Elementary Number Theory Notes

Jason Sass

August 18, 2025

Mathematics is the abstract science of measure and number.

Natural number system

Definition 1. natural number

A **natural number** is a ratio in which the denominator is 1.

Observe that $\frac{1}{1} = 1 \div 1$ and $\frac{2}{1} = 2 \div 1$ and $\frac{3}{1} = 3 \div 1$ and so on.

Therefore, $1, 2, 3, ...$ are each natural numbers.

Counting in natural numbers is an act of division, as each number represents a measure.

Let n be a natural number.

Then n is a ratio in which the denominator is 1, so $n = \frac{n}{1}$.

The **natural numbers** are $1, 2, 3, 4, 5, 6, 7, ...$

The unit 1 is factor of all natural numbers because 1 measures each natural number exactly.

We can write 1 divides each natural number as $1|n$ for every natural number n.

Definition 2. zero

Zero, denoted 0, is a placeholder symbol(constant) that denotes nothing.

Observe that zero is not a natural number.

Definition 3. integer

An **integer** is either a natural number, the negative of a natural number, or zero.

Let n be a natural number.

Let k be an integer.

Then $k = n$ or $k = -n$ or $k = 0$.

The integers are $..., -4, -3, -2, -1, 0, 1, 2, 3, 4, ...$

Definition 4. positive integer
A **positive integer** is an integer that is greater than zero.

Let n be a positive integer.
Then $n > 0$.
The positive integers are $1, 2, 3, 4, 5, ...$

Definition 5. non-zero integer
A **non-zero integer** is an integer that is not zero.

Let n be a non-zero integer.
Then $n \neq 0$.
The non-zero integers are $1, -1, 2, -2, 3, -3, 4, -4, 5, -5, ...$

Definition 6. non-negative integer
A **non-negative integer** is an integer that is a natural number or zero.

Let n be a non-negative integer.
Then n is a natural number or $n = 0$.
The non-negative integers are $0, 1, 2, 3, 4, 5, 6, ...$

Definition 7. multiple of an integer
A **multiple of an integer** n is an integer kn for some integer k.

Let n be an integer.
If k is an integer, then kn is a multiple of n.

Arithmetic Operations

OLD
Rework the below stuff to eliminate set theory.
We model the natural numbers as strings of ones.

Definition 8. one
one is a vertical stroke |.

Definition 9. natural number
A **natural number** is a string of ones.

Example 10. examples of natural numbers
| is 'one'
|| is 'two'
||| is 'three'
|||| is 'four'
||||| is 'five'

Definition 11. equal natural numbers
Let m and n be natural numbers.
Then $m = n$ means all of the ones in m can be paired up with all of the ones in n.

Example 12. Let m be $|||||$ and let n be $|||||$.

Then m is five and n is five.

Since all of the ones of m can be paired with all of the ones in n, then $m = n$.

Therefore, five equals five, so $5 = 5$.

Definition 13. successor of a natural number

Let n be a natural number.

The **successor of** n, denoted n', is the natural number n concatenated by one.

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

Then $n' \in \mathbb{N}$ is the successor of n and n' is n concatenated by 1.

Example 14. successor operation

$s(|) = ||$,
$s(||) = |||$,
$s(|||) = ||||$,
...

The successor operation takes a natural number and returns the natural number concatenated by $|$.

The successor operation is a function that takes a natural number and returns the next natural number in the sequence of natural numbers.

OLD REJECT PEANO AXIOM CRAP and re-write the foundations of natural numbers!

Peano Axioms for natural number system

Axiom 15. ***Each natural number has a successor.***

For every $n \in \mathbb{N}$ there exists $n' \in \mathbb{N}$ called the ***successor*** *of n.*

Axiom 16. *1 is not the successor of any natural number.*

Axiom 17. *Let $m, n \in \mathbb{N}$.*

Let $m' \in \mathbb{N}$ be the successor of m.

Let $n' \in \mathbb{N}$ be the successor of n.

If $m' = n'$, then $m = n$.

Axiom 18. ***induction property of*** $\mathbb{N}$

Let $S \subset \mathbb{N}$ be a set such that

1. $1 \in S$.

2. For all $n \in S$, if $n \in S$, then $n' \in S$.

Then $S = \mathbb{N}$.

Proposition 19. *The successor of a natural number is unique.*

Since every natural number has a successor and the successor of a natural number is unique, then every natural number n has a unique successor.

Addition is the successor operation applied repeatedly.

Addition is an operation that takes two numbers and returns a number called the **sum**.

Definition 20. Addition is defined in terms of successor. THIS IS WRONG!!!

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

Let $n' \in \mathbb{N}$ be the successor of n.

Define $n + 1 = n'$.

Define $n + 2 = (n')'$.

Define $n + 3 = ((n')')'$.

In general, define $n + k = (((n')')...)'$ to be the k^{th} successor of n for each $k \in \mathbb{N}$.

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

Let $n' \in \mathbb{N}$ be the unique successor of n.

Then $n' = n + 1$.

Observe that $n + 2 = n'' = (n + 1)' = (n + 1) + 1$.

Observe that $n + 3 = n''' = (n + 1)'' = ((n + 1) + 1)' = ((n + 1) + 1) + 1$.

Definition 21. addition

Let m and n be natural numbers.

The **sum of** m **and** n, denoted $m + n$, is the concatenation of the ones of n to the ones of m.

Example 22. $|||||+|||=||||||||$.

Therefore, $5 + 3 = 8$.

Theorem 23. ***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 $s(n) = n + 1$.

Multiplication is repeated addition.

Multiplication is an operation that takes two numbers and returns a number called the **product**.

Definition 24. multiplication

Let m and n be natural numbers.

The **product of** m **and** n, denoted mn, is the string formed by a copy of n for every $|$ in m.

Example 25. $||| \times |||| = ||||||||||||$ (three copies of four)

$|||| \times ||| = ||||||||||||$ (four copies of three)

$||| \times | = |||$ (three copies of 1)

$| \times ||| = |||$ (1 copy of three)

Theorem 26. ***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)

Take two natural numbers and pair the corresponding ones.

The natural number which has any left over ones is larger.

Example 27. larger natural number

||||| is five

|||||||| is eight

We pair each one in the first number with the corresponding one in the second natural number.

In this case, there are some ones left over: ||| (three ones left over).

Therefore, eight is larger than five.

Equivalently, five is smaller than eight.

Definition 28. is less than

Let m and n be natural numbers.

A natural number m is less than a natural number n, denoted $m < n$, iff there are some left over ones in n when the ones in m are paired with the ones in n.

Let m and n be natural numbers.

Then m is less than n, denoted $m < n$, iff n is larger than m.

Example 29. Let $m =$ |||||.

Let $n =$ ||||||||.

Then m is five and n is eight.

Since ||| is left over in n when all of the ones in m are paired with the ones of n, then $m < n$.

Therefore, five is less than eight, so $5 < 8$.

Definition 30. relation $<$ over natural numbers

A natural number a is less than b, denoted $a < b$, iff there is a natural number c such that $a + c = b$.

Observe that $1 < 2 < 3 < 4 < ....$

The natural numbers are ordered by $<$.

|, ||, |||, ||||,...

Let $m, n \in \mathbb{N}$.

Then $m < n$ indicates that m comes before n in the sequence of natural numbers.

Definition 31. relation $>$ over $\mathbb{N}$

Let $m, n \in \mathbb{N}$.

Then m is larger than n, denoted $m > n$, iff $n < m$.

Definition 32. relation $\leq$ over $\mathbb{N}$
Let $m, n \in \mathbb{N}$.
Then m is less than or equal to n, denoted $m \leq n$, iff either $m < n$ or $m = n$.

Definition 33. relation $\geq$ over $\mathbb{N}$
Let $m, n \in \mathbb{N}$.
Then m is greater than or equal to n, denoted $m \geq n$, iff either $m > n$ or $m = n$.

Proposition 34. ***The relation $<$ over $\mathbb{N}$ is transitive.***
Let $a, b, c \in \mathbb{N}$.
If $a < b$ and $b < c$, then $a < c$.

Construction of $\mathbb{Z}$

Arithmetic Operations: addition, subtraction, multiplication, division

Axiom 35. ***closure of $\mathbb{Z}$ under addition and multiplication***
$\mathbb{Z}$ is closed under addition and multiplication.

Let $a, b \in \mathbb{Z}$.
Then $a + b \in \mathbb{Z}$ and $ab \in \mathbb{Z}$.
The sum $a + b$ is unique.
The product $a \cdot b$ is unique.

Theorem 36. ***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 $a + (-a) = 0$.

Theorem 37. ***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)*

Let $a, b \in \mathbb{Z}$.
Since $b \in \mathbb{Z}$, there exists $-b \in \mathbb{Z}$ such that $b + (-b) = 0$.
Since $a \in \mathbb{Z}$ and $-b \in \mathbb{Z}$, then $a + (-b) \in \mathbb{Z}$.
Hence, we define subtraction by $a - b = a + (-b)$.

Definition 38. subtraction in $\mathbb{Z}$
Let $a, b \in \mathbb{Z}$.
Define $a - b = a + (-b)$.
Then $a - b$ is the **difference** between a and b.

Let $a, b \in \mathbb{Z}$.
Since $b \in \mathbb{Z}$, then $-b \in \mathbb{Z}$, so $a - b = a + (-b) \in \mathbb{Z}$.
Therefore, $\mathbb{Z}$ is closed under subtraction.
Since the sum of two integers is unique, then $a + (-b) = a - b$ is unique.
Therefore, the difference $a - b$ is unique.

Axiom 39. *axioms for* $\mathbb{Z}^+$
1. $\mathbb{Z}^+$ is closed under addition defined on $\mathbb{Z}$.
$(\forall a, b \in \mathbb{Z}^+)(a + b \in \mathbb{Z}^+)$. *Sum of positive integers is positive.*
2. $\mathbb{Z}^+$ is closed under multiplication defined on $\mathbb{Z}$.
$(\forall a, b \in \mathbb{Z}^+)(ab \in \mathbb{Z}^+)$. *Product of positive integers is positive.*
3. Trichotomy.
For every $a \in \mathbb{Z}$ exactly one of the following statements is true:
i. $a \in \mathbb{Z}^+$
ii. $a = 0$.
iii. $-a \in \mathbb{Z}^+$.

Since $0 \in \mathbb{Z}$ and $0 = 0$, then by trichotomy, $0 \notin \mathbb{Z}^+$.
$1 \in \mathbb{Z}^+$.

Definition 40. relation $<$ over $\mathbb{Z}$
Let $a, b \in \mathbb{Z}$.
Define a relation "is less than", denoted $<$, on $\mathbb{Z}$ by $a < b$ iff $b - a$ is a positive integer.

Let $a, b \in \mathbb{Z}$.
Then $a < b$ iff $b - a \in \mathbb{Z}^+$.

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

Definition 41. relation $\leq$ over $\mathbb{Z}$
Let $a, b \in \mathbb{Z}$.
Then a is less than or equal to b, denoted $a \leq b$, iff either $a < b$ or $a = b$.

Definition 42. relation $>$ over $\mathbb{Z}$
Let $a, b \in \mathbb{Z}$.
Then a is greater than b, denoted $a > b$, iff $b < a$.

Definition 43. relation $\geq$ over $\mathbb{Z}$

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

Then a is greater than or equal to b, denoted $a \geq b$, iff either $a > b$ or $a = b$.

Proposition 44. *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 $b - a > 0$.

Theorem 45. *$\mathbb{Z}$ 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. $a < b$

Theorem 46. ***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 $ac > bc$.

Proposition 47. *Let $a, b, c, d \in \mathbb{Z}^+$.*

If $a < b$ and $c < d$, then $ac < bd$.

TODO: Write up a proposition and add it above for if $a < b$ and $c < d$, then $a + c < b + d$.

Proposition 48. ***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 $ab > 0$.

Therefore,

1. positive times positive = positive.
2. positive times negative = negative.
3. negative times negative = positive.

Theorem 49. ***multiplicative property of zero***
Let $a, b \in \mathbb{Z}$.
Then $ab = 0$ iff $a = 0$ or $b = 0$.

Let $a, b \in \mathbb{Z}$.
If $a = 0$ or $b = 0$, then $ab = 0$.
If $ab = 0$, then $a = 0$ or $b = 0$.

Since $ab = 0$ iff $a = 0$ or $b = 0$, then $ab \neq 0$ iff $a \neq 0$ and $b \neq 0$.
If $ab \neq 0$, then $a \neq 0$ and $b \neq 0$.
If $a \neq 0$ and $b \neq 0$, then $ab \neq 0$.

Corollary 50. ***cancellation law for*** $\mathbb{Z}$
Let $a, b, k \in \mathbb{Z}$.
If $ak = bk$ and $k \neq 0$, then $a = b$.

Theorem 51. *The relation $\leq$ is a partial order over $\mathbb{Z}$.*

Therefore,
1. $\leq$ is reflexive.
For all $a \in \mathbb{Z}$, $a \leq a$.
2. $\leq$ is anti-symmetric.
For all $a, b \in \mathbb{Z}$, if $a \leq b$ and $b \leq a$, then $a = b$.
3. $\leq$ is transitive.
For all $a, b, c \in \mathbb{Z}$, if $a \leq b$ and $b \leq c$, then $a \leq c$.

Since $\leq$ is a partial order over $\mathbb{Z}$, then $\mathbb{Z}$ is partially ordered under the $\leq$ relation.
Therefore, $(\mathbb{Z}, \leq)$ is a partially ordered set(poset).

Theorem 52. *The relation $\leq$ is a total order over $\mathbb{Z}$.*

Since $\leq$ is a total order over $\mathbb{Z}$, then any two integers are comparable and $\mathbb{Z}$ is totally ordered under the $\leq$ relation.
Since any two integers are comparable, then $a \leq b$ or $b \leq a$ for all $a, b \in \mathbb{Z}$.
Since $\mathbb{Z}$ is totally ordered under the $\leq$ relation, then $(\mathbb{Z}, \leq)$ is a totally (linearly) ordered set.

Since $\mathbb{Z}^+ \subset \mathbb{Z}$ and $\mathbb{Z}$ is a totally ordered set under the $\leq$ relation, then $\mathbb{Z}^+$ is a totally ordered set under the $\leq$ relation.
We assume $\mathbb{Z}^+$ under the $\leq$ relation is well-ordered.

Axiom 53. ***well-ordering principle of*** $\mathbb{Z}^+$
Every nonempty subset of $\mathbb{Z}^+$ has a least element.

Let S be a nonempty subset of $\mathbb{Z}^+$.
Then $S \subset \mathbb{Z}^+$ and $S \neq \emptyset$.
Hence, by WOP(well-ordering principle), S has a least element.
Therefore, $(\exists m \in S)(\forall s \in S)(m \leq s)$.

Lemma 54. ***There is no integer between zero and one.***
There is no $n \in \mathbb{Z}$ such that $0 < n < 1$.

Lemma 55. *For all $n \in \mathbb{Z}^+$, $n \geq 1$.*

Since $n \geq 1$ for all $n \in \mathbb{Z}^+$, then $1 \leq n$ for all $n \in \mathbb{Z}^+$, so 1 is the least positive integer.

Therefore, 1 is the least element of $\mathbb{Z}^+$.

Theorem 56. ***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 $S = \mathbb{Z}^+$.

In some sense, the well-ordering property is logically equivalent to the principle of mathematical induction.

Theorem 57. ***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 $S = \mathbb{Z}^+$.

Proposition 58. *The set of all non-negative integers is well-ordered.*

Therefore, every nonempty subset of non-negative integers has a least element.

Theorem 59. ***Archimedean property of*** $\mathbb{Z}^+$
Let $a, b \in \mathbb{Z}^+$.
Then there exists $n \in \mathbb{Z}^+$ such that $nb > a$.

Proposition 60. *There is no greatest positive integer.*

Lemma 61. *Let $a, b \in \mathbb{N}$.*
If $a < b$ then $b \not\leq a$.

Axiom 62. ***laws of exponents***
For all $m, n \in \mathbb{N}$ and $a, b \in \mathbb{R}$
1. $(a^m)^n = a^{mn}$.
2. $(ab)^n = a^n b^n$.
3. $a^m a^n = a^{m+n}$.
These laws hold for all $m, n \in \mathbb{Z}$ if a and b are not zero.

Elementary Aspects of Integers

Definition 63. consecutive natural numbers
The natural numbers n and $n+1$ are said to be **consecutive**.

Proposition 64. ***No integer exists between two consecutive integers.***
Let $n \in \mathbb{Z}$.
There is no $m \in \mathbb{Z}$ such that $n < m < n+1$.

Definition 65. even number
$(\forall n \in \mathbb{Z})$ n is **even** iff $(\exists k \in \mathbb{Z})(n = 2k)$.

The set of even integers is $2\mathbb{Z} = \{n : n \text{ is even}\} = \{2k : k \in \mathbb{Z}\} = \{..., -4, -2, 0, 2, 4, 6, ...\}$.
The sequence of even positive numbers is $(2n)_{n=1}^{\infty} = (2, 4, 6, 8, ...)$.

Let n be an even integer.
Then $n \equiv 0 \pmod 2$, so n leaves remainder 0 when divided by 2.
Therefore, $2|n$.
In base 10 n ends in 0,2,4,6, or 8.

Definition 66. odd number
$(\forall n \in \mathbb{Z})$ n is **odd** iff $(\exists k \in \mathbb{Z})(n = 2k+1)$.

The set of odd integers is $2\mathbb{Z}+1 = \{n : n \text{ is odd}\} = \{2k+1 : k \in \mathbb{Z}\} = \{..., -3, -1, 1, 3, 5, 7, ...\}$.
The sequence of odd positive numbers is $(2n-1)_{n=1}^{\infty} = (1, 3, 5, 7, ...)$.

Let n be an odd integer.
Then $n \equiv 1 \pmod 2$, so n leaves remainder 1 when divided by 2.
Therefore, $2 \not| n$.
In base 10 n ends in 1,3,5,7, or 9.

Proposition 67. *Every positive integer is either even or odd.*

Proposition 68. *An integer is not both even and odd.*

Let $n \in \mathbb{Z}^+$.
By proposition 67, every positive integer is even or odd.
Hence, n is even or odd.
By proposition 68, an integer is not both even and odd.
Since n is an integer, then n is not both even and odd.
Therefore, n is even or odd, but not both even and odd.

Definition 69. parity
An even number has parity 0.

An odd number has parity 1.

Two integers have the **same parity** iff they are both even or they are both odd; otherwise they have **opposite parity**.

Sum:
even + even = even
even + odd = odd
odd + even = odd
odd + odd = even
Product:
even * even = even
even * odd = even
odd * even = even
odd * odd = odd

Definition 70. consecutive integers
The integers n and $n+1$ are said to be **consecutive**.

Proposition 71. ***A product of two consecutive integers is even.***
If $n \in \mathbb{Z}$, then $n(n+1)$ is even.

Natural Number Formulae

Proposition 72. *Let $n \in \mathbb{Z}^+$.*
The sum of the first n positive integers is $\frac{n(n+1)}{2}$.

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

Proposition 73. *Let $n \in \mathbb{Z}^+$.*
The sum of the first n odd positive integers is n^2.

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

Proposition 74. *Let $n \in \mathbb{Z}^+$.*
The sum of the squares of the first n positive integers is $\frac{n(n+1)(2n+1)}{6}$.

Therefore, $\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$ for all $n \in \mathbb{Z}^+$.

Proposition 75. *The sum of the cubes of the first n positive integers is $(\frac{n(n+1)}{2})^2$.*

Therefore, $\sum_{k=1}^{n} k^3 = (\frac{n(n+1)}{2})^2$ for all $n \in \mathbb{Z}^+$.

Definition 76. square number
$(\forall n \in \mathbb{Z}^+)$ n is a **perfect square** iff $(\exists k \in \mathbb{Z}^+)(n = k^2)$.

A square number is visualized as an arrangement of points in a square whose area is n^2.

Let k be the number of dots in the side of a square, with $k \geq 1$.

Let s_k be the number of dots in a square with k side dots.

We say s_k is the k^{th} square number and

$s_k : \mathbb{N} \to \mathbb{N}$ is a function that maps k side dots to the total number of dots in the square.

The k^{th} square is formed from the $(k-1)$ square by adding sides that is 2 times the side of a $(k-1)$ square plus one corner dot.

Therefore,

$s_k = s_{k-1} + 2(k-1) + 1 = s_{k-1} + 2k - 1$ and $s_1 = 1$ with $k > 1$, and

s_k = number of side dots * number of side dots $= k^2$.

Therefore, s_n is the n^{th} **square number** and

$s_n = s_{n-1} + 2n - 1$ and $s_1 = 1$ with $n > 1$, and

$s_n = n^2$.

The set of all square numbers is $\{n^2 : n \in \mathbb{Z}^+\} = \{1, 4, 9, 16, 25, ...\}$.

The sequence of square numbers is $(s_n) = (n^2)_{n=1}^{\infty} = (1, 4, 9, 16, 25, ...)$.

Definition 77. cubic number

$(\forall n \in \mathbb{Z}^+)$ n is a **perfect cube** iff $(\exists k \in \mathbb{Z}^+)(n = k^3)$.

A cubic number is visualized as an arrangement of n unit cubes into a larger solid cube whose volume is n^3.

The set of all cubic numbers is $\{n^3 : n \in \mathbb{Z}^+\} = \{1, 8, 27, 64, 125, ...\}$.

The sequence of cubic numbers is $(n^3)_{n=1}^{\infty} = (1, 8, 27, 64, 125, ...)$.

Definition 78. triangular number

A positive integer is triangular iff it is the sum of consecutive integers, beginning with one.

Proposition 79. *A positive integer is triangular iff it is of the form* $\dfrac{n(n+1)}{2}$ *for some* $n \in \mathbb{Z}^+$.

Therefore, a positive integer t is triangular iff $t = \dfrac{n(n+1)}{2}$ for some $n \in \mathbb{Z}^+$.

Proposition 80. *Let* t_n *denote the* n^{th} *triangular number.*

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

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

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

A triangular number is visualized as a grid of points arranged as an equilateral triangle such that the first row has 1 element and each subsequent row contains one more element than the previous row.

Let k be the row in the triangular arrangement of dots, with $k \geq 1$.
Let t_k be the number of all dots from row 1 to row k..
We say t_k is the k^{th} triangular number and
$t_k : \mathbb{N} \to \mathbb{N}$ is a function that maps the k^{th} row to its corresponding t_k.
The k^{th} row has k dots.
Then k^{th} triangular number is the $(k-1)$ triangular number + the number of dots in row k.
Therefore, $t_k = t_{k-1} + k$ and $t_1 = 1$ with $k > 1$.
Since t_k is the sum of dots in all preceding rows up to row k, then
$t_k = 1 + 2 + 3 + ... + k = \sum_{i=1}^{k} i = \frac{k(k+1)}{2}$.

Therefore, t_n is the n^{th} **triangular number** and
$t_n = t_{n-1} + n$ and $t_1 = 1$ with $n > 1$, and
$t_n = \sum_{k=1}^{n} k = \frac{n(n+1)}{2} = \binom{n+1}{2}$.
The set of all triangular numbers is $\{\frac{n(n+1)}{2} : n \in \mathbb{Z}^+\} = \{1, 3, 6, 10, 15, 21, ...\}$.
The sequence of triangular numbers is $(t_n) = (\frac{n(n+1)}{2})_{n=1}^{\infty} = (1, 3, 6, 10, 15, 21, ...)$.

Definition 81. perfect number
$\forall n \in \mathbb{Z}^+, n$ is **perfect** iff n equals the sum of its positive divisors less than itself.

Equivalent definition:
$\forall p \in \mathbb{Z}^+, n$ is **perfect** iff its positive divisors add up to $2n$.

The set of all perfect numbers is $\{n \in \mathbb{Z}^+ : n \text{ is perfect}\} = \{6, 28, 496, 8128, ...\}$.
It is not known whether there are infinitely many perfect numbers.
Every even perfect number ends with a 6 or 8.
It is not known whether there are any odd perfect numbers.

Definition 82. Fibonacci numbers
F_n is the n^{th} term of the **Fibonacci sequence** defined by
$F_n = F_{n-1} + F_{n-2}, n > 2$, and $F_1 = F_2 = 1$.

The Fibonacci sequence is $(F_n)_{n=1}^{\infty} = (1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, ...)$.

Pythagorean Triples

Pythagorean triples $= \{(a, b, c) : c^2 = a^2 + b^2, a, b, c \in \mathbb{N}\}$
A Pythagorean triple (a, b, c) is **primitive** iff a, b, c have no common factors greater than 1.

Let s, t be any odd integers where $s > t \geq 1$ and $\gcd(s, t) = 1$.

Then (a, b, c) is a primitive Pythagorean triple where odd $a = st$,even $b = \frac{s^2-t^2}{2}$, and $c = \frac{s^2+t^2}{2}$.

Divisibility in $\mathbb{Z}$

Theorem 83. ***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 $0 \leq r < b$.

This is just long division from arithmetic. Division by zero is not defined.

We divide a by b.

a = dividend

b = divisor

q = quotient

r = remainder

Division is repeated subtraction of multiples of the divisor from the dividend until a nonnegative remainder is obtained that is less than the divisor.

Definition 84. divisibility relation over $\mathbb{Z}$

Define the relation 'divides' over $\mathbb{Z}$ for all $a, b \in \mathbb{Z}$ by $b \mid a$ iff $(\exists n \in \mathbb{Z})(a = bn)$.

The statement **'b divides a'**, denoted $b|a$, means there exists an integer n such that $a = bn$.

Therefore $b|a$ iff $(\exists n \in \mathbb{Z})(a = bn)$.

The statement **'b does not divide a'**, denoted $b \not| a$, means there is no integer n such that $a = bn$.

Therefore $b \not| a$ iff $\neg(\exists n \in \mathbb{Z})(a = bn)$.

Equivalent meanings for $b|a$ are:

1. a is **divisible by** b
2. b is a **divisor of** a
3. a is a **multiple of** b
4. b is a **factor of** a

Proposition 85. *Every integer divides zero.* $(\forall n \in \mathbb{Z})(n|0)$.

Therefore $0|0$ and $1|0$.

Proposition 86. *The number 1 divides every integer.* $(\forall n \in \mathbb{Z})(1|n)$.

Proposition 87. *Every integer divides itself.* $(\forall n \in \mathbb{Z})(n|n)$.

Therefore, the divides relation on $\mathbb{Z}$ is reflexive.

Theorem 88. ***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.

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

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

When a is divided by b, by the division algorithm, there exist unique integers q and r such that $a = bq + r$ and $0 \leq r < b$.

Therefore, $b|a$ iff $r = 0$ when a is divided by b.

This means $b|a$ iff a is divisible by b.

Theorem 89. ***A divisor of*** a ***is smaller than*** a***.***

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

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

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

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

Therefore, if $d > a$, then $d \nmid a$.

Proposition 90. *Let* $a, b, c, d \in \mathbb{Z}$.

If $a|b$ *and* $c|d$*, then* $ac|bd$.

Proposition 91. ***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* $a = b = -1$.

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

If $a = b = 1$ or $a = b = -1$, then $ab = 1$.

If $ab = 1$, then $a = b = 1$ or $a = b = -1$.

Proposition 92. *Let* $a \in \mathbb{Z}$ *and* $b \in \mathbb{Z}$.

If $a|b$ *and* $b|a$*, then* $a = \pm b$.

Theorem 93. *Let* $a, d \in \mathbb{Z}$.

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

If d divides a, then d divides any multiple of a.

Proposition 94. *Let* $a, b, n \in \mathbb{Z}$.

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

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

Theorem 95. ***The divides relation on*** $\mathbb{Z}$ ***is transitive.***

For any integers a, b *and* c*, if* $a|b$ *and* $b|c$*, then* $a|c$.

Theorem 96. *The divides relation is a partial order over* $\mathbb{Z}^+$.

Therefore,

1. $|$ is reflexive.

$(\forall a \in \mathbb{Z}^+)(a|a)$.

2. $|$ is antisymmetric.

$(\forall a, b \in \mathbb{Z}^+)(a|b \wedge b|a \rightarrow a = b)$.

3. $|$ is transitive.

$(\forall a, b, c \in \mathbb{Z}^+)(a|b \wedge b|c \rightarrow a|c)$.

The set of all positive integers is partially ordered under the divides relation, so $(\mathbb{Z}^+, |)$ is a poset.

Greatest common divisor

Definition 97. divisors of an integer

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

The set of all divisors of n is $\{d \in \mathbb{Z} : d|n\}$.

The set of all positive divisors of n is $\{d \in \mathbb{Z}^+ : d|n\}$.

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

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

If $d|n$, then $d \leq n$.

Therefore, $1 \leq d \leq n$.

Therefore, a positive divisor of a positive integer n is bounded between 1 and n.

Proposition 98. *Let $n \in \mathbb{Z}$.*

Then n and $-n$ have the same set of divisors.

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

Then $\{d \in \mathbb{Z} : d|n\} = \{d \in \mathbb{Z} : d| - n\}$.

Definition 99. common divisor

Let a and b be any integers.

An integer d is a **common divisor** of a and b iff $d|a$ and $d|b$.

$$\begin{aligned} \text{positive divisors of } a &= \{d \in \mathbb{Z}^+ : d|a\} \\ \text{positive divisors of } b &= \{d \in \mathbb{Z}^+ : d|b\} \\ \text{positive common divisors of a and b} &= \{d \in \mathbb{Z}^+ : d|a \wedge d|b\} \end{aligned}$$

Let a and b be any integers.

Since the positive integer 1 divides every integer, then $1|a$ and $1|b$, so 1 is a positive common divisor for any integers a and b.

Proposition 100. ***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 $1 \leq d \leq \min(a, b)$.

Definition 101. linear combination

Let a and b be integers.

A **linear combination of a and b** is an expression of the form $ma + nb$ for some integers m and n.

Let a and b be integers.

Let c be a linear combination of a and b.

Then there exist integers m and n such that $c = ma + nb$.

Since a, b, m, n are integers, then c is an integer.

Let a and b be integers.

If m and n are integers, then the expression $ma+nb$ is a linear combination of a and b.

Lemma 102. ***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* $d|(a-b)$.

Theorem 103. ***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.

Corollary 104. ***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* $c_1, c_2, ..., c_n$.

Definition 105. greatest common divisor

The greatest common divisor is the largest positive common divisor of two integers not both zero.

Let a and b be integers with a and b not both zero.

Then d is a **greatest common divisor of** a **and** b iff

1. d is a positive common divisor of a and b.

d is a positive integer and $d|a$ and $d|b$.

2. Any common divisor of a and b is a divisor of d.

For every integer c, if $c|a$ and $c|b$, then $c|d$.

Theorem 106. ***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.

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

The greatest common divisor of a and b is denoted by $\gcd(a, b)$.

Since any integer divides 0, then there are infinitely many integers that are common divisors of 0 and 0, so we do not define $\gcd(0, 0)$.

Therefore, in the definition of gcd, we do not allow a and b to be both zero.

This is why a and b are not both zero in the definition of gcd.

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

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

Let $a, b \in \mathbb{Z}^+$.
Let $d = \gcd(a, b)$.
Then d is a positive common divisor of a and b.
Since any positive common divisor is bounded, then $1 \leq d \leq min(a, b)$.
Therefore, $1 \leq \gcd(a, b) \leq min(a, b)$ for all $a, b \in \mathbb{Z}^+$.

Proposition 107. ***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* $k \in \mathbb{Z}^+$.

Lemma 108. *The only positive integer that divides* 1 *is* 1.

Theorem 109. *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* $\gcd(a, b)$.

Therefore every linear combination of a and b is a multiple of $\gcd(a, b)$ and every multiple of $\gcd(a, b)$ is a linear combination of a and b.

Corollary 110. *Let* $a, b \in \mathbb{Z}$.
Then $\gcd(a, b) = 1$ *iff there exist* $m, n \in \mathbb{Z}$ *such that* $ma + nb = 1$.

Let $a, b \in \mathbb{Z}$.
Then $\gcd(a, b) = 1$ iff there exist $m, n \in \mathbb{Z}$ such that $ma + nb = 1$.
Therefore, $\gcd(a, b) = 1$ iff 1 is a linear combination of a and b.

Corollary 111. *Let* $a, b \in \mathbb{Z}$.
Let $d \in \mathbb{Z}^+$.
If $d = \gcd(a, b)$, *then* $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$.

Definition 112. relatively prime integers
Two integers are relatively prime iff their only common positive divisor is 1.
Let $a, b \in \mathbb{Z}$.
Then a and b are **relatively prime** iff $\gcd(a, b) = 1$.

Let $a, b \in \mathbb{Z}$.
Then a and b are relatively prime iff $\gcd(a, b) = 1$.
Hence, if a and b are relatively prime, then $\gcd(a, b) = 1$, so 1 is their only common positive divisor.
Therefore, there is no integer greater than one that divides them both.
Therefore relatively prime numbers have no common positive divisor other than 1.

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

Then a and b are relatively prime iff $\gcd(a, b) = 1$ iff there exist $m, n \in \mathbb{Z}$ such that $ma + nb = 1$ iff 1 is a linear combination of a and b.

Theorem 113. *Let $a, b, d \in \mathbb{Z}$.*
If $d|ab$ and $\gcd(d, a) = 1$, then $d|b$.

Theorem 114. *Let $a, b, m \in \mathbb{Z}$.*
If $a|m$ and $b|m$ and $\gcd(a, b) = 1$, then $ab|m$.

Therefore, if m is a common multiple of a and b, and a and b are relatively prime, then m is a multiple of ab.

Euclidean Algorithm

Let a and b be any two integers.

We use the Euclidean algorithm to compute $\gcd(a, b)$ and to write $\gcd(a, b)$ as a linear combination of a and b.

Lemma 115. ***Euclidean Algorithm lemma***
Let $a, b \in \mathbb{Z}$ and $b > 0$.
If a is divided by b with remainder r, then $\gcd(a, b) = \gcd(b, r)$.

Theorem 116. ***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 $\gcd(a, b) = r_{n-1}$.

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

To compute $\gcd(a, b)$, apply the division algorithm repeatedly by dividing the previous divisor by the previous remainder.

First, we divide a by b and obtain $a = bq + r$ with $0 \leq r < b$.

Each time we divide, the positive remainder gets smaller until it becomes 0.

The last nonzero remainder in this division process will equal $\gcd(a, b)$.

Observe that $b > r_1 > r_2 > r_3 > ... > r_k > r_{n-1} > 0$, so the algorithm terminates in n steps.

Least common multiple

Definition 117. multiples of an integer

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

The set of all multiples of n is $\{m \in \mathbb{Z} : n|m\}$.

The set of all positive multiples of n is $\{m \in \mathbb{Z}^+ : n|m\}$.

Theorem 118. ***definition of*** $n\mathbb{Z}$

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

The set of all multiples of n is $\{nk : k \in \mathbb{Z}\}$.

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

Then $\{m \in \mathbb{Z} : n|m\} = \{nk : k \in \mathbb{Z}\}$.

The set of all multiples of n is denoted by $n\mathbb{Z}$.

Therefore, $\{m \in \mathbb{Z} : n|m\} = n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$.

Proposition 119. *Let $n \in \mathbb{Z}^+$.*

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

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

The set of all positive multiples of n is $\{m \in \mathbb{Z}^+ : n|m\} = \{nk : k \in \mathbb{Z}^+\} = \{n, 2n, 3n, 4n, ...\}$.

Definition 120. common multiple

Let a and b be any integers.

An integer m is a **common multiple** of a and b iff $a|m$ and $b|m$.

Let a and b be any integers.

Since every integer divides zero, then $a|0$ and $b|0$, so 0 is a common multiple of any integers a and b.

$$\begin{aligned} \text{positive multiples of } a &= \{m \in \mathbb{Z}^+ : a|m\} \\ \text{positive multiples of } b &= \{m \in \mathbb{Z}^+ : b|m\} \\ \text{positive common multiples of a and b} &= \{m \in \mathbb{Z}^+ : a|m \wedge b|m\} \end{aligned}$$

Definition 121. least common multiple

The least common multiple is the smallest positive common multiple of two integers.

Let a and b be positive integers.

Then m is a **least common multiple of a and b** iff

1. m is a positive common multiple of a and b.

m is a positive integer and $a|m$ and $b|m$.

2. Any positive common multiple of a and b is a multiple of m.

For every positive integer c, if $a|c$ and $b|c$, then $m|c$.

Let m be the least common multiple of any positive integers a and b.

Then any positive common multiple of a and b is a multiple of m.

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

Then c is a multiple of m, so m divides c.

Hence, m divides $-c$, so m divides any negative common multiple of a and b.

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

Since $a|0$ and $b|0$, then zero is a common multiple of a and b.

Since every integer divides zero and m is an integer, then m divides zero, so zero is a multiple of m.

Since zero is a common multiple of a and b, and zero is a multiple of m, then zero is a common multiple of a and b implies zero is a multiple of m.

Since any positive common multiple of a and b is a multiple of m, and any negative common multiple of a and b is a multiple of m, and zero is a common multiple of a and b implies zero is a multiple of m, then any common multiple of a and b is a multiple of m.

Therefore, if m is the least common multiple of any positive integers a and b, then any common multiple of a and b is a multiple of m.

Theorem 122. ***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.

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

The least common multiple of a and b is denoted by $lcm(a, b)$.

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

Therefore, $lcm(0, 0)$ is undefined.

Proposition 123. *For all $a, b \in \mathbb{Z}^+$, $lcm(a, b)$ divides ab.*

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

Then $ab \in \mathbb{Z}^+$ and $lcm(a, b) \in \mathbb{Z}^+$.

Since $lcm(a, b) \in \mathbb{Z}^+$, then $lcm(a, b) \geq 1$, so $1 \leq lcm(a, b)$.

Since $lcm(a, b)$ divides ab, then $lcm(a, b) \leq ab$.

Thus, $1 \leq lcm(a, b)$ and $lcm(a, b) \leq ab$, so $1 \leq lcm(a, b) \leq ab$.

Therefore, $1 \leq lcm(a, b) \leq ab$ for all $a, b \in \mathbb{Z}^+$.

Theorem 124. ***lcm and gcd relationship***
Let $a, b \in \mathbb{Z}^+$.
Then $\gcd(a, b) \cdot lcm(a, b) = ab$.

Corollary 125. *Let $a, b \in \mathbb{Z}^+$.*
Then $lcm(a, b) = ab$ iff $\gcd(a, b) = 1$.

Proposition 126. ***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* $lcm(a, b) = b$.

Let $a, b \in \mathbb{Z}^+$.
Then $\gcd(a, b)$ divides $lcm(a, b)$ and $lcm(a, b)$ divides ab.

Linear Diophantine Equations

Definition 127. Diophantine equation
A **Diophantine equation** is an equation in one or more unknowns whose solution is in the set of integers.

Definition 128. linear Diophantine equation
Let $a, b, c \in \mathbb{Z}$.
A **linear Diophantine equation in two unknowns** is a Diophantine equation $ax + by = c$.

The solution set of a linear Diophantine equation is the set $\{(x, y) \in \mathbb{Z} \times \mathbb{Z} : ax + by = c\}$.

Theorem 129. ***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* $\gcd(a, b) \mid c$.

Theorem 130. ***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* $d = \gcd(a, b)$.

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 $d|c$, where $d = \gcd(a, b)$.
Moreover, if (x_0, y_0) is a particular solution, then a general solution is given by $x = x_0 + \frac{bt}{d}$ and $y = y_0 - \frac{at}{d}$ for all $t \in \mathbb{Z}$.
If $\gcd(a, b) = 1$, then $x = x_0 + \frac{bt}{1} = x_0 + bt$ and $y = y_0 - \frac{at}{1} = y_0 - at$ for all $t \in \mathbb{Z}$.

Fundamental Theorem of Arithmetic

Definition 131. prime number
A positive integer p other than 1 is **prime** iff the only positive divisors of p are 1 and p.

Therefore, a positive integer p other than 1 is not prime iff there is some positive divisor of p other than 1 or p.

Let p be a prime number.
Then p is a positive integer and $p \neq 1$ and the only positive divisors of p are 1 and p.

Let p be a positive integer.
If the only positive divisors of p are 1 and p, then p is a prime number.

The prime numbers are $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, ...$

Definition 132. composite number
A positive integer other than 1 is **composite** iff it is not prime.

The composite numbers are $4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, 21, 22, 24, ...$

The number 1 is neither prime nor composite. (1 is a unit of the integers.)

Let n be a positive integer.
Then n is composite iff n is neither 1 nor prime.

A positive integer n is exactly one of the following:
1. $n = 1$.
2. n is prime.
3. n is composite.

Lemma 133. ***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 $1 < d < n$.

Theorem 134. ***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 $n = ab$.

Theorem 135. *Every integer greater than 1 has a prime factor.*

Let n be any integer greater than 1.
Then n has a prime factor.
Therefore, there exists a positive integer p such that p is prime and $p|n$.

Lemma 136. ***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 $p|b$.

Corollary 137. ***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 $1 \leq k \leq n$.

Therefore, if p is prime and p divides a product of integers, then p divides one of those integers.
Therefore, if prime p divides a product of integers, then p divides one of those integers.

Corollary 138. *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 $1 \leq k \leq n$.

Therefore, if p is prime and p divides a product of primes, then p is one of those primes.
Therefore, if prime p divides a product of primes, then p is one of those primes.

Definition 139. prime factorization of an integer
Let $n \in \mathbb{Z}$ and $n > 1$.
A **prime factorization of** n is a representation of n as a product of primes.

Any prime factorizations of a positive integer that differ only in the order of the factors are considered identical factorizations.

Theorem 140. ***Fundamental Theorem of Arithmetic(Existence)***
Every integer greater than one can be represented as a product of one or more primes.

Therefore, every integer greater than one has a prime factorization.

Lemma 141. *A product of primes is greater than one.*

Let $p_1, p_2, ..., p_n \in \mathbb{Z}^+$.
If $p_1, p_2, ..., p_n$ are all primes, then $p_1p_2...p_n > 1$.

Theorem 142. ***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.

Let n be an integer greater than 1.

Then $n \in \mathbb{Z}$ and $n > 1$.

Therefore, n can be represented as a product of one or more primes in exactly one way.

Hence, $n = p_1 \cdot p_2 \cdot \ldots \cdot p_k$ for some primes $p_1, p_2, ..., p_k$.

Therefore, every integer greater than one has a unique prime factorization.

Corollary 143. ***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 $p_1 < p_2 < ... < p_k$.

Let n be an integer greater than 1.

Then $n \in \mathbb{Z}$ and $n > 1$.

Therefore, $n = p_1^{e_1} p_2^{e_2} ... p_k^{e_k}$ where for each $i = 1, 2, ..., k$, each exponent e_i is a positive integer, and each p_i is a prime with $p_1 < p_2 < ... < p_k$.

This is the **prime power factorization** of n, also known as the **canonical prime factorization** of n.

Prime numbers are used to build, by multiplication, the entire set of positive integers $\mathbb{Z}^+$.

Therefore, prime numbers are the building blocks from which all other integers are composed.

Theorem 144. *Let $n \in \mathbb{Z}^+$.*

The positive divisors of n are integers whose prime power factorizations have the same primes as n with powers less than or equal to those powers occurring in n.

TODO: DO THIS PROOF.

Let $n \in \mathbb{Z}$ with $n > 1$.

The positive divisors of n are made up of powers in the prime factorization of n with powers less than or equal to the powers appearing in n.

Theorem 145. ***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.

Theorem 146. ***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.

Distribution of Primes

Proposition 147. *Any distinct primes are relatively prime.*

Let p and q be distinct primes.
Then p and q are primes and $p \neq q$.
Therefore, p and q are relatively prime, so $\gcd(p, q) = 1$.
Therefore, if p and q are distinct primes, then $\gcd(p, q) = 1$.

Theorem 148. ***Euclid's Theorem***
There are more prime numbers than in any given list of them.

The theorem is interpreted to mean the number of primes is infinite, meaning that a collection of primes is infinite; that is, no list of primes is complete; there is no limit to those primes that we could name. It does not mean there is a list of primes that never ends. A list of primes that never ends does not exist.

Euclid's theorem is from Euclid's Elements Book IX proposition 20 which states 'prime numbers are more than any assigned multitude of prime numbers.'

Sieve of Eratosthenes

Lemma 149. *Let $n \in \mathbb{Z}^+$.*
If n is composite, then there exists $d \in \mathbb{Z}$ such that $d|n$ and $1 < d \leq \sqrt{n}$.

Proposition 150. *Let $n \in \mathbb{Z}^+$.*
If n is composite, then n has a prime factor less than or equal to $\sqrt{n}$.

Let $n \in \mathbb{Z}^+$ and $n > 1$.
If n is composite, then n has a prime factor less than or equal to $\sqrt{n}$.
Thus, if n does not have a prime factor less than or equal to $\sqrt{n}$, then n is not composite.
Hence, either $n = 1$ is n is prime.
Since $n > 1$, then $n \neq 1$, so n is prime.
Therefore, if n is an integer greater than one, and n does not have a prime factor less than or equal to $\sqrt{n}$, then n is prime.
This fact is used in the Sieve of Eratosthenes.

The **Sieve of Eratosthenes** algorithm is used to find all primes less than or equal to a given positive integer $n > 1$.

1. List all integers from 2 to n in ascending order.

2. Systematically eliminate all the composite numbers by striking out all multiples $2p, 3p, 4p, 5p, ...$ of primes $p \leq \sqrt{n}$.

3. The integers left on the list(those that do not fall through the sieve) are primes.

Let k be any integer that remains after the sieving process is completed.

Then $k > 1$ and k is not divisible by any prime less than k.

Hence, k is not divisible by any prime $p \leq \sqrt{k}$, so k does not have a prime factor less than or equal to $\sqrt{k}$.

Since $k > 1$, and k does not have a prime factor less than or equal to $\sqrt{k}$, then k must be prime.

Therefore, any integer that remains after the sieving process is completed must be prime.

Definition 151. n^{th} **prime number**

Let n be a positive integer.

The sequence of prime numbers satisfies $2 < 3 < 5 < 7 < 11 < 13 < 17 < 19 < ....$

Let p_n denote the n^{th} prime number of this sequence of primes in increasing order.

By Euclid's theorem, there are infinitely many prime numbers.

Therefore, there is a sequence $f : \mathbb{Z}^+ \to \mathbb{Z}^+$ defined by $f(n) = p_n$, where all of the prime numbers are arranged in ascending order.

Let (p_n) be the **sequence of prime numbers** arranged in increasing order.

Since $2 < 3 < 5 < 7 < ...$, then $p_1 = 2$ and $p_2 = 3$ and $p_3 = 5$ and $p_4 = 7$ and ... and $p_1 < p_2 < p_3 < ... < p_n < ....$

Therefore, p_n is the n^{th} term of the **sequence of prime numbers** $(p_1, p_2, p_3, ...)$.

Observe that $1 < p_1 < p_2 < p_3 < ... < p_n < ....$

Proposition 152. *For every integer $n > 2$, there is a prime p such that $p < n$.*

Proposition 153. *For every $n \in \mathbb{Z}^+$, there is a prime p such that $p > n$.*

Lemma 154. *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 $n \in \mathbb{Z}^+$.

Proposition 155. *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 $n \in \mathbb{Z}^+$.

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 $n \in \mathbb{Z}^+$, and $p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1 \leq p_n^n + 1$ for all $n \in \mathbb{Z}^+$, so $p_{n+1} \leq p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1 \leq p_n^n + 1$ for all $n \in \mathbb{Z}^+$.

Proposition 156. ***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 $n \in \mathbb{Z}^+$.

Corollary 157. *Let $n \in \mathbb{Z}^+$.*
Then there are at least $n+1$ primes less than 2^{2^n}.

Goldbach Conjecture

Definition 158. twin primes
Twin primes are a pair of primes which differ by two.

Let p be a prime.
Then p and $p+2$ are twin primes.

Proposition 159. ***Twin primes are odd.***
Let p and $p+2$ be twin primes.
Then p and $p+2$ are odd.

Therefore, twin primes are two odd primes that differ by two.

The **twin prime conjecture** states that there are infinitely many pairs of twin primes.

Conjecture 160. ***twin prime conjecture***
There are infinitely many primes p such that $p+2$ is also prime.

Proposition 161. *For every integer $n \geq 2$, there are n consecutive positive integers which are all composite.*

Conjecture 162. ***binary(strong) Goldbach conjecture***
Every even integer greater than 2 is the sum of two primes.

Conjecture 163. ***ternary(weak) Goldbach conjecture***
Every odd integer greater than 5 is the sum of three primes.

If we assume the strong Goldbach conjecture, then the weak Goldbach conjecture is true.
Therefore, the binary Goldbach conjecture implies the ternary Goldbach conjecture.

Conjecture 164. ***slightly stronger version of the ternary Goldbach conjecture***
Every odd integer greater than 7 is the sum of three odd primes.

Proposition 165. *Every odd integer is of the form $4n+1$ or $4n+3$ for some integer n.*

Lemma 166. *The product of any finite number of integers of the form* $4a+1$ *is of the same form.*

Theorem 167. *There are infinitely many primes of the form* $4n+3$*, where* $n \in \mathbb{Z}$*.*

Theorem 168. ***Dirichlet's theorem on primes in arithmetic progressions***

If a *and* m *are relatively prime positive integers, then the arithmetic sequence* $a, a+m, a+2m, a+3m, ...$ *contains infinitely many primes.*

The proof of Dirichlet's theorem is difficult and uses analytic number theory techniques.

Proposition 169. *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.*

Lemma 170. *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.*

Proposition 171. *Let* $a, m \in \mathbb{Z}^+$*.*

There is no arithmetic sequence $a, a+m, a+2m, a+3m, ...$ *that contains only prime numbers.*

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

Let $a, a+m, a+2m, a+3m, ...$ be an arithmetic sequence.

Then the sequence does not contain only prime numbers.

Since consecutive terms of the sequence are at a distance m from each other, then the terms of the sequence are equally spaced.

Therefore, the prime numbers are not equally spaced in $\mathbb{Z}^+$.

Congruences

Definition 172. congruence modulo relation over $\mathbb{Z}$

Let n be a fixed positive integer.

Let $R = \{(a,b) \in \mathbb{Z} \times \mathbb{Z} : n|(a-b)\}$.

Since $R \subset \mathbb{Z} \times \mathbb{Z}$, then R is a relation on $\mathbb{Z}$.

The relation R is called **congruence modulo** n **over** $\mathbb{Z}$.

Define the relation 'is congruent to modulo n' over $\mathbb{Z}$ for all $a, b \in \mathbb{Z}$ by $a \equiv b \pmod{n}$ iff $n|(a-b)$.

The statement **'**a **is congruent to** b **modulo** n**'**, denoted $a \equiv b \pmod{n}$, means $n|(a-b)$.

Therefore $a \equiv b \pmod{n}$ iff $n|(a-b)$.

The positive integer n in the definition $a \equiv b \pmod{n}$ is called the **modulus**.

The statement **'**a **is not congruent to** b **modulo** n**'**, denoted $a \not\equiv b \pmod{n}$, means $n \not| (a-b)$.

Therefore $a \not\equiv b \pmod{n}$ iff $n \not| (a-b)$.

Theorem 173. ***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.

Theorem 174. *The congruence modulo relation is an equivalence relation on $\mathbb{Z}$.*

Let n be a fixed positive integer.

Let a, b, and c be any integers.

Then

1. $\equiv$ is reflexive

$a \equiv a \pmod{n}$.

2. $\equiv$ is symmetric

If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$.

3. $\equiv$ is is transitive

If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

Proposition 175. *Let n be a fixed positive integer.*

Let a and b be any integers.

If $a = b$, then $a \equiv b \pmod{n}$.

Theorem 176. ***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)

Theorem 177. ***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.

Theorem 178. ***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* $a \equiv b \pmod{\frac{n}{\gcd(n,k)}}$.

Corollary 179. ***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* $a \equiv b \pmod{n}$.

Lemma 180. *Let* p *be a positive integer.*
Let a *be any integer.*
If p *is prime and* $p \not| a$*, then* $\gcd(p,a) = 1$.

Corollary 181. ***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* $p \not| k$*, then* $a \equiv b \pmod{p}$.

Proposition 182. *Let* k *and* n *be positive integers.*
Let a *and* b *be any integers.*
Then $ak \equiv bk \pmod{nk}$ *iff* $a \equiv b \pmod{n}$.

Proposition 183. *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* $b \equiv 0 \pmod{n}$.

Proposition 184. *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* $b \equiv 0 \pmod{p}$.

TODO: Move the content of Burton chapter 4.2 section about residues to my notes in a later section.

Linear Congruences

Definition 185. linear congruence
Let $n \in \mathbb{Z}^+$.
Let $a, b \in \mathbb{Z}$.
The equation $ax \equiv b \pmod{n}$ is called a **linear congruence**.

Let $n \in \mathbb{Z}^+$.
Let $a, b \in \mathbb{Z}$.
Let $S = \{x \in \mathbb{Z} : ax \equiv b \pmod{n}\}$.
Then S is the solution set to the linear congruence $ax \equiv b \pmod{n}$.

Proposition 186. *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.

Definition 187. multiplicative inverse of a modulo n

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

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

Then a **has a multiplicative inverse modulo** n iff there is an integer b such that $ab \equiv 1 \pmod{n}$ and $0 < b < n$.

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

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

Then a has a multiplicative inverse modulo n iff there exists $b \in \mathbb{Z}$ such that $ab \equiv 1 \pmod{n}$ and $0 < b < n$.

We say that b is a **multiplicative inverse** of a.

Theorem 188. ***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 $\gcd(a, n) = 1$.

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

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

Then a has a multiplicative inverse modulo n iff there is a unique integer b such that $ab \equiv 1 \pmod{n}$ and $0 < b < n$ iff $\gcd(a, n) = 1$.

Therefore, a has a multiplicative inverse modulo n iff a and n are relatively prime.

A multiplicative inverse of a, if it exists, is unique.

Proposition 189. *Let $n \in \mathbb{Z}^+$.*

Every integer is congruent to exactly one of the remainders $0, 1, ..., n-1$ when divided by n.

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

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

Then a is congruent to exactly one of $0, 1, ..., n-1$ when a is divided by n.

Hence, a is congruent to exactly one integer in the set $\{0, 1, ..., n-1\}$ when a is divided by n.

Therefore, there is a unique integer $r \in \{0, 1, ..., n-1\}$ such that $a \equiv r \pmod{n}$.

Proposition 190. *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.

Theorem 191. ***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 $\frac{n}{d}$.

Integers Modulo n

Definition 192. congruence class of a modulo n
Let $n \in \mathbb{Z}^+$.
Let $a \in \mathbb{Z}$.
The **congruence class of** a, denoted $[a]$ or $[a]_n$, is the set of all integers congruent to a modulo n.

Let $n \in \mathbb{Z}^+$.
Let $a \in \mathbb{Z}$.
Then $[a]$ is the congruence class of a modulo n.
Hence, $[a]$ is the set of all integers congruent to a modulo n.
Therefore, $[a] = \{x \in \mathbb{Z} : x \equiv a \pmod{n}\}$.
Observe that $b \in [a]$ iff $b \in \mathbb{Z}$ and $b \equiv a \pmod{n}$.
Observe that $[a]$ is a subset of $\mathbb{Z}$.
Therefore, $[a] \subset \mathbb{Z}$.

Let $n \in \mathbb{Z}^+$.
Let $a \in \mathbb{Z}$.
Then $[a] = \{x \in \mathbb{Z} : x \equiv a \pmod{n}\}$ and

$$\begin{aligned}
[a] &= \{x \in \mathbb{Z} : n|(x-a)\} \\
&= \{x \in \mathbb{Z} : (\exists k \in \mathbb{Z})(x - a = nk)\} \\
&= \{a + nk : k \in \mathbb{Z}\} \\
&= a + n\mathbb{Z} \\
&= n\mathbb{Z} + a.
\end{aligned}$$

Since congruence modulo is an equivalence relation, then $[a] = [b]$ iff $a \equiv b \pmod{n}$.

Therefore, $[a] = [b]$ iff $a \equiv b \pmod{n}$ iff a and b leave the same remainder when divided by n.

Theorem 193. *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 $[0], [1], ..., [n-1]$.

Let $n \in \mathbb{Z}^+$.
Then there are exactly n distinct congruence classes $[0], [1], ..., [n-1]$.
Therefore, $[a] \neq [b]$ for every $a, b \in \{0, 1, ..., n-1\}$ with $a \neq b$.

Proposition 194. *Let $n \in \mathbb{Z}^+$.*
Then $[n] = [0]$.

Proposition 195. *Let $n \in \mathbb{Z}^+$.*
Then $[-a] = [n - a]$ for all $[a] \in \mathbb{Z}_n$.

Definition 196. set of integers modulo n
Let $n \in \mathbb{Z}^+$.
The **set of integers modulo** n, denoted $\frac{\mathbb{Z}}{n\mathbb{Z}}$ or $\mathbb{Z}_n$, is the set of all congruence classes of integers modulo n.
Therefore, $\mathbb{Z}_n = \frac{\mathbb{Z}}{n\mathbb{Z}} = \{[a] : a \in \mathbb{Z}\}$.

Theorem 197. *Let $n \in \mathbb{Z}^+$.*
Then $\mathbb{Z}_n = \frac{\mathbb{Z}}{n\mathbb{Z}} = \{[0], [1], ..., [n-1]\}$ and $|\mathbb{Z}_n| = n$.

Let $n \in \mathbb{Z}^+$.
Then $\frac{\mathbb{Z}}{n\mathbb{Z}} = \mathbb{Z}_n$ is the set of integers modulo n, so $\frac{\mathbb{Z}}{n\mathbb{Z}} = \mathbb{Z}_n$ is the set of all congruence classes of integers modulo n and $\frac{\mathbb{Z}}{n\mathbb{Z}} = \mathbb{Z}_n = \{[0], [1], ..., [n-1]\}$.
The number of congruence classes is $|\mathbb{Z}_n| = |\frac{\mathbb{Z}}{n\mathbb{Z}}| = n$.
Therefore, $\frac{\mathbb{Z}}{n\mathbb{Z}} = \mathbb{Z}_n$ contains exactly n congruence classes modulo n.

Let $[a] \in \frac{\mathbb{Z}}{n\mathbb{Z}}$.
Then $[a] = n\mathbb{Z} + a = \{nk + a : k \in \mathbb{Z}\}$ and $a \in \{0, 1, ..., n-1\}$.
Let $x \in [a]$.
Then $x = nk + a$ for some $k \in \mathbb{Z}$.
By the Division algorithm, when x is divided by n, then k and a are unique integers such that $0 \leq a < n$ and a is the remainder.
Hence, if $x \in [a]$, then a is the remainder when x is divided by n.

Conversely, suppose a is the remainder when x is divided by n.
Then by the Division algorithm $x = nq + a, 0 \leq a < n$ for unique $q, a \in \mathbb{Z}$.
Since $q \in \mathbb{Z}$ and $x = nq + a$, then $x \in [a]$.
Hence, if a is the remainder when x is divided by n, then $x \in [a]$.

Therefore, $x \in [a]$ iff a is the remainder when x is divided by n.

Each integer is contained in exactly one of the congruence classes. The set $\frac{\mathbb{Z}}{n\mathbb{Z}}$ is a partition of $\mathbb{Z}$ under the congruence modulo relation.
TODO Need to prove both of the above statements!

Lemma 198. ***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 $[x + y] = [x' + y']$.

Let $n \in \mathbb{Z}^+$.
Let $[a], [b] \in \mathbb{Z}_n$.
If $x, x' \in [a]$ and $y, y' \in [b]$, then $[x + y] = [x' + y']$.

Theorem 199. ***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* $\mathbb{Z}_n$.

Definition 200. Addition modulo n
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 $\mathbb{Z}_n$ called **addition modulo** n.

Let $a, b \in \mathbb{Z}$ such that $[a] + [b] = [a + b]$.
Since $a, b \in \mathbb{Z}$, then $a + b \in \mathbb{Z}$.
Since $\equiv$ is an equivalence relation on $\mathbb{Z}$, then $a + b \in [a + b]$.
Let $c = a + b$.
We know $a + b \in [c]$ iff c is the remainder when $a + b$ is divided by n.
Therefore, $[a] + [b] = [c]$ means c is the remainder when $a + b$ is divided by n.

Theorem 201. ***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* $[a] + [-a] = [-a] + [a] = [0]$.

Definition 202. Additive order of $[a]$ **modulo** n
Let $n \in \mathbb{Z}^+$.
Let $[a] \in \mathbb{Z}_n$.
The smallest positive integer k such that $k[a] = [0] \pmod{n}$ is called the **additive order of** $[a]$.

Let $n \in \mathbb{Z}^+$.
Let $[a] \in \mathbb{Z}_n$.
Since $k[a] = [a] + [a] + ... + [a] = [a + a + ... + a] = [ka] = [0] \pmod{n}$ iff $ka \equiv 0 \pmod{n}$, then the smallest positive integer k such that $ka \equiv 0 \pmod{n}$ is the additive order of $[a]$.

Lemma 203. ***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 $[xy] = [x'y']$.

Let $n \in \mathbb{Z}^+$.
Let $[a], [b] \in \mathbb{Z}_n$.
If $x, x' \in [a]$ and $y, y' \in [b]$, then $[xy] = [x'y']$.

Theorem 204. ***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* $\mathbb{Z}_n$.

Definition 205. Multiplication modulo n

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 $\mathbb{Z}_n$ called **multiplication modulo** n.

Let $a, b \in \mathbb{Z}$ such that $[a][b] = [ab]$.
Since $a, b \in \mathbb{Z}$, then $ab \in \mathbb{Z}$.
Since $\equiv$ is an equivalence relation on $\mathbb{Z}$, then $ab \in [ab]$.
Let $ab = c$.
We know $ab \in [c]$ iff c is the remainder when ab is divided by n.
Therefore, $[a][b] = [c]$ means c is the remainder when ab is divided by n.

Theorem 206. ***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* $[a], [b], [c] \in \mathbb{Z}_n$.

TODO Determine if the definition for multiplicative inverse is correct.

Definition 207. Multiplicative inverse of $[a]$ modulo n

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

Let $[a] \in \mathbb{Z}_n$.

Then $[a]$ has a **multiplicative inverse modulo** n iff there exists $[b] \in \mathbb{Z}_n$ such that $[a][b] = [1]$.

We say that $[b]$ is a multiplicative inverse of $[a]$, so $[a]$ and $[b]$ are invertible elements, or **units of** $\mathbb{Z}_n$.

Inverse of $[a]$ is denoted $[a]^{-1}$.

Theorem 208. ***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* $\gcd(a, n) = 1$.

We should prove the multiplicative inverse of $[a]$ is unique.

This would then justify the notation that the inverse of $[a]$ is denoted $[a]^{-1}$.

Corollary 209. *The inverse of* $[0]$ *in* $\mathbb{Z}_1$ *is* $[0]$.

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

If $n > 1$, *then* $[0]$ *has no multiplicative inverse.*

Definition 210. Divisor of zero modulo n

Let $[a] \in \mathbb{Z}_n$.

Then $[a]$ is a **divisor of zero modulo** n iff there exists nonzero $[b] \in \mathbb{Z}_n$ such that $[a][b] = [0]$.

If $n > 1$, then $[0]$ is a divisor of $[0]$ because $[0][n-1] = [0(n-1)] = [0]$ and $[n-1] \neq [0] \in \mathbb{Z}_n$.

Theorem 211. *Let* $n \in \mathbb{Z}^+$.

A nonzero element of $\mathbb{Z}_n$ *either has a multiplicative inverse or is a divisor of zero.*

Proposition 212. *Let* $n \in \mathbb{Z}^+$.

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

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

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

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

Suppose $[ab] = [0]$ and n is prime.

Since $[ab] = [0]$ and $[ab] = [0] \Leftrightarrow ab \equiv 0 \pmod{n} \Leftrightarrow n|(ab - 0) \Leftrightarrow n|ab$, then $n|ab$.

Since $n|ab$ and n is prime, then $n|a$ or $n|b$

Since $n|a$ and $n|a \Leftrightarrow n|a - 0 \Leftrightarrow a \equiv 0 \pmod{n} \Leftrightarrow [a] = [0]$, then $[a] = [0]$.

Since $n|b$ and $n|b \Leftrightarrow n|b - 0 \Leftrightarrow b \equiv 0 \pmod{n} \Leftrightarrow [b] = [0]$, then $[b] = [0]$.

Thus, either $[a] = [0]$ or $[b] = [0]$.

Therefore, if $[ab] = [0]$ and n is prime, then $[a] = [0]$ or $[b] = [0]$.

Definition 213. Euler totient function

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

The number of positive integers less than or equal to n which are relatively prime to n is denoted by $\phi(n)$.

This function is called **Euler's phi function**, or **totient function**.

Example values for ϕ are below.

$$\begin{aligned}
\phi(1) &= 1 \\
\phi(2) &= 1 \\
\phi(3) &= 2 \\
\phi(4) &= 2 \\
\phi(5) &= 4 \\
\phi(6) &= 2 \\
\phi(7) &= 6 \\
\phi(8) &= 4.
\end{aligned}$$

If the prime factorization of n is $n = p_1^{m_1} p_2^{m_2} ... p_k^{m_k}$, then $\phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2})...(1 - \frac{1}{p_k})$.

Need to prove this!

Proposition 214. *If p is prime, then $\phi(p) = p - 1$.*

Definition 215. Nilpotent element

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

Let $[a] \in \mathbb{Z}_n$.

Then $[a]$ is **nilpotent** iff $(\exists k \in \mathbb{Z})([a]^k = [0])$.

Definition 216. Multiplicative order of $[a]$ modulo n

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

Let $[a] \in \mathbb{Z}_n^*$.

The smallest positive integer k such that $[a]^k = [1] \pmod{n}$ is called the **multiplicative order of** $[a]$.

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

Let $[a] \in \mathbb{Z}_n^*$.

Since $[a]^k = [a] \cdot [a] \cdot ... \cdot [a] = [a \cdot a \cdot ... \cdot a] = [a^k] = [1] \pmod{n}$ iff $a^k \equiv 1 \pmod{n}$, then the smallest positive integer k such that $a^k \equiv 1 \pmod{n}$ is the multiplicative order of $[a]$.

Fermat's Theorem

Theorem 217. ***Fermat's Little Theorem***
Let $p, a \in \mathbb{Z}^+$.
If p is prime and $p \not| a$, then $p|a^{p-1} - 1$.

Let $p, a \in \mathbb{Z}^+$.
If p is prime and $p \not| a$, then $p|a^{p-1} - 1$.
Hence, if p is prime and $p \not| a$, then $a^{p-1} \equiv 1 \pmod{p}$.
Therefore, if p is prime and $p \not| a$, then $a^p \equiv a \pmod{p}$.

Theorem 218. ***Euler's Theorem***
Let $a \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$.
If $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$.

Corollary 219. ***Fermat's Little Theorem***
Let $a \in \mathbb{Z}$.
If p is prime, then $a^p \equiv a \pmod{p}$.

Miscellaneous Stuff

Proposition 220. ***Every integer is congruent modulo n to exactly one of the integers $0, 1, 2, ..., n-1$.***

Definition 221. least positive residues modulo n
Let $n \in \mathbb{Z}^+$.
The set of n integers $\{0, 1, 2, ..., n-1\}$ is called the set of **least positive residues modulo n**.

Therefore, every integer is congruent modulo n to exactly one of the integers in the set of least positive residues modulo n.

Definition 222. complete set of residues modulo n
Let $n \in \mathbb{Z}^+$.
A set of integers $S = \{a_1, a_2, ..., a_n\}$ is a **complete set(system) of residues modulo n** iff every integer is congruent modulo n to exactly one of the $a_k \in S$.

Equivalently, $S = \{a_1, a_2, ..., a_n\}$ is a complete system of residues modulo n iff each $a_k \in S$ is congruent modulo n to exactly one integer in $\{0, 1, 2, ..., n-1\}$.

Example 223. The set $\{-12, -4, 11, 13, 22, 82, 91\}$ is a complete set of residues modulo 7.

Proposition 224. ***Any set of n integers is a complete set of residues modulo n iff no two of the integers are congruent modulo n.***

Definition 225. divisors function σ_0
Let $\sigma_0 : \mathbb{Z}^+ \to \mathbb{Z}^+$ be the function defined such that $\sigma_0(n)$ is the number of positive divisors of $n \in \mathbb{Z}^+$.
We call σ_0 the **divisor function**.

Number theoretic functions.
1. π is the prime distribution function.
2. σ is the number of divisors function.
3. τ is the sum of divisors function.
4. phi is the Euler totient function.