermat's Little Theorem***
Let $p, a \in \mathbb{Z}^+$.
If p is prime and $p \not| a$, then $p|a^{p-1} - 1$.

Proof. Suppose p is prime and $p \not| a$.
By the division algorithm, $a = pq+r$ for some integers q and r with $0 \leq r < p$.
Since $p \not| a$, then $r \neq 0$, so $0 < r < p$.
Hence, $1 \leq r \leq p - 1$.

Let $s \in \mathbb{Z}$ such that $1 \leq s \leq p - 1$.
We prove if $r \neq s$ then $ra \not\equiv sa \pmod{p}$ by contrapositive.
Suppose $ra \equiv sa \pmod{p}$.
Then p divides $ra - sa = (r - s)a$.
Since p is prime and p divides $(r - s)a$, then by Euclid's lemma, either $p|(r - s)$ or $p|a$.
By assumption, $p \not| a$, so we conclude $p|r - s$.
Hence, $r \equiv s \pmod{p}$.
Therefore, $ra \equiv sa \pmod{p}$ implies $r \equiv s \pmod{p}$, so $r \not\equiv s \pmod{p}$ implies $ra \not\equiv sa \pmod{p}$.

Thus, any distinct pair of these integers s$a, 2a, 3a, ..., (p-1)a$ are not congruent $\pmod p$, so $a, 2a, 3a, ..., (p-1)a$ are all distinct.

Hence, the congruence classes $[a], [2a], [3a], ..., [(p-1)a]$ are all distinct.

Let S be the set of these elements.

Then $S = \{[ra] : 1 \leq r \leq p-1\} = \{[a], [2a], ..., [(p-1)a]\}$.

We prove $[0] \notin S$.

Suppose $[0] \in S$.

Then $[0] = [ra]$ for $1 \leq r \leq p-1$.

Thus, $0 \equiv ra \pmod p$, so $ra \equiv 0 \pmod p$.

Hence, p divides $ra - 0 = ra$.

Since p is prime and p divides ra, then by Euclid's lemma, either $p|r$ or $p|a$.

By assumption, $p \not| a$, so we conclude $p|r$.

Since p and r are positive integers and $p|r$, then $p \leq r$.

Since $r \leq p - 1 < p$,then $r < p$, so $p > r$.

Thus, we have $p > r$ and $p \leq r$, a contradiction.

Therefore, $[0] \notin S$.

Let $T = \{[k] : 1 \leq k \leq p-1\}$.

Then $T = \{[1], [2], ..., [p-1]\}$.

We prove $S \subset T$.

Let $x \in S$.

Then $x = [ra]$ and $1 \leq r \leq p-1$.

By the division algorithm, $ra = pq' + r'$ for integers q', r' with $0 \leq r' < p$.

Since $r' \in \mathbb{Z}$ and $r' < p$, then $r' \leq p-1$, so $0 \leq r' \leq p-1$.

Observe that

$$\begin{aligned} x &= [ra] \\ &= [pq' + r'] \\ &= [pq'] + [r'] \\ &= [p][q'] + [r'] \\ &= [0][q'] + [r'] \\ &= [0q'] + [r'] \\ &= [0] + [r'] \\ &= [0 + r'] \\ &= [r']. \end{aligned}$$

Since $x = [r']$ and $x \in S$ and $[0] \notin S$, then $[r'] \neq [0]$, so $r' \neq 0$.

Since $0 \leq r' \leq p-1$ and $r' \neq 0$, then $0 < r' \leq p-1$, so $1 \leq r' \leq p-1$.

Since $x = [r']$ and $1 \leq r' \leq p-1$, then $x \in T$, so $S \subset T$.

We prove $T \subset S$.

Let $y \in T$.

Then $y = [k]$ for some integer k with $1 \leq k \leq p-1$.

The linear congruence $ar \equiv k \pmod p$ has a solution iff $\gcd(a,p)$ divides k and there are $\gcd(a,p)$ distinct solutions modulo p.

Since p is prime, then either $p|a$ or $\gcd(p,a) = 1$.

By assumption, $p \not| a$, so we conclude $\gcd(p,a) = 1$.

Since $\gcd(p,a) = 1$ and 1 divides integer k, then we conclude the linear congruence $ar \equiv k \pmod p$ has 1 distinct solution modulo p.

Hence, there exists an integer r with $0 \leq r < p$ such that $ar \equiv k \pmod p$, so $k \equiv ar \pmod p$.

Thus, $k \equiv ra \pmod p$, so $[k] = [ra]$.

Since $k \geq 1$, the $k \neq 0$.

Since $k \neq 0$ and $ar \equiv k \pmod p$, then $ar \not\equiv 0 \pmod p$, so $r \neq 0$.

Since $0 \leq r < p$ and $r \neq 0$, then $0 < r < p$, so $1 \leq r \leq p-1$.

Hence, $y = [ra]$ and $1 \leq r \leq p-1$, so $y \in S$.

Therefore, $y \in T$ implies $y \in S$, so $T \subset S$.

Since $S \subset T$ and $T \subset S$, then $S = T$.

Observe that

$[a] \cdot [2a] \cdot ... \cdot [(p-1)a] = [1] \cdot [2] \cdot ... \cdot [p-1]$

$[a \cdot 2a \cdot ... \cdot (p-1)a] = [1 \cdot 2 \cdot ... \cdot (p-1)]$

$[a \cdot 2a \cdot ... \cdot (p-1)a] = [(p-1)!]$

$[1 \cdot 2 \cdot ...(p-1) \cdot a^{p-1}] = [(p-1)!]$

$[(p-1)! \cdot a^{p-1}] = [(p-1)!]$

$[a^{p-1}] = [1]$

Therefore, $a^{p-1} \equiv 1 \pmod p$, so p divides $a^{p-1} - 1$. □

Corollary 92. *Let $p, a \in \mathbb{Z}$.*

If p is prime, then $a^p \equiv a \pmod p$.

Proof. Suppose p is prime.

Either $p|a$ or $p \not| a$.

We consider these cases separately.

Case 1: Suppose $p|a$.

Then $p|a - 0$, so $a \equiv 0 \pmod p$.

Since p is prime, then $p \in \mathbb{Z}^+$.

Since $p \in \mathbb{Z}^+$ and exponentiation preserves congruences and $a \equiv 0 \pmod p$, then we raise to the p power to obtain $a^p \equiv 0^p = 0 \equiv a$, so $a^p \equiv a \pmod p$.

Case 2: Suppose $p \not| a$.

Since p is prime and $p \not| a$, then by Fermat's Little theorem, p divides $a^{p-1} - 1$, so $a^{p-1} \equiv 1 \pmod p$.

Since $a \equiv a \pmod p$, we multiply these congruences to obtain $a^p = a^{p-1} \cdot a \equiv 1 \cdot a = a$, so $a^p \equiv a \pmod p$. □

Theorem 93. ***Euler's Theorem***

Let $a \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$.

If $\gcd(a, n) = 1$, *then* $a^{\phi(n)} \equiv 1 \pmod{n}$.

Proof. Let $\mathbb{Z}_n^*$ be the group of units of $\mathbb{Z}_n$.

Then $\mathbb{Z}_n^* = \{[a] \in \mathbb{Z}_n : \gcd(a, n) = 1\}$.

Let $[a] \in \mathbb{Z}_n^*$.

Then $[a] \in \mathbb{Z}_n$ and $\gcd(a, n) = 1$.

Let $m = |\mathbb{Z}_n^*| = \phi(n)$.

Then m is a positive integer, so $\mathbb{Z}_n^*$ is a finite group of order m.

Hence, $g^m = e$ for all $g \in \mathbb{Z}_n^*$.

Thus, $[a]^m = [1]$, so $[1] = [a]^m = [a^m]$.

Hence, $1 \equiv a^m \pmod{n}$, so $a^m \equiv 1 \pmod{n}$.

Therefore, $a^{\phi(n)} \equiv 1 \pmod{n}$.

Thus, $\gcd(a, n) = 1$ and $a^{\phi(n)} \equiv 1 \pmod{n}$, so $\gcd(a, n) = 1$ implies $a^{\phi(n)} \equiv 1 \pmod{n}$. $\square$

Corollary 94. ***Fermat's Little Theorem***

Let $a \in \mathbb{Z}$.

If p is prime, then $a^p \equiv a \pmod{p}$.

Proof. Suppose p is prime.

Then either p divides a, or p and a are relatively prime.

We consider these cases separately.

Case 1: Suppose $p|a$.

Then there exists an integer k such that $a = pk$.

Hence, $a^p - a = a(a^{p-1} - 1) = pk(a^{p-1} - 1)$.

Since $p > 1$, then $p - 1 > 0$, so $p - 1$ is a positive integer.

Consequently, a^{p-1} is an integer, so $k(a^{p-1} - 1)$ is an integer.

Thus, p divides $a^p - a$, so $a^p \equiv a \pmod{p}$.

Case 2: Suppose p and a are relatively prime.

Then $\gcd(a, p) = 1$.

By Euler's thm, $a^{\phi(p)} \equiv 1 \pmod{p}$.

Since p is prime, then $\phi(p) = p - 1$, so $a^{p-1} \equiv 1 \pmod{p}$.

Multiplying the congruence by a, we obtain $a^p \equiv a \pmod{p}$. $\square$

Miscellaneous Stuff

Proposition 95. ***Every integer is congruent modulo*** n ***to exactly one of the integers*** $0, 1, 2, ..., n - 1$***.***

Proof. Let $a \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$.

By the division algorithm, when a is divided by n, then there exist unique integers q and r such that $a = nq + r$ and $0 \leq r < n$.

Thus, $a - r = nq$, so $n|(a - r)$.

Therefore, $a \equiv r \pmod{n}$.

Since $0 \leq r < n$, then either $r = 0$ or $r = 1$ or $r = 2$ or ... or $r = n - 1$, so $r \in \{0, 1, 2, ..., n - 1\}$.

Hence, a is congruent modulo n to either 0 or 1 or 2 or ... or $n - 1$.

Therefore, every integer is congruent modulo n to exactly one of the integers in $\{0, 1, 2, ..., n - 1\}$. □

Proposition 96. ***Any set of*** n ***integers is a complete set of residues modulo*** n ***iff no two of the integers are congruent modulo*** n***.***

Proof. TODO □