Elementary Number Theory

Jason Sass

August 18, 2025

Natural number system

TODO

Rework the propositions regarding natural numbers so that do not rely on any axioms or set theory nonsense.

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. ***The 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 in $\mathbb{Z}$***

1. Addition is associative.

$(a + b) + c = a + (b + c)$ for all $a, b, c \in \mathbb{Z}$.

2. Addition is commutative.

$a + b = b + a$ for all $a, b \in \mathbb{Z}$.

3. Additive identity is zero.

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

4. Additive inverse of a is $-a$.

For all $a \in \mathbb{Z}$ there exists $-a \in \mathbb{Z}$ such that $a + (-a) = 0$.

Proof. TODO □

Proof. We prove 3.

TODO Prove $a + 0 = a$ or confirm if this should be an axiom for integers.

Since addition is commutative, then $a + 0 = 0 + a$.

Therefore, $a = a + 0 = 0 + a$. □

Theorem 6. ***algebraic properties of multiplication in*** $\mathbb{Z}$

1. Multiplication is associative.
$(ab)c = a(bc)$ *for all* $a, b, c \in \mathbb{Z}$.
2. Multiplication is commutative.
$ab = ba$ *for all* $a, b \in \mathbb{Z}$.
3. Multiplicative identity is one.
$a \cdot 1 = 1 \cdot a = a$ *for all* $a \in \mathbb{Z}$.
4. Multiplication by zero.
$a0 = 0a = 0$ *for all* $a \in \mathbb{Z}$.
5. Multiplication is distributive over addition.
$a(b + c) = ab + ac$ *for all* $a, b, c \in \mathbb{Z}$. *(left distributive law)*
$(b + c)a = ba + ca$ *for all* $a, b, c \in \mathbb{Z}$. *(right distributive law)*

Proof. TODO □

Proof. We prove 3.
TODO Prove $a \cdot 1 = a$ or confirm if this should be an axiom for integers.
Since multiplication is commutative, then $a \cdot 1 = 1 \cdot a$.
Therefore, $a = a \cdot 1 = 1 \cdot a$. □

Proposition 7. *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 8. $\mathbb{Z}$ ***satisfies transitivity and trichotomy laws.***

1. $a < a$ *is false for all* $a \in \mathbb{Z}$*. (Therefore,* $<$ *is not reflexive.)*

2. $<$ *is transitive.*

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

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 the trichotomy axiom for $\mathbb{Z}^+$, exactly one of the following is true: $a \in \mathbb{Z}^+$, $a = 0$, $-a \in \mathbb{Z}^+$.

By proposition 7, we have $a \in \mathbb{Z}^+$ 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 closed under subtraction, then $a - b \in \mathbb{Z}$.

By the trichotomy axiom for $\mathbb{Z}^+$, 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 9. ***order relation rules with ring operations in*** $\mathbb{Z}$
Let $a, b, c \in \mathbb{Z}$.
1. Addition preserves order.
If $a < b$, *then* $a + c < b + c$.
2. Subtraction preserves order.
If $a < b$, *then* $a - c < b - c$.
3. Multiplication by positive integer preserves order.
If $a < b$ *and* $c > 0$, *then* $ac < bc$.
4. Multiplication by negative integer reverses order.
If $a < b$ *and* $c < 0$, *then* $ac > bc$.

Proof. We prove 1.
Suppose $a < b$.
Then $b - a \in \mathbb{Z}^+$.
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 $b - a \in \mathbb{Z}^+$.
Observe that

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

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

Proof. We prove 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, $ac > bc$. □

Proposition 10. *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 $ac < bd$. □

Proposition 11. ***multiplication with positive and negative integers***

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

1. If $a > 0$ and $b > 0$, then $ab > 0$.

2. If $a > 0$ and $b < 0$, then $ab < 0$.

3. If $a < 0$ and $b < 0$, then $ab > 0$.

Proof. We prove 1.
Suppose $a > 0$ and $b > 0$.
Since $a > 0$, then $0 < a$.
By theorem 9, multiplication by a positive integer preserves order.
Since $0 < a$ and $b > 0$, then we conclude $0b < ab$.
Therefore, $0 < ab$, so $ab > 0$. □

Proof. We prove 2.
Suppose $a > 0$ and $b < 0$.
Since $a > 0$, then $0 < a$.
By theorem 9, multiplication by a negative integer reverses order.
Since $0 < a$ and $b < 0$, then we conclude $0b > ab$.
Therefore, $0 > ab$, so $ab < 0$. □

Proof. We prove 3.
Suppose $a < 0$ and $b < 0$.
By theorem 9, multiplication by a negative integer reverses order.
Since $a < 0$ and $b < 0$, then we conclude $ab > 0b$.
Therefore, $ab > 0$. □

Theorem 12. ***multiplicative property of zero***
Let $a, b \in \mathbb{Z}$.
Then $ab = 0$ *iff* $a = 0$ *or* $b = 0$.

Proof. We prove if $a = 0$ or $b = 0$, then $ab = 0$.
Suppose $a = 0$ or $b = 0$.
We consider these cases separately.
Case 1: Suppose $a = 0$.
Then $ab = 0 \cdot b = 0$, so $ab = 0$.
Case 2: Suppose $b = 0$.
Then $ab = a \cdot 0 = 0$, so $ab = 0$. □

Proof. Conversely, we prove if $ab = 0$, then either $a = 0$ or $b = 0$ by contrapositive.
Suppose $a \neq 0$ and $b \neq 0$.
Then by trichotomy, either $a > 0$ or $a < 0$, and either $b > 0$ or $b < 0$.
Hence, either $a > 0$ and $b > 0$, or $a > 0$ and $b < 0$, or $a < 0$ and $b > 0$, or $a < 0$ and $b < 0$.
We consider these cases separately.
Case 1: Suppose $a > 0$ and $b > 0$.
By proposition 11, a positive integer times a positive integer is positive.
Since $a > 0$ and $b > 0$, then we conclude $ab > 0$.
Therefore, by trichotomy, $ab \neq 0$.
Case 2: Suppose $a > 0$ and $b < 0$.
By proposition 11, a positive integer times a negative integer is negative.
Since $a > 0$ and $b < 0$, then we conclude $ab < 0$.
Therefore, by trichotomy, $ab \neq 0$.

Case 3: Suppose $a < 0$ and $b > 0$.
By proposition 11, a positive integer times a negative integer is negative.
Since $a < 0$ and $b > 0$, then we conclude $ab < 0$.
Therefore, by trichotomy, $ab \neq 0$.
Case 4: Suppose $a < 0$ and $b < 0$.
By proposition 11, a negative integer times a negative integer is positive.
Since $a < 0$ and $b < 0$, then we conclude $ab > 0$.
Therefore, by trichotomy, $ab \neq 0$.

In all cases, we have $ab \neq 0$, as desired. □

Corollary 13. ***cancellation law for*** $\mathbb{Z}$
Let $a, b, k \in \mathbb{Z}$.
If $ak = bk$ *and* $k \neq 0$, *then* $a = b$.

Proof. Suppose $ak = bk$ and $k \neq 0$.
Since $ak = bk$, then $0 = ak - bk = (a - b)k$.
By theorem 12, if $(a - b)k = 0$, then either $a - b = 0$ or $k = 0$.
Since $k \neq 0$, then we conclude $a - b = 0$.
Therefore, $a = b$. □

Theorem 14. *The relation* $\leq$ *is a partial order over* $\mathbb{Z}$.

Proof. We prove $\leq$ is reflexive.
Let $a \in \mathbb{Z}$.
Then $a = a$, so either $a = a$ or $a < a$.
Hence, either $a < a$ or $a = a$.
Therefore, $a \leq a$, so $\leq$ is reflexive. □

Proof. We prove $\leq$ is anti-symmetric.
To prove for all $a, b \in \mathbb{Z}$, if $a \leq b$ and $b \leq a$, then $a = b$, we 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 $a < b$, so $b > a$.
By the trichotomy law of $\mathbb{Z}$, exactly one of the following is true: $b < a$, $b = a$, $b > a$.
Since $b > a$, then we conclude $b \not< a$ and $b \neq a$.
Hence, $b \not\leq a$, as desired.
Therefore, $\leq$ is anti-symmetric. □

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

Then

$$\begin{aligned}
(a \leq b) \wedge (b \leq c) &\Rightarrow (a \leq b) \wedge (b < c \vee b = c) \\
&\Rightarrow (a \leq b \wedge b < c) \vee (a \leq b \wedge b = c) \\
&\Rightarrow (a \leq b \wedge b < c) \vee (a \leq c) \\
&\Rightarrow [(a < b \vee a = b) \wedge b < c] \vee (a \leq c) \\
&\Rightarrow [(a < b \wedge b < c) \vee (a = b \wedge b < c)] \vee (a \leq c) \\
&\Rightarrow [a < c \vee (a = b \wedge b < c)] \vee (a \leq c) \\
&\Rightarrow (a < c \vee a < c) \vee (a \leq c) \\
&\Rightarrow (a < c) \vee (a \leq c) \\
&\Rightarrow (a < c) \vee (a < c \vee a = c) \\
&\Rightarrow (a < c \vee a < c) \vee (a = c) \\
&\Rightarrow (a < c) \vee (a = c) \\
&\Rightarrow a \leq c.
\end{aligned}$$

Therefore, $a \leq c$, so $\leq$ is transitive. □

Proof. Since $\leq$ over $\mathbb{Z}$ is reflexive, anti-symmetric, and transitive, then $\leq$ is a partial order over $\mathbb{Z}$. □

Theorem 15. *The relation $\leq$ is a total order over $\mathbb{Z}$.*

Proof. By theorem 14, the relation $\leq$ is a partial order over $\mathbb{Z}$, so $(\mathbb{Z}, \leq)$ is a partially ordered set.

To prove $\leq$ is a total order over $\mathbb{Z}$, we must prove any two integers are comparable.

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

We must prove either $a \leq b$ or $b \leq a$.

By theorem 8, the trichotomy law implies exactly one of the following is true: $a < b$, $a = b$, $a > b$.

We consider these cases separately.

Case 1: Suppose $a < b$.

Then $a < b$ or $a = b$, so $a \leq b$.

Case 2: Suppose $a = b$.

Then $a < b$ or $a = b$, so $a \leq b$.

Case 3: Suppose $a > b$.

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

Therefore, $b \leq a$.

In all cases, we have either $a \leq b$ or $b \leq a$, as desired. □

Lemma 16. ***There is no integer between zero and one.***

There is no $n \in \mathbb{Z}$ such that $0 < n < 1$.

Proof. Suppose for the sake of contradiction there is $n \in \mathbb{Z}$ such that $0 < n < 1$.
Let $S = \{n \in \mathbb{Z} : 0 < n < 1\}$.
Then $n \in S$, so $S \neq \emptyset$.

Let $s \in S$.
Then $s \in \mathbb{Z}$ and $0 < s < 1$, so $0 < s$.
Since $s \in \mathbb{Z}$ and $s > 0$, then $s \in \mathbb{Z}^+$.
Hence, $s \in S$ implies $s \in \mathbb{Z}^+$, so $S \subset \mathbb{Z}^+$.

Since $S \subset \mathbb{Z}^+$ and $S \neq \emptyset$, then by WOP, S has a least element.
Let m be the least element of S.
Then $m \in S$ and $m \leq s$ for all $s \in S$.
Since $m \in S$, then $m \in \mathbb{Z}$ and $0 < m < 1$.
Since $0 < m < 1$, then $0 < m$ and $m < 1$ and $0 < m^2 < 1$.
Since $m \in \mathbb{Z}$, then $m^2 \in \mathbb{Z}$.
Since $m^2 \in \mathbb{Z}$ and $0 < m^2 < 1$, then $m^2 \in S$.
Since $m < 1$ and $m > 0$, then $m^2 = m \cdot m < m \cdot 1 = m$, so $m^2 < m$.
Thus, there is $m^2 \in S$ such that $m^2 < m$.
This contradicts the fact that m is the least element of S.
Therefore, there is no $n \in \mathbb{Z}$ such that $0 < n < 1$. □

Lemma 17. *For all $n \in \mathbb{Z}^+$, $n \geq 1$.*

Proof. Let $n \in \mathbb{Z}^+$ such that $n \neq 1$.
We must prove $n > 1$.

Suppose n is not greater than 1.
Then, by trichotomy, either $n = 1$ or $n < 1$.
Since $n \neq 1$, then we conclude $n < 1$.
Since $n \in \mathbb{Z}^+$, then $n > 0$.
Thus, $0 < n$ and $n < 1$, so $0 < n < 1$.
Hence, n is an integer between 0 and 1.
But, there is no integer between 0 and 1, by lemma 16.
Therefore, n is greater than 1, so $n > 1$, as desired. □

Theorem 18. ***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. Let T be the set of all positive integers not in S.
Then $T = \{t \in \mathbb{Z}^+ : t \notin S\}$.

Suppose $T \neq \emptyset$.

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

Let m be the least element of T.

Then $m \in T$ and $m \leq x$ for all $x \in T$.

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

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

By lemma 17, $n \geq 1$ for all $n \in \mathbb{Z}^+$.

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

Hence, either $m > 1$ or $m = 1$.

Since $m \neq 1$, then we conclude $m > 1$, 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 $m - 1 \in \mathbb{Z}^+$.

If $n \in \mathbb{Z}^+$, then either $n \in S$ or $n \notin S$, so either $n \in S$ or $n \in T$.

Since $m - 1 \in \mathbb{Z}^+$, then either $m - 1 \in S$ or $m - 1 \in T$.

Since $m - 1 < m$ and m is the least element of T, then $m - 1$ cannot be in T.

Hence, $m - 1 \notin T$.

Since either $m - 1 \in S$ or $m - 1 \in T$ and $m - 1 \notin T$, then we conclude $m - 1 \in S$.

By the induction hypothesis, if $m-1 \in \mathbb{Z}^+$ and $m-1 \in S$, then $(m-1)+1 = m \in S$.

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

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

Therefore, $T = \emptyset$.

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

Theorem 19. ***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. Let T be the set of all positive integers not in S.

Then $T = \{t \in \mathbb{Z}^+ : t \notin S\}$.

Suppose $T \neq \emptyset$.

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

Let m be the least element of T.

Then $m \in T$ and $m \leq x$ for all $x \in T$.

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

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

By lemma 17, $n \geq 1$ for all $n \in \mathbb{Z}^+$.
Since $m \in \mathbb{Z}^+$, then we conclude $m \geq 1$.
Hence, either $m > 1$ or $m = 1$.
Since $m \neq 1$, then we conclude $m > 1$, 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 $m - 1 \in \mathbb{Z}^+$.

If $n \in \mathbb{Z}^+$, then either $n \in S$ or $n \notin S$, so either $n \in S$ or $n \in T$.

Since $1, 2, ..., m - 1$ are positive integers, then $1, 2, ..., m - 1 \in \mathbb{Z}^+$.
Thus, each of $1, 2, ..., m - 1$ is either an element of S or an element of T.
Since $1 < 2 < ... < m - 1 < m$, then $1 < m$ and $2 < m$ and ... and $m - 1 < m$.
Hence, each of $1, 2, ..., m - 1$ is less than m, the least element of T.
Thus, each of $1, 2, ..., m - 1$ cannot be in T.
Hence, $1 \notin T$ and $2 \notin T$ and ... and $m - 1 \notin T$.
Since each of $1, 2, ..., m - 1$ is either an element of S or an element of T, and $1 \notin T$ and $2 \notin T$ and ... and $m - 1 \notin T$, then we conclude $1, 2, .., m - 1 \in S$.
By the induction hypothesis, if $m - 1 \in \mathbb{Z}^+$ and $1, 2, .., m - 1 \in S$, then $(m - 1) + 1 = m \in S$.
Since $m - 1 \in \mathbb{Z}^+$ and $1, 2, .., m - 1 \in S$, then we conclude $m \in S$.
Thus, we have $m \in S$ and $m \notin S$, a contradiction.
Therefore, $T = \emptyset$.

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

Proposition 20. *The set of all non-negative integers is well-ordered.*

Proof. Let S be the set of all non-negative integers.
Then $S = \{n \in \mathbb{Z} : n \geq 0\}$.
Let T be a non-empty subset of S.
Then $T \subset S$ and $T \neq \emptyset$.
Either $0 \in T$ or $0 \notin T$.
We consider these cases separately.
Case 1: Suppose $0 \notin T$.
Since $T \neq \emptyset$, then let $t \in T$.
Since $T \subset S$, then $t \in S$, so $t \in \mathbb{Z}$ and $t \geq 0$.
Since $t \geq 0$, then either $t > 0$ or $t = 0$.
Since $0 \notin T$ and $t \in T$, then $t \neq 0$.
Hence, $t > 0$.
Since $t \in \mathbb{Z}$ and $t > 0$, then $t \in \mathbb{Z}^+$.
Thus, $t \in T$ implies $t \in \mathbb{Z}^+$, so $T \subset \mathbb{Z}^+$.

By the well-ordering principle of $\mathbb{Z}^+$, every nonempty subset of $\mathbb{Z}^+$ has a least element.

Since $T \subset \mathbb{Z}^+$ and $T \neq \emptyset$, then T is a nonempty subset of $\mathbb{Z}^+$, so T has a least element.

Case 2: Suppose $0 \in T$.

Since $T \neq \emptyset$, let $x \in T$.

Then $x \in \mathbb{Z}$ and $x \geq 0$.

Thus, $x \geq 0$ for all $x \in T$, so $0 \leq x$ for all $x \in T$.

Since $0 \in T$ and $0 \leq x$ for all $x \in T$, then 0 is the least element of T.

Therefore, T has a least element.

In all cases, T has a least element.

Hence, if T is a nonempty subset of S, then T has a least element, so every nonempty subset of S has a least element.

Therefore, S is well-ordered. □

Theorem 21. ***Archimedean property of*** $\mathbb{Z}^+$

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

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

Proof. Suppose for the sake of contradiction $nb \leq a$ 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 $S \subset \mathbb{Z}^+ \cup \{0\}$.

Let $x \in S$.

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

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

Hence, $a - nb \geq 0$.

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 $a - nb \geq 0$, then $a - nb \in \mathbb{Z}^+ \cup \{0\}$, so $x \in \mathbb{Z}^+ \cup \{0\}$.

Therefore, $S \subset \mathbb{Z}^+ \cup \{0\}$.

By proposition 20, the set of all non-negative integers is well-ordered, so every nonempty subset of non-negative integers has a least element.

Since $S \subset \mathbb{Z}^+ \cup \{0\}$ and $S \neq \emptyset$, then we conclude S has a least element.

Let m be the least element of S.

Then $m \in S$ 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, $a - (k+1)b = a - kb - b < a - kb + 0 = m$, so $a - (k+1)b < m$.

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

Thus, there exists $a - (k+1)b \in S$ such that $a - (k+1)b < m$.

But, this contradicts the fact that m is the least element of S.

Therefore, the assumption is false, so there exists $n \in \mathbb{Z}^+$ such that $nb > a$. □

Proposition 22. *There is no greatest positive integer.*

Proof. Suppose there is a greatest positive integer.

Let g be a greatest positive integer.

Then $g \in \mathbb{Z}^+$ and $g \geq x$ for all $x \in \mathbb{Z}^+$.

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

Since $(g + 1) - g = g + 1 - g = g - g + 1 = 0 + 1 = 1$ and $1 \in \mathbb{Z}^+$, then $(g + 1) - g \in \mathbb{Z}^+$, so $g < g + 1$.

Hence, $g + 1 > g$.

Thus, there exists $g + 1 \in \mathbb{Z}^+$ such that $g + 1 > g$.

But, this contradicts g is a greatest positive integer.

Therefore, there is no greatest positive integer. □

Lemma 23. *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 $b \not\leq a$. □

Elementary Aspects of Integers

Proposition 24. ***No integer exists between two consecutive integers.***
Let $n \in \mathbb{Z}$.
There is no $m \in \mathbb{Z}$ such that $n < m < n + 1$.

Proof. Suppose there is $m \in \mathbb{Z}$ such that $n < m < n + 1$.
Then $n < m$ and $m < n + 1$.
Since $n < m$, then there exists $k \in \mathbb{Z}^+$ such that $n + k = m$.
Since $k \in \mathbb{Z}^+$, then $k \geq 1$, so $m - n \geq 1$ and $m - n \in \mathbb{Z}^+$.
Since $m < n + 1$, then $m - n < 1$.
Since $m - n \in \mathbb{Z}^+$ and $\mathbb{Z}^+ \subset \mathbb{Z}$, then $m - n \in \mathbb{Z}$.
Since $m - n \in \mathbb{Z}$ and $m - n < 1$ and $m - n \geq 1$, then we have a violation of trichotomy.
Therefore, there is no $m \in \mathbb{Z}$ such that $n < m < n + 1$. □

Proposition 25. *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 $k + 1 \in S$.
Thus, $k \in S$ implies $k + 1 \in S$ for all $k \in \mathbb{Z}^+$.

Since $1 \in S$ and $k \in S$ implies $k + 1 \in S$ for all $k \in \mathbb{Z}^+$, then by induction, $S = \mathbb{Z}$.
Hence, $S = \mathbb{Z}^+$, so if $n \in \mathbb{Z}^+$, then n is even or n is odd.
Therefore, every positive integer is even or odd. □

Proposition 26. *An integer is not both even and odd.*

Proof. Let n be an integer.
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, $1 = 2k - 2m = 2(k - m)$.
Since $k - m \in \mathbb{Z}$ and $1 = 2(k - m)$, then 1 is even.
But, this contradicts the fact that 1 is not even.
Therefore, n is not both even and odd. □

Proposition 27. ***A product of two consecutive integers is even.***
If $n \in \mathbb{Z}$, then $n(n + 1)$ is even.

Proof. Let $n \in \mathbb{Z}$.
Either n is even or n is not even.
We consider these cases separately.
Case 1: Suppose n is even.
Then $n = 2s$ for some integer s.
Thus, $n(n + 1) = 2s(2s + 1)$.
Since $s(2s + 1) \in \mathbb{Z}$ and $n(n + 1) = 2s(2s + 1)$, then $n(n + 1)$ is even.
Case 2: Suppose n is not even.
Then n is odd, so $n = 2t + 1$ for some integer t.
Thus, $n(n + 1) = (2t + 1)[(2t + 1) + 1] = (2t + 1)(2t + 2) = 2(2t + 1)(t + 1)$.
Since $(2t + 1)(t + 1) \in \mathbb{Z}$ and $n(n + 1) = 2(2t + 1)(t + 1)$, then $n(n + 1)$ is even.

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

Natural Number Formulae

Proposition 28. *Let $n \in \mathbb{Z}^+$.*
The sum of the first n positive integers is $\dfrac{n(n + 1)}{2}$.

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. Define predicate $p(n)$ over $\mathbb{Z}^+$ by '$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$'.

We prove $p(n)$ is true for all $n \in \mathbb{Z}^+$ by induction on n.

Basis:

Let $n = 1$.

Then $\sum_{k=1}^{1} k = 1 = \frac{2}{2} = \frac{1 \cdot 2}{2} = \frac{1(1+1)}{2}$, so $p(1)$ is true.

Induction:

Let $m \in \mathbb{Z}^+$ such that $p(m)$ is true.

Then $\sum_{k=1}^{m} k = \frac{m(m+1)}{2}$.

Observe that

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

Thus, $p(m+1)$ is true, so $p(m)$ implies $p(m+1)$ for all $m \in \mathbb{Z}^+$.

Since $p(1)$ is true and $p(m)$ implies $p(m+1)$ for all $m \in \mathbb{Z}^+$, then $p(n)$ is true for all $n \in \mathbb{Z}^+$.

Therefore, $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$ for all $n \in \mathbb{Z}^+$. □

Proposition 29. *Let $n \in \mathbb{Z}^+$.*

The sum of the first n odd positive integers 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

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

Let

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

We expand this sum to show the terms

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

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 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 positive integers).

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

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

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

Let $S = \{n \in \mathbb{Z}^+ : \sum_{k=1}^{n}(2k-1) = n^2\}$.
Basis:
Since $1 \in \mathbb{Z}^+$ 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 $m \in \mathbb{Z}^+$ and $\sum_{k=1}^{m}(2k-1) = m^2$.
Since $m \in \mathbb{Z}^+$, then $m+1 \in \mathbb{Z}^+$.
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 30. *Let $n \in \mathbb{Z}^+$.*

The sum of the squares of the first n positive integers is $\dfrac{n(n+1)(2n+1)}{6}$.

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

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 31. *The sum of the cubes of the first n positive integers 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 $n \in \mathbb{Z}^+$.

We prove by induction on n.

Let $S = \{n \in \mathbb{Z}^+ : \sum_{k=1}^{n} k^3 = \frac{n^2(n+1)^2}{4}\}$.

Basis:

Since $1 \in \mathbb{Z}^+$ 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 $m \in \mathbb{Z}^+$ and $\sum_{k=1}^{m} k^3 = \frac{m^2(m+1)^2}{4}$.

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

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

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

□

Proposition 32. *A positive integer is triangular iff it is of the form* $\frac{n(n+1)}{2}$ *for some* $n \in \mathbb{Z}^+$.

Proof. We prove 'if a positive integer is triangular, then it is of the form $\frac{n(n+1)}{2}$ for some $n \in \mathbb{Z}^+$.

Suppose a positive integer is triangular.

Let t be a positive integer that is triangular.

Then $t \in \mathbb{Z}^+$ and t is triangular.

Since t is triangular, then t is the sum of consecutive integers, beginning with 1.

Therefore, there exists an integer n such that t is the sum of n consecutive integers, beginning with 1.

Hence, $t = \sum_{i=1}^{n} i$.

Thus, t is the sum of the first n positive integers, so $t = \frac{n(n+1)}{2}$.

Therefore, $t = \frac{n(n+1)}{2}$ for some $n \in \mathbb{Z}^+$. □

Proof. Conversely, we prove 'if a positive integer is of the form $\frac{n(n+1)}{2}$ for some $n \in \mathbb{Z}^+$, then it is triangular".

Suppose a positive integer is of the form $\frac{n(n+1)}{2}$ for some $n \in \mathbb{Z}^+$.

Let t be a positive integer of the form $\frac{n(n+1)}{2}$ for some $n \in \mathbb{Z}^+$.

Then $t \in \mathbb{Z}^+$ and $t = \frac{n(n+1)}{2}$ for some $n \in \mathbb{Z}^+$.

Since $t = \dfrac{n(n+1)}{2} = \sum_{k=1}^{n} k$, then t is the sum of the first n positive integers.

Hence, t is the sum of n consecutive integers, beginning with one.

Therefore, t is triangular. □

Proposition 33. *Let t_n denote the n^{th} triangular number.*

Then $t_n = \binom{n+1}{2}$ for all $n \in \mathbb{Z}^+$.

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

Observe that

$$\begin{aligned} t_n &= \frac{n(n+1)}{2} \\ &= \frac{(n+1)n}{2} \\ &= \frac{(n+1)n}{2!} \\ &= \frac{(n+1)n(n-1)!}{(n-1)!2!} \\ &= \frac{(n+1)!}{(n-1)!2!} \\ &= \frac{(n+1)!}{(n+1-2)!2!} \\ &= \binom{n+1}{2}. \end{aligned}$$

□

Divisibility in $\mathbb{Z}$

Theorem 34. ***Division Algorithm***

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

Then there exist unique integers q and r such that $a = bq + r$ and $0 \leq r < b$.

Proof. **Existence:**

Let $S = \{a - bk : (\exists k \in \mathbb{Z})(a - bk \geq 0)\}$.

Since $a \in \mathbb{Z}$, then either $a \geq 0$ or $a < 0$.

We consider these cases separately.

Case 1: Suppose $a \geq 0$.

Let $k = 0$.

Then $k \in \mathbb{Z}$ and $a - bk = a - b(0) = a - 0 = a \geq 0$.

Hence, there exists $k \in \mathbb{Z}$ such that $a - bk \geq 0$, so $a - bk \in S$.

Therefore, $S \neq \emptyset$.

Case 2: Suppose $a < 0$.

Let $k = a$.
Since $a \in \mathbb{Z}$, then $k \in \mathbb{Z}$.
Since $b \in \mathbb{Z}$ and $b > 0$, then $b \geq 1$, so $0 \geq 1 - b$.
Since $a < 0$ and $1 - b \leq 0$, then $a(1 - b) \geq 0$.
Observe that $a - bk = a - ba = a(1 - b) \geq 0$.
Hence, there exists $k \in \mathbb{Z}$ such that $a - bk \geq 0$, so $a - bk \in S$.
Therefore, $S \neq \emptyset$.

In all cases, we have $S \neq \emptyset$,
Let $s \in S$.
Then $s = a - bk$ and $s \geq 0$ for some integer k.
Since $a, b, k \in \mathbb{Z}$, then $a - bk \in \mathbb{Z}$, so $s \in \mathbb{Z}$
Since $s \in \mathbb{Z}$ and $s \geq 0$, then S is a set of non-negative integers.
Since S is a set of non-negative integers and $S \neq \emptyset$, then S is a nonempty set of nonnegative integers.
By proposition 20, the set of all nonnegative integers is well-ordered, so every nonempty subset of nonnegative integers has a least element.
Hence, S has a least element.

Let r be the least element of S.
Then $r \in S$ 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 $r = a - bq$, then $a = bq + r$.
Either $r > b$ or $r = b$ or $r < b$.

Suppose $r \geq b$.
Then $a - bq \geq b$, so $a - bq - b \geq 0$.
Thus, $a - b(q + 1) \geq 0$.
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 $b > 0 = r - r$, then $r + b > r$, so $r > r - b = (a - bq) - b = a - bq - b = a - b(q + 1)$.
Thus, $r > a - b(q + 1)$.
Since $r \leq x$ for all $x \in S$ and $a - b(q+1) \in S$, then we conclude $r \leq a - b(q+1)$.
Hence, we have $r > a - b(q + 1)$ and $r \leq a - b(q + 1)$, a contradiction.
Therefore, r cannot be greater than or equal to b.

Since either $r > b$ or $r = b$ or $r < b$ and r cannot be greater than or equal to b, then we conclude $r < b$.
Since $0 \leq r$ and $r < b$, then $0 \leq r < b$.

Therefore, there exist integers q and r such that $a = bq + r$ and $0 \leq r < b$. $\square$

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 $b(q_1 - q_2) = r_2 - r_1$.

Since $q_1 - q_2 \in \mathbb{Z}$ and $r_2 - r_1 = b(q_1 - q_2)$, then $b|(r_2 - r_1)$, 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, $-b < r_2 - r_1 < b$.

Since $r_2 - r_1$ is a multiple of b and $-b < r_2 - r_1 < b$ and the only multiple of b between $-b$ and b is zero, then we must conclude $r_2 - r_1 = 0$.

Therefore, $r_2 = r_1$, so $r_1 = r_2$.

Hence, $0 = r_2 - r_1 = b(q_1 - q_2)$, so either $b = 0$ or $q_1 - q_2 = 0$.

Since $b > 0$, then $b \neq 0$, so $q_1 - q_2 = 0$.

Therefore, $q_1 = q_2$.

Since $r_1 = r_2$ and $q_1 = q_2$, then r is unique and q is unique. $\square$

Proposition 35. *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 $n|0$. $\square$

Proposition 36. *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 $1|n$. $\square$

Proposition 37. *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 $n|n$. $\square$

Theorem 38. ***necessary and sufficient condition for*** $b|a$

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

Then $b|a$ iff the remainder is zero when a is divided by b.

Proof. We prove if the remainder is zero when a is divided by b, then $b|a$.

Suppose the remainder is zero when a is divided by b.

Since $a, b \in \mathbb{Z}$ and $b > 0$, then by the division algorithm, there exist unique integers q and r such that $a = bq + r$ and $0 \leq r < b$.

Since the remainder is zero when a is divided by b, then $r = 0$.

Thus, $a = bq + 0 = bq$.

Since $q \in \mathbb{Z}$ and $a = bq$, then $b|a$. $\square$

Proof. Conversely, we prove if $b|a$, then the remainder is zero when a is divided by b.

Suppose $b|a$.

Then $a = bn$ for some integer n, so $a = bn + 0$.

Since $a, b \in \mathbb{Z}$ and $b > 0$, then by the division algorithm, there exist unique integers q and r such that $a = bq + r$ and $0 \leq r < b$.

Since q and r are unique integers and $a = bq+r$ and $a = bn+0$ and $0 \leq r < b$, then we must conclude $q = n$ and $r = 0$.

Therefore, $r = 0$, so the remainder is zero when a is divided by b. □

Theorem 39. ***A divisor of*** a ***is smaller than*** a**.**

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

If $d|a$*, then* $d \leq a$.

Proof. Suppose $d|a$.

Then $a = dn$ for some integer n.

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

Since $a = dn$ and $a > 0$ and $d > 0$, then $n > 0$.

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

Hence, $n \geq 1$, by lemma 17.

Since $n \geq 1$ and $d > 0$, then $a = dn \geq d \cdot 1 = d$.

Therefore, $a \geq d$, so $d \leq a$. □

Proof. Suppose $d|a$.

Then $a = dn$ for some integer n.

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

Since $a = dn$ and $a > 0$ and $d > 0$, 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 $d = d \cdot 1 = dn = a$, so $d = a$.

Case 2: Suppose $n > 1$.

Then $0 > 1 - n$.

Since $d > 0$ and $1 - n < 0$, then $d(1 - n) < 0$.

Since $d - a = d - dn = d(1 - n) < 0$, then $d - a < 0$, so $d < a$.

Therefore, in all cases, $d \leq a$. □

Proposition 40. *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.

Thus, $bd = (am)(cn) = a(mc)n = a(cm)n = (ac)(mn)$.

Since mn is an integer and $bd = (ac)(mn)$, then $ac|bd$. □

Proposition 41. ***The only integers whose product is one are one and negative one.***

Let $a, b \in \mathbb{Z}$.
Then $ab = 1$ iff $a = b = 1$ or $a = b = -1$.

Proof. We prove if $a = b = 1$ or $a = b = -1$, then $ab = 1$.
Suppose $a = b = 1$ or $a = b = -1$.
We consider these cases separately.
Case 1: Suppose $a = b = 1$.
Then $ab = 1 \cdot 1 = 1$, so $ab = 1$.
Case 2: Suppose $a = b = -1$.
Then $ab = (-1)(-1) = 1$, so $ab = 1$. □

Proof. Conversely, we prove if $ab = 1$, then either $a = b = 1$ or $a = b = -1$.
Suppose $ab = 1$.
Since $ab = 1 > 0$, then $ab > 0$, so either $a > 0$ and $b > 0$ or $a < 0$ and $b < 0$.
We consider these cases separately.
Case 1: Suppose $a > 0$ and $b > 0$.
Suppose $a \neq 1$.
Since $a \in \mathbb{Z}$ and $a > 0$ and $a \neq 1$, then $a > 1$.
Since $a > 1$ and $b > 0$, then $ab > b$.
Since $b \in \mathbb{Z}$ and $b > 0$, then $b \geq 1$.
Thus, $ab > b \geq 1$, so $ab > 1$.
But, this contradicts the hypothesis $ab = 1$.
Thus, $a = 1$.

Hence, $1 = ab = (1)b = b$, so $b = 1$.
Therefore, $a = 1 = b$.
Case 2: Suppose $a < 0$ and $b < 0$.
Suppose $a \neq -1$.
Since $a \in \mathbb{Z}$ and $a < 0$ and $a \neq -1$, then $a < -1$.
Since $a < -1$ and $b < 0$, then $ab > -b$, so $-ab < b$.
Since $b \in \mathbb{Z}$ and $b < 0$, then $b \leq -1$.
Thus, $-ab < b \leq -1$, so $-ab < -1$.
Hence, $ab > 1$.
But, this contradicts the hypothesis $ab = 1$.
Thus, $a = -1$.

Hence, $1 = ab = (-1)b = -b$, so $b = -1$.
Therefore, $a = -1 = b$.

We conclude either $a = b = 1$ or $a = b = -1$, as desired. □

Proposition 42. *Let $a \in \mathbb{Z}$ and $b \in \mathbb{Z}$.*
If $a|b$ and $b|a$, then $a = \pm b$.

Proof. Suppose $a|b$ and $b|a$.

Then $b = ak_1$ and $a = bk_2$ for some integers k_1 and k_2.

Thus, $b = (bk_2)k_1 = b(k_2k_1) = b(k_1k_2)$, so $b(k_1k_2) - b = 0$.

Hence, $b(k_1k_2 - 1) = 0$.

Either $b = 0$ or $b \neq 0$.

We consider these cases separately.

Case 1: Suppose $b = 0$.

Since $b|a$, then $0|a$, so $a = 0k_3 = 0$ for some integer k_3.

Hence, $a = 0 = b$, so $a = b$.

Case 2: Suppose $b \neq 0$.

Then $k_1k_2 - 1 = 0$, so $k_1k_2 = 1$.

By proposition 41, the only integers whose product is one are one and negative one.

Since k_1 and k_2 are integers and $k_1k_2 = 1$, then we conclude either $k_1 = k_2 = 1$ or $k_1 = k_2 = -1$.

Hence, either $b = a(k_1) = a(1) = a$ or $b = a(k_1) = a(-1) = -a$, so either $b = a$ or $b = -a$.

Therefore, either $a = b$ or $a = -b$, so $a = \pm b$. □

Theorem 43. *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 $mk \in \mathbb{Z}$.

Since $mk \in \mathbb{Z}$ and $ma = d(mk)$, then $d \mid ma$. □

Proposition 44. *Let $a, b, n \in \mathbb{Z}$.*

1. If $a|b$, then $na|nb$.

2. If $n \neq 0$ and $na|nb$, then $a|b$.

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 and $nb = (na)k$, then $na|nb$. □

Proof. We prove 2.

Suppose $n \neq 0$ and $na|nb$.

Since $na|nb$, then $nb = (na)k$ for some integer k.

Thus, $0 = nb - (na)k = nb - n(ak) = n(b - ak)$, so either $n = 0$ or $b - ak = 0$.

Since $n \neq 0$, then we conclude $b - ak = 0$, so $b = ak$.

Since $k \in \mathbb{Z}$ and $b = ak$, then $a|b$. □

Theorem 45. ***The divides relation on $\mathbb{Z}$ 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, $c = bn = (am)n = a(mn)$.
Since mn is an integer and $c = a(mn)$, then $a|c$. □

Theorem 46. *The divides relation is a partial order over $\mathbb{Z}^+$.*

Proof. We prove the divides relation is reflexive.
Let $a \in \mathbb{Z}^+$ be arbitrary.
Since $a \in \mathbb{Z}^+$ and $\mathbb{Z}^+ \subseteq \mathbb{Z}$, then $a \in \mathbb{Z}$.
By proposition 37, every integer divides itself, so $a|a$.
Therefore, $|$ is reflexive. □

Proof. We prove the divides relation is antisymmetric.
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, $a = bk_2 = (ak_1)k_2 = a(k_1k_2)$, so $a(k_1k_2) - a = 0$.
Thus, $a(k_1k_2 - 1) = 0$, so either $a = 0$ or $k_1k_2 - 1 = 0$.
Since $a > 0$, then $a \neq 0$, so we conclude $k_1k_2 - 1 = 0$.
Therefore, $k_1k_2 = 1$.
By proposition 41, 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, $a = bk_2 = b(1) = b$, so $a = b$. □

Proof. We prove the divides relation is transitive.
Let $a, b, c \in \mathbb{Z}^+$.
The divides relation defined on $\mathbb{Z}$ is transitive, by theorem 45.
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 on $\mathbb{Z}^+$ is reflexive, antisymmetric, and transitive, then the divides relation is a partial order over $\mathbb{Z}^+$. □

Greatest common divisor

Proposition 47. *Let $n \in \mathbb{Z}$.*
Then n and $-n$ have the same set of divisors.

Proof. Let S be the set of all divisors of n.
Let T be the set of all divisors of $-n$.
Then $S = \{d \in \mathbb{Z} : d|n\}$ and $T = \{d \in \mathbb{Z} : d| - n\}$.
We must prove $S = T$.

We prove $T \subset S$.
Let $t \in T$.
Then $t \in \mathbb{Z}$ and $t| - n$.
Since $t| - n$, then $-n = ta$ for some integer a.
Thus, $n = -(-n) = -(ta) = t(-a)$.
Since $-a \in \mathbb{Z}$ and $n = t(-a)$, then $t|n$.
Since $t \in \mathbb{Z}$ and $t|n$, then $t \in S$.
Thus, $t \in T$ implies $t \in S$, so $T \subset S$. □

Proof. We prove $S \subset T$.
Let $s \in S$.
Then $s \in \mathbb{Z}$ and $s|n$.
Since $s|n$, then $n = sb$ for some integer b.
Thus, $-n = -sb = s(-b)$.
Since $-b \in \mathbb{Z}$ and $-n = s(-b)$, then $s| - n$.
Since $s \in \mathbb{Z}$ and $s| - n$, then $s \in T$.
Hence, $s \in S$ implies $s \in T$, so $S \subset T$. □

Proof. Since $S \subset T$ and $T \subset S$, then $S = T$. □

Proposition 48. ***A positive common divisor is bounded.***
Let $a, b \in \mathbb{Z}^+$ and $a \neq b$.
Let d be a positive common divisor of a and b.
Then $1 \leq d \leq \min(a, b)$.

Proof. Since d is a positive common divisor of a and b, then $d \in \mathbb{Z}^+$ and $d|a$ and $d|b$.
Since $d \in \mathbb{Z}^+$, then $d \in \mathbb{Z}$ and $d > 0$, so $d \geq 1$.
Let m be the minimum of a and b.
Since $a \neq b$, then either $a < b$ or $a > b$.
We consider these cases separately.
Case 1: Suppose $a < b$.
Then the minimum of a and b is a, so $m = a$.
Since $d, a \in \mathbb{Z}^+$ and $d|a$, then $d \leq a$, so $d \leq m$.
Since $d \geq 1$ and $d \leq m$, then $1 \leq d \leq m$.
Case 2: Suppose $b < a$.
Then the minimum of a and b is b, so $m = b$.

Since $d, b \in \mathbb{Z}^+$ and $d|b$, then $d \leq b$, so $d \leq m$.
Since $d \geq 1$ and $d \leq m$, then $1 \leq d \leq m$.

Therefore, in all cases, $1 \leq d \leq m$, as desired. □

Lemma 49. ***Any common divisor of*** a ***and*** b ***divides their sum and difference.***
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 $a = ds$ and $b = dt$ for some integers s and t.
Hence, $a + b = ds + dt = d(s + t)$ and $a - b = ds - dt = d(s - t)$.
Since $s + t \in \mathbb{Z}$ and $a + b = d(s + t)$, then $d|(a + b)$.
Since $s - t \in \mathbb{Z}$ and $a - b = d(s - t)$, then $d|(a - b)$. □

Theorem 50. ***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 s and t such that $a = ds$ and $b = dt$.
Let m and n be arbitrary integers.
Then $ma + nb = m(ds) + n(dt) = m(sd) + n(td) = (ms)d + (nt)d = (ms + nt)d = d(ms + nt)$.
Since $ms + nt$ is an integer and $ma + nb = d(ms + nt)$, then $d|(ma + nb)$. □

Corollary 51. ***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. We prove by induction on n.
Define predicate $p(n)$ over $\mathbb{Z}^+$ by 'if $d|a_1$, $d|a_2$, ..., $d|a_n$, then $d|(c_1a_1 + c_2a_2 + ... + c_na_n)$ for any integers $c_1, c_2, ..., c_n$'.
Basis:
Let $n = 1$.
Suppose $d|a_1$.
Then d divides any multiple of a_1, by theorem 43.
Hence, $d|c_1a_1$ for some integer c_1.
Therefore, $p(1)$ is true.

Let $n = 2$.

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

Then d divides any linear combination of a_1 and a_2, by theorem 50.

Therefore, $d|(c_1a_1 + c_2a_2)$ for some integers c_1 and c_2, so $p(2)$ is true.

Induction:

Let $k \in \mathbb{Z}^+$ with $k \geq 2$ such that $p(k)$ is true.

Since $p(k)$ is true, then $d|(c_1a_1+c_2a_2+...+c_ka_k)$ for any integers $c_1, c_2, ..., c_k$ whenever $d|a_1$ and $d|a_2$ and ... and $d|a_k$.

We must prove $p(k+1)$ is true.

Suppose $d|a_1$ and $d|a_2$ and ... and $d|a_k$ and $d|a_{k+1}$.

Since $d|a_1$ and $d|a_2$ and ... and $d|a_k$, then by the induction hypothesis, $d|(c_1a_1 + c_2a_2 + ... + c_ka_k)$ for any integers $c_1, c_2, ..., c_k$.

Since $d|a_{k+1}$, then d divides any multiple of a_{k+1}, by theorem 43.

Hence, $d|c_{k+1}a_{k+1}$ for some integer c_{k+1}.

Since d divides the integer $c_1a_1 + c_2a_2 + ... + c_ka_k$ and d divides the integer $c_{k+1}a_{k+1}$, then d divides the sum $(c_1a_1+c_2a_2+...+c_ka_k)+c_{k+1}a_{k+1}$, by lemma 49.

Thus, d divides $c_1a_1 + c_2a_2 + ... + c_ka_k + c_{k+1}a_{k+1}$, so $p(k+1)$ is true.

Hence, $p(k+1)$ is true whenever $p(k)$ is true for all $k \in \mathbb{Z}^+$ with $k \geq 2$.

Since $p(1)$ is true and $p(2)$ is true, and $p(k+1)$ is true whenever $p(k)$ is true for all $k \in \mathbb{Z}^+$ with $k \geq 2$, then by induction, $p(k)$ is true for all $k \in \mathbb{Z}^+$.

Therefore, for all $n \in \mathbb{Z}^+$, if $d|a_1$, $d|a_2$, ..., $d|a_n$, then $d|(c_1a_1+c_2a_2+...+c_na_n)$ for any integers $c_1, c_2, ..., c_n$. □

Theorem 52. ***existence and uniqueness of greatest common divisor***

Let $a, b \in \mathbb{Z}$ with a and b not both zero..

The greatest common divisor of a and b exists and is unique.

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

Proof. **Existence:**

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

We prove $S \neq \emptyset$.

Since a and b are integers not both zero, then either $a \neq 0$ or $b \neq 0$.

We consider these cases separately.

Case 1: Suppose $a \neq 0$.

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

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

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

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

Case 2: Suppose $b \neq 0$.

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

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

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

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

In all cases, $S \neq \emptyset$.

Since $S \subset \mathbb{Z}^+$ and $S \neq \emptyset$, then by the well-ordering principle, 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 $d \leq x$ for every $x \in S$.

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

By the Division Algorithm, when a is divided by d, 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 $1 - m_0q$ and $-n_0q$ are integers and $r = a(1 - m_0q) + b(-n_0q)$, then r is a linear combination of a and b.

Since $r = a(1 - m_0q) + b(-n_0q)$ and $r > 0$ and $1 - m_0q$ and $-n_0q$ are integers, then $r \in S$.

Since $d \leq x$ for every $x \in S$ and $r \in S$, then we conclude $d \leq r$, 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 $d = m_0a + n_0b = m_0(ck_1) + n_0(ck_2) = c(m_0k_1) + c(n_0k_2) = c(m_0k_1 + n_0k_2)$.

Since $m_0k_1 + n_0k_2$ is an integer and $d = c(m_0k_1 + n_0k_2)$, 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.

Therefore, 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 53. ***properties of gcd***

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

Proof. We prove 1.

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

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

By proposition 37, every integer divides itself, so $a|a$.

By proposition 35, 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.

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

By proposition 36, 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 37, 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 $a = \gcd(a, a)$. $\square$

Proof. We prove 4.

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

Then a and b are nonzero integers, so $a \neq 0$ and $b \neq 0$.

Hence, a and b are not both zero, so $\gcd(a, b)$ 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 $c|b$.

Since $c|a$ and $c|b$, then we conclude $c|d$.

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

Proof. We prove 5.

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

Then a and b are nonzero integers, so $a \neq 0$ and $b \neq 0$.

Hence, a and b are not both zero, so $\gcd(a, b)$ 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 $d = \gcd(-a, -b)$. □

Proof. We prove 6.

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

Since a and b are non-negative integers, then $a \neq 0$ and $b \neq 0$, so a and b are not both zero.

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

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 $k|k$ and $d|a$, then $kd|ka$, by proposition 40.

Since $k|k$ and $d|b$, then $kd|kb$, by proposition 40.

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

Let c be 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 by theorem 50, 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, $\gcd(ka, kb) = kd = k\gcd(a, b)$. □

Lemma 54. *The only positive integer that divides* 1 *is* 1.

Proof. We must prove 1 divides 1 and any positive integer other than 1 does not divide 1.

We prove 1 divides 1.

Since $1 \in \mathbb{Z}$ and $1 = 1 \cdot 1$, then 1 divides 1. □

Proof. To prove any positive integer other than 1 does not divide 1, let $a \in \mathbb{Z}^+$ and $a \neq 1$.

We must prove a does not divide 1.

Suppose for the sake of contradiction a divides 1.

Then $1 = ak$ for some integer k.

Since $a \in \mathbb{Z}^+$ and $a \neq 1$, then $a > 1$, so $a \neq 0$.

Since $ak = 1$ and $a \neq 0$, then $k = \frac{1}{a}$.

Since $a > 1$, then $\frac{1}{a}$ is not an integer, so k is not an integer.

But, this contradicts that k is an integer.

Thus, a does not divide 1.

Therefore, any positive integer other than 1 does not divide 1.

Since 1 divides 1 and any positive integer other than 1 does not divide 1, then 1 is the only positive integer that divides 1. □

Theorem 55. *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 50, 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 $\gcd(a, b)$. □

Proof. 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 and $c = (km)a + (kn)b$, then c is a linear combination of a and b. □

Corollary 56. *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.

Therefore, there exist integers m and n such that $1 = ma+nb$, as desired. □

Proof. 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 $\gcd(a, b)$ by theorem 55, then 1 is a multiple of $\gcd(a, b)$.

Therefore, $\gcd(a, b)$ divides 1.

By lemma 54, the only positive integer that divides 1 is 1.

Since $\gcd(a, b)$ is a positive integer and the only positive integer that divides 1 is 1, then $\gcd(a, b) = 1$, as desired. □

Corollary 57. *Let $a, b \in \mathbb{Z}$.*

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

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

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

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

Since $d \in \mathbb{Z}^+$, then $d > 0$, so $d \neq 0$.

Since $d|a$, then $a = dr$ for some integer r, so $r = \frac{a}{d}$.

Since $d|b$, then $b = ds$ for some integer s, so $s = \frac{b}{d}$.

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 obtain $m(\frac{a}{d}) + n(\frac{b}{d}) = 1$.

Since $\frac{a}{d} \in \mathbb{Z}$ and $\frac{b}{d} \in \mathbb{Z}$ and $m \in \mathbb{Z}$ and $n \in \mathbb{Z}$ and $m(\frac{a}{d}) + n(\frac{b}{d}) = 1$, then $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$, by corollary 56. □

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

Then $d \in \mathbb{Z}^+$ and $d|a$ and $d|b$, and any common divisor of a and b divides d.

Since $d|a$, then $a = dr$ for some integer r, so $r = \frac{a}{d}$.

Since $d|b$, then $b = ds$ for some integer s, so $s = \frac{b}{d}$.

Since $d = \gcd(a, b)$, then a and b are integers not both zero, so either $a \neq 0$ or $b \neq 0$.

Since $d \in \mathbb{Z}^+$, then $d > 0$, so $d \neq 0$.

Since $r = \dfrac{a}{d}$ and $s = \dfrac{b}{d}$ and $d \neq 0$, and either $a \neq 0$ or $b \neq 0$, then either $r \neq 0$ or $s \neq 0$, so r and s are not both zero.

Since r and s are integers, and r and s are not both zero, then $\gcd(r, s)$ exists and is unique.

Let $c = \gcd(r, s)$.

Then $c \in \mathbb{Z}^+$ and $c|r$ and $c|s$.

Since $c|r$, then $r = cx$ for some integer x.

Since $c|s$, then $s = cy$ for some integer y.

Since $r = cx$, then $a = dr = d(cx) = (dc)x$.

Since $s = cy$, then $b = ds = d(cy) = (dc)y$.

Since $x \in \mathbb{Z}$ and $a = (dc)x$, then $dc|a$.

Since $y \in \mathbb{Z}$ and $b = (dc)y$, then $dc|b$.

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

Since any common divisor of a and b divides d, then we conclude $dc|d$.

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

Since $c > 0$, then $c \neq 0$.

Since $c \in \mathbb{Z}$ and $c \neq 0$ and $dc|d$, then $c|1$, by proposition 44.

By proposition 36, 1 divides every integer.

Since $c \in \mathbb{Z}$, then we conclude $1|c$.

By theorem 46, the divides relation is antisymmetric.

Since $c \in \mathbb{Z}^+$ and $c|1$ and $1|c$, then we conclude $c = 1$.

Therefore, $\gcd(\dfrac{a}{d}, \dfrac{b}{d}) = \gcd(r, s) = c = 1$, so $\gcd(\dfrac{a}{d}, \dfrac{b}{d}) = 1$, as desired. $\square$

Theorem 58. *Let $a, b, d \in \mathbb{Z}$.*

If $d|ab$ and $\gcd(d, a) = 1$, 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 $kd + ma = 1$, by corollary 56.

Since $d|ab$, then $ab = dn$ for some integer n.

Observe that

$$\begin{aligned} b &= b \cdot 1 \\ &= b(kd + ma) \\ &= bkd + bma \\ &= bkd + mba \\ &= bkd + m(ab) \\ &= bkd + m(dn) \\ &= bkd + mdn \\ &= d(bk + mn). \end{aligned}$$

Since $b = d(bk + mn)$ and $bk + mn$ is an integer, 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 $kd+ma = 1$, by corollary 56.

Thus, $b = b \cdot 1 = b(kd + ma) = bkd + bma = bkd + mba = bkd + mab = (bk)d + m(ab)$ 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 $d|b$. □

Theorem 59. *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 $x, y \in \mathbb{Z}$, by corollary 56.

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 $k_2x + k_1y \in \mathbb{Z}$.

Since $k_2x + k_1y \in \mathbb{Z}$ and $m = ab(k_2x + k_1y)$, then $ab|m$. □

Proof. Suppose $a|m$ and $b|m$ and $\gcd(a, b) = 1$.

Since $b|m$, then $m = bs$ for some integer s.

Since $a|m$ and $m = bs$, then $a|bs$.

Since $a|bs$ and $\gcd(a, b) = 1$, then $a|s$, by theorem 58.

Thus, $s = at$ for some integer t.

Hence, $m = bs = b(at) = (ba)t = (ab)t$.

Since $t \in \mathbb{Z}$ and $m = (ab)t$, then $ab|m$. □

Euclidean Algorithm

Lemma 60. ***Euclidean Algorithm lemma***

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 61. ***Euclidean Algorithm***

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

Let n be the number of iterative steps and

$$\begin{aligned}
a &= bq_1 + r_1, \text{ where } 0 < r_1 < b \\
b &= r_1q_2 + r_2, \text{ where } 0 < r_2 < r_1 \\
r_1 &= r_2q_3 + r_3, \text{ where } 0 < r_3 < r_2 \\
&\cdots \\
r_k &= r_{k+1}q_{k+2} + r_{k+2}, \text{ where } 0 < r_{k+2} < r_{k+1} \\
&\cdots \\
r_{n-3} &= r_{n-2}q_{n-1} + r_{n-1}, \text{ where } 0 < r_{n-1} < r_{n-2} \\
r_{n-2} &= r_{n-1}q_n + 0.
\end{aligned}$$

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 60.

By the division algorithm, $b = r_1q_2 + r_2$ and $0 < r_2 < r_1$, so $\gcd(b, r_1) = \gcd(r_1, r_2)$ by lemma 60.

By the division algorithm, $r_1 = r_2q_3 + r_3$ and $0 < r_3 < r_2$, so $\gcd(r_1, r_2) = \gcd(r_2, r_3)$ by lemma 60.

We repeat this process a finite number of times, so $r_k = r_{k+1}q_{k+2} + r_{k+2}$ and $0 < r_{k+2} < r_{k+1}$, so $\gcd(r, r_{k+1}) = \gcd(r_{k+1}, r_{k+2})$ by lemma 60.

On the final n^{th} step, we have $r_{n-2} = r_{n-1}q_n + r_n$ and $r_n = 0$, so $\gcd(r_{n-2}, r_{n-1}) = \gcd(r_{n-1}, r_n) = \gcd(r_{n-1}, 0) = r_{n-1}$.

On the final n^{th} step, the quotient is q_n and the remainder is $r_n = 0$ and the previous remainder r_{n-1} is the greatest common divisor of a and b. $\square$

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

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

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}.

Since $r_{n-3} = r_{n-2}q_{n-1} + r_{n-1}$ is a linear combination of r_{n-1} and r_{n-2}, then $r_{n-1}|r_{n-3}$.

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

Since $r_{n-4} = r_{n-3}q_{n-2} + r_{n-2}$ is a linear combination of r_{n-2} and r_{n-3}, then $r_{n-1}|r_{n-4}$.

This reasoning process is repeated a finite number of times.

Since $r_{n-1}|r_k$ and $r_{n-1}|r_{k-1}$, then r_{n-1} divides any linear combination of r_k and r_{k-1}.

Since $r_{k-2} = r_{k-1}q_k + r_k$ is a linear combination of r_k and r_{k-1}, then $r_{n-1}|r_{k-2}$.

Since $r_{n-1}|r_2$ and $r_{n-1}|r_1$, then r_{n-1} divides any linear combination of r_2 and r_1.

Since $b = r_1q_2 + r_2$ is a linear combination of r_2 and r_1, then $r_{n-1}|b$.

Since $r_{n-1}|r_1$ and $r_{n-1}|b$, then r_{n-1} divides any linear combination of r_1 and b.

Since $a = bq_1 + r_1$ is a linear combination of r_1 and b, then $r_{n-1}|a$.

Since $r_{n-1}|a$ and $r_{n-1}|b$, then 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.

Since $r_1 = a - bq_1$ is a linear combination of a and b, then $d|r_1$.

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

Since $r_2 = b - r_1q_2$ is a linear combination of b and r_1, then $d|r_2$.

Since $d|r_1$ and $d|r_2$, then d divides any linear combination of r_1 and r_2.

Since $r_3 = r_1 - r_2q_3$ is a linear combination of r_1 and r_2, then $d|r_3$.

This reasoning process is repeated a finite number of times.

Since $d|r_k$ and $d|r_{k+1}$, then d divides any linear combination of r_k and r_{k+1}.

Since $r_{k+2} = r_k - r_{k+1}q_{k+2}$ is a linear combination of r_k and r_{k+1}, then $d|r_{k+2}$.

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

Since $r_{n-1} = r_{n-3} - r_{n-2}q_{n-1}$ is a linear combination of r_{n-3} and r_{n-2}, then $d|r_{n-1}$.

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

Least common multiple

Theorem 62. ***definition of*** $n\mathbb{Z}$
Let $n \in \mathbb{Z}$.
The set of all multiples of n is $\{nk : k \in \mathbb{Z}\}$.

Proof. Let S be the set of all multiples of n.
Then $S = \{m \in \mathbb{Z} : n|m\}$.
Let $T = \{nk : k \in \mathbb{Z}\}$.

We prove $S \subset T$.
Let $s \in S$.
Then $s \in \mathbb{Z}$ and $n|s$.
Since $n|s$, then $s = na$ for some integer a.
Since $s = na$ and $a \in \mathbb{Z}$, then $s \in T$.
Therefore, $s \in S$ implies $s \in T$, so $S \subset T$.

Conversely, we prove $T \subset S$.
Let $t \in T$.
Then $t = nb$ for some integer b.
Since $b \in \mathbb{Z}$ and $t = nb$, then $n|t$.
Since $t \in \mathbb{Z}$ and $n|t$, then $t \in S$.
Therefore, $t \in T$ implies $t \in S$, so $T \subset S$.

Since $S \subset T$ and $T \subset S$, then $S = T$, as desired. □

Proposition 63. *Let $n \in \mathbb{Z}^+$.*
The set of all positive multiples of n is $\{nk : k \in \mathbb{Z}^+\}$.

Proof. Let S be the set of all positive multiples of n.
Then $S = \{m \in \mathbb{Z}^+ : n|m\}$.
Let $T = \{nk : k \in \mathbb{Z}^+\}$.

We prove $S \subset T$.
Let $s \in S$.
Then $s \in \mathbb{Z}^+$ and $n|s$.
Since $n|s$, then $s = na$ for some integer a.
Since $s \in \mathbb{Z}^+$ and $n \in \mathbb{Z}^+$ and $s = na$, then $a \in \mathbb{Z}^+$.
Since $s = na$ and $a \in \mathbb{Z}^+$, then $s \in T$.
Therefore, $s \in S$ implies $s \in T$, so $S \subset T$.

We prove $T \subset S$.

Let $t \in T$.

Then $t = nb$ for some $b \in \mathbb{Z}^+$.

Since $b \in \mathbb{Z}$ and $t = nb$, then $n|t$.

Since $n \in \mathbb{Z}^+$ and $b \in \mathbb{Z}^+$ and $t = nb$, then $t \in \mathbb{Z}^+$.

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

Therefore, $t \in T$ implies $t \in S$, so $T \subset S$.

Since $S \subset T$ and $T \subset S$, then $S = T$, as desired. □

Theorem 64. ***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.

Proof. **Existence:**

Let S be the set of all positive common multiples of a and b.

Then $S = \{s \in \mathbb{Z}^+ : a|s \text{ and } b|s\}$.

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

Since $b \in \mathbb{Z}$ and $ab = ab$, then $a|ab$.

Since $a \in \mathbb{Z}$ and $ab = ba$, then $b|ab$.

Since $ab \in \mathbb{Z}^+$ and $a|ab$ and $b|ab$, then $ab \in S$, 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.

Let m be the least element of S.

Then $m \in S$ and $m \leq s$ for all $s \in S$.

We prove m is a least common multiple of a and b.

Since $m \in S$, then $m \in \mathbb{Z}^+$ and $a|m$ and $b|m$, so m is a positive common multiple of a and b.

Let c be any positive common multiple of a and b.

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

We must prove $m|c$.

We divide c by m.

By the division algorithm, there are unique integers q and r such that $c = mq + r$ and $0 \leq r < m$.

Since $0 \leq r < m$, then $0 \leq r$ and $r < m$.

Since $0 \leq r$, then $r \geq 0$, so either $r > 0$ or $r = 0$.

Suppose $r > 0$.

Since $c = mq + r$, then $r = c - mq$ is a linear combination of c and m.

Since $a|c$ and $a|m$, then a divides any linear combination of c and m, so $a|r$.

Since $b|c$ and $b|m$, then b divides any linear combination of c and m, so $b|r$.

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

Since $r \in \mathbb{Z}^+$ and $a|r$ and $b|r$, then $r \in S$.
Thus, $r \in S$ and $r < m$.
This contradicts that m is the least element of S.
Therefore, $r \not> 0$.

Since either $r > 0$ or $r = 0$ and $r \not> 0$, then $r = 0$.
Thus, $c = mq + r = mq + 0 = mq$.
Since $q \in \mathbb{Z}$ and $c = mq$, then $m|c$, as desired.
Therefore, any positive common multiple of a and b is a multiple of m.

Since m is a positive common multiple of a and b, and any positive common multiple of a and b is a multiple of m, then m is a least common multiple of a and b. □

Proof. **Uniqueness:**
Suppose m is a least common multiple of a and b and m' is a least common multiple of a and b.
We must prove $m = m'$.
Since m is a least common multiple of a and b, then $m \in \mathbb{Z}^+$ and $a|m$ and $b|m$ and for all $c \in \mathbb{Z}^+$, if $a|c$ and $b|c$, then $m|c$.
Since m' is a least common multiple of a and b, then $m' \in \mathbb{Z}^+$ and $a|m'$ and $b|m'$ and for all $c \in \mathbb{Z}^+$, if $a|c$ and $b|c$, then $m'|c$.
Since $m \in \mathbb{Z}^+$, then $a|m$ and $b|m$ implies $m'|m$.
Since $a|m$ and $b|m$, then we conclude $m'|m$.
Since $m' \in \mathbb{Z}^+$, then $a|m'$ and $b|m'$ implies $m|m'$.
Since $a|m'$ and $b|m'$, then we conclude $m|m'$.
Since $m \in \mathbb{Z}^+$ and $m' \in \mathbb{Z}^+$ and $m|m'$ and $m'|m$, then we conclude $m = m'$, by the the anti-symmetric property of the divides relation on $\mathbb{Z}^+$. □

Proposition 65. *For all $a, b \in \mathbb{Z}^+$, $lcm(a, b)$ divides ab.*

Proof. Let $a, b \in \mathbb{Z}^+$.
Let $m = lcm(a, b)$.
Then $m \in \mathbb{Z}^+$ and any positive common multiple of a and b is a multiple of m.

Since $a \in \mathbb{Z}^+$ and $b \in \mathbb{Z}^+$, then $ab \in \mathbb{Z}^+$.
Since $b \in \mathbb{Z}$ and $ab = ab$, then $a|ab$.
Since $a \in \mathbb{Z}$ and $ab = ba$, then $b|ab$.
Since $ab \in \mathbb{Z}^+$ and $a|ab$ and $b|ab$, then ab is a positive common multiple of a and b.
Therefore, ab is a multiple of m, so $m|ab$, as desired. □

Theorem 66. ***lcm and gcd relationship***
Let $a, b \in \mathbb{Z}^+$.
Then $\gcd(a, b) \cdot lcm(a, b) = ab$.

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

Thus, a and b are both nonzero, so a and b are not both zero.

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

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 $m = \dfrac{ab}{d}$.

We first prove $m = lcm(a, b)$.

We prove m is a positive common multiple of a and b.

Observe that

$$\begin{aligned} as &= (dr)s \\ &= drs \\ &= rds \\ &= r(ds) \\ &= rb. \end{aligned}$$

Thus, $as = rb$.

Since $b = ds$, then $s = \dfrac{b}{d}$.

Observe that

$$\begin{aligned} m &= \frac{ab}{d} \\ &= a \cdot \frac{b}{d} \\ &= as \\ &= rb. \end{aligned}$$

Hence, $m = as = rb = br$.

Since $a \in \mathbb{Z}^+$ and $b \in \mathbb{Z}^+$ and $d \in \mathbb{Z}^+$ and $m = \dfrac{ab}{d}$, then $m > 0$.

Since $a \in \mathbb{Z}$ and $s \in \mathbb{Z}$ and $m = as$, then $m \in \mathbb{Z}$.

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

Since $s \in \mathbb{Z}$ and $m = as$, then $a|m$.

Since $r \in \mathbb{Z}$ and $m = br$, then $b|m$.

Since $m \in \mathbb{Z}^+$ and $a|m$ and $b|m$, then m is a positive common multiple of a and b.

We next prove any positive common multiple of a and b is a multiple of m.

Let $c \in \mathbb{Z}^+$ such that $a|c$ and $b|c$.

Then $c = au$ and $c = bv$ for some integers u and v.

Hence, $\dfrac{c}{a} = u$ and $\dfrac{c}{b} = v$.

Since $m = \dfrac{ab}{d}$ and $d > 0$, then $md = ab$.

Since $ab > 0$, then $ab \neq 0$, so we divide to obtain $\dfrac{md}{ab} = 1$.

Since $d = \gcd(a, b)$ is the least positive linear combination of a and b, then $d = xa + yb$ for some integers x and y.

Observe that

$$\begin{aligned} c &= c \cdot 1 \\ &= c \cdot \frac{md}{ab} \\ &= \frac{cm}{ab} \cdot d \\ &= \frac{cm}{ab} \cdot (xa + yb) \\ &= \frac{cmxa}{ab} + \frac{cmyb}{ab} \\ &= \frac{cmx}{b} + \frac{cmy}{a} \\ &= \frac{c}{b} \cdot mx + \frac{c}{a} \cdot my \\ &= vmx + umy \\ &= m(vx + uy). \end{aligned}$$

Since $vx + uy \in \mathbb{Z}$ and $c = m(vx + uy)$, then $m|c$.

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

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

Since $\gcd(a, b) \cdot lcm(a, b) = dm = ab$, then $\gcd(a, b) \cdot lcm(a, b) = ab$, as desired. □

Corollary 67. *Let $a, b \in \mathbb{Z}^+$.*

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

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

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

Thus, $ab \neq 0$, so $lcm(a, b) \neq 0$.

By theorem 66, $\gcd(a, b) \cdot lcm(a, b) = ab$.

Since $\gcd(a, b) \cdot lcm(a, b) = ab$ and $lcm(a, b) \neq 0$, then $\gcd(a, b) = \dfrac{ab}{lcm(a, b)}$.

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 $\gcd(a,b) > 0$, then $\gcd(a,b) \neq 0$.

By theorem 66, $\gcd(a,b) \cdot lcm(a,b) = ab$.

Since $\gcd(a,b) \cdot lcm(a,b) = ab$ and $\gcd(a,b) \neq 0$, then $lcm(a,b) = \dfrac{ab}{\gcd(a,b)}$.

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 68. ***properties of lcm***

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

Then

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

Proof. We prove 1.

By proposition 37, every integer divides itself, so $a|a$.

By proposition 36, one divides every integer, so $1|a$.

Since $a \in \mathbb{Z}^+$ and $a|a$ and $1|a$, then a is a positive common multiple of a and 1.

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

Then $a|m$, so $a|m$ for all $m \in \mathbb{Z}^+$ such that $a|m$ and $1|m$.

Hence, any positive common multiple of a and 1 is a multiple of a.

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

Proof. We prove 2.

By proposition 37, every integer divides itself, so $a|a$.

Since $a \in \mathbb{Z}^+$ and $a|a$ and $a|a$, then a is a positive common multiple of a and a.

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

Then $a|m$, so $a|m$ for all $m \in \mathbb{Z}^+$ such that $a|m$ and $a|m$.

Hence, any positive common multiple of a and a is a multiple of a.

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

Proof. We prove 3.

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

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

Since $m \in \mathbb{Z}^+$ and $b|m$ and $a|m$, then m is a positive common multiple of b and a.

Let c be any positive common multiple of b and a.

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

Since $b|c$ and $a|c$, then $a|c$ and $b|c$.

Since $c \in \mathbb{Z}^+$ and $a|c$ and $b|c$, then we conclude $m|c$.

Hence, any positive common multiple of b and a is a multiple of m.

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

Proof. We prove 4.

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 5.

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

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

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

Thus, $d \in \mathbb{Z}^+$ and $d|a$.

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

Hence, $m \in \mathbb{Z}^+$ and $a|m$.

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

Proof. We prove 6.

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 positive common divisor of a and b, so $d \in \mathbb{Z}^+$ and $d|a$ and $d|b$.

Since $d = lcm(a, b)$, then d is a positive common multiple of a and b, so $d \in \mathbb{Z}^+$ and $a|d$ and $b|d$.

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

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

Therefore, $a = d = b$, so $a = b$. □

Proof. We prove 7.

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

Suppose $a|b$.

By proposition 37, every integer divides itself, so $a|a$.

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 $c \in \mathbb{Z}$ and $c|a$ 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, $a|b$. □

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

□

Proof. 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 $lcm(a,b) = b$. □

Linear Diophantine Equations

Theorem 69. ***existence of a solution to a linear Diophantine equation***

Let $a, b, c \in \mathbb{Z}$ and $a \neq 0$ 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. Observe that $\gcd(a,b)|c$ if and only if c is a multiple of $\gcd(a,b)$.

By theorem 55, c is a linear combination of a and b if and only if c is a multiple of $\gcd(a,b)$.

Observe that c is a linear combination of a and b if and only if there exist integers x_0 and y_0 such that $ax_0 + by_0 = c$.

Hence, $\gcd(a,b)|c$ if and only if c is a multiple of $\gcd(a,b)$ if and only if c is a linear combination of a and b if and only if there exist integers x_0 and y_0 such that $ax_0 + by_0 = c$.

Therefore, $\gcd(a,b)|c$ if and only if there exist integers x_0 and y_0 such that $ax_0 + by_0 = c$. □

Theorem 70. ***characterization of a general solution to a linear Diophantine equation***

Let $a, b, c \in \mathbb{Z}$ and $a \neq 0$ 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 $x = x_0 + \frac{bt}{d}$ and $y = y_0 - \frac{at}{d}$ for all $t \in \mathbb{Z}$, where $d = \gcd(a, b)$.

Proof. Suppose $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$ 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 $a(x'-x_0) = b(y_0-y')$.

Since $a \neq 0$ and $b \neq 0$, then a and b are both not zero.

Hence, a and b are not both zero, so let $d = \gcd(a, b)$.

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

Since $d \in \mathbb{Z}^+$, then $d > 0$, so $d \neq 0$.

Since $d|a$, then $a = dr$ for some integer r.

Since $d \neq 0$, then $r = \frac{a}{d}$.

Since $d \neq 0$ and $a \neq 0$, then $r \neq 0$.

Since $d|b$, then $b = ds$ for some integer s.

Since $d \neq 0$, then $s = \frac{b}{d}$.

Observe that

$$\begin{aligned} 0 &= a(x' - x_0) - b(y_0 - y') \\ &= (dr)(x' - x_0) - (ds)(y_0 - y') \\ &= dr(x' - x_0) - ds(y_0 - y') \\ &= d[r(x' - x_0) - s(y_0 - y')]. \end{aligned}$$

Since $d[r(x'-x_0)-s(y_0-y')] = 0$, then either $d = 0$ or $r(x'-x_0)-s(y_0-y') = 0$.

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

Since $x' - x_0 \in \mathbb{Z}$ and $s(y_0 - y') = r(x' - x_0)$, then $r|s(y_0 - y')$.

Since $d = \gcd(a, b)$, then by corollary 57, $1 = \gcd(\frac{a}{d}, \frac{b}{d}) = \gcd(r, s)$.

Since $r|s(y_0 - y')$ and $\gcd(r, s) = 1$, then $r|(y_0 - y')$, by theorem 58.

Hence, $y_0 - y' = rt$ for some integer t.

Thus, $y' = y_0 - rt$.

Observe that

$$\begin{aligned} 0 &= r(x' - x_0) - s(y_0 - y') \\ &= r(x' - x_0) - s(rt) \\ &= r(x' - x_0) - srt \\ &= r[(x' - x_0) - st]. \end{aligned}$$

Since $r[(x' - x_0) - st] = 0$, then either $r = 0$ or $(x' - x_0) - st = 0$.

Since $r \neq 0$, then we conclude $(x' - x_0) - st = 0$, so $x' - x_0 = st$.

Hence, $x' = x_0 + st = x_0 + (\frac{b}{d})t = x_0 + \frac{bt}{d}$ and $y' = y_0 - rt = y_0 - (\frac{a}{d})t = y_0 - \frac{at}{d}$.

Therefore, $x' = x_0 + \frac{bt}{d}$ and $y' = y_0 - \frac{at}{d}$.

We verify x' and y' satisfy the diophantine equation.

Observe that

$$\begin{aligned} ax' + by' &= a(x_0 + \frac{bt}{d}) + b(y_0 - \frac{at}{d}) \\ &= ax_0 + \frac{abt}{d} + by_0 - \frac{abt}{d} \\ &= (ax_0 + by_0) + \frac{abt}{d} - \frac{abt}{d} \\ &= (ax_0 + by_0) + 0 \\ &= ax_0 + by_0 \\ &= c. \end{aligned}$$

□

Fundamental Theorem of Arithmetic

Lemma 71. ***A composite number has a positive divisor between 1 and itself.***

Let n be a positive integer.

Then n is composite iff there exists a positive integer d such that $d|n$ and $1 < d < n$.

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 a positive integer d such that $d|n$ and $d \neq 1$ and $d \neq n$.

Since d is a positive integer and $d \neq 1$, then $d > 1$.

Since d and n are positive integers and $d|n$, then $d \leq n$ by theorem 39.

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

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

Therefore, there exists a positive integer d such that $d|n$ and $1 < d < n$. $\square$

Proof. Conversely, suppose there exists a positive integer d such that $d|n$ and $1 < d < n$.

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 is a positive integer and $n \neq 1$, then n is a positive integer other than 1.

Since d is a positive integer 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. $\square$

Theorem 72. ***A composite number is composed of smaller positive factors.***

Let n be a positive integer.

Then n is composite iff there exist positive integers a and b with $1 < a < n$ and $1 < b < n$ such that $n = ab$.

Proof. Suppose n is composite.

By lemma 71, a composite number has a positive divisor between 1 and itself, so there exists a positive integer a such that $a|n$ and $1 < a < n$.

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 a positive integer b such that $n = ab$.

Since $n > 0$ and $a > 0$ and $n = ab$, then $b > 0$.

Since b is an integer and $b > 0$, then b is a positive integer.

Since $a > 1$ and $b > 0$, then $ab > b$.

Since $n = ab$ and $ab > b$, then $n > b$.

Since $n = ab$ and $n > a$, then $ab > a$, so $ab - a > 0$.

Thus, $a(b - 1) > 0$.

Since $a(b - 1) > 0$ and $a > 0$, then $b - 1 > 0$, so $b > 1$.

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

Therefore, there exist positive integers a and b with $1 < a < n$ and $1 < b < n$ such that $n = ab$. $\square$

Proof. Conversely, suppose there exist positive integers a and b with $1 < a < n$ and $1 < b < n$ such that $n = ab$.

Since b is a positive integer, and every positive integer is an integer, then b is an integer.

Since b is an integer and $n = ab$, then $a|n$.

By lemma 71, a composite number has a positive divisor between 1 and itself.

Since a is a positive integer and $a|n$ and $1 < a < n$, then this implies n is composite. □

Theorem 73. *Every integer greater than 1 has a prime factor.*

Proof. Let n be any integer greater than 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.

Therefore, n has a prime factor.

Case 2: Suppose n is not prime.

Since $n > 1$ and $1 > 0$, then $n > 0$.

Since n is an integer and $n > 0$, then n is a positive integer.

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

Since n is a positive integer and $n \neq 1$ and n is not prime, then n is composite.

By lemma 71, a composite number has a positive divisor between 1 and itself.

Thus, there exists a positive integer d such that $d|n$ and $1 < d < n$.

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.

By lemma 71, a composite number has a positive divisor between 1 and itself.

Therefore, there exists $a \in \mathbb{Z}^+$ such that $a|p$ and $1 < a < p$.

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.

Therefore, n has a prime factor.

In all cases, n has a prime factor.

Therefore, any integer greater than 1 has a prime factor. □

Proof. Let $x(n)$ be the predicate 'n has a prime factor' defined for all $n \in \mathbb{Z}^+$ with $n > 1$.

To prove $x(n)$ is true for all integers $n > 1$, we prove $x(n)$ is true for all integers $n \geq 2$ by strong induction on n.

Basis:

Let $n = 2$.

Since $2|2$ and 2 is prime, then 2 is a prime factor of 2, so 2 has a prime factor.

Therefore, $x(2)$ is true.

Induction:

For any integer $n \geq 3$, assume $x(2)$ and $x(3)$ and ... and $x(n-1)$ are all true.

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

Thus, $x(k)$ is true for any integer k such that $1 < k < n$.

We must prove $x(n)$ is true.

Since $n \geq 3 > 1 > 0$, then $n > 1$ and $n > 0$.

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

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

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

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, so n has a prime factor.

Case 2: Suppose n is composite.

By lemma 71, a composite number has a positive divisor between 1 and itself.

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

Since $d \in \mathbb{Z}^+$ and $1 < d < n$, then by the induction hypothesis, $p(d)$ is true, so d has a prime factor.

Let $p \in \mathbb{Z}^+$ be a prime factor of d.

Then p is prime and $p|d$.

Since $p|d$ and $d|n$, then $p|n$.

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

In all cases, n has a prime factor, so $x(n)$ is true.

Therefore, $x(n)$ is true whenever $x(2)$ and $x(3)$ and ... and $x(n-1)$ are all true for any integer $n \geq 3$.

Since $x(2)$ is true, and $x(n)$ is true whenever $x(2)$ and $x(3)$ and ... and $x(n-1)$ are all true for any integer $n \geq 3$, then by strong induction, $x(n)$ is true for all integers $n \geq 2$.

Thus, $x(n)$ is true for all integers $n > 1$, so n has a prime factor for all integers $n > 1$.

Therefore, every integer greater than one has a prime factor. □

Lemma 74. ***Euclid's Lemma***

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

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

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

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

Since $p \in \mathbb{Z}^+$, then $p \in \mathbb{Z}$ and $p > 0$, so $p \neq 0$.

Since $p \in \mathbb{Z}$ and $a \in \mathbb{Z}$ and $p \neq 0$, then p and a are integers not both zero.

Therefore, $\gcd(p, a)$ exists and is unique.

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

We consider these cases separately.

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

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

Then $d \neq 1$.

Since $d = \gcd(p, a)$, then d is a positive common divisor of p and a, so $d \in \mathbb{Z}^+$ and $d|p$ and $d|a$.

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

Since d is positive and $d|p$, then this implies either $d = 1$ or $d = p$.

Since $d \neq 1$, then we conclude $d = p$.

Since $d|a$ and $d = p$, then $p|a$.

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

Since $p|ab$ and $\gcd(p, a) = 1$, then by theorem 58, $p|b$. □

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

Since $p \in \mathbb{Z}^+$, then $p \in \mathbb{Z}$ and $p > 0$, so $p \neq 0$.

Since $p \in \mathbb{Z}$ and $a \in \mathbb{Z}$ and $p \neq 0$, then p and a are integers not both zero.

Therefore, $\gcd(p, a)$ exists and is unique.

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

We consider these cases separately.

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

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

Then $d \neq 1$.

Since $d = \gcd(p, a)$, then d is a positive common divisor of p and a, so $d \in \mathbb{Z}^+$ and $d|p$ and $d|a$.

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

Since d is positive and $d|p$, then this implies either $d = 1$ or $d = p$.

Since $d \neq 1$, then we conclude $d = p$.

Since $d|a$ and $d = p$, then $p|a$.

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

Then 1 is a linear combination of p and a, by corollary 56.

Therefore, $1 = xp + ya$ for some integers x and y.

Observe that $b = b \cdot 1 = b(xp + ya) = bxp + bya = (bx)p + y(ab)$ is a linear combination of p and ab.

By proposition 37, every integer divides itself.

Since $p \in \mathbb{Z}$, then we conclude $p|p$.

By theorem 50, any common divisor of p and ab divides any linear combination of p and ab.

Since $p|p$ and $p|ab$, then p divides any linear combination of p and ab, so $p|b$. □

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

We must prove $p|b$.

Since p is prime, then $p \in \mathbb{Z}^+$ and the only positive divisors of p are 1 and p.

Since the only positive divisors of p are 1 and p, then 1 and p are the only possible positive common divisors of p and a.

By proposition 36, one divides every integer.

Since $p \in \mathbb{Z}$ and $a \in \mathbb{Z}$, then we conclude $1|p$ and $1|a$.

Since $1 \in \mathbb{Z}^+$ and $1|p$ and $1|a$, then 1 is a positive common divisor of p and a.

By proposition 37, every integer divides itself.

Since $p \in \mathbb{Z}^+$, then we conclude $p|p$.

Since $p|p$, but $p \nmid a$, then p is not a common divisor of p and a, so p cannot be a positive common divisor of p and a.

Since 1 and p are the only possible positive common divisors of p and a, and 1 is a positive common divisor of p and a, but p is not a positive common divisor of p and a, then 1 is the only positive common divisor of p and a.

Therefore, the only positive common divisor of p and a is 1.

Since $\gcd(p, a)$ is a positive common divisor of p and a, then we must conclude $\gcd(p, a) = 1$.

Since $p|ab$ and $\gcd(p, a) = 1$, then by theorem 58, $p|b$. □

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

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

Hence, any positive common divisor of p and a must be either 1 or p.

Thus, either $\gcd(p, a) = 1$ or $\gcd(p, a) = p$.

We consider these cases separately.

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

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

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

Since $p|ab$ and $\gcd(p, a) = 1$, then by theorem 58, $p|b$. □

Corollary 75. ***If prime*** $p|a_1...a_n$***, then*** $p|a_k$ ***for some*** k***.***

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

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

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 $a_1a_2...a_n$.

Define predicate $p(n)$ over $\mathbb{Z}^+$ by '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:

Let $n = 1$.

Suppose 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, $p(1)$ is true.

Let $n = 2$.

Suppose p is prime and $p|a_1a_2$.

Then either $p|a_1$ or $p|a_2$, by Euclid's lemma (lemma 74).

Hence, $p|a_k$ for some integer k with $1 \leq k \leq 2$.

Therefore, $p(2)$ is true.

Induction:

Let $n \in \mathbb{Z}^+$ with $n \geq 2$ such that $p(n)$ is true.

Since $p(n)$ is true, then $p|a_k$ for some integer k with $1 \leq k \leq n$ whenever p is prime and $p|a_1a_2...a_n$.

We must prove $p(n+1)$ is true.

Suppose p is prime and $p|(a_1a_2...a_na_{n+1})$.

Then either $p|a_1a_2...a_n$ or $p|a_{n+1}$, by Euclid's lemma (lemma 74).

We consider each case separately.

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

Let $k = n + 1$.

Since $n + 1 \in \mathbb{Z}^+$ and $\mathbb{Z}^+ \subset \mathbb{Z}$, then $n + 1 \in \mathbb{Z}$.

Since $n + 1 \in \mathbb{Z}$ and $k = n + 1$, then $k \in \mathbb{Z}$.

Since $n + 1 > n$ and $n \geq 2$ and $2 > 1$, then $n + 1 > 1$, so $k > 1$.

Therefore, $p|a_k$ for some integer k with $1 < k = n + 1$.

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

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

Since $1 \leq k \leq n$ and $n < n + 1$, then $1 \leq k \leq n < n + 1$, so $1 \leq k < n + 1$.

Therefore, $p|a_k$ for some integer k with $1 \leq k < n + 1$.

Hence, in all cases, $p|a_k$ for some integer k with $1 \leq k \leq n + 1$.

Thus, $p|a_k$ for some integer k with $1 \leq k \leq n + 1$ whenever p is prime and $p|(a_1a_2...a_na_{n+1})$, so $p(n + 1)$ is true.

Therefore, $p(n + 1)$ is true whenever $p(n)$ is true for all $n \in \mathbb{Z}^+$ with $n \geq 2$.

Since $p(1)$ is true and $p(2)$ is true, and $p(n + 1)$ is true whenever $p(n)$ is true for all $n \in \mathbb{Z}^+$ with $n \geq 2$, then by induction, $p(n)$ is true for all $n \in \mathbb{Z}^+$.

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

Corollary 76. *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.

By corollary 75, if p is prime and p divides a product of integers, then p divides one of those integers.

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

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 $p \neq 1$.

Hence, $p = q_k$.

Therefore, $p = q_k$ for some integer k with $1 \leq k \leq n$. □

Theorem 77. ***Fundamental Theorem of Arithmetic(Existence)***

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

Proof. **Existence:**

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

Suppose not every integer greater than one can be represented as a product of one or more primes.

Then there is some integer greater than one that cannot be represented as a product of one or more primes.

Let k be an integer greater than one that cannot be represented as a product of one or more primes.

Then $k \in \mathbb{Z}$ and $k > 1$ and k is not a product of one or more primes.

Since $k > 1$ and $1 > 0$, then $k > 0$.

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

Hence, there exists $k \in \mathbb{Z}^+$ such that $k > 1$ and k is not a product of one or more primes.

Let S be the set of all positive integers greater than 1 that cannot be represented as a product of one or more primes.

Then $S = \{n \in \mathbb{Z}^+ : n > 1$ and n is not a product of one or more primes$\}$.

Since $k \in \mathbb{Z}^+$ and $k > 1$ and k is not a product of one or more primes, then $k \in S$, 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.

Let m be the least element of S.

Then $m \in S$ and $m \leq x$ for all $x \in S$.

Since $m \in S$, then $m \in \mathbb{Z}^+$ and $m > 1$ and m is not a product of one or more primes.

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

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

We consider these cases separately.

Case 1: Suppose m is prime.

Then m is a product of one prime, itself.

But, m is not a product of one or more primes.

Therefore, m is not prime.

Case 2: Suppose m is composite.

By theorem 72, a composite number is composed of smaller positive factors, so there exist $a \in \mathbb{Z}^+$ and $b \in \mathbb{Z}^+$ such that $m = ab$ with $1 < a < m$ and $1 < b < m$.

Since $1 < a < m$, then $1 < a$ and $a < m$.

Since $1 < a$, then $a > 1$.

Since $a < m$ and m is the least element of S, then $a \notin S$.

Since $a \in \mathbb{Z}^+$ and $a > 1$ and $a \notin S$, then we conclude a is a product of one or more primes.

Since $1 < b < m$, then $1 < b$ and $b < m$.

Since $1 < b$, then $b > 1$.

Since $b < m$ and m is the least element of S, then $b \notin S$.

Since $b \in \mathbb{Z}^+$ and $b > 1$ and $b \notin S$, then we conclude b is a product of one or more primes.

Since $m = ab$ and a is a product of one or more primes and b is a product of one or more primes, then m is a product of one or more primes.

But, this contradicts m is not a product of one or more primes.

Therefore, m is not composite.

Therefore, m is not prime and m is not composite.

Since $m \in \mathbb{Z}^+$ and $m \neq 1$ and m is not prime and m is not composite, then m does not exist.

Hence, there is no integer greater than one that cannot be represented as a product of one or more primes.

Therefore, every integer greater than one can be represented as a product of one or more 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' defined for all positive integers $n > 1$.

To prove n is a product of one or more primes, we prove $p(n)$ is true for all positive integers $n \geq 2$ by strong induction on n.

Basis:

Let $n = 2$.

Since 2 is prime, then 2 is product of one prime(itself), so $p(2)$ is true.
Induction:
For any integer $n \geq 3$, assume $p(2)$ and $p(3)$ and ... and $p(n-1)$ are all true.
Then $p(x)$ is true for any integer x such that $2 \leq x \leq n-1$.
Hence, $p(x)$ is true for any integer x such that $1 < x < n$.

Since $n \geq 3$ and $3 > 1$, then $n > 1$, so $n \neq 1$.
Since $n \in \mathbb{Z}^+$ and $n \neq 1$, 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.
By theorem 72, a composite number is composed of smaller positive factors.
Hence, n is composed of smaller positive factors, so there exists $a, b \in \mathbb{Z}^+$ such that $n = ab$ and $1 < a < n$ and $1 < b < n$.

Since $a \in \mathbb{Z}$ and $1 < a < n$, then by the induction hypothesis, $p(a)$ is true.
Thus, a is a product of one or more primes, so there exist s primes $p_1, p_2, ..., p_s$ such that $a = p_1 p_2 ... p_s$.
Since $b \in \mathbb{Z}$ and $1 < b < n$, then by the induction hypothesis, $p(b)$ is true.
Thus, b is a product of one or more primes, so there exist t primes $q_1, q_2, ..., q_t$ such that $b = q_1 q_2 ... q_t$.
Therefore, $n = ab = (p_1 p_2 ... p_s)(q_1 q_2 ... q_t)$ is a product of primes.

In all cases, n is a product of one or more primes, so $p(n)$ is true.
Hence, $p(n)$ is true whenever $p(2)$ and $p(3)$ and ... and $p(n-1)$ are all true for any integer $n \geq 3$.

Since $p(2)$ is true, and $p(n)$ is true whenever $p(2)$ and $p(3)$ and ... and $p(n-1)$ are all true for any integer $n \geq 3$, then by strong induction, $p(n)$ is true for all integers $n \geq 2$.
Hence, $p(n)$ is true for all integers $n > 1$.
Thus, n is a product of one or more primes for all integers $n > 1$.
Therefore, every integer greater than one is a product of one or more primes.
□

Proof. **Existence:**
Let $n \in \mathbb{Z}$ and $n > 1$.
Since $n > 1$ and $1 > 0$, then $n > 0$.
Since $n \in \mathbb{Z}$ and $n > 0$, then $n \in \mathbb{Z}^+$.
Since $n > 1$, then $n \neq 1$.
Since $n \in \mathbb{Z}^+$ and $n \neq 1$, 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.

By theorem 73, every integer greater than 1 has a prime factor.

Since $n \in \mathbb{Z}$ and $n > 1$, then n has a prime factor.

Therefore, there exists a prime $p_1 \in \mathbb{Z}^+$ such that $p_1|n$.

Since $p_1 \in \mathbb{Z}^+$ and $n \in \mathbb{Z}^+$ and $p_1|n$, then $p_1 \leq n$, by theorem 39.

Thus, either $p_1 < n$ or $p_1 = n$.

Since p_1 is prime and n is composite, and a prime does not equal a composite, then $p_1 \neq n$, so $p_1 < n$.

Since p_1 is prime, then $p_1 > 1$.

Thus, $1 < p_1$ and $p_1 < n$, so $1 < p_1 < n$.

Since $p_1|n$, then $n = p_1 n_1$ for some integer n_1.

Since $n \in \mathbb{Z}^+$ and $p_1 \in \mathbb{Z}^+$, then $n_1 \in \mathbb{Z}^+$, so $n_1 \geq 1$.

Hence, either $n_1 > 1$ or $n_1 = 1$.

Suppose $n_1 = 1$.

Then $n = p_1 n_1 = p_1(1) = p_1$.

But, this implies composite n equals prime p_1.

This is a contradiction, since a prime number cannot equal a composite number.

Therefore, $n_1 \neq 1$.

Since either $n_1 > 1$ or $n_1 = 1$ and $n_1 \neq 1$, then we conclude $n_1 > 1$.

Since $p_1 \in \mathbb{Z}$ and $n = p_1 n_1 = n_1 p_1$, then $n_1|n$.

Since $n_1 \in \mathbb{Z}^+$ and $n \in \mathbb{Z}^+$ and $n_1|n$, then $n_1 \leq n$, by theorem 39, so either $n_1 < n$ or $n_1 = n$.

Suppose $n_1 = n$.

Then $0 = n - p_1 n_1 = n - p_1 n = n(1 - p_1)$, so either $n = 0$ or $1 - p_1 = 0$.

Since $n > 1$, then $n \neq 0$, so we conclude $1 - p_1 = 0$.

Thus, $p_1 = 1$, so prime p_1 is 1.

But, this contradicts the fact that any prime integer is not one.

Therefore, $n_1 \neq n$.

Since either $n_1 < n$ or $n_1 = n$ and $n_1 \neq n$, then we conclude $n_1 < n$.

Therefore, $1 < n_1$ and $n_1 < n$, so $1 < n_1 < n$.

Since $n_1 \in \mathbb{Z}^+$ and $n_1 \neq 1$, 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 and we are done.

If n_1 is composite, then we apply the argument in case 2 to n_1.

Therefore, there exists a prime $p_2 \in \mathbb{Z}^+$ such that $p_2|n_1$ and $1 < p_2 < n_1$ and there exists $n_2 \in \mathbb{Z}^+$ such that $n_1 = p_2 n_2$ and $1 < n_2 < n_1$.

Since $1 < n_2 < n_1$, then $1 < n_2$, so $n_2 > 1$.

Thus, $n_2 \neq 1$.

Since $n_2 \in \mathbb{Z}^+$ and $n_2 \neq 1$, 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 and we are done.

If n_2 is composite, then we apply the argument in case 2 to n_2.

Therefore, there exists a prime $p_3 \in \mathbb{Z}^+$ such that $p_3 | n_2$ and $1 < p_3 < n_2$ and there exists $n_3 \in \mathbb{Z}^+$ such that $n_2 = p_3 n_3$ and $1 < n_3 < n_2$.

Since $1 < n_3 < n_2$, then $1 < n_3$, so $n_3 > 1$.

Thus, $n_3 \neq 1$.

Since $n_3 \in \mathbb{Z}^+$ and $n_3 \neq 1$, then either n_3 is prime or n_3 is composite.

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

If n_3 is composite, then we apply the argument in case 2 to n_3.

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

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. □

Lemma 78. *A product of primes is greater than one.*

Proof. To prove a product of primes is greater than one, define the predicate $r(n)$ over $\mathbb{Z}^+$ by '$p_1 p_2 ... p_n > 1$ for primes $p_1, p_2, ..., p_n$'.

We prove $r(n)$ is true for all $n \in \mathbb{Z}^+$ by induction on n.

Basis:

Let $n = 1$.

Suppose p_1 is prime.

Then $p_1 \in \mathbb{Z}^+$ and $p_1 > 1$.

Since $p_1 > 1$, then $r(1)$ is true.

Let $n = 2$.

Suppose p_1 and p_2 are prime.

Then $p_1, p_2 \in \mathbb{Z}^+$ and $p_1 > 1$ and $p_2 > 1$.

Hence, $p_1 p_2 > 1 \cdot 1$, so $p_1 p_2 > 1$.

Therefore, $r(2)$ is true.

Induction:

Let $k \in \mathbb{Z}^+$ with $k \geq 2$ such that $r(k)$ is true.

Then $p_1 p_2 ... p_k > 1$ for primes $p_1, p_2, ..., p_k$.

Suppose p_1 and p_2 and ... and p_k and p_{k+1} are all primes.

Since p_1 and p_2 and ... and p_k are all primes, then $p_1 p_2 ... p_k > 1$, by the induction hypothesis.

Since p_{k+1} is a prime, then $p_{k+1} \in \mathbb{Z}^+$ and $p_{k+1} > 1$.

Since $p_1p_2...p_k > 1$ and $p_{k+1} > 1$, then $(p_1p_2...p_k)p_{k+1} > 1 \cdot 1$, so $p_1p_2...p_kp_{k+1} > 1$.

Hence, $r(k+1)$ is true.

Thus, $r(k)$ implies $r(k+1)$ for all $k \in \mathbb{Z}^+$ with $k \geq 2$.

Since $r(1)$ is true and $r(2)$ is true, and $r(k)$ implies $r(k+1)$ for all $k \in \mathbb{Z}^+$ with $k \geq 2$, then by induction, $r(n)$ is true for all $n \in \mathbb{Z}^+$.

Therefore, $p_1p_2...p_n > 1$ for primes $p_1, p_2, ..., p_n$ for all $n \in \mathbb{Z}^+$, so a product of primes is greater than one. □

Theorem 79. ***Fundamental Theorem of Arithmetic(Unique Factorization)***

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

Proof. **Uniqueness:**

To prove every integer greater than one can be represented as a product of one or more primes in exactly one way, we prove every integer greater than one has a unique prime factorization.

Let $x(n)$ be the predicate defined over $\mathbb{Z}^+$ by 'n has a unique prime factorization'.

To prove $x(n)$ is true for all $n \in \mathbb{Z}^+$ with $n > 1$, we prove $x(n)$ is true for all $n \in \mathbb{Z}^+$ with $n \geq 2$ by strong induction on n.

Basis:

Let $n = 2$.

Since 2 is prime, then the only prime factor of 2 is 2 itself, so $2 = 2$ is the only prime factorization of 2.

Therefore, $x(2)$ is true.

Induction:

For any integer $n \geq 2$, assume $x(2)$ and $x(3)$ and ... and $x(n)$ are all true.

Then $x(k)$ is true for any integer k such that $2 \leq k \leq n$.

Hence, $x(k)$ is true for any integer k such that $1 < k < n + 1$.

To prove $x(n+1)$ is true, we must prove $n+1$ has a unique prime factorization.

Suppose $n + 1$ has two representations as a product of one or more primes.

Then $n + 1 = p_1p_2...p_r = q_1q_2...q_s$, where p_i and q_j are all primes and $p_1 \leq p_2 \leq ... \leq p_r$ and $q_1 \leq q_2 \leq ... \leq q_s$.

Since p_1 divides $p_1p_2 \dots p_r$ and $p_1p_2 \dots p_r = q_1q_2 \dots q_s$, then p_1 divides $q_1q_2 \dots q_s$.

By Euclid's lemma corollary, corollary 76, if a prime p divides a product of primes, then p is one of those primes.

Since p_1 is prime and p_1 divides the product $q_1q_2 \dots q_s$ and $q_1, q_2, ..., q_s$ are all primes, then we conclude p_1 is one of those primes, so $p_1 = q_k$ for some integer k with $1 \leq k \leq s$.

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

Since q_1 divides $q_1q_2 \dots q_s$ and $q_1q_2 \dots q_s = p_1p_2 \dots p_r$, then q_1 divides $p_1p_2 \dots p_r$.

By Euclid's lemma corollary, corollary 76, if a prime p divides a product of primes, then p is one of those primes.

Since q_1 is prime and q_1 divides the product $p_1p_2 \dots p_r$ and $p_1, p_2, ..., p_r$ are all primes, then we conclude q_1 is one of those primes, so $q_1 = p_m$ for some integer m with $1 \leq m \leq r$.

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

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 $\mathbb{Z}$.

Since p_1 is prime, then $p_1 > 1$, so $p_1 > 0$.

Hence, $p_1 \neq 0$.

Since $p_1 = q_1$ and $p_1 \neq 0$, then $q_1 \neq 0$.

Since $p_1 = q_1$ and $p_1 \neq 0$ and $q_1 \neq 0$, then we may cancel the factor $p_1 = q_1$ to obtain the equation $p_2p_3 \dots p_r = q_2q_3 \dots q_s$.

Let $y = p_2p_3 \dots p_r = q_2q_3 \dots q_s$.

Then $y \in \mathbb{Z}$ and $n + 1 = p_1y$.

Since p_1 is prime, then $p_1 > 1$.

By lemma 78, a product of primes is greater than one.

Since $p_2p_3 \dots p_r$ is a product of primes, then $y > 1$.

Since $y > 1$ and $1 > 0$, then $y > 0$.

Since $p_1 > 1$ and $y > 0$, then we multiply to obtain $p_1y > 1 \cdot y$, so $n+1 > y$.

Thus, $1 < y$ and $y < n + 1$, so $1 < y < n + 1$.

Since $y \in \mathbb{Z}$ and $1 < y < n + 1$, then by the induction hypothesis, $x(y)$ is true, so y has a unique prime factorization.

Since $n + 1 = p_1y$ and p_1 is prime and y has a unique prime factorization, then $n + 1$ must also have a unique prime factorization, so $x(n + 1)$ is true.

Hence, $x(n+1)$ is true whenever $x(2)$ and $x(3)$ and ... and $x(n)$ are all true for any integer $n \geq 2$.

Since $x(2)$ is true, and $x(n + 1)$ is true whenever $x(2)$ and $x(3)$ and ... and $x(n)$ are all true for any integer $n \geq 2$, then by strong induction, $x(n)$ is true for all integers $n \geq 2$.

Thus, $x(n)$ is true for all integers $n > 1$, so n has a unique prime factorization for all integers $n > 1$.

Therefore, every integer greater than one has a unique prime factorization, so every integer greater than one can be represented as a product of one or more primes in exactly one way. □

Proof. **Uniqueness:**

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

By theorem 77, the Fundamental Theorem of Arithmetic(Existence), every integer greater than one can be represented as a product of one or more primes.

Therefore, n can be represented as a product of one or more primes.

Suppose n has two representations as a product of one or more primes.

Let $n = p_1p_2 \dots p_r = q_1q_2 \dots q_s$, where p_i and q_j are all primes and $p_1 \leq p_2 \leq \dots \leq p_r$ and $q_1 \leq q_2 \dots \leq q_s$.

Without loss of generality, assume $r \leq s$.

Since p_1 divides $p_1p_2 \dots p_r$ and $p_1p_2 \dots p_r = q_1q_2 \dots q_s$, then p_1 divides $q_1q_2 \dots q_s$.

By Euclid's lemma corollary, corollary 76, if a prime p divides a product of primes, then p is one of those primes.

Since p_1 is prime and p_1 divides the product $q_1q_2 \dots q_s$ and $q_1, q_2, ..., q_s$ are all primes, then we conclude p_1 is one of those primes, so $p_1 = q_k$ for some integer k with $1 \leq k \leq s$.

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

Since q_1 divides $q_1q_2 \dots q_s$ and $q_1q_2 \dots q_s = p_1p_2 \dots p_r$, then q_1 divides $p_1p_2 \dots p_r$.

By Euclid's lemma corollary, corollary 76, if a prime p divides a product of primes, then p is one of those primes.

Since q_1 is prime and q_1 divides the product $p_1p_2 \dots p_r$ and $p_1, p_2, ..., p_r$ are all primes, then we conclude q_1 is one of those primes, so $q_1 = p_m$ for some integer m with $1 \leq m \leq r$.

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

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 $\mathbb{Z}$.

Since p_1 is prime, then $p_1 > 1$, so $p_1 > 0$.

Hence, $p_1 \neq 0$.

Since $p_1 = q_1$ and $p_1 \neq 0$, then $q_1 \neq 0$.

Since $p_1 = q_1$ and $p_1 \neq 0$ and $q_1 \neq 0$, then we may cancel the factor $p_1 = q_1$ to obtain the equation $p_2p_3 \dots p_r = q_2q_3 \dots q_s$.

We repeat this process to obtain $p_2 = q_2$ and the equation $p_3p_4 \dots p_r = q_3q_4 \dots q_s$.

We repeat this process.

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

Suppose $r < s$.

Then there are $s - r$ factors remaining on the right side of the equation, namely, $q_{r+1}, q_{r+2}, ..., q_s$, and there is only one factor 1 on the left side of the equation.

Thus, the equation will be $1 = q_{r+1}q_{r+2} \dots q_s$.

By lemma 78, a product of primes is greater than one.

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

Thus, $q_{r+1}q_{r+2} \dots q_s > 1$.

But, 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. □

Corollary 80. ***Every integer greater than one has a unique prime power 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 theorem 79, the Fundamental Theorem of Arithmetic(Unique Factorization), every integer greater than one can be represented as a product of one or more primes in exactly one way.

Therefore, n can be represented as a product of one or more primes in exactly one way.

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 each prime p_i in the prime factorization of n.

Then each e_i is a positive integer and $n = p_1^{e_1} p_2^{e_2} ... p_k^{e_k}$. □

Theorem 81. ***The gcd of two integers equals the product of the intersection of the primes to the smallest power which appears in each integer.***

Let $a, b \in \mathbb{Z}^+$ with $a > 1$ and $b > 1$.

Then either $\gcd(a, b) = 1$, or $\gcd(a, b)$ is the integer d whose prime factorization contains primes common to the prime factorizations of a and b such that each prime of d has a power equal to the minimum power occurring in the prime factorizations of a and b.

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

Hence, a and b are not both zero, so $\gcd(a, b)$ exists and is unique.

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

Then $d \in \mathbb{Z}^+$, so $d \geq 1$.

Hence, either $d > 1$ or $d = 1$.

We consider these cases separately.

Case 1: Suppose $d = 1$.

Then $\gcd(a, b) = d = 1$, so $\gcd(a, b) = 1$.

Case 2: Suppose $d > 1$.

Since $d \in \mathbb{Z}$ and $d > 1$, then by theorem 80, the fundamental theorem of arithmetic, d has a unique prime power factorization.

Since $a \in \mathbb{Z}$ and $a > 1$, then by theorem 80, the fundamental theorem of arithmetic, a has a unique prime power factorization.

Since $b \in \mathbb{Z}$ and $b > 1$, then by theorem 80, the fundamental theorem of arithmetic, b has a unique prime power factorization.

If p is a prime factor of a or b, then either p is prime factor of a and not b, or p is a prime factor of b and not a, or p is a common prime factor of a and b.

We consider these cases separately.

Case 2a: Suppose p is a common prime factor of a and b.

Then p is prime and $p|a$ and $p|b$.

Since p is prime, then $p \in \mathbb{Z}^+$ and $p > 1$.

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

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

Since $p \in \mathbb{Z}$ and $p|a$ and $p|b$, then we conclude $p|d$.

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

Since p is a prime factor of d, and d has a unique prime factorization, then p is a prime factor in the prime factorization of d.

Therefore, if p is a common prime factor of a and b, then p is a prime factor in the prime factorization of d.

Since a has a unique prime power factorization, let e be the number of occurrences of p in the prime factorization of a.

Then $e \in \mathbb{Z}^+$ and p^e is a factor in the prime factorization of a, so $p^e|a$.

Since b has a unique prime power factorization, let f be the number of occurrences of p in the prime factorization of b.

Then $f \in \mathbb{Z}^+$ and p^f is a factor in the prime factorization of b, so $p^f|b$.

Since d has a unique prime power factorization, let g be the number of occurrences of p in the prime factorization of d.

Then $g \in \mathbb{Z}^+$ and p^g is a factor in the prime factorization of d, so $p^g|d$.

We must prove $g = \min(e, f)$.

Since $p^g|d$ and $d|a$, then $p^g|a$.

Since $p^g|d$ and $d|b$, then $p^g|b$.

Since g is the largest power of p that divides a, and g is the largest power of p that divides b, and $p^e|a$ and $p^f|b$, then either $g = e$ or $g = f$.

Since $e \in \mathbb{Z}^+$ and p^e is a factor in the prime factorization of a, then e is the largest power of p that divides a.

Hence, if n is a positive integer greater than e, then p^n cannot divide a.

Thus, if $n \in \mathbb{Z}^+$ and $n > e$, then $p^n \not| a$, so if $n \in \mathbb{Z}^+$ and $p^n|a$, then $n \leq e$.

Since $g \in \mathbb{Z}^+$ and $p^g|a$, then we conclude $g \leq e$.

Since $f \in \mathbb{Z}^+$ and p^f is a factor in the prime factorization of b, then f is the largest power of p that divides b.

Hence, if n is a positive integer greater than f, then p^n cannot divide b.

Thus, if $n \in \mathbb{Z}^+$ and $n > f$, then $p^n \not| b$, so if $n \in \mathbb{Z}^+$ and $p^n|b$, then $n \leq f$.

Since $g \in \mathbb{Z}^+$ and $p^g|b$, then we conclude $g \leq f$.

Since either $g = e$ or $g = f$, and $g \leq e$ and $g \leq f$, then $g = \min(e, f)$.

Hence $p^{\min(e,f)}$ divides d, so $p^{\min(e,f)}$ is a factor in the prime factorization of d.

Therefore, if p is a common prime factor of a and b, then $p^{\min(e,f)}$ is a factor in the prime factorization of d, where p^e is a factor in the prime factorization of a, and p^f is a factor in the prime factorization of b.

Case 2b: Suppose p is a prime factor of a and not b.

Then $p|a$ and $p \not| b$.

Suppose $p|d$.

Since $p|d$ and $d|b$, then $p|b$.

Hence, we have $p|b$ and $p \not| b$, a contradiction.

Therefore, $p \not| d$.

Consequently, if p is a prime factor of a, but not of b, then p is not a prime factor of d, so p is not in the prime factorization of d.

Therefore, if p is a prime factor of a, but not of b, then p is not in the prime factorization of d.

Case 2c: Suppose p is a prime factor of b and not a.

Then $p|b$ and $p \not| a$.

Suppose $p|d$.

Since $p|d$ and $d|a$, then $p|a$.

Hence, we have $p|a$ and $p \not| a$, a contradiction.

Therefore, $p \not| d$.

Consequently, if p is a prime factor of b, but not of a, then p is not a prime factor of d, so p is not in the prime factorization of d.

Therefore, if p is a prime factor of b, but not of a, then p is not in the prime factorization of d.

If p is a common prime factor of a and b, then p is a prime factor in the prime factorization of d.

If p is a prime factor of a, but not of b, then p is not in the prime factorization of d.

If p is a prime factor of b, but not of a, then p is not in the prime factorization of d.

Therefore, the only prime factors in the prime factorization of d are the common prime factors of a and b.

If p is a common prime factor of a and b, then $p^{\min(e,f)}$ is a factor in the prime factorization of d, where p^e is a factor in the prime factorization of a, and p^f is a factor in the prime factorization of b.

Thus, for every common prime factor p of a and b, $p^{\min(e,f)}$ is a factor in the prime factorization of d, where p^e is a factor in the prime factorization of a, and p^f is a factor in the prime factorization of b.

Hence, for every common prime factor p of a and b, p has a power equal to the minimum power occurring in the prime factorizations of a and b.

Therefore, $\gcd(a, b)$ is the product of all common prime factors p of a and b such that each prime p power is the minimum of the powers of p in the prime

factorizations of a and b. $\square$

Theorem 82. ***The lcm of two integers equals the product of the union of the primes to the largest power which appears in each integer.***

Let $a, b \in \mathbb{Z}^+$ with $a > 1$ and $b > 1$.

Then either $lcm(a, b) = ab$, or $lcm(a, b)$ is the integer m whose prime factorization contains primes in either of the prime factorizations of a and b such that each prime of m has a power equal to the maximum power occurring in the prime factorizations of a and b.

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

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

Either $m = ab$ or $m \neq ab$.

We consider these cases separately.

Case 1: Suppose $m = ab$.

Then $lcm(a, b) = m = ab$.

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

Case 2: Suppose $m \neq ab$.

Since $a \in \mathbb{Z}$ and $a > 1$, then by theorem 80, the fundamental theorem of arithmetic, a has a unique prime power factorization.

Since $b \in \mathbb{Z}$ and $b > 1$, then by theorem 80, the fundamental theorem of arithmetic, b has a unique prime power factorization.

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

Hence, $m \in \mathbb{Z}^+$ and $a|m$ and $b|m$, and for every $c \in \mathbb{Z}^+$, if $a|c$ and $b|c$, then $m|c$.

Since $a \in \mathbb{Z}^+$ and $m \in \mathbb{Z}^+$ and $a|m$, then $a \leq m$, by theorem 39.

Since $m \geq a$ and $a > 1$, then $m > 1$.

Since $m \in \mathbb{Z}^+$ and $m > 1$, then by theorem 80, the fundamental theorem of arithmetic, m has a unique prime power factorization.

If p is a prime factor of a or b, then either p is prime factor of a and not b, or p is a prime factor of b and not a, or p is a common prime factor of a and b.

We consider these cases separately.

Case 2a: Suppose p is a common prime factor of a and b.

Since a has a unique prime factorization, let e be the number of occurrences of p in the prime factorization of a.

Then $e \in \mathbb{Z}^+$ and p^e is a factor in the prime factorization of a, so $p^e|a$.

Since b has a unique prime factorization, let f be the number of occurrences of p in the prime factorization of b.

Then $f \in \mathbb{Z}^+$ and p^f is a factor in the prime factorization of b, so $p^f|b$.

Since $p^e|a$ and $a|m$, then $p^e|m$.

Since $p^f|b$ and $b|m$, then $p^f|m$.

We prove $p|m$.

Since $p^e|m$, then $m = p^e \cdot k$ for some integer k.

Since $e \in \mathbb{Z}^+$, then $e \geq 1$, so $e - 1 \geq 0$.

Hence, $p^{e-1} \in \mathbb{Z}$.

Observe that

$$\begin{aligned} m &= p^e \cdot k \\ &= (p \cdot p^{e-1}) \cdot k \\ &= p(p^{e-1} \cdot k). \end{aligned}$$

Since $m = p(p^{e-1} \cdot k)$ and $p^{e-1} \cdot k \in \mathbb{Z}$, then $p|m$.

Since p is prime and $p|m$ and m has a unique prime factorization, then p is a prime factor in the prime factorization of m.

Therefore, if p is a common prime factor of a and b, then p is a prime factor in the prime factorization of m.

Let g be the number of occurrences of p in the prime factorization of m.

Then $g \in \mathbb{Z}^+$ and p^g is a factor in the prime factorization of m, so $p^g|m$.

We must prove $g = \max(e, f)$.

Since $p^e|m$ and $p^g|m$, then g is the smallest power of p such that m is a multiple of p^e.

Since $p^f|m$ and $p^g|m$, then g is the smallest power of p such that m is a multiple of p^f.

Since g is the smallest power of p such that m is a multiple of p^e, and g is the smallest power of p such that m is a multiple of p^f, and $p^e|m$ and $p^f|m$, then either $g = e$ or $g = f$.

Since $e \in \mathbb{Z}^+$ and $p^e|m$, then e is the smallest power of p such that m is a multiple of p^e.

Hence, if n is a positive integer less than e, then m is not a multiple of p^e.

Thus, if $n \in \mathbb{Z}^+$ and $n < e$, then $p^e \not| m$, so if $n \in \mathbb{Z}^+$ and $p^e|m$, then $n \geq e$.

Since $g \in \mathbb{Z}^+$ and $p^g|m$, then we conclude $g \geq e$.

Since $f \in \mathbb{Z}^+$ and $p^f|m$, then f is the smallest power of p such that m is a multiple of p^f.

Hence, if n is a positive integer less than f, then m is not a multiple of p^f.

Thus, if $n \in \mathbb{Z}^+$ and $n < f$, then $p^f \not| m$, so if $n \in \mathbb{Z}^+$ and $p^f|m$, then $n \geq f$.

Since $g \in \mathbb{Z}^+$ and $p^g|m$, then we conclude $g \geq f$.

Since either $g = e$ or $g = f$, and $g \geq e$ and $g \geq f$, then $g = \max(e, f)$.

Hence, $p^{max(e,f)}$ divides m, so $p^{max(e,f)}$ is a factor in the prime factorization of m.

Therefore, if p is a common prime factor of a and b, then $p^{max(e,f)}$ is a factor in the prime factorization of m, where p^e is a factor in the prime factorization of a, and p^f is a factor in the prime factorization of b.

Case 2b: Suppose p is a prime factor of a and not b.

Let e be the number of occurrences of p in the prime factorization of a.

Then p^e is a prime factor of a, so $p^e|a$.

Since $p^e|a$ and $a|m$, then $p^e|m$, so p^e is a factor in the prime factorization of m.

Therefore, if p is a prime factor of a, but not of b, and p^e is a factor in the prime factorization of a, then p^e is a factor in the prime factorization of m.

Case 2c: Suppose p is a prime factor of b and not a.

Let f be the number of occurrences of p in the prime factorization of b.

Then p^f is a prime factor of b, so $p^f|b$.

Since $p^f|b$ and $b|m$, then $p^f|m$, so p^f is a factor in the prime factorization of m.

Therefore, if p is a prime factor of b, but not of a, and p^f is a factor in the prime factorization of b, then p^f is a factor in the prime factorization of m.

If p is a prime factor of a, but not of b, and p^e is a factor in the prime factorization of a, then p^e is a factor in the prime factorization of m.

If p is a prime factor of b, but not of a, and p^f is a factor in the prime factorization of b, then p^f is a factor in the prime factorization of m.

Therefore, if p is a prime factor of a or b, but not a common prime factor of a and b, then p is a factor in the prime factorization of m with power equal to the power occurring in the prime factorizations of a or b.

If p is a common prime factor of a and b, then $p^{max(e,f)}$ is a factor in the prime factorization of m, where p^e is a factor in the prime factorization of a, and p^f is a factor in the prime factorization of b.

Hence, if p is a common prime factor of a and b, then p has a power equal to the maximum power occurring in the prime factorizations of a and b.

Therefore, the prime factorization of m contains primes in either of the prime factorizations of a and b such that each prime of m has a power equal to the maximum power occurring in the prime factorizations of a and b. □

Distribution of Primes

Proposition 83. *Any distinct primes are relatively prime.*

Proof. Let p and q be distinct primes.

Then $p \in \mathbb{Z}^+$ and $q \in \mathbb{Z}^+$ and p is prime and q is prime and $p \neq q$.

Suppose for the sake of contradiction $p|q$.

Since $p \in \mathbb{Z}^+$ and $p|q$, then p is a positive divisor of q.

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

Hence, either $p = 1$ or $p = q$.

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

Since either $p = 1$ or $p = q$, and $p \neq 1$, then we conclude $p = q$.

But, this contradicts the hypothesis $p \neq q$.

Therefore, $p \not| q$.

Since $1 \in \mathbb{Z}^+$ and $1|p$ and $1|q$, then 1 is a positive common divisor of p and q.

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

Since $p|p$, but $p \not| q$, then p cannot be a common divisor of p and q, so p cannot be a positive common divisor of p and q.

Hence, the only positive common divisor of p and q is 1.

Since $\gcd(p, q)$ is a positive common divisor of p and q, then $\gcd(p, q)$ must be 1, so $\gcd(p, q) = 1$.

Therefore, p and q are relatively prime. □

Theorem 84. ***Euclid's Theorem***

There are infinitely many prime numbers.

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

Let $p_1, p_2, ..., p_n$ be any finite list of prime numbers.

We prove there is a prime number not included in the list.

Let $N = p_1 p_2 \cdots p_n + 1$.

Since each prime $p_1, p_2, ..., p_n$ is an integer, then the product $p_1 \dots p_n$ is an integer, so $p_1 \dots p_n + 1$ is an integer.

Hence, N is an integer.

Since each prime $p_1, p_2, ..., p_n$ is positive, then $p_1 p_2 \cdots p_n > 0$, so $N = p_1 p_2 \cdots p_n + 1 > 0 + 1 = 1$.

Hence, $N > 1$.

By theorem 73, every integer greater than one has a prime factor.

Since $N \in \mathbb{Z}$ and $N > 1$, then N has a prime factor.

Let p be a prime factor of N.

Then p is prime and $p|N$.

Suppose p is a prime in the list.

Then p is one of the primes $p_1, p_2, ..., p_n$.

Thus, p is one of the factors of the product $p_1 p_2 \cdots p_n$, so p divides $p_1 p_2 \cdots p_n$.

Since $p|N$ and $p|(p_1 p_2 \cdots p_n)$, then p is a common divisor of N and $(p_1 p_2 \cdots p_n)$.

By theorem 50, any common divisor of N and $(p_1 p_2 \cdots p_n)$ divides any linear combination of N and $(p_1 p_2 \cdots p_n)$.

Hence, p divides any linear combination of N and $(p_1 p_2 \cdots p_n)$.

Since $1 = N - p_1 p_2 \cdots p_n$ is a linear combination of N and $p_1 p_2 \cdots p_n$, then p must divide 1.

Since p is prime, then $p \in \mathbb{Z}^+$.

Since $p \in \mathbb{Z}^+$ and $p|1$, then $p = 1$.

But, p is prime and 1 is not prime, so $p \neq 1$.

Therefore, p is a prime not in the list, so there is a prime number that is not in the list. □

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.

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.

Since each prime p_k for $k = 1, 2, ..., n$ is greater than one, then the product p of all of these primes must be greater than one.

Thus, $p > 1$.

Hence, $q = p + 1 > 1 + 1 = 2 > 1$, so $q > 1$.

By theorem 73, every integer greater than one has a prime factor.

Therefore, q has a prime factor.

Let r be a prime factor of q.

Then, $r|q$.

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

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

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

By theorem 50, any common divisor of p and q divides any linear combination of p and q.

Since $1 = q - p$ is a linear combination of p and q, then this implies $r|1$.

Since r is prime, then $r > 1$, so $r > 0$.

Since $r > 0$ and $1 > 0$ and $r|1$, then $r \leq 1$, by theorem 39.

Thus, we have $r > 1$ and $r \leq 1$, a contradiction.

Therefore, $r \notin S$.

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

Thus, in all cases, there exists some prime that is not in S.

Therefore, there must be infinitely many prime numbers. □

Proof. Suppose for the sake of contradiction that there are 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.

Let a be the product of all prime numbers plus one.

Then $a = (p_1 p_2 p_3 \cdots p_n) + 1$.

Hence, $a > 1$.

By theorem 73, every integer greater than one has a prime factor, so a has a prime factor.

Therefore, one of the primes $p_1, p_2, ..., p_n$ must divide a, so $p_k | a$ for at least one of the primes p_k, where $k = 1, 2, ..., n$.

Since $p_k | a$, then $a = p_k b$ for some integer b.

Observe that

$$\begin{aligned} 1 &= a - (p_1 p_2 \cdot ... \cdot p_n) \\ &= p_k b - (p_1 p_2 \cdot ... \cdot p_n) \\ &= p_k b - (p_1 p_2 \cdot ... p_{k-1} p_k p_{k+1} ... \cdot p_n) \\ &= p_k (b - p_1 p_2 \cdot ... p_{k-1} p_{k+1} ... \cdot p_n). \end{aligned}$$

Since $b - p_1 p_2 \cdot ... p_{k-1} p_{k+1} ... \cdot p_n \in \mathbb{Z}$ and $1 = p_k (b - p_1 p_2 \cdot ... p_{k-1} p_{k+1} ... \cdot p_n)$, then $p_k | 1$.

Since p_k is prime, then $p_k > 1$.

Since $p_k > 1$ and $1 > 0$, then $p_k > 0$.

Since $p_k > 0$ and $1 > 0$ and $p_k | 1$, then $p_k \leq 1$, by theorem 39.

Hence, we have $p_k > 1$ and $p_k \leq 1$, a contradiction.

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

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 $p = p_1 p_2 * * * p_n + 1$.

Clearly, p is not in the list and each p_i divides the product $p_1 p_2 * * * p_n$.

Therefore, none of the p_i can divide p.

For if a certain p_i divided both p and $p_1 p_2 * * * p_n$, then p_i would divide their difference $p - p_1 p_2 * * * p_n = 1$.

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. □

Sieve of Eratosthenes

Lemma 85. *Let $n \in \mathbb{Z}^+$.*

If n is composite, then there exists $d \in \mathbb{Z}$ such that $d | n$ and $1 < d \leq \sqrt{n}$.

Proof. Suppose n is composite.

By theorem 72, a composite number is composed of smaller positive factors.

Since n is composite, then there exist integers a and b with $1 < a < n$ and $1 < b < n$ such that $n = ab$.
Since $1 < a < n$, then $1 < a$ and $a < n$.
Since $1 < b < n$, then $1 < b$ and $b < n$.
Since $n = ab = ba$, then $a|n$ and $b|n$.

Suppose $a > \sqrt{n}$ and $b > \sqrt{n}$.
Since $n \in \mathbb{Z}^+$, then $n \geq 1$.
Since $n \geq 1$ and $1 > 0$, then $n > 0$, so $\sqrt{n} > 0$.
Since $a > \sqrt{n}$ and $b > \sqrt{n}$ and $\sqrt{n} > 0$, then $n = ab > \sqrt{n} \cdot \sqrt{n} = (\sqrt{n})^2 = n$, so $n > n$, a contradiction.

Hence, either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.
We consider these cases separately.
Case 1: Suppose $a \leq \sqrt{n}$.
Since $1 < a$ and $a \leq \sqrt{n}$, then $1 < a \leq \sqrt{n}$.
Therefore, a is an integer and $a|n$ and $1 < a \leq \sqrt{n}$.
Case 2: Suppose $b \leq \sqrt{n}$.
Since $1 < b$ and $b \leq \sqrt{n}$, then $1 < b \leq \sqrt{n}$.
Therefore, b is an integer and $b|n$ and $1 < b \leq \sqrt{n}$.

In all cases, there is an integer d such that $d|n$ and $1 < d \leq \sqrt{n}$. □

Proposition 86. *Let $n \in \mathbb{Z}^+$.*
If n is composite, then n has a prime factor less than or equal to $\sqrt{n}$.

Proof. Suppose n is composite.
By lemma 85, there exists $d \in \mathbb{Z}$ such that $d|n$ and $1 < d \leq \sqrt{n}$.
Since $1 < d \leq \sqrt{n}$, then $1 < d$ and $d \leq \sqrt{n}$.
By theorem 73, every integer greater than one has a prime factor.
Since $d \in \mathbb{Z}$ and $d > 1$, then d has a prime factor.

Let p be a prime factor of d.
Then $p \in \mathbb{Z}^+$ and p is prime and $p|d$.
Since $p|d$ and $d|n$, then $p|n$.
Since $d > 1$ and $1 > 0$, then $d > 0$.
Since $d \in \mathbb{Z}$ and $d > 0$, then $d \in \mathbb{Z}^+$.
Since $p \in \mathbb{Z}^+$ and p is prime, then $p > 1$, so $p > 0$.
Since $p \in \mathbb{Z}^+$ and $d \in \mathbb{Z}^+$ and $p|d$, then $p \leq d$.
Since $p \leq d$ and $d \leq \sqrt{n}$, then $p \leq \sqrt{n}$.
Since p is prime and $p|n$, then p is a prime factor of n.
Therefore, p is a prime factor of n and $p \leq \sqrt{n}$. □

Proposition 87. *For every integer $n > 2$, there is a prime p such that $p < n$.*

Proof. Let n be an integer greater than 2.
Then $n \in \mathbb{Z}$ and $n > 2$.
Let $p = 2$.
Since 2 is prime and $2 < n$, then there is a prime p such that $p < n$. □

Proposition 88. *For every $n \in \mathbb{Z}^+$, there is a prime p such that $p > n$.*

Proof. Let $n \in \mathbb{Z}^+$.
Then $n \geq 1$, so either $n > 1$ or $n = 1$.
We consider these cases separately.
Case 1: Suppose $n = 1$.
Since 2 is prime and $2 > 1$, then there is a prime p such that $p > n$.
Case 2: Suppose $n > 1$.
Suppose for the sake of contradiction there is no prime p greater than n.
Then $p \leq n$ for every prime p.
Hence, $p < n + 1$ for every prime p.

Let S be the set of all primes less than $n + 1$.
Then $S = \{p \in \mathbb{Z}^+ : p \text{ is prime and } p < n + 1\}$.
Since $n \in \mathbb{Z}^+$ and $n > 1$, then $n \geq 2$, so $n + 1 \geq 3$.
Since $n + 1 \geq 3$ and $3 > 2$, then $n + 1 > 2$.
Since $n \in \mathbb{Z}^+$, then $n + 1 \in \mathbb{Z}^+$.
Since $n + 1 \in \mathbb{Z}$ and $n + 1 > 2$, then there is a prime p such that $p < n + 1$, by proposition 87.
Since p is prime, then $p \in \mathbb{Z}^+$.
Since $p \in \mathbb{Z}^+$ and p is prime and $p < n + 1$, then $p \in S$, so S is not empty.

We prove S is finite.
Let T be the set of all positive integers less than $n + 1$.
Then $T = \{t \in \mathbb{Z}^+ : t < n+1\} = \{1, ..., n-1, n\}$ is a finite set of cardinality n.

Let $x \in S$.
Then $x \in \mathbb{Z}^+$ and x is prime and $x < n + 1$.
Since $x \in \mathbb{Z}^+$ and $x < n + 1$, then $x \in T$.
Hence, $x \in S$ implies $x \in T$, so $S \subseteq T$.

A subset of a finite set is finite.
Since $S \subseteq T$ and T is finite, then S is finite.

Since S is a non-empty finite set of prime numbers, then S contains exactly k primes $p_1, p_2, ..., p_k$ such that $p_1 < p_2 < ... < p_k$ for $k \in \mathbb{Z}^+$.
Since $p_k \in S$, then $p_k < n + 1$.
By Euclid's theorem, there are infinitely many prime numbers, so there exists a prime p_{k+1} such that $p_{k+1} > p_k$.

Suppose $p_{k+1} < n+1$.
Since p_{k+1} is prime, then $p_{k+1} \in \mathbb{Z}^+$.
Since $p_{k+1} \in \mathbb{Z}^+$ and p_{k+1} is prime and $p_{k+1} < n+1$, then $p_{k+1} \in S$.
Hence, S contains at least $k+1$ elements, so S contains more than k elements.
But, this contradicts that S contains exactly k elements.
Therefore, p_{k+1} cannot be less than $n+1$, so $p_{k+1} \geq n+1$.

Since $p_{k+1} \geq n+1$ and $n+1 > n$, then $p_{k+1} > n$.
Thus, p_{k+1} is prime and $p_{k+1} > n$, so there is a prime greater than n.
But, this contradicts the assumption there is no prime greater than n.
Therefore, there must be a prime p such that $p > n$. □

Lemma 89. *Let $n \in \mathbb{Z}^+$.*
Let p_n be the n^{th} prime number when the sequence of primes is arranged in ascending order.
Then $p_{n+1} \leq p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$ for all $n \in \mathbb{Z}^+$.

Proof. Suppose for the sake of contradiction there exists $n \in \mathbb{Z}^+$ such that $p_{n+1} > p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$.
Let $N = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$.
Then $p_{n+1} > N$.
Since each prime $p_1, p_2, ..., p_n$ is positive, then $p_1 p_2 \cdot \cdot \cdot p_n > 0$, so $N = p_1 p_2 \cdot \cdot \cdot p_n + 1 > 0 + 1 = 1$.
Hence, $N > 1$.
Since $p_1, p_2, ..., p_n \in \mathbb{Z}^+$ and $N = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$, then $N \in \mathbb{Z}$.
By theorem 73, every integer greater than 1 has a prime factor.
Since $N \in \mathbb{Z}$ and $N > 1$, then N has a prime factor.

Let $p \in \mathbb{Z}^+$ be a prime factor of N.
Then p is prime and $p|N$.
Since $p_n|p_n$, then p_n divides any multiple of p_n, by theorem 43.
Hence, p_n divides the product $p_1 p_2 ... p_n$, so p_n divides $N-1$.
Since $N > 1$, then $N - 1 > 0$.
Since $N \in \mathbb{Z}$, then $N - 1 \in \mathbb{Z}$.
Since $N - 1 \in \mathbb{Z}$ and $N - 1 > 0$, then $N - 1 \in \mathbb{Z}^+$.
Since p_n is prime, then $p_n \in \mathbb{Z}^+$.
By theorem 39, a divisor of a is smaller than a.
Since $p_n \in \mathbb{Z}^+$ and $N - 1 \in \mathbb{Z}^+$ and p_n divides $N - 1$, then $p_n \leq N - 1$.
Thus, $p_n \leq N - 1 < N$, so $p_n < N$.
Since p_1 is prime, then $p_1 > 1$.
Since the sequence of primes is arranged in ascending order, and $p_1, p_2, ... p_n$ are all primes, and $p_1 > 1$ and $p_{n+1} > N$ and $p_n < N$, then $1 < p_1 < p_2 < ... < p_n < N < p_{n+1}$.
Since $N \in \mathbb{Z}$ and $N > 1$, then $N \in \mathbb{Z}^+$.
Since $p \in \mathbb{Z}^+$ and $N \in \mathbb{Z}^+$ and p divides N, then $p \leq N$.
Since p is prime, then $p > 1$, so $1 < p \leq N$.

Since p is prime, and p divides N, and $1 < p_1 < p_2 < ... < p_n < N < p_{n+1}$, and $1 < p \leq N$, then p must be one of the primes $p_1, p_2, ..., p_n$, so $p = p_k$ for some integer $k \in \{1, 2, ..., n\}$.

Since p_k is one of the factors of the product $p_1p_2...p_n$, then p_k divides $p_1p_2...p_n$.

Since $p_k|N$ and p_k divides $p_1p_2...p_n$, then p_k is a common divisor of N and $p_1p_2...p_n$.

By theorem 50, any common divisor of N and $(p_1p_2 \cdots p_n)$ divides any linear combination of N and $(p_1p_2 \cdots p_n)$.

Since $1 = N - p_1p_2 \cdots p_n$ is a linear combination of N and $p_1p_2 \cdots p_n$, then p_k must divide 1.

Since p_k is prime, then $p_k \in \mathbb{Z}^+$.

Since $p_k \in \mathbb{Z}^+$ and $p_k|1$, then $p_k = 1$.

But, p_k is prime and 1 is not prime, so $p_k \neq 1$.

Consequently, there is no $n \in \mathbb{Z}^+$ such that $p_{n+1} > p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$.

Therefore, $p_{n+1} \leq p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$ for all $n \in \mathbb{Z}^+$. □

Proposition 90. *Let $n \in \mathbb{Z}^+$.*

Let p_n be the n^{th} prime number when the sequence of primes is arranged in ascending order.

Then $p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1 \leq {p_n}^n + 1$ for all $n \in \mathbb{Z}^+$.

Proof. Let $q(n)$ be the predicate defined by $p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1 \leq {p_n}^n + 1$ over $\mathbb{Z}^+$.

We prove $q(n)$ is true for all $n \in \mathbb{Z}^+$ by induction on n.

Basis:

Let $n = 1$.

Since $p_1 + 1 = {p_1}^1 + 1$, then $q(1)$ is true.

Let $n = 2$.

Since $p_1p_2 + 1 = 2 \cdot 3 + 1 = 7 < 10 = 3^2 + 1 = {p_2}^2 + 1$, then $q(2)$ is true.

Induction:

Let $k \in \mathbb{Z}^+$ with $k \geq 2$ such that $q(k)$ is true.

Then $p_1p_2 \cdot ... \cdot p_k + 1 \leq {p_k}^k + 1$, so $p_1p_2 \cdot ... \cdot p_k \leq {p_k}^k$.

Hence, $p_1p_2 \cdot ... \cdot p_k \leq {p_k}^k < {p_{k+1}}^k$, so $p_1p_2 \cdot ... \cdot p_k < {p_{k+1}}^k$.

Thus, $p_1p_2 \cdot ... \cdot p_k \cdot p_{k+1} < {p_{k+1}}^k \cdot p_{k+1}$, so $p_1p_2 \cdot ... \cdot p_k \cdot p_{k+1} < {p_{k+1}}^{k+1}$.

Therefore, $p_1p_2 \cdot ... \cdot p_k \cdot p_{k+1} + 1 < {p_{k+1}}^{k+1} + 1$, so $q(k+1)$ is true.

Consequently, $q(k)$ implies $q(k+1)$ for all $k \in \mathbb{Z}^+$ with $k \geq 2$.

Since $q(1)$ and $q(2)$ are true, and $q(k)$ implies $q(k+1)$ for all $k \in \mathbb{Z}^+$ with $k \geq 2$, then by induction, $q(k)$ is true for all $k \in \mathbb{Z}^+$, so $q(n)$ is true for all $n \in \mathbb{Z}^+$.

Therefore, $p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1 \leq {p_n}^n + 1$ for all $n \in \mathbb{Z}^+$. □

Proposition 91. ***growth of the prime number sequence***

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

Let p_n be the n^{th} prime number when the sequence of primes is arranged in ascending order.

Then $p_n \leq 2^{2^{n-1}}$ for all $n \in \mathbb{Z}^+$.

Proof. Let $q(n)$ be the predicate $p_n \leq 2^{2^{n-1}}$ defined over $\mathbb{Z}^+$.

We prove $q(n)$ is true for all $n \in \mathbb{Z}^+$ by strong induction on n.

Basis:

Let $n = 1$.

Since $p_1 = 2 = 2^1 = 2^{2^0} = 2^{2^{1-1}}$, then $q(1)$ is true.

Let $n = 2$.

Since $p_2 = 3 < 4 = 2^2 = 2^{2^{2-1}}$, then $p_2 < 2^{2^{2-1}}$, so $q(2)$ is true.

Induction:

Let $k \in \mathbb{Z}^+$ with $k \geq 2$ such that $q(1)$ and $q(2)$ and ... and $q(k)$ are all true.

Then $p_1 \leq 2$ and $p_2 \leq 2^2$ and $p_3 \leq 2^4$ and ... and $p_k \leq 2^{2^{k-1}}$.

Since $p_1, p_2, ..., p_k$ are all greater than zero, then $p_1 p_2 \cdot ... \cdot p_k \leq 2^1 \cdot 2^2 \cdot 2^4 \cdot ... \cdot 2^{2^{k-1}} = 2^{1+2+4+...+2^{k-1}}$.

Let $S = 1 + 2 + 4 + ... + 2^{k-1}$.

Then $S = \sum_{k=0}^{k-1} 2^k$ is the sum of the first k terms of a geometric series, so $S = 2^k - 1$.

Hence, $p_1 p_2 \cdot ... \cdot p_k \leq 2^S = 2^{2^k - 1}$, so $p_1 p_2 \cdot ... \cdot p_k \leq 2^{2^k - 1}$.

Thus, $p_1 p_2 \cdot ... \cdot p_k + 1 \leq 2^{2^k - 1} + 1$.

Since p_n is the n^{th} prime number when the sequence of primes is arranged in ascending order, then $p_{n+1} \leq p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$ for all $n \in \mathbb{Z}^+$, by lemma 89.

Thus, $p_{k+1} \leq p_1 \cdot p_2 \cdot \ldots \cdot p_k + 1$.

Since $p_{k+1} \leq p_1 \cdot p_2 \cdot \ldots \cdot p_k + 1$ and $p_1 p_2 \cdot ... \cdot p_k + 1 \leq 2^{2^k - 1} + 1$, then $p_{k+1} \leq 2^{2^k - 1} + 1$.

Since $k \geq 2 > 0$, then $k > 0$.

Observe that

$$\begin{aligned} k > 0 &\Rightarrow 2^k > 1 \\ &\Rightarrow 2^k - 1 > 0 \\ &\Rightarrow 2^{2^k - 1} > 1 \\ &\Rightarrow 1 < 2^{2^k - 1} \\ &\Rightarrow 2^{2^k - 1} + 1 < 2^{2^k - 1} + 2^{2^k - 1} \\ &\Rightarrow 2^{2^k - 1} + 1 < 2 \cdot 2^{2^k - 1} \\ &\Rightarrow 2^{2^k - 1} + 1 < 2^{2^k}. \end{aligned}$$

Thus, $2^{2^k - 1} + 1 < 2^{2^k}$.

Since $p_{k+1} \leq 2^{2^k-1}+1$ and $2^{2^k-1}+1 < 2^{2^k}$, then $p_{k+1} < 2^{2^k}$, so $q(k+1)$ is true.

Therefore, $q(k+1)$ is true whenever $q(1)$ and $q(2)$ and ... and $q(k)$ are all true for all $k \in \mathbb{Z}^+$ with $k \geq 2$.

Since $q(1)$ and $q(2)$ are true, and $q(k+1)$ is true whenever $q(1)$ and $q(2)$ and ... and $q(k)$ are all true for all $k \in \mathbb{Z}^+$ with $k \geq 2$, then by induction, $q(k)$ is true for all $k \in \mathbb{Z}^+$, so $q(n)$ is true for all $n \in \mathbb{Z}^+$.

Therefore, $p_n \leq 2^{2^{n-1}}$ for all $n \in \mathbb{Z}^+$. □

Corollary 92. *Let $n \in \mathbb{Z}^+$.*

Then there are at least $n+1$ primes less than 2^{2^n}.

Proof. Let p_n be the n^{th} prime number when the sequence of primes is arranged in ascending order.

Since $n \in \mathbb{Z}^+$, then $p_n \leq 2^{2^{n-1}}$, by proposition 91.

Since $n \in \mathbb{Z}^+$, then $n+1 \in \mathbb{Z}^+$, so $p_{n+1} \leq 2^{2^n}$, by proposition 91.

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

Since $1 < 2 = p_1 \leq p_n < p_{n+1}$, then $2 < p_{n+1}$.

Since p_{n+1} is prime and $p_{n+1} > 2$, then p_{n+1} is odd.

Since $2^{2^{n-1}}$ and 2^{2^n} are even, and p_{n+1} is odd, then $p_{n+1} \neq 2^{2^{n-1}}$ and $p_{n+1} \neq 2^{2^n}$, so $1 < p_1 < ... < p_n \leq 2^{2^{n-1}} < p_{n+1} < 2^{2^n}$.

Thus, $1 < p_1 < ... < p_n < p_{n+1} < 2^{2^n}$, so $p_1, ..., p_n, p_{n+1}$ are primes less than 2^{2^n}.

Therefore, there are at least $n+1$ primes less than 2^{2^n}. □

Goldbach Conjecture

Proposition 93. ***Twin primes are odd.***

Let p and $p+2$ be twin primes.

Then p and $p+2$ are odd.

Proof. Since p and $p+2$ are twin primes, then p is prime and $p+2$ is prime.

Since p is prime, then $p \in \mathbb{Z}^+$.

Suppose p is not odd.

Since $p \in \mathbb{Z}^+$ and p is not odd, then p is even.

Since p is prime and p is even, then $p = 2$, so $p+2 = 2+2 = 4 = 2 \cdot 2$ is composite.

Since $p+2$ is composite, then $p+2$ is not prime.

But, this contradicts the assumption $p+2$ is prime.

Thus, p is odd, so $p = 2n+1$ for some integer n.

Hence, $p+2 = (2n+1)+2 = 2n+2+1 = 2(n+1)+1$ is odd.

Therefore, p is odd and $p+2$ is odd. □

Proposition 94. *For every integer $n \geq 2$, there are n consecutive positive integers which are all composite.*

Proof. Let n be an integer greater than or equal to 2.

Then $n \geq 2$, so $n \in \mathbb{Z}^+$.

Let S be the set of all numbers $(n+1)!+k$ for each integer $k = 2, 3, ..., n+1$.

Then $S = \{(n+1)! + k : k \in \{2, 3, ..., n+1\}\}$, so $S = \{(n+1)! + 2, (n+1)! + 3, ..., (n+1)! + (n+1)\}$.

Since $n \in \mathbb{Z}^+$, then $(n+1)! \in \mathbb{Z}^+$, so $(n+1)! + k \in \mathbb{Z}^+$ for each $k = 2, 3, ..., n+1$.

Hence, each element of S is a positive integer.

Since $(n+1)!+2 < (n+1)!+3 < ... < (n+1)!+(n+1)$, then each successive integer is one greater than the previous integer, so there are n consecutive positive integers.

We prove each element of S is composite.

First, we prove $(n+1)! + k$ is divisible by k for each $k = 2, 3, ..., n+1$.

Since $k = 2, 3, ..., n+1$, then $2 \leq k \leq n+1$.

Since $(n+1)! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n(n+1)$, and k is an integer and $2 \leq k \leq n+1$, then k is a factor of $(n+1)!$, so k divides $(n+1)!$.

Since k divides $(n+1)!$ and k divides k, then k divides the sum $(n+1)!+k$, so $(n+1)! + k = km$ for some integer m.

Since $n \geq 2$, then $n + 1 \geq 3$.

Thus, $(n+1)! \geq 3! = 6 > 0$, so $(n+1)! > 0$.

Hence, $(n+1)! + k > k$.

Since $k \geq 2$ and $2 > 1$, then $k > 1$.

Since $k > 1$ and $(n+1)! + k > k$, then $1 < k < (n+1)! + k$.

Since $(n+1)! + k \in \mathbb{Z}^+$ and $k \in \mathbb{Z}^+$ and $(n+1)! + k = km$, then $m \in \mathbb{Z}^+$, so $m \geq 1$.

Hence, either $m > 1$ or $m = 1$.

Suppose $m = 1$.

Then $(n+1)! + k = k(1) = k$, so $(n+1)! = 0$.

But, this contradicts $(n+1)! > 0$.

Hence, $m \neq 1$, so $m > 1$.

Since $m \in \mathbb{Z}^+$ and $(n+1)! + k \in \mathbb{Z}^+$ and m divides $(n+1)! + k$, then $m \leq (n+1)! + k$, by theorem 39.

Thus, either $m < (n+1)! + k$ or $m = (n+1)! + k$.

Suppose $m = (n+1)! + k$.

Then $m = (n+1)! + k = km$, so $m = km$.

Hence, $0 = km - m = m(k-1)$, so either $m = 0$ or $k = 1$.

Since $m > 1$, then $m \neq 0$, so $k = 1$.

But, this contradicts $k > 1$.

Therefore, $m \neq (n+1)! + k$, so $m < (n+1)! + k$.

Since $m > 1$ and $m < (n+1)! + k$, then $1 < m < (n+1)! + k$.

By theorem 72, a composite number is composed of smaller positive factors.

Since k and m are integers, and $1 < k < (n+1)!+k$, and $1 < m < (n+1)!+k$, and $(n+1)! + k = km$, then $(n+1)! + k$ is composite.

Therefore, $(n+1)!+k$ is composite for each $k = 2, 3, ..., n+1$, so each element of S is composite. □

Conjecture 95. ***ternary(weak) Goldbach conjecture***

Every odd integer greater than 5 is the sum of three primes.

Proof. Suppose the strong Goldbach conjecture is true.

Let n be an odd integer greater than 5.

Then n is odd and $n > 5$.

Since n is odd and 3 is odd, then the difference $n - 3$ is even.

Since $n > 5$, then $n - 3 > 2$.

Since $n - 3$ is even and $n - 3 > 2$, then $n - 3 = p + q$ for some primes p and q, since we're assuming the strong Goldbach conjecture is true.

Since $n = 3 + p + q$, and $3, p$, and q are all primes, then n is the sum of three primes. □

Proposition 96. *Every odd integer is of the form $4n + 1$ or $4n + 3$ for some integer n.*

Proof. Let a be any odd integer.

Then a is an integer and a is odd.

By the division algorithm, when a is divided by 4, there are unique integers q and r such that $a = 4q + r$ and $0 \leq r < 4$, so either $a = 4q$ or $a = 4q + 1$ or $a = 4q + 2$ or $a = 4q + 3$.

Hence, either $a = 4q = 2(2q)$ or $a = 4q + 1$ or $a = 4q + 2 = 2(2q + 1)$ or $a = 4q + 3$.

Since a is odd, then a is not even, so $a \neq 4q$ and $a \neq 4q + 2$.

Therefore, either $a = 4q + 1$ or $a = 4q + 3$, so either $a = 4q + 1$ or $a = 4q + 3$ for some integer q. □

Proof. Let a be any odd integer.

Since a is odd, then $a = 2b + 1$ for some integer b.

Either b is even or b is not even.

We consider these cases separately.

Case 1: Suppose b is even.

Then $b = 2n$ for some integer n.

Hence, $a = 2b + 1 = 2(2n) + 1 = 4n + 1$.
Therefore, $a = 4n + 1$ for some integer n.
Case 2: Suppose b is not even.
Then b is odd, so $b = 2n + 1$ for some integer n.
Hence, $a = 2b + 1 = 2(2n + 1) + 1 = 4n + 2 + 1 = 4n + 3$.
Therefore, $a = 4n + 3$ for some integer n. □

Lemma 97. *The product of any finite number of integers of the form $4a + 1$ is of the same form.*

Proof. We must prove $(4a_1 + 1)(4a_2 + 1) \cdot \ldots \cdot (4a_n + 1) = 4m + 1$ for some integer m for all $n \in \mathbb{Z}^+$.

Thus, we must prove: for all $n \in \mathbb{Z}^+$, $\prod_{i=1}^{n}(4a_i + 1) = 4m + 1$ for some integer m.

Let $p(n)$ be the predicate defined over $\mathbb{Z}^+$ by '$\prod_{i=1}^{n}(4a_i + 1) = 4m + 1$ for some integer m'.

We prove $p(n)$ is true for all $n \in \mathbb{Z}^+$ by induction on n.
Basis:
Let $n = 1$.
Then $\prod_{i=1}^{1}(4a_i + 1) = 4a_1 + 1$ for some integer a_1.
Therefore, $p(1)$ is true.

Let $n = 2$.
Then $\prod_{i=1}^{2}(4a_i + 1) = (4a_1 + 1)(4a_2 + 1)$ for some integers a_1 and a_2.
Observe that

$$\begin{aligned}\prod_{i=1}^{2}(4a_i + 1) &= (4a_1 + 1)(4a_2 + 1)\\ &= 16a_1a_2 + 4a_1 + 4a_2 + 1\\ &= 4(4a_1a_2 + a_1 + a_2) + 1\\ &= 4m + 1.\end{aligned}$$

Hence, $\prod_{i=1}^{2}(4a_i+1) = 4m+1$ for some integer m, where $m = 4a_1a_2+a_1+a_2$.
Therefore, $p(2)$ is true.
Induction:
Let $k \in \mathbb{Z}^+$ with $k \geq 2$ such that $p(k)$ is true.
Then $\prod_{i=1}^{k}(4a_i + 1) = 4s + 1$ for some integer s.

Observe that

$$\begin{aligned}\prod_{i=1}^{k+1}(4a_i + 1) &= \prod_{i=1}^{k}(4a_i + 1) \cdot (4a_{k+1} + 1)\\ &= (4s + 1)(4a_{k+1} + 1)\\ &= 16sa_{k+1} + 4s + 4a_{k+1} + 1\\ &= 4(4sa_{k+1} + s + a_{k+1}) + 1\\ &= 4t + 1.\end{aligned}$$

Hence, $\prod_{i=1}^{k+1}(4a_i+1) = 4t+1$ for some integer t, where $t = 4sa_{k+1}+s+a_{k+1}$.

Therefore, $p(k+1)$ is true.

Thus, $p(k)$ implies $p(k+1)$ for all $k \in \mathbb{Z}^+$ with $k \geq 2$.

Since $p(1)$ is true and $p(2)$ is true, and $p(k)$ implies $p(k+1)$ for all $k \in \mathbb{Z}^+$ with $k \geq 2$, then by induction, $p(k)$ is true for all $k \in \mathbb{Z}^+$.

Therefore, for all $n \in \mathbb{Z}^+$, $\prod_{i=1}^{n}(4a_i+1) = 4m+1$ for some integer m. □

Theorem 98. *There are infinitely many primes of the form $4n+3$, where $n \in \mathbb{Z}$.*

Proof. Suppose for the sake of contradiction there are finitely many primes of the form $4n+3$.

Let $p_1, p_2, ..., p_k$ be k primes such that each p_i is of the form $4n+3$ for some integer n, where $i = 1, 2, ..., k$.

Let $N = 4p_1p_2 \dots p_k - 1$.

Then $N = 4p_1p_2 \dots p_k - 4 + 3 = 4(p_1p_2 \dots p_k - 1) + 3$, so $N = 4(p_1p_2 \dots p_k - 1) + 3$.

Thus, by the division algorithm, 3 is the unique remainder when N is divided by 4.

Since each prime p_i is an integer and $N = 4p_1p_2 \dots p_k - 1$, then $N \in \mathbb{Z}$.

By lemma 78, a product of primes is greater than 1.

Thus, $p_1p_2 \dots p_k > 1$, so $4p_1p_2 \dots p_k > 4$.

Hence, $N = 4p_1p_2 \dots p_k - 1 > 4 - 1 = 3 > 1$, so $N > 1$.

Since $N \in \mathbb{Z}$ and $N > 1$, then N is a product of primes, by the fundamental theorem of arithmetic.

Thus, there are m primes $q_1, q_2, ..., q_m$ such that $N = q_1q_2 \dots q_m$, where $m \in \mathbb{Z}^+$.

Since the product $4p_1p_2 \dots p_k = 2(2p_1p_2 \dots p_k)$ is even, then $4p_1p_2 \dots p_k - 1$ is odd, so N is odd.

Thus, N is not even, so 2 does not divide N.

Hence, 2 is not a prime factor of N, so each prime factor $q_j \neq 2$ for $j = 1, 2, ..., m$.

Consequently, each prime q_j is greater than 2, so each q_j is odd.

Therefore, each q_j is of the form $4n+1$ or $4n+3$ for some integer n, by proposition 96.

Suppose every prime q_j is of the form $4n+1$ for some integer n.

By lemma 97, the product of any finite number of integers of the form $4n+1$ is of the same form.

Hence, the product $q_1q_2 \dots q_m$ is of the form $4n+1$, so $q_1q_2 \dots q_m = 4a+1$ for some integer a.

Thus, $N = 4a+1$, so 1 is the remainder when N is divided by 4.

But, this contradicts 3 is the unique remainder when N is divided by 4.

Therefore, not every prime q_j is of the form $4n+1$, so there is some prime q_s that is not of the form $4n+1$ for some $s \in \{1, 2, ..., m\}$.

Since q_s is of the form $4n+1$ or $4n+3$, and q_s is not of the form $4n+1$, then q_s is of the form $4n+3$, so $q_s = 4t+3$ for some integer t.

Since q_s is prime and $s \in \{1, 2, ..., m\}$, then q_s is one of the prime factors in the product $q_1 q_2 \dots q_m$, so q_s divides $q_1 q_2 \dots q_m$.

Therefore, q_s divides N.

Since q_s is prime and $q_s = 4t+3$, then q_s is one of the primes $p_1, p_2, ..., p_k$, so q_s divides the product $p_1 p_2 \dots p_k$.

Since q_s divides $p_1 p_2 \dots p_k$ and q_s divides N, then q_s divides any linear combination of $p_1 p_2 \dots p_k$ and N, so q_s divides $1 = 4p_1 p_2 \dots p_k - N$.

Thus, $q_s | 1$.

Since q_s is prime, then $q_s \in \mathbb{Z}^+$.

Since $q_s \in \mathbb{Z}^+$ and $q_s | 1$, then $q_s = 1$.

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

Therefore, there are not finitely many primes of the form $4n+3$, so there are infinitely many primes of the form $4n+3$. □

Proof. Let (a_n) be the sequence of positive integers given by $a_n = 4n+3$ and $a_0 = 3$.

Then the sequence is $3, 7, 11, 15, 19, 23, 27, 31, ...$

Since $\gcd(3, 4) = 1$, then 3 and 4 are relatively prime.

Therefore, by Dirichlet's theorem, the sequence contains infinitely many primes, so there are infinitely many primes of the form $4n+3$. □

Proposition 99. *Let $a, m \in \mathbb{Z}^+$.*

If $\gcd(a, m) > 1$ and a is composite, then the arithmetic sequence $a, a+m, a+2m, a+3m, ...$ contains only composite numbers.

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

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

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

Suppose $d > 1$ and a is composite.

Let (a_n) be the arithmetic sequence defined by $a_0 = a$ and $a_n = a + nm$ for all $n \in \mathbb{Z}^+$.

To prove (a_n) consists of only composite numbers, we must prove a is composite and a_n is composite for all $n \in \mathbb{Z}^+$.

By hypothesis, a is composite.

By theorem 73, every integer greater than 1 has a prime factor.

Since $d \in \mathbb{Z}$ and $d > 1$, then d has a prime factor.

Let p be a prime factor of d.

Then $p \in \mathbb{Z}^+$ and p is prime and $p|d$.

Since $p|d$ and $d|a$, then $p|a$.

Since $p|d$ and $d|m$, then $p|m$.

Since $p|a$ and $p|m$, then p divides any linear combination of a and m, by theorem 50.

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

Then $a_n = a + nm$.

Since $a + nm$ is a linear combination of a and m, then $p|(a + nm)$, so $p|a_n$.

Since $n \in \mathbb{Z}^+$ and $m \in \mathbb{Z}^+$, then $nm \in \mathbb{Z}^+$, so $nm > 0$.

Hence, $a + nm > a$, so $a_n > a$.

Since p is prime, then $p > 1$.

Since $p \in \mathbb{Z}^+$ and $a \in \mathbb{Z}^+$ and $p|a$, then $p \leq a$, by theorem 39.

Since $p \leq a$ and $a < a_n$, then $p < a_n$.

Since $1 < p$ and $p < a_n$, then $1 < p < a_n$.

By lemma 71, a composite number has a positive divisor between 1 and itself.

Since $p \in \mathbb{Z}^+$ and $p|a_n$ and $1 < p < a_n$, then a_n is composite.

Hence, a_n is composite for all $n \in \mathbb{Z}^+$.

Since a is composite, and a_n is composite for all $n \in \mathbb{Z}^+$, then every term of the sequence (a_n) is composite, so the sequence (a_n) contains only composite numbers. □

Lemma 100. *Let $a, m \in \mathbb{Z}^+$.*

If the arithmetic sequence $a, a + m, a + 2m, a + 3m, ...$ contains a prime number, then it contains infinitely many composite numbers.

Proof. Let (a_n) be the arithmetic sequence defined by $a_0 = a$ and $a_n = a + nm$ for all $n \in \mathbb{Z}^+$.

Suppose (a_n) contains a prime number.

Then there is a prime $p = a + nm$ for some integer n with $n \geq 0$.

Since p is prime, then $p \in \mathbb{Z}^+$ and $p > 1$.

Let (b_k) be the arithmetic sequence $n + p, n + 2p, n + 3p, ...$

Then $b_k = n + kp$ for all $k \in \mathbb{Z}^+$, so the sequence (b_k) is the function $f : \mathbb{Z}^+ \to S$ defined by $f(k) = n + kp = b_k$ and $S = \{b_k : k \in \mathbb{Z}^+\}$.

We prove f is bijective.

We first prove f is injective.

Suppose $f(k) = f(m)$.

Then $n + kp = n + mp$ for some $k, m \in \mathbb{Z}^+$, so $kp = mp$.

Hence, $0 = kp - mp = p(k - m)$, so either $p = 0$ or $k = m$.

Since $p \in \mathbb{Z}^+$, then $p > 0$, so $p \neq 0$.

Thus, $k = m$, so $f(k) = f(m)$ implies $k = m$.

Therefore, f is injective.

We prove f is surjective.

Let $b_k \in S$.

Then $b_k = n + kp$ for some $k \in \mathbb{Z}^+$.

Since $k \in \mathbb{Z}^+$ and $f(k) = n + kp = b_k$, then f is surjective.

Since f is injective and f is surjective, then f is bijective, so $|\mathbb{Z}^+| = |S|$.

Since $\mathbb{Z}^+$ is an infinite set, then this implies S is an infinite set, so the sequence (b_k) has infinitely many terms.

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

Since $k \in \mathbb{Z}^+$ and $p \in \mathbb{Z}^+$, then $kp \in \mathbb{Z}^+$, so $kp > 0$.

Since $n \in \mathbb{Z}$ and $kp \in \mathbb{Z}$, then $n + kp \in \mathbb{Z}$, so $b_k \in \mathbb{Z}$.

Since $n \geq 0$ and $kp > 0$, then $n + kp > 0$, so $b_k > 0$.

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

Observe that

$$\begin{aligned} a_{b_k} &= a + b_k m \\ &= a + (n + kp)m \\ &= a + nm + kpm \\ &= p + kpm \\ &= p(1 + km). \end{aligned}$$

Hence, $a_{b_k} = p(1 + km)$, so p divides a_{b_k}.

Since $k \in \mathbb{Z}^+$ and $m \in \mathbb{Z}^+$, then $km \in \mathbb{Z}^+$, so $km > 0$.

Thus, $1 + km > 1$.

Since $1 + km > 1$ and $p > 0$, then $p(1 + km) > p$, so $a_{b_k} > p$.

Since $a_{b_k} > p$ and $p > 1$, then $a_{b_k} > p > 1$.

By lemma 71, a composite number has a positive divisor between 1 and itself.

Since $p \in \mathbb{Z}^+$ and p divides a_{b_k} and $1 < p < a_{b_k}$, then a_{b_k} is composite.

Hence, a_{b_k} is composite for all $k \in \mathbb{Z}^+$,

Since the sequence (b_k) has infinitely many terms, and a_{b_k} is composite for all $k \in \mathbb{Z}^+$, then there are infinitely many terms of (a_n) that are composite.

Therefore, the sequence (a_n) contains infinitely many composite numbers. □

Proposition 101. *Let $a, m \in \mathbb{Z}^+$.*

There is no arithmetic sequence $a, a + m, a + 2m, a + 3m, ...$ that contains only prime numbers.

Proof. Suppose for the sake of contradiction there is an arithmetic sequence $a, a + m, a + 2m, a + 3m, ...$ that contains only prime numbers.

Then every term of the sequence is a prime number.

In particular, a is a prime number.

By lemma 100, the sequence contains infinitely many composite numbers.

Hence, there is at least one composite number that is a term of the sequence, so there is at least one term of the sequence that is composite.

This contradicts the assumption that every term of the sequence is a prime number.

Therefore, there is no arithmetic sequence $a, a + m, a + 2m, a + 3m, ...$ that contains only prime numbers. □

Congruences

Theorem 102. ***Congruent integers leave the same remainder when divided by*** n***.***

Let n be a fixed positive integer.

Let a and b be any integers.

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 $a - b = n(q_1 - q_2)$ and $q_1 - q_2$ is an integer, 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, when b is divided by n, there exist unique integers q and r such that $b = nq + r$ and $0 \leq r < n$.

Thus, r is the remainder when b is divided by n.

Hence, $a = nk + b = nk + (nq + r) = (nk + nq) + r = n(k + q) + r$.

Since $a = n(k+q)+r$ and $0 \leq r < n$, then by the division algorithm, r must be 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 103. *The congruence modulo relation is an equivalence relation on $\mathbb{Z}$.*

Proof. Let n be a fixed positive integer.

Let a, b, and c be any integers.

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 $\mathbb{Z}$.

By proposition 35, every integer divides zero, so $n|0$.

Hence, $n|a - a$, so $a \equiv a \pmod{n}$.

Therefore, R is reflexive. □

Proof. 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. □

Proof. 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 $a-c = n(k_1+k_2)$ and k_1+k_2 is an integer, then $n|a-c$, 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 $\mathbb{Z}$. □

Proposition 104. *Let n be a fixed positive integer.*
Let a and b be any integers.
If $a = b$, then $a \equiv b \pmod{n}$.

Proof. Suppose $a = b$.

Then $a - b = 0$.

By proposition 35, every integer divides 0, so n divides 0.

Therefore, n divides $a-b$, so $a \equiv b \pmod{n}$. □

Theorem 105. ***arithmetic operations on congruences***
Let n be a fixed positive integer.
Let a, b, c, and d be any integers.
If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then
1. $a + c \equiv b + d \pmod{n}$ (addition of congruences)
2. $a - c \equiv b - d \pmod{n}$ (subtraction of congruences)
3. $ac \equiv bd \pmod{n}$. (multiplication of congruences)

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

$$a - b = nk_1 \tag{2}$$
$$c - d = nk_2 \tag{3}$$

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 106. ***operations that preserve congruences***

Let n be a fixed positive integer.

Let a and b be any integers.

1. Addition preserves congruence.

If $a \equiv b \pmod{n}$, then $a + k \equiv b + k \pmod{n}$ for any integer k.

2. Subtraction preserves congruence.

If $a \equiv b \pmod{n}$, then $a - k \equiv b - k \pmod{n}$ for any integer k.

3. Multiplication preserves congruence.

If $a \equiv b \pmod{n}$, then $ak \equiv bk \pmod{n}$ for any integer k.

4. Exponentiation preserves congruence.

If $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$ for any positive integer k.

Proof. We prove 1.

Suppose $a \equiv b \pmod{n}$.

Then $n|a - b$.

Let k be any integer.

Since $a-b = a+0-b = a+(k-k)-b = (a+k)-k-b = (a+k)-(k+b) = (a+k)-(b+k)$, then $n|(a+k)-(b+k)$.

Therefore, $a + k \equiv b + k \pmod{n}$. □

Proof. We prove 2.

Suppose $a \equiv b \pmod{n}$.

Then $n|a - b$.

Let k be any integer.

Since $a - b = a - b + 0 = a - b + (k - k) = a - b + k - k = a - b - k + k = a - k - b + k = (a - k) - (b - k)$, then $n|(a - k) - (b - k)$.

Therefore, $a - k \equiv b - k \pmod{n}$. □

Proof. We prove 3.

Suppose $a \equiv b \pmod{n}$.

Then $n|a - b$, so n divides any multiple of $a - b$, by theorem 43.

Let k be any integer.

Then $n|k(a - b)$, so $n|(a - b)k$.

Therefore, $n|(ak - bk)$, so $ak \equiv bk \pmod{n}$. □

Proof. We prove 4.

Suppose $a \equiv b \pmod{n}$.

We prove $a^k \equiv b^k \pmod{n}$ for any positive integer k by induction on k.

Let $p(k)$ be the predicate $a^k \equiv b^k \pmod{n}$ defined over the positive integers.

Basis:

Since $a \equiv b \pmod{n}$, then $a^1 \equiv b^1 \pmod{n}$, so $p(1)$ is true.

Induction:

Let k be any positive integer such that $p(k)$ is true.

Then $a^k \equiv b^k \pmod{n}$.

Since $a^k \equiv b^k \pmod{n}$ and $a \equiv b \pmod{n}$, we multiply congruences to obtain $a^k a \equiv b^k b \pmod{n}$.

Hence, $a^{k+1} \equiv b^{k+1} \pmod{n}$.

Thus, $p(k+1)$ is true, so $p(k)$ implies $p(k+1)$ for any positive integer k.

Since $p(1)$ is true, and $p(k)$ implies $p(k+1)$ for any positive integer k, then by induction, $p(k)$ is true for any positive integer k.

Therefore, $a^k \equiv b^k \pmod{n}$ for any positive integer k. □

Theorem 107. ***cancellation laws for congruences***

Let n be a fixed positive integer.

Let a, b, and k be any integers.

1. Addition cancellation law

If $a + k \equiv b + k \pmod{n}$, then $a \equiv b \pmod{n}$.

2. Multiplication cancellation law

If $ak \equiv bk \pmod{n}$, then $a \equiv b \pmod{\frac{n}{\gcd(n,k)}}$.

Proof. We prove 1.

Suppose $a + k \equiv b + k \pmod{n}$.

Then n divides $(a + k) - (b + k)$.

Observe that

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

Hence, $(a + k) - (b + k) = a - b$, so n divides $a - b$.

Therefore, $a \equiv b \pmod{n}$. □

Proof. We prove 2.

Suppose $ak \equiv bk \pmod{n}$.

Then n divides $ak - bk$, so $ak - bk = nm$ for some integer m.

Thus, $nm = (a - b)k = k(a - b)$.

Let $d = \gcd(n, k)$.

Since $\gcd(n, k) = d$, then $\gcd(\frac{n}{d}, \frac{k}{d}) = 1$, by corollary 57 and $\frac{n}{d}$ and $\frac{k}{d}$ are integers.

Since $\frac{n}{d}$ and m are integers, then $\frac{n}{d} \cdot m$ is an integer.

Since $\frac{k}{d} \cdot (a - b) = \frac{k(a-b)}{d} = \frac{nm}{d} = \frac{n}{d} \cdot m$, then $\frac{n}{d}$ divides $\frac{k}{d} \cdot (a - b)$.

Since $\frac{n}{d}$ divides $\frac{k}{d} \cdot (a - b)$ and $\gcd(\frac{n}{d}, \frac{k}{d}) = 1$, then $\frac{n}{d}$ divides $a - b$, by theorem 58.

Therefore, $a \equiv b \pmod{\frac{n}{d}}$. □

Corollary 108. ***cancellation multiplication relatively prime***

Let n be a fixed positive integer.

Let a, b, and k be any integers.

If $ak \equiv bk \pmod{n}$ and $\gcd(n, k) = 1$, then $a \equiv b \pmod{n}$.

Proof. Suppose $ak \equiv bk \pmod{n}$ and $\gcd(n,k) = 1$.
Since $ak \equiv bk \pmod{n}$, then $n|ak - bk$, so $n|(a-b)k$.
Thus, $n|k(a-b)$.
Since $n|k(a-b)$ and $\gcd(n,k) = 1$, then $n|a-b$, by theorem 58.
Therefore, $a \equiv b \pmod{n}$. □

Proof. Suppose $ak \equiv bk \pmod{n}$ and $\gcd(n,k) = 1$.
By theorem 107 part 2, if $ak \equiv bk \pmod{n}$ and $\gcd(n,k) = 1$, then $a \equiv b \pmod{\frac{n}{1}}$.
Therefore, if $ak \equiv bk \pmod{n}$ and $\gcd(n,k) = 1$, then $a \equiv b \pmod{n}$. □

Lemma 109. *Let p be a positive integer.*
Let a be any integer.
If p is prime and $p \nmid a$, then $\gcd(p,a) = 1$.

Proof. Suppose p is prime and $p \nmid a$.
Let $d = \gcd(p,a)$.
Then d is a positive integer and $d|p$ and $d|a$.
Since p is prime, then the only positive divisors of p are 1 and p.
Since d is a positive integer and $d|p$, then this implies either $d = 1$ or $d = p$.

Suppose $d = p$.
Since $d = p$ and $d|a$, then $p|a$.
But, this contradicts the hypothesis $p \nmid a$.
Therefore, $d \neq p$.

Since either $d = 1$ or $d = p$, and $d \neq p$, then $d = 1$, so $\gcd(p,a) = 1$. □

Corollary 110. ***cancellation multiplication prime modulus***
Let p be a positive integer.
Let $a, b,$ and k be any integers.
If $ak \equiv bk \pmod{p}$ and p is prime and $p \nmid k$, then $a \equiv b \pmod{p}$.

Proof. Suppose $ak \equiv bk \pmod{p}$ and p is prime and $p \nmid k$.
Since p is prime and $p \nmid k$, then $\gcd(p,k) = 1$, by lemma 109.

Since $ak \equiv bk \pmod{p}$ and $\gcd(p,k) = 1$, then $a \equiv b \pmod{p}$, by corollary 108. □

Proposition 111. *Let k and n be positive integers.*
Let a and b be any integers.
Then $ak \equiv bk \pmod{nk}$ iff $a \equiv b \pmod{n}$.

Proof. Since n and k are positive integers, then nk is a positive integer.
Suppose $ak \equiv bk \pmod{nk}$.
Then $nk|(ak - bk)$, so $nk|(a-b)k$.
Hence, $kn|k(a-b)$.
Since k is positive, then $k > 0$, so $k \neq 0$.

Since $k \neq 0$ and $kn|k(a-b)$, then $n|(a-b)$, by proposition 44.
Therefore, $a \equiv b \pmod{n}$. □

Proof. Conversely, suppose $a \equiv b \pmod{n}$.
Then $n|(a-b)$, so $kn|k(a-b)$, by proposition 44.
Hence, $nk|(a-b)k$, so $nk|ak-bk$.
Therefore, $ak \equiv bk \pmod{nk}$. □

Proposition 112. *Let n be a fixed positive integer.*
Let a and b be any integers.
If $ab \equiv 0 \pmod{n}$ and $\gcd(n,a) = 1$, then $b \equiv 0 \pmod{n}$.

Proof. Suppose $ab \equiv 0 \pmod{n}$ and $\gcd(n,a) = 1$.
Since $ab \equiv 0 \pmod{n}$, then n divides $ab - 0$, so n divides ab.
Since n divides ab and $\gcd(n,a) = 1$, then n divides b, by theorem 58.
Therefore, n divides $b - 0$, so $b \equiv 0 \pmod{n}$. □

Proof. Suppose $ab \equiv 0 \pmod{n}$ and $\gcd(n,a) = 1$.
Since $a \cdot 0 = 0$, then $a \cdot 0 \equiv 0 \pmod{n}$, by proposition 104.
By theorem 103, congruence modulo is symmetric.
Hence, $a \cdot 0 \equiv 0 \pmod{n}$ implies $0 \equiv a \cdot 0 \pmod{n}$.
By theorem 103, congruence modulo is transitive.
Hence, $ab \equiv 0 \pmod{n}$ and $0 \equiv a \cdot 0 \pmod{n}$ implies $ab \equiv a \cdot 0 \pmod{n}$.
Since $ab \equiv a \cdot 0 \pmod{n}$ and $\gcd(n,a) = 1$, then $b \equiv 0 \pmod{n}$, by corollary 108. □

Proposition 113. *Let p be a positive integer.*
Let a and b be any integers.
If $ab \equiv 0 \pmod{p}$ and p is prime, then $a \equiv 0 \pmod{p}$ or $b \equiv 0 \pmod{p}$.

Proof. Suppose $ab \equiv 0 \pmod{p}$ and p is prime.
Since $ab \equiv 0 \pmod{p}$, then $p|ab$.
Since p is prime and $p|ab$, then $p|a$ or $p|b$, by Euclid's lemma 74.
Therefore, $p|(a-0)$ or $p|(b-0)$, so $a \equiv 0 \pmod{p}$ or $b \equiv 0 \pmod{p}$. □

Proof. Suppose $ab \equiv 0 \pmod{p}$ and p is prime and $a \not\equiv 0 \pmod{p}$.
Since $a \not\equiv 0 \pmod{p}$, then $p \not| a$.
Since p is prime and $p \not| a$, then $\gcd(p,a) = 1$, by lemma 109.
Since $ab \equiv 0 \pmod{p}$ and $\gcd(p,a) = 1$, then $b \equiv 0 \pmod{p}$, by proposition 112.

□

Proof. Suppose $ab \equiv 0 \pmod{p}$ and p is prime and $a \not\equiv 0 \pmod{p}$.
Since $a \not\equiv 0 \pmod{p}$, then $p \not| a$.

Since $a \cdot 0 = 0$, then $a \cdot 0 \equiv 0 \pmod{p}$, by proposition 104.
By theorem 103, congruence modulo is symmetric.
Hence, $a \cdot 0 \equiv 0 \pmod{p}$ implies $0 \equiv a \cdot 0 \pmod{p}$.
By theorem 103, congruence modulo is transitive.
Hence, $ab \equiv 0 \pmod{p}$ and $0 \equiv a \cdot 0 \pmod{p}$ implies $ab \equiv a \cdot 0 \pmod{p}$.

Since $ab \equiv a \cdot 0 \pmod{p}$ and p is prime and $p \nmid a$, then $b \equiv 0 \pmod{p}$, by corollary 110. □

Linear Congruences

Proposition 114. *Let $n \in \mathbb{Z}^+$.*
Let $a, b, x, x_0 \in \mathbb{Z}$.
If x_0 is a solution to $ax \equiv b \pmod{n}$, then so is $x_0 + nk$ for any integer k.

Proof. Suppose x_0 is a solution to $ax \equiv b \pmod{n}$.
Then $ax_0 \equiv b \pmod{n}$.
Let k be an arbitrary integer.
Since $a \in \mathbb{Z}$ and $k \in \mathbb{Z}$, then $ak \in \mathbb{Z}$.
By proposition 37, every integer divides itself.
Since $n \in \mathbb{Z}$, then $n|n$.
Hence, n divides any multiple of n, so $n|(ak)n$.
Since

$$\begin{aligned} n|(ak)n &\Leftrightarrow n|akn \\ &\Leftrightarrow n|ank \\ &\Leftrightarrow n|ank - 0 \\ &\Leftrightarrow ank \equiv 0 \pmod{n}, \end{aligned}$$

then we conclude $ank \equiv 0 \pmod{n}$.
Since $ax_0 \equiv b \pmod{n}$ and $ank \equiv 0 \pmod{n}$, then we add congruences to obtain $ax_0 + ank \equiv b + 0 \pmod{n}$.
Therefore, $a(x_0 + nk) \equiv b \pmod{n}$. □

Proof. Suppose x_0 is a solution to $ax \equiv b \pmod{n}$.
Then $ax_0 \equiv b \pmod{n}$.
Let k be an arbitrary integer.
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 115. ***Existence and uniqueness of multiplicative inverse of*** a ***modulo*** n

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

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

Then there exists a unique integer b *such that* $ab \equiv 1 \pmod{n}$ *and* $0 < b < n$ *if and only if* $\gcd(a, n) = 1$.

Proof. We prove if $\gcd(a, n) = 1$, then there exists a unique integer b such that $ab \equiv 1 \pmod{n}$ and $0 < b < n$.

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 s and t such that $sa + tn = 1$.

Thus, $as - 1 = sa - 1 = -tn = (-t)n = n(-t)$.

Since $-t \in \mathbb{Z}$ and $as - 1 = n(-t)$, then $n|(as - 1)$, so $as \equiv 1 \pmod{n}$.

By the division algorithm, when s is divided by n, there exist unique integers q and b such that $s = nq + b$ and $0 \leq b < n$.

Since $s = nq + b$, then $s - b = nq$, so n divides $s - b$.

Hence, $s \equiv b \pmod{n}$, so $b \equiv s \pmod{n}$.

Since $a \equiv a \pmod{n}$ and $b \equiv s \pmod{n}$, then we multiply congruences to obtain $ab \equiv as \pmod{n}$.

Since $ab \equiv as \pmod{n}$ and $as \equiv 1 \pmod{n}$, then $ab \equiv 1 \pmod{n}$, so $1 \equiv ab \pmod{n}$.

Since $0 \leq b < n$, then $0 \leq b$ and $b < n$.

Since $0 \leq b$, then $b \geq 0$, so either $b > 0$ or $b = 0$.

Suppose $b = 0$.

Then $1 \equiv ab \pmod{n}$ implies $1 \equiv a(0) \pmod{n}$.

Hence, $1 \equiv 0 \pmod{n}$, so n divides $1 - 0 = 1$.

By lemma 54, the only positive integer that divides 1 is 1.

Since $n \in \mathbb{Z}^+$ and $n|1$, then we must conclude $n = 1$.

But, $n > 1$ by hypothesis, so $n \neq 1$.

Therefore, $b \neq 0$.

Since either $b > 0$ or $b = 0$ and $b \neq 0$, then $b > 0$.

Thus, $0 < b$ and $b < n$, so $0 < b < n$.

Therefore, there exists a unique integer b such that $ab \equiv 1 \pmod{n}$ and $0 < b < n$, as desired. □

Proof. Conversely, we prove if there exists a unique integer b such that $ab \equiv 1 \pmod{n}$ and $0 < b < n$, then $\gcd(a, n) = 1$.

Suppose there exists an integer b such that $ab \equiv 1 \pmod{n}$ and $0 < b < n$.

Since $ab \equiv 1 \pmod{n}$, then n divides $ab - 1$, so $ab - 1 = nk$ for some integer k.

Thus, $1 = ab - nk = ab + (-nk) = ab + n(-k) = ba + (-k)n$ is a linear combination of a and n.

By corollary 56, $\gcd(a, n) = 1$ if and only if 1 is a linear combination of a and n.

Therefore, we conclude $\gcd(a, n) = 1$. □

Proposition 116. *Let $n \in \mathbb{Z}^+$.*

Every integer is congruent to exactly one of the remainders $0, 1, ..., n-1$ when divided by n.

Proof. Let $a \in \mathbb{Z}$.

By the division algorithm, there exist unique integers q and r such that $a = nq + r$ with $0 \leq r < n$ when a is divided by n.

Since $a = nq + r$, then $a - r = nq$, so n divides $a - r$.

Hence, $a \equiv r \pmod{n}$.

Since $r \in \mathbb{Z}$ and $0 \leq r < n$, then either $r = 0$ or $r = 1$ or ... or $r = n - 1$.

Thus, either $r \in \{0\}$ or $r \in \{1\}$ or ... or $r \in \{n-1\}$, so r is an element of the union $\{0\} \cup \{1\} \cup ... \cup \{n-1\}$.

Hence, $r \in \{0, 1, ..., n-1\}$.

Therefore, r is a unique integer such that $a \equiv r \pmod{n}$ and $r \in \{0, 1, ..., n-1\}$. □

Proposition 117. *Let $n \in \mathbb{Z}^+$.*

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

No pair of distinct integers in the set $\{0, 1, ..., n-1\}$ are congruent to each other modulo n.

Proof. Let $S = \{0, 1, ..., n-1\}$.

We must prove there is no pair of distinct integers in the set S that are congruent to each other.

The statement is: there are no distinct integers $a \in S$ and $b \in S$ such that $a \equiv b \pmod{n}$.

Suppose for the sake of contradiction there are distinct integers $a \in S$ and $b \in S$ such that $a \equiv b \pmod{n}$.

Since a and b are distinct integers, then $a \neq b$.

Since $a \in S$, then $a \leq n - 1$.

Since $b \in S$, then $b \geq 0$, so $0 \leq b$.

Since a and b are integers and $a \neq b$, then either $a < b$ or $a > b$.

Without loss of generality, assume $a > b$.

Since $a > b$, then $a - b > 0$.

Since a and b are integers and $a - b > 0$, then $a - b$ is a positive integer.

Since $n \in \mathbb{Z}^+$ and $a - b \in \mathbb{Z}^+$, then n divides $a - b$ implies $n \leq a - b$, so $n > a - b$ implies n does not divide $a - b$.

Since $a \leq n-1$ and $n-1 < n$, then $a < n$, so $a - b < n - b$.

Since $0 \leq b$ and $0 \leq b \Leftrightarrow n \leq n + b \Leftrightarrow n - b \leq n$, then $n - b \leq n$.

Since $a - b < n - b$ and $n - b \leq n$, then $a - b < n$, so $n > a - b$.

Since $n > a - b$ and $n > a - b$ implies n does not divide $a - b$, then we conclude n does not divide $a - b$.

Since n divides $a - b$ iff $a \equiv b \pmod{n}$, then n does not divide $a - b$ iff $a \not\equiv b \pmod{n}$.

Since n does not divide $a - b$, then we conclude $a \not\equiv b \pmod{n}$.

Thus, we have $a \equiv b \pmod{n}$ and $a \not\equiv b \pmod{n}$, a contradiction.

Therefore, there are no distinct integers $a \in S$ and $b \in S$ such that $a \equiv b \pmod{n}$, so no pair of distinct integers in S are congruent to each other modulo n. □

Theorem 118. ***Existence of solution to linear congruence***

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

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

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 $\frac{n}{d}$.

Proof. 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, $ax_0 - b = nk$ for some integer k.

Thus, $b = ax_0 - nk = ax_0 + (-nk) = ax_0 + n(-k)$.

Since $x_0, -k \in \mathbb{Z}$ and $b = ax_0 + n(-k)$, then b is a linear combination of a and n.

By theorem 55, b is a multiple of $\gcd(a, n)$ if and only if b is a linear combination of a and n.

Therefore, we conclude b is a multiple of $\gcd(a, n)$, so $\gcd(a, n)|b$, as desired. □

Proof. Conversely, suppose $\gcd(a, n)|b$.

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

Then $d|b$, so $b = dk$ for some integer k.

Since d is the least positive linear combination of a and n, then there exist integers r and s such that $ra + sn = d$.

Thus, $b = dk = (ra + sn)k = rak + snk$, so $-snk = rak - b$.

Let $x_0 = rk$.

Then $x_0 \in \mathbb{Z}$ and $n(-sk) = -nsk = -snk = rak - b = ark - b = ax_0 - b$.

Since $-sk \in \mathbb{Z}$ and $n(-sk) = ax_0 - b$, then $n|(ax_0 - b)$, so $ax_0 \equiv b \pmod{n}$.

Therefore, there exists $x_0 \in \mathbb{Z}$ such that $ax_0 \equiv b \pmod{n}$, so a solution to the congruence exists, as desired. □

Proof. We prove if a solution exists to the linear congruence, then there are d distinct solutions modulo n and these solutions are congruent modulo $\frac{n}{d}$.

Suppose a solution exists to the linear congruence $ax \equiv b \pmod{n}$.

Then there exists $c \in \mathbb{Z}$ such that $ac \equiv b \pmod{n}$ and $\gcd(a, n)|b$.

By proposition 116, every integer is congruent to exactly one of the remainders $0, 1, ..., n-1$ when divided by n, so c is congruent to exactly one of the remainders $0, 1, ..., n-1$ when divided by n.

Thus, there exists a unique $x_0 \in \{0, 1, ..., n-1\}$ such that $c \equiv x_0 \pmod{n}$.

Since $c \equiv x_0 \pmod{n}$, then $ac \equiv ax_0 \pmod{n}$, so $ax_0 \equiv ac \pmod{n}$.

Since $ax_0 \equiv ac \pmod{n}$ and $ac \equiv b \pmod{n}$, then $ax_0 \equiv b \pmod{n}$.

Therefore, $x_0 \in \{0, 1, ..., n-1\}$ is a particular solution of the congruence $ax \equiv b \pmod{n}$.

Let S be the solution set of the congruence $ax \equiv b \pmod{n}$.

Then $S = \{x \in \mathbb{Z} : ax \equiv b \pmod{n}\}$.

Let $T = \{x_0 + \frac{n}{d} \cdot k, k \in \mathbb{Z}\}$.

We prove $S = T$.

Since $d = \gcd(a, n)$, then $d|a$ and $d|n$, so $\frac{a}{d}$ and $\frac{n}{d} \in \mathbb{Z}$.

We first prove $T \subset S$.

Let $t \in T$.

Then $t = x_0 + \frac{n}{d} \cdot k$ for some integer k.

Since $x_0 \in \mathbb{Z}$ and $\frac{n}{d} \in \mathbb{Z}$ and $k \in \mathbb{Z}$ and $\mathbb{Z}$ is closed under addition and multiplication, then $t \in \mathbb{Z}$.

Since $\frac{a}{d} \in \mathbb{Z}$ and $k \in \mathbb{Z}$, then $\frac{a}{d} \cdot k \in \mathbb{Z}$.

By proposition 37, every integer divides itself.

Since $n \in \mathbb{Z}$, then $n|n$.

By theorem 43, if $n|n$, then n divides any multiple of n.

Thus, n divides any multiple of n, so n divides $(\frac{a}{d} \cdot k)n = \frac{akn}{d} = \frac{ank}{d} = a \cdot \frac{n}{d} \cdot k = a \cdot \frac{n}{d} \cdot k - 0$.

Hence, $a \cdot \frac{n}{d} \cdot k \equiv 0 \pmod{n}$.

Since $ax_0 \equiv b \pmod{n}$ and $a \cdot \frac{n}{d} \cdot k \equiv 0 \pmod{n}$, then we add the congruences to obtain $ax_0 + a \cdot \frac{n}{d} \cdot k \equiv b + 0 \pmod{n}$.

Hence, $a(x_0 + \frac{n}{d} \cdot k) \equiv b \pmod{n}$, so $at \equiv b \pmod{n}$.

Since $t \in \mathbb{Z}$ and $at \equiv b \pmod{n}$, then $t \in S$.

Since $t \in T$ implies $t \in S$, then $T \subset S$.

We next prove $S \subset T$.

Let $s \in S$.

Then $s \in \mathbb{Z}$ and $as \equiv b \pmod{n}$.

Since $as \equiv b \pmod{n}$, then $b \equiv as \pmod{n}$.

Since $ax_0 \equiv b \pmod{n}$ and $b \equiv as \pmod{n}$, then $ax_0 \equiv as \pmod{n}$.

Since $ax_0 \equiv as \pmod{n}$ and $d = \gcd(a, n)$, then by theorem 107, we have $x_0 \equiv s \pmod{\frac{n}{d}}$.

Thus, $\frac{n}{d}$ divides $x_0 - s$, so $x_0 - s = \frac{n}{d} \cdot k$ for some integer k.

Hence, $s = x_0 - \frac{n}{d} \cdot k = x_0 + \frac{n}{d}(-k)$.

Since $-k \in \mathbb{Z}$ and $s = x_0 + \frac{n}{d}(-k)$, then $s \in T$.

Therefore, $s \in S$ implies $s \in T$, so $S \subset T$.

Since $S \subset T$ and $T \subset S$, then $S = T$, as desired.

Therefore, the solution set of the congruence $ax \equiv b \pmod{n}$ with particular solution $x_0 \in \{0, 1, ..., n-1\}$ is the set $\{x_0 + \frac{n}{d} \cdot k, k \in \mathbb{Z}\}$, where $d = \gcd(a, n)$. $\square$

Proof. We prove there are d distinct solutions modulo n and these solutions are congruent modulo $\frac{n}{d}$.

Let x' and x'' be arbitrary distinct solutions of the congruence $ax \equiv b \pmod{n}$.

Then $x' = x_0 + \frac{n}{d}k_1$ for some integer k_1 and $x'' = x_0 + \frac{n}{d}k_2$ for some integer k_2 and $k_1 \neq k_2$.

Suppose $x' \equiv x'' \pmod{n}$.

Then $x_0 + \frac{n}{d}k_1 \equiv x_0 + \frac{n}{d}k_2 \pmod{n}$, so $\frac{n}{d}k_1 \equiv \frac{n}{d}k_2 \pmod{n}$, by theorem 107.

Thus, by theorem 107, we have $k_1 \equiv k_2 \pmod{\frac{n}{\gcd(n, \frac{n}{d})}}$.

Let $g = \frac{n}{\gcd(n, \frac{n}{d})}$.

Then $k_1 \equiv k_2 \pmod{g}$.

Since $d|n$, then $n = dm$ for some integer m.

Thus, $m = \frac{n}{d}$.

Since $d \in \mathbb{Z}^+$ and $n \in \mathbb{Z}^+$, then $m \in \mathbb{Z}^+$.

Hence, $g = \frac{n}{\gcd(n,m)} = \frac{n}{\gcd(dm,m)} = \frac{n}{m \cdot \gcd(d,1)} = \frac{n}{m \cdot 1} = \frac{n}{m} = \frac{n}{\frac{n}{d}} = d$.

Thus, $k_1 \equiv k_2 \pmod{d}$.

Therefore, if $x' \equiv x'' \pmod{n}$, then $k_1 \equiv k_2 \pmod{d}$.

Conversely, suppose $k_1 \equiv k_2 \pmod{d}$.

Then $d|k_1 - k_2$, so $k_1 - k_2 = d\alpha$ for some $\alpha \in \mathbb{Z}$.

Thus, $k_1 = k_2 + d\alpha$.

Hence, $\frac{n}{d}k_1 = \frac{n}{d}k_2 + n\alpha$, so $x_0 + \frac{n}{d}k_1 = x_0 + \frac{n}{d}k_2 + \alpha n$.

Consequently, $x' = x'' + \alpha n$, so $x' - x'' = \alpha n$.

Thus, n divides $x' - x''$, so $x' \equiv x'' \pmod{n}$.

Therefore, if $k_1 \equiv k_2 \pmod{d}$, then $x' \equiv x'' \pmod{n}$.

Since $x' \equiv x'' \pmod{n}$ implies $k_1 \equiv k_2 \pmod{d}$ and $k_1 \equiv k_2 \pmod{d}$ implies $x' \equiv x'' \pmod{n}$, then $x' \equiv x'' \pmod{n}$ if and only if $k_1 \equiv k_2 \pmod{d}$.

Therefore, $x' \not\equiv x'' \pmod{n}$ if and only if $k_1 \not\equiv k_2 \pmod{d}$.

No pair of distinct integers in the set $\{0, 1, ..., d-1\}$ are congruent to each other modulo d, by proposition 117.

Thus, there is no pair $k_1, k_2 \in \{0, 1, ..., d-1\}$ with $k_1 \neq k_2$ such that $k_1 \equiv k_2 \pmod{d}$.

Hence, $k_1 \not\equiv k_2 \pmod{d}$ for every $k_1, k_2 \in \{0, 1, ..., d-1\}$ with $k_1 \neq k_2$.

Let k_1 and k_2 be distinct integers in the set $\{0, 1, ..., d-1\}$.

Then $k_1 \in \{0, 1, ..., d-1\}$ and $k_2 \in \{0, 1, ..., d-1\}$ and $k_1 \neq k_2$, so $k_1 \not\equiv k_2 \pmod{d}$.

Since $x' \not\equiv x'' \pmod{n}$ if and only if $k_1 \not\equiv k_2 \pmod{d}$, then we conclude $x' \not\equiv x'' \pmod{n}$.

Therefore, if k_1 and k_2 are distinct integers in the set $\{0, 1, ..., d-1\}$, then $x' \not\equiv x'' \pmod{n}$ for any distinct $x', x'' \in T$.

Let $k \in \{0, 1, ..., d-1\}$.

Then there are d solutions that are not congruent modulo n.

The solutions are $x_0, x_0 + \frac{n}{d}, x_0 + 2\frac{n}{d}, ..., x_0 + (d-1)\frac{n}{d}$.

Therefore, there are d distinct solutions modulo n.

The set of solutions modulo n is $\{x_0, x_0 + \frac{n}{d}, x_0 + 2\frac{n}{d}, ..., x_0 + (d-1)\frac{n}{d}\}$. □

Proof. We prove the solutions are congruent modulo $\frac{n}{d}$.

Let k_1, k_2 be distinct integers in the set $\{0, 1, ..., d-1\}$.

Then $x' = x_0 + \frac{n}{d}k_1$ and $x'' = x_0 + \frac{n}{d}k_2$ are distinct solutions of the congruence $ax \equiv b \pmod{n}$.

We must prove $x' \equiv x'' \pmod{\frac{n}{d}}$.

Since every integer divides itself and $\frac{n}{d} \in \mathbb{Z}$, then $\frac{n}{d}$ divides $\frac{n}{d}$.

Hence, $\frac{n}{d}$ divides any multiple of $\frac{n}{d}$, so $\frac{n}{d}$ divides $(k_1 - k_2)\frac{n}{d}$.

Observe that

$$\begin{aligned}
(k_1 - k_2)\frac{n}{d} = \quad & \tfrac{n}{d}(k_1 - k_2) \\
= \quad & \frac{n}{d}k_1 - \frac{n}{d}k_2 \\
= \quad & x_0 + \frac{n}{d}k_1 - x_0 - \frac{n}{d}k_2 \\
= \quad & (x_0 + \frac{n}{d}k_1) - (x_0 + \frac{n}{d}k_2) \\
= \quad & x' - x''.
\end{aligned}$$

Since $\frac{n}{d}$ divides $(k_1 - k_2)\frac{n}{d}$ and $(k_1 - k_2)\frac{n}{d} = x' - x''$, then $\frac{n}{d}$ divides $x' - x''$, so $x' \equiv x'' \pmod{\frac{n}{d}}$.

Since x and x' are arbitrary, then each of the d solutions is congruent modulo $\frac{n}{d}$. □

Integers Modulo n

Theorem 119. *Let $n \in \mathbb{Z}^+$.*

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

Let r be the remainder when a is divided by n.

Then $[a] = [r]$ and there are exactly n distinct congruence classes $[0], [1], ..., [n-1]$.

Proof. We prove $[a] = [r]$.

By proposition 116, every integer is congruent to a unique integer in the set $\{0, 1, ..., n-1\}$ when divided by n.

Since $n \in \mathbb{Z}^+$ and $a \in \mathbb{Z}$, then a is congruent to a unique integer in the set $\{0, 1, ..., n-1\}$ when divided by n.

Therefore, there is a unique integer $r \in \{0, 1, ..., n-1\}$ such that $a \equiv r \pmod{n}$.

Since $a \equiv r \pmod{n}$, then $[a] = [r]$. □

Proof. To prove there are exactly n distinct congruence classes $[0], [1], ..., [n-1]$, we first prove the congruence classes $[0], [1], ..., [n-1]$ are all distinct.

Let $S = \{0, 1, ..., n-1\}$.

To prove the congruence classes $[0], [1], ..., [n-1]$ are all distinct, we must prove $[x] \neq [y]$ for every $x, y \in S$ with $x \neq y$.

Let $x, y \in S$ with $x \neq y$.

Since $x \in S$ and $y \in S$ and $x \neq y$, then x and y are a pair of distinct integers in the set S.

By proposition 117, we know that no pair of distinct integers in the set S are congruent to each other.

Hence, x cannot be congruent to y modulo n, so $x \not\equiv y \pmod{n}$.

Therefore, $[x] \neq [y]$.

Consequently, $[x] \neq [y]$ for all $x, y \in S$ with $x \neq y$, so the congruence classes $[0], [1], ..., [n-1]$ are all distinct.

Since there are n such classes, then there are n distinct congruence classes $[0], [1], ..., [n-1]$. □

Proposition 120. *Let $n \in \mathbb{Z}^+$.*
Then $[n] = [0]$.

Proof. Since every integer divides itself, then $n|n$.

Since $n|n$ and $n = n - 0$, then n divides $n - 0$, so $n \equiv 0 \pmod{n}$.

Therefore, $[n] = [0]$. □

Proposition 121. *Let $n \in \mathbb{Z}^+$.*
Then $[-a] = [n - a]$ for all $[a] \in \mathbb{Z}_n$.

Proof. Let $[a] \in \mathbb{Z}_n$.

Then $a \in \mathbb{Z}$, so $-a \in \mathbb{Z}$.

Thus, $[-a] \in \mathbb{Z}_n$.

Since $n \in \mathbb{Z}$ and $a \in \mathbb{Z}$, then $n - a \in \mathbb{Z}$, so $[n - a] \in \mathbb{Z}_n$.

Since n divides $-n = 0 - n = (-a + a) - n = -a + (a - n) = -a - (-a + n) = -a - (n - a)$, then n divides $-a - (n - a)$, so $-a \equiv (n - a) \pmod{n}$.

Therefore, $[-a] = [n - a]$. □

Theorem 122. *Let $n \in \mathbb{Z}^+$.*
Then $\mathbb{Z}_n = \frac{\mathbb{Z}}{n\mathbb{Z}} = \{[0], [1], ..., [n-1]\}$ and $|\mathbb{Z}_n| = n$.

Proof. Since $n \in \mathbb{Z}^+$, then there are exactly n distinct congruence classes $[0], [1], ..., [n-1]$.

Let $S = \{[0], [1], ..., [n-1]\}$.

Observe that $\mathbb{Z}_n = \{[a] : a \in \mathbb{Z}\}$.

We must prove $\mathbb{Z}_n = S$.

We prove $S \subset \mathbb{Z}_n$.

Let $s \in S$.

Then $s = [x]$ for some $x \in \{0, 1, ..., n-1\}$.

Since $x \in \{0, 1, ..., n-1\}$ and $\{0, 1, ..., n-1\} \subset \mathbb{Z}$, then $x \in \mathbb{Z}$.

Since $x \in \mathbb{Z}$ and $s = [x]$, then $s \in \mathbb{Z}_n$.

Hence, $s \in S$ implies $s \in \mathbb{Z}_n$, so $S \subset \mathbb{Z}_n$.

We prove $\mathbb{Z}_n \subset S$.

Let $t \in \mathbb{Z}_n$.

Then $t = [a]$ for some $a \in \mathbb{Z}$.

By the division algorithm, there exist unique integers q, r such that $a = nq + r$ with $0 \leq r < n$.

Since $a = nq + r$, then $a - r = nq$, so $n|a - r$.

Hence, $a \equiv r \pmod{n}$, so $[a] = [r]$.

Since $t = [a]$ and $[a] = [r]$, then $t = [r]$.

Since r is an integer and $0 \leq r < n$, then either $r = 0$ or $r = 1$ or ... or $r = n - 1$.

Hence, either $[r] = [0]$ or $[r] = [1]$ or ... or $[r] = [n-1]$.

Thus, $[r]$ is one of the congruence classes $[0], [1], ..., [n-1]$.

Since $t = [r]$, then t is one of the congruence classess $[0], [1], ..., [n-1]$.

Thus, $t \in S$.

Since $t \in \mathbb{Z}_n$ implies $t \in S$, then $\mathbb{Z}_n \subset S$.

Since $\mathbb{Z}_n \subset S$ and $S \subset \mathbb{Z}_n$, then $\mathbb{Z}_n = S$, as desired.

Since $\mathbb{Z}_n = S = \{[0], [1], ..., [n-1]\}$ and the set { [0], [1], ..., [n-1] } contains exactly n elements, then the set $\mathbb{Z}_n$ contains exactly n elements, so $|\mathbb{Z}_n| = n$. □

Lemma 123. ***Addition modulo*** n ***is well-defined.***

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

Let $[a], [b] \in \mathbb{Z}_n$.

Let $x, x' \in [a]$ *and* $y, y' \in [b]$.

Then $[x + y] = [x' + y']$.

Solution. We must prove the result does not depend on the choice of a particular representative of the equivalence class. □

Proof. Since $[a], [b] \in \mathbb{Z}_n$, then $a, b \in \mathbb{Z}$.

Suppose $x, x' \in [a]$ and $y, y' \in [b]$.

Then $[a] = \{x \in \mathbb{Z} : x \equiv a \pmod{n}\}$ and $[b] = \{x \in \mathbb{Z} : x \equiv b \pmod{n}\}$.

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 $x + y \equiv (x' + y') \pmod{n}$.

Therefore, $[x + y] = [x' + y']$. □

Theorem 124. ***Addition modulo*** n ***is a binary operation.***

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

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 $b \equiv b' \pmod{n}$.

Since $a \equiv a' \pmod{n}$, then $a, a' \in [a]$.

Since $b \equiv b' \pmod{n}$, then $b, b' \in [b]$.

Therefore, we must prove the result does not depend on the choice of a particular representative of the equivalence class. □

Proof. Let $[a], [b] \in \mathbb{Z}_n$.

Then a and b are integers.

Thus, $a + b$ is an integer, so $[a + b] \in \mathbb{Z}_n$.

Since $[a + b] = [a] + [b]$, then $[a] + [b] \in \mathbb{Z}_n$.

Therefore, $\mathbb{Z}_n$ is closed under addition modulo n.

Addition modulo n is well defined, by lemma 123.

Since $\mathbb{Z}_n$ is closed under addition modulo n and addition modulo n is well defined, then addition modulo n is a binary operation on $\mathbb{Z}_n$. □

Theorem 125. ***algebraic properties of addition modulo*** n
Let $n \in \mathbb{Z}^+$.
1. Addition is associative.
$([a] + [b]) + [c] = [a] + ([b] + [c])$ *for all* $[a], [b], [c] \in \mathbb{Z}_n$.
2. Addition is commutative.
$[a] + [b] = [b] + [a]$ *for all* $[a], [b] \in \mathbb{Z}_n$.
3. Additive identity is $[0]$.
There exists $[0] \in \mathbb{Z}_n$ *such that* $[a] + [0] = [0] + [a] = [a]$ *for all* $[a] \in \mathbb{Z}_n$.
4. Each element has an additive inverse.
For every $[a] \in \mathbb{Z}_n$, *there exists* $[-a] \in \mathbb{Z}_n$ *such that* $[a] + [-a] = [-a] + [a] = [0]$.

Proof. We prove 1.
Let $[a], [b], [c] \in \mathbb{Z}_n$.
Then $([a]+[b])+[c] = [a+b]+[c] = [(a+b)+c] = [a+(b+c)] = [a]+[b+c] = [a] + ([b] + [c])$. □

Proof. We prove 2.
Let $[a], [b] \in \mathbb{Z}_n$.
Then $[a] + [b] = [a + b] = [b + a] = [b] + [a]$. □

Proof. We prove 3.
Since $0 \in \mathbb{Z}$, then $[0] \in \mathbb{Z}_n$.
Let $[a] \in \mathbb{Z}_n$.
Then $[a] + [0] = [a + 0] = [a] = [0 + a] = [0] + [a]$.
Therefore, there exists $[0] \in \mathbb{Z}_n$ such that $[a] + [0] = [a] = [0] + [a]$ for all $[a] \in \mathbb{Z}_n$. □

Proof. We prove 4.
Let $[a] \in \mathbb{Z}_n$.
Then $a \in \mathbb{Z}$, so $-a \in \mathbb{Z}$.
Thus, $[-a] \in \mathbb{Z}_n$.
Observe that $[a] + [-a] = [a + (-a)] = [0] = [-a + a] = [-a] + [a]$.
Therefore, for every $[a] \in \mathbb{Z}_n$ there exists $[-a] \in \mathbb{Z}_n$ such that $[a] + [-a] = [0] = [-a] + [a]$. □

Lemma 126. ***Multiplication modulo*** n ***is well-defined.***
Let $n \in \mathbb{Z}^+$.
Let $[a], [b] \in \mathbb{Z}_n$.
Let $x, x' \in [a]$ *and* $y, y' \in [b]$.
Then $[xy] = [x'y']$.

Solution. We must prove the result does not depend on the choice of a particular representative of the equivalence class. □

Proof. Since $[a], [b] \in \mathbb{Z}_n$, then $a, b \in \mathbb{Z}$.

Suppose $x, x' \in [a]$ and $y, y' \in [b]$.

Then $[a] = \{x \in \mathbb{Z} : x \equiv a \pmod{n}\}$ and $[b] = \{x \in \mathbb{Z} : x \equiv b \pmod{n}\}$.

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 $y \equiv y' \pmod{n}$.

Multiplying the congruences $x \equiv x' \pmod{n}$ and $y \equiv y' \pmod{n}$, we obtain $xy \equiv (x'y') \pmod{n}$.

Therefore, $[xy] = [x'y']$. □

Theorem 127. ***Multiplication modulo*** n ***is a binary operation.***

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

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 $b \equiv b' \pmod{n}$.

Since $a \equiv a' \pmod{n}$, then $a, a' \in [a]$.

Since $b \equiv b' \pmod{n}$, then $b, b' \in [b]$.

Therefore, we must prove the result does not depend on the choice of a particular representative of the equivalence class. □

Proof. Let $[a], [b] \in \mathbb{Z}_n$.

Then a and b are integers.

Thus, ab is an integer, so $[ab] \in \mathbb{Z}_n$.

Since $[ab] = [a][b]$, then $[a][b] \in \mathbb{Z}_n$.

Therefore, $\mathbb{Z}_n$ is closed under multiplication modulo n.

Multiplication modulo n is well defined, by lemma 126.

Since $\mathbb{Z}_n$ is closed under multiplication modulo n and multiplication modulo n is well defined, then multiplication modulo n is a binary operation on $\mathbb{Z}_n$. □

Theorem 128. ***algebraic properties of multiplication modulo*** n
Let $n \in \mathbb{Z}^+$.
1. Multiplication is associative.
$([a][b])[c] = [a]([b][c])$ *for all* $[a], [b], [c] \in \mathbb{Z}_n$.
2. Multiplication is commutative.
$[a][b] = [b][a]$ *for all* $[a], [b] \in \mathbb{Z}_n$.
3. Multiplicative identity is $[1]$.
There exists $[1] \in \mathbb{Z}_n$ *such that* $[a][1] = [1][a] = [a]$ *for all* $[a] \in \mathbb{Z}_n$.
4. Multiplication by $[0]$.
$[a][0] = [0][a] = [0]$ *for all* $[a] \in \mathbb{Z}_n$.
5. Multiplication is left distributive over addition.
$[a]([b] + [c]) = [a][b] + [a][c]$ *for all* $[a], [b], [c] \in \mathbb{Z}_n$.
6. Multiplication is right distributive over addition.
$([b] + [c])[a] = [b][a] + [c][a]$ *for all* $[a], [b], [c] \in \mathbb{Z}_n$.

Proof. We prove 1.
Let $[a], [b], [c] \in \mathbb{Z}_n$.
Then $([a][b])[c] = [ab][c] = [(ab)c] = [a(bc)] = [a][bc] = [a]([b][c])$. □

Proof. We prove 2.
Let $[a], [b] \in \mathbb{Z}_n$.
Then $[a][b] = [ab] = [ba] = [b][a]$. □

Proof. We prove 3.
Since $1 \in \mathbb{Z}$, then $[1] \in \mathbb{Z}_n$.
Let $[a] \in \mathbb{Z}_n$.
Then $[a][1] = [a1] = [a] = [1a] = [1][a]$.
Therefore, there exists $[1] \in \mathbb{Z}_n$ such that $[a][1] = [a] = [1][a]$ for all $[a] \in \mathbb{Z}_n$. □

Proof. We prove 4.
Since $0 \in \mathbb{Z}$, then $[0] \in \mathbb{Z}_n$.
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 $([b] + [c])[a] = [b + c][a] = [(b + c)a] = [ba + ca] = [ba] + [ca] = [b][a] + [c][a]$. □

Theorem 129. ***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 130. *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 131. *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. □

Proposition 132. *Let $n \in \mathbb{Z}^+$.*

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

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

Proof. We prove the equivalent statement: if $n|ab$ and n is prime and $n \not| a$, then $n|b$.

Suppose $n|ab$ and n is prime and $n \not| a$

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

Since $n \not| a$, then we conclude $\gcd(n, a) = 1$.

Since $n|ab$ and $\gcd(n, a) = 1$, then $n|b$. □

Proposition 133. *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 $p \nmid a$.

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

Since $p \nmid a$, 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, $\phi(p) = p - 1$. □

Fermat's Theorem

Theorem 134. ***Fermat's Little Theorem***

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

If p is prime and $p \nmid a$, then $p|a^{p-1} - 1$.

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

By the division algorithm, $a = pq+r$ for some integers q and r with $0 \leq r < p$.

Since $p \nmid a$, 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, $p \nmid a$, 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 $sa, 2a, 3a, ..., (p - 1)a$ 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, $p \nmid a$, 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 135. *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 $p \nmid a$.

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 $p \nmid a$.

Since p is prime and $p \nmid a$, 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 136. ***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 $a^{\phi(n)} \equiv 1 \pmod{n}$. □

Corollary 137. ***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 $a^p \equiv a \pmod{p}$. □

Miscellaneous Stuff

Proposition 138. ***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 139. ***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 □