Number Theory Notes

Jason Sass

July 17, 2023

Sets of Numbers

$\mathbb{N} = \{1, 2, 3, ...\} =$ set of all natural numbers
$\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\} =$ set of all integers
$\mathbb{Z}^+ = \{1, 2, 3, ...\} = \{n \in \mathbb{Z} : n > 0\} =$ set of all positive integers
$\mathbb{Z}^* = \{..., -3, -2, -1, 1, 2, 3, ...\} = \mathbb{Z} - \{0\} =$ set of all nonzero integers
$\mathbb{Z}^+ \cup \{0\} = \{0, 1, 2, 3, ...\} =$ set of all nonnegative integers
$n\mathbb{Z} = \{kn : k \in \mathbb{Z}\} =$ set of all multiples of integer n

Natural number system

We model the natural numbers as strings of ones.

Definition 1. one
one is a vertical stroke $|$.

Definition 2. natural number
A **natural number** is a string of ones.

Example 3. examples of natural numbers
$|$ is 'one'
$||$ is 'two'
$|||$ is 'three'
$||||$ is 'four'
$|||||$ is 'five'

Definition 4. 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 5. 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 6. 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 7. 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.

Peano Axioms for natural number system

Axiom 8. 1 *is a natural number.*

Axiom 9. ***Each natural number has a successor.***
*For every $n \in \mathbb{N}$ there exists $n' \in \mathbb{N}$ called the **successor** of n.*

Axiom 10. 1 *is not the successor of any natural number.*

Axiom 11. *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 12. ***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 13. *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 14. addition is defined in terms of successor

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 15. 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 16. $||||| + ||| = ||||||||$.
Therefore, $5 + 3 = 8$.

Theorem 17. ***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 18. 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 19. $||| \times |||| = ||||||||||||$ (three copies of four)
$|||| \times ||| = ||||||||||||$ (four copies of three)
$||| \times | = |||$ (three copies of 1)
$| \times ||| = |||$ (1 copy of three)

Theorem 20. ***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 21. 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 22. less than

Let m and n be natural numbers.

Then $m < n$ means there are some left over ones in n when the ones in m are paired with the ones in n.

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

Then $m < n$ means n is larger than m.

Example 23. 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 24. relation $<$ over $\mathbb{N}$

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

Define a relation "is less than", denoted $<$, on $\mathbb{N}$ by $a < b$ iff $(\exists c \in \mathbb{N})(a+c = b)$.

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 25. relation $>$ over $\mathbb{N}$

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

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

Definition 26. 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 27. 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 28. ***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(binary operations): addition, subtraction, multiplication, division

Axiom 29. ***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 30. ***Algebraic properties of addition and multiplication in $\mathbb{Z}$***
1. For all $a, b, c \in \mathbb{Z}$, $(a + b) + c = a + (b + c)$. Addition is associative.
2. For all $a, b \in \mathbb{Z}$, $a + b = b + a$. Addition is commutative.
3. For all $a, b, c \in \mathbb{Z}$, $(ab)c = a(bc)$. Multiplication is associative.
4. For all $a, b \in \mathbb{Z}$, $ab = ba$. Multiplication is commutative.
5. For all $a, b, c \in \mathbb{Z}$, $a(b + c) = ab + ac$. Multiplication is distributive over addition.

Proposition 31. ***Zero is additive identity in $\mathbb{Z}$***
For all $a \in \mathbb{Z}$, $a + 0 = a$.

Proposition 32. ***One is multiplicative identity in $\mathbb{Z}$***
For all $a \in \mathbb{Z}$, $1 \cdot a = a$.

Proposition 33. ***Additive inverse of a is $-a$ in $\mathbb{Z}$***
Let $a \in \mathbb{Z}$.
Then there exists $-a \in \mathbb{Z}$ such that $a + (-a) = 0$.

Definition 34. 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.

Proposition 35. ***The only integers whose product is one are one and negative one.***
Let $a, b \in \mathbb{Z}$.
If $ab = 1$, then either $a = b = 1$ or $a = b = -1$.

Proposition 36. ***Cancellation law for $\mathbb{Z}$***
Let $a, b, c \in \mathbb{Z}$.
If $c \neq 0$ and $ac = bc$, then $a = b$.

Axiom 37. ***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. $-a \in \mathbb{Z}^+$.

Trichotomy law implies $0 \notin \mathbb{Z}^+$.

Definition 38. 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.

Definition 39. 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 40. relation $>$ over $\mathbb{Z}$
Let $a, b \in \mathbb{Z}$.
Then a is larger than b, denoted $a > b$, iff $b < a$.

Definition 41. 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 42. *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 43. ***$\mathbb{Z}$ satisfies transitivity and trichotomy laws***
1. $a < a$ is false for all $a \in \mathbb{Z}$. (Therefore, $<$ is not reflexive.)
2. For all $a, b, c \in \mathbb{Z}$, if $a < b$ and $b < c$, then $a < c$. ($<$ is transitive)
3. For every $a \in \mathbb{Z}$, exactly one of the following is true (trichotomy):
i. $a > 0$
ii. $a = 0$
iii. $a < 0$
4. For every $a, b \in \mathbb{Z}$, exactly one of the following is true (trichotomy):
i. $a > b$
ii. $a = b$
iii. $a < b$

Theorem 44. ***order is preserved by the ring operations in*** $\mathbb{Z}$

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

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

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

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

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

Axiom 45. ***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, S has a least element.
Therefore, $(\exists m \in S)(\forall s \in S)(m \leq s)$.

Theorem 46. ***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 of $\mathbb{Z}^+$ is logically equivalent to the principle of mathematical induction.

Theorem 47. ***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 $S = \mathbb{Z}^+$.

Theorem 48. ***Archimedean Property of*** $\mathbb{Z}^+$

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

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

Proposition 49. *For all* $n \in \mathbb{N}$, $n \geq 1$.

Since $n \geq 1$ for all $n \in \mathbb{N}$, then $1 \leq n$ for all $n \in \mathbb{N}$, so 1 is the least positive natural number.
Hence, 1 is the least element of $\mathbb{Z}^+$.
Therefore, $1 \leq n$ for all $n \in \mathbb{Z}^+$.

Proposition 50. *There is no greatest natural number.*

Proposition 51. *Let* $a, b, c, d \in \mathbb{Z}^+$.

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

Lemma 52. *Let $a, b \in \mathbb{N}$.*
If $a < b$ then $b \not\leq a$.

Theorem 53. ***$\leq$ is a partial order on $\mathbb{Z}$***
1. *For all $a \in \mathbb{Z}$, $a \leq a$. (Reflexive)*
2. *For all $a, b \in \mathbb{Z}$, if $a \leq b$ and $b \leq a$, then $a = b$. (Anti-symmetric)*
3. *For all $a, b, c \in \mathbb{Z}$, if $a \leq b$ and $b \leq c$, then $a \leq c$. (Transitive)*

Let $a, b \in \mathbb{N}$.
Since $\mathbb{N}$ is a total order, then by defn of total order, either $a \leq b$ or $b \leq a$.
Thus, either $a < b$ or $a = b$ or $b < a$ or $b = a$.
Hence, either $a < b$ or $a = b$ or $a > b$.
Therefore, $\mathbb{N}$ satisfies the trichotomy law: either $a < b$ or $a = b$ or $a > b$.

$(\mathbb{Z}^+, \leq)$ is a total ordering that is well ordered.

Axiom 54. ***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.

Definition 55. consecutive natural numbers
The natural numbers n and $n + 1$ are said to be **consecutive**.

Proposition 56. ***No natural number exists between two consecutive natural numbers.***
Let n be a natural number.
There is no $m \in \mathbb{N}$ such that $n < m < n + 1$.

Elementary Aspects of Integers

Definition 57. 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 natural 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 58. 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 natural 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, $2 \nmid n$.
In base 10 n ends in 1,3,5,7, or 9.

Lemma 59. *Every positive integer is either even or odd.*

Lemma 60. *An integer is not both even and odd.*

Proposition 61. *A positive integer is either even or odd, but not both.*

Let $n \in \mathbb{Z}^+$.
Then either n is even or n is odd, but n is not both even and odd.

Definition 62. 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 63. consecutive integers
The integers n and $n+1$ are said to be **consecutive**.

Proposition 64. ***A product of two consecutive integers is even.***
If $n \in \mathbb{Z}$, then $n(n+1)$ is even.

Natural Number Formulae

Proposition 65. *The sum of the first n natural numbers is $\frac{n(n+1)}{2}$.*

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

Proposition 66. *The sum of the first n odd natural numbers is n^2.*

Let $k \in \mathbb{N}$.
Then $\sum_{k=1}^{n}(2k-1) = n^2$ for all $n \in \mathbb{N}$.

Proposition 67. *The sum of the squares of the first n natural numbers is $\frac{n(n+1)(2n+1)}{6}$.*

Let $k \in \mathbb{N}$.
Then $\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$ for all $n \in \mathbb{N}$.

Proposition 68. *The sum of the cubes of the first n natural numbers is $(\frac{n(n+1)}{2})^2$.*

Let $k \in \mathbb{N}$.
Then $\sum_{k=1}^{n} k^3 = (\frac{n(n+1)}{2})^2$ for all $n \in \mathbb{N}$.

Definition 69. Square Numbers
arrangement of points in a square (area is n^2)
$(\forall n \in \mathbb{Z})$ n is a **perfect square** iff $(\exists k \in \mathbb{N})(n = k^2)$.
Let k = number of dots in the side of a square, $k \geq 1$.
Let S_k = number of dots in a square with k side dots (k^{th} square number).
$S_k : \mathbb{N} \to \mathbb{N}$ (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 * side of (k-1) square + 1 corner dot.
Thus,
$S_k = S_{k-1} + 2(k-1) + 1 = S_{k-1} + 2k - 1$ and $S_1 = 1$.
S_k = number of side dots * number of side dots = k^2
Thus,
$S_n = n^{th}$ **square number**
$S_n = S_{n-1} + 2n - 1, n > 1$ and $S_1 = 1$.
$S_n = n^2$
set of square numbers = $\{n^2 : n \in \mathbb{N}\} = \{1, 4, 9, 16, 25, 36, ...\}$
sequence of square numbers = $\{S_n\} = \{n^2\}_{n=1}^{\infty} = \{1, 4, 9, 16, 25, 36, ...\}$

Definition 70. Cubic Numbers
arrange n unit cubes into a larger solid cube (volume is n^3)
$(\forall n \in \mathbb{Z})$ n is a **perfect cube** iff $(\exists k \in \mathbb{N})(n = k^3)$.
set of cubic numbers = $\{n^3 : n \in N\} = \{1, 8, 27, 64, 125, ...\}$
sequence of cubic numbers = $\{n^3\}_{n=1}^{\infty} = \{1, 8, 27, 64, 125, ...\}$

Definition 71. Triangular Numbers
triangular grid of points such that the first row has 1 element and each subsequent row contains one more element than the previous row
Let k = row in the triangular arrangement of dots, $k \geq 1$
Let T_k = the number of all dots from row 1 to row k (k^{th} triangular number)
$T_k : \mathbb{N} \to \mathbb{N}$ (maps k^{th} row to its corresponding T_k)
The k^{th} row has k dots.
k^{th} triangular number = $(k-1)$ triangular number + the number of dots in row k, so

$T_k = T_{k-1} + k, k > 1$ and $T_1 = 1$.
$T_k =$ the sum of dots in all preceding rows up to row k, so
$T_k = 1 + 2 + 3 + ... + k = \sum_{i=1}^{k} i = \frac{k(k+1)}{2}$
Thus,
$T_n = n^{th}$ **triangular number**
$T_n = T_{n-1} + n, n > 1$ and $T_1 = 1$
$T_n = \sum_{k=1}^{n} k = \frac{n(n+1)}{2} = \binom{n+1}{2}$
set of triangular numbers $= \{\frac{n(n+1)}{2} : n \in N\} = \{1, 3, 6, 10, 15, 21, ...\}$
sequence of triangular numbers $= \{T_n\} = \{\frac{n(n+1)}{2}\}_{n=1}^{\infty} = \{1, 3, 6, 10, 15, 21, ...\}$

Definition 72. Perfect Numbers
$\forall p \in \mathbb{N}, p$ is **perfect** iff p equals the sum of its positive divisors less than itself.
alternate defn: $\forall p \in \mathbb{N}, p$ is perfect iff its positive divisors add up to $2p$.
set of perfect numbers $= \{p \in \mathbb{N} : p \text{ is perfect}\} = \{6, 28, 496, 8128, ...\}$
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 73. Fibonacci Numbers
$F_n = n^{th}$ term of the **Fibonacci sequence**
$F_n = F_{n-1} + F_{n-2}, n > 2$, and $F_1 = F_2 = 1$
Fibonacci sequence $= \{F_n\}_{n=1}^{\infty} = \{1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987...\}$

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 and greatest common divisor

Definition 74. divides relation over $\mathbb{Z}$
Define the relation 'divides' over $\mathbb{Z}$ for all $a, b \in \mathbb{Z}$ by $a \mid b$ iff $(\exists n \in \mathbb{Z})(b = an)$.
The statement **'a divides b'**, denoted $a|b$, means there exists an integer n such that $b = an$.
Therefore $a|b$ iff $(\exists n \in \mathbb{Z})(b = an)$.

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

Therefore $a \nmid b$ iff $\neg(\exists n \in \mathbb{Z})(b = an)$.
Equivalent meanings for $a|b$ are:
1. b is **divisible by** a
2. a is a **divisor of** b
3. b is a **multiple of** a
4. a is a **factor of** b

Proposition 75. *Every integer divides zero.* $(\forall n \in \mathbb{Z})(n|0)$.

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

Proposition 76. *The number 1 divides every integer.* $(\forall n \in \mathbb{Z})(1|n)$.

-1 also divides every integer.

Proposition 77. *Every integer divides itself.* $(\forall n \in \mathbb{Z})(n|n)$.

Therefore $1|1$.

Proposition 78. *Let $a, b, c, d \in \mathbb{Z}$.*
If $a|b$ and $c|d$, then $ac|bd$.

Proposition 79. $(\forall a, b \in \mathbb{Z}^*)(a|b \wedge b|a \rightarrow a = \pm b)$.

Theorem 80. ***divides relation is transitive***
For any integers a, b and c, if $a|b$ and $b|c$, then $a|c$.

Theorem 81. *The divides relation defined on $\mathbb{Z}^+$ is a partial order.*

Therefore, the set of all positive integers is partially ordered under the divides relation, so $(\mathbb{Z}^+, |)$ is a poset.
This means
1. reflexive $(\forall a \in \mathbb{Z}^+)(a|a)$.
2. antisymmetric $(\forall a, b \in \mathbb{Z}^+)(a|b \wedge b|a \rightarrow a = b)$.
3. transitive $(\forall a, b, c \in \mathbb{Z}^+)(a|b \wedge b|c \rightarrow a|c)$.

Proposition 82. *Let $a, b \in \mathbb{Z}^+$.*
If $a|b$, then $a \leq b$.

Proposition 83. *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 84. *Let $a, b, n \in \mathbb{Z}$.*
1. If $a|b$, then $na|nb$.
2. If $n \neq 0$, then $na|nb$ implies $a|b$.

Theorem 85. ***Division Algorithm***
Let $a, b \in \mathbb{Z}$ with $b > 0$.
Then there exist unique integers q and r such that $a = bq+r$, with $0 \leq r < b$.

This is just long division from arithmetic (division by zero is not defined).
We divide a by b.
If $r = 0$, then b divides a, so a is divisible by b.
a = dividend
b = divisor
q = quotient
r = remainder

Definition 86. common divisor
Let $a, b \in \mathbb{Z}$.
Then $d \in \mathbb{Z}$ is a **common divisor** of a and b iff $d|a$ and $d|b$.

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

1 is a common positive divisor for any $a, b \in \mathbb{Z}$.

A positive common divisor d is bounded: $1 \leq d \leq min(a, b)$.

Definition 87. linear combination
Let $a, b \in \mathbb{Z}$.
Then $c \in \mathbb{Z}$ is a **linear combination of** a **and** b iff $(\exists m, n \in \mathbb{Z})(c = ma + nb)$.

Theorem 88. ***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 89. *Let $a, b, d \in \mathbb{Z}$.*
If $d|a$ and $d|b$, then $d|(a + b)$ and $d|(a - b)$.

Corollary 90. ***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 91. greatest common divisor
The greatest common divisor is the largest positive common divisor of two integers not both zero.
Let $a, b \in \mathbb{Z}^*$.
Let $d \in \mathbb{Z}^+$.
Then d is a **gcd of** a **and** b iff
1. $d|a$ and $d|b$. (d is a common divisor)
2. For every $c \in \mathbb{Z}$, if $c|a$ and $c|b$, then $c|d$. (Any common divisor of a and b divides $\gcd(a, b)$.)

The greatest common divisor of a and b is denoted $\gcd(a,b)$ or (a,b).
The $\gcd(0,0)$ is undefined.
The greatest common divisor is a positive integer.

Theorem 92. ***existence and uniqueness of greatest common divisor***
Let $a,b \in \mathbb{Z}^*$.
Then $\gcd(a,b)$ exists and is unique.
Moreover, $\gcd(a,b)$ is the least positive linear combination of a and b.

Let $a,b \in \mathbb{Z}^*$.
Then $\gcd(a,b)$ is the least positive linear combination of a and b.
Let $S = \{ma + nb : ma + nb > 0, m, n \in \mathbb{Z}\}$.
Then $\gcd(a,b)$ is the least element of S and there exist integers m and n such that $\gcd(a,b) = ma + nb$.

Proposition 93. ***Properties of gcd***
Let $a,b \in \mathbb{Z}^+$.
Then
1. $\gcd(a,0) = a$.
2. $\gcd(a,1) = 1$.
3. $\gcd(a,a) = a$.
4. $\gcd(a,b) = \gcd(b,a)$.
5. $\gcd(a,b) = \gcd(-a,b) = \gcd(a,-b) = \gcd(-a,-b)$.
6. $\gcd(ka,kb) = k\gcd(a,b)$ *for all* $k \in \mathbb{Z}^+$.

Theorem 94. *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 95. *Let $a,b \in \mathbb{Z}^*$.*
Then $\gcd(a,b) = 1$ iff there exist $m,n \in \mathbb{Z}$ such that $ma + nb = 1$.

Corollary 96. *Let $a,b \in \mathbb{Z}^*$ and $d \in \mathbb{Z}^+$.*
If $\gcd(a,b) = d$, then $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$.

Definition 97. 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 $ma + nb = 1$.

Theorem 98. *Let $a, b, d \in \mathbb{Z}$.*

If $d|ab$ and $(d, a) = 1$, then $d|b$.

Proposition 99. *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

The Euclidean algorithm specifies how to compute $\gcd(a, b)$ for integers a and b.

Lemma 100. *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 101. ***Euclidean Algorithm***

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

Let n be the number of iterative steps and

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

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

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

To compute $\gcd(a, b)$, we 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 102. Let $a, b \in \mathbb{Z}$.

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

Definition 103. least common multiple

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

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

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

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

1. $a|m$ and $b|m$. (m is a common multiple)

2. For every $c \in \mathbb{Z}$, if $a|c$ and $b|c$, then $m|c$. (Any multiple of a and b is a multiple of $lcm(a, b)$).

Theorem 104. ***existence and uniqueness of least common multiple***

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

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

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

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

We denote the least common multiple of a and b by $lcm(a, b)$ or $[a, b]$.

Corollary 105. *Let $a, b \in \mathbb{Z}^+$.*

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

Proposition 106. ***Properties of lcm***

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

Then

1. $lcm(a, 0) = 0$.

2. $lcm(a, 1) = a$.

3. $lcm(a, a) = a$.

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

5. $lcm(ka, kb) = k \cdot lcm(a, b)$ for all $k \in \mathbb{Z}^+$.

6. $\gcd(a, b) \mid lcm(a, b)$.

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

8. $a|b$ iff $\gcd(a, b) = a$ iff $lcm(a, b) = b$.

Prime Numbers and Fundamental Theorem of Arithmetic

Definition 107. 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 $p \in \mathbb{Z}^+$.
Then $1|p$ and $p|p$.
Suppose p is prime.
Then $p \neq 1$ and the only positive divisors of p are 1 and p.
Since $p \in \mathbb{Z}^+$ and $p \neq 1$, then $p > 1$.
Since the only positive divisors of p are 1 and p, then the set of common positive divisors of p is $\{1, p\}$.

The set of prime numbers is $\{n \in \mathbb{Z}^+ : n \text{ is prime}\} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, ...\}$

Definition 108. composite number
A positive integer other than 1 is **composite** iff it is not prime.

The number 1 is neither prime nor composite.

The set of composite numbers is $\{n \in \mathbb{Z}^+ : n \text{ is composite}\} = \{4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, ...\}$.

Let $n \in \mathbb{Z}^+$.
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 109. ***A composite number has a positive divisor other than 1 or itself.***
Let $n \in \mathbb{Z}^+$.
Then n is composite iff there exists $d \in \mathbb{Z}^+$ with $1 < d < n$ such that $d|n$.

Proposition 110. ***A composite number is composed of smaller positive factors.***
Let $n \in \mathbb{Z}^+$.
Then n is composite iff there exist $a, b \in \mathbb{Z}^+$ with $1 < a < n$ and $1 < b < n$ such that $n = ab$.

Proposition 111. *Every integer greater than 1 has a prime factor.*

Theorem 112. ***Euclid's Theorem***
There are infinitely many prime numbers.

Lemma 113. *Let $p, n \in \mathbb{Z}^+$.*
If p is prime, then either $p|n$ or $\gcd(p, n) = 1$.

Therefore, if p is prime and $p \nmid n$, then $\gcd(p, n) = 1$.
In particular, if n is a distinct prime, then $\gcd(p, n) = 1$.
Therefore, any distinct primes are relatively prime.

Lemma 114. ***Euclid's Lemma***

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

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

Corollary 115. *Let $p, a_1, a_2, ..., a_n \in \mathbb{Z}^+$.*

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

Corollary 116. *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 $1 \leq k \leq n$.

Theorem 117. ***Fundamental Theorem of Arithmetic(Existence)***

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

Theorem 118. ***Fundamental Theorem of Arithmetic(Unique Factorization)***

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

Example 119. Observe that $360 = 2 \cdot 3 \cdot 5 \cdot 2 \cdot 2 \cdot 3 = 3 \cdot 2 \cdot 5 \cdot 2 \cdot 3 \cdot 2 = 5 \cdot 2 \cdot 3 \cdot 3 \cdot 2 \cdot 2$.

While they differ only in the order of the factors, they are the same prime factorization of 360.

Corollary 120. ***Every integer greater than one has a unique canonical prime factorization***

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

Example 121. The canonical prime factorization of 360 is $360 = 2^3 \cdot 3^2 \cdot 5$.

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.

Linear Diophantine Equations

Definition 122. Diophantine equation

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

Definition 123. Linear Diophantine equation

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

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 124. ***Existence of a solution to linear Diophantine equation***
Let $a, b, c \in \mathbb{Z}$ with $a \neq 0$ and $b \neq 0$.

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

Corollary 125. ***Characterization of solution to linear Diophantine equation***
Let $a, b, c \in \mathbb{Z}$ with $a \neq 0$ and $b \neq 0$.

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

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 solution, then the solution set is $\{(x_0 + (\frac{b}{d})t, y_0 - (\frac{a}{d})t) \in \mathbb{Z} \times \mathbb{Z} : t \in \mathbb{Z}\}$.

If $\gcd(a, b) = 1$, then $x = x_0 + (\frac{b}{1})t = x_0 + bt$ and $y = y_0 - (\frac{a}{1})t = y_0 - at$.

Congruences

Definition 126. congruence modulo relation over $\mathbb{Z}$
Let $n \in \mathbb{Z}^+$.

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

Since $R \subset \mathbb{Z} \times \mathbb{Z}$, then R is 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 127. *Let $n \in \mathbb{Z}^+$.*

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

Then $a \equiv b \pmod{n}$ if and only if a and b leave the same remainder when divided by n.

Theorem 128. *The congruence modulo relation is an equivalence relation over $\mathbb{Z}$.*

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

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

1. reflexive $a \equiv a \pmod{n}$.
2. symmetric $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$.
3. transitive $a \equiv b \pmod{n} \wedge b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$.

Theorem 129. *Let $n \in \mathbb{Z}^+$.*
Let $a, b, c, d \in \mathbb{Z}$.
If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then
1. $a + c \equiv b + d \pmod{n}$ (addition)
2. $a - c \equiv b - d \pmod{n}$ (subtraction)
3. $ac \equiv bd \pmod{n}$. (multiplication)

Theorem 130. *Let $n \in \mathbb{Z}^+$.*
Let $a, b \in \mathbb{Z}$.
1. If $a \equiv b \pmod{n}$, then $a + c \equiv b + c \pmod{n}$ for all $c \in \mathbb{Z}$. (addition preserves congruence)
2. If $a \equiv b \pmod{n}$, then $ac \equiv bc \pmod{n}$ for all $c \in \mathbb{Z}$. (multiplication preserves congruence)
3. If $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$ for all $k \in \mathbb{Z}^+$. (exponentiation preserves congruence)

Theorem 131. *Let $n \in \mathbb{Z}^+$.*
Let $a, b, c \in \mathbb{Z}$.
1. If $a + c \equiv b + c \pmod{n}$, then $a \equiv b \pmod{n}$. (cancellation addition)
2. If $ac \equiv bc \pmod{n}$ and $d = \gcd(n, c)$, then $a \equiv b \pmod{\frac{n}{d}}$. (cancellation multiplication)

Corollary 132. *Let $n \in \mathbb{Z}^+$.*
Let $a, b, c \in \mathbb{Z}$.
If $ac \equiv bc \pmod{n}$ and $\gcd(n, c) = 1$, then $a \equiv b \pmod{n}$. (cancellation multiplication relatively prime)

Corollary 133. *Let $p \in \mathbb{Z}^+$.*
Let $a, b, c \in \mathbb{Z}$.
If $ac \equiv bc \pmod{p}$ and p is prime and $p \nmid c$, then $a \equiv b \pmod{p}$. (cancellation multiplication prime modulus)

Proposition 134. *Let $n \in \mathbb{Z}^+$.*
Let $a, b, c \in \mathbb{Z}$.
If $c \neq 0$, then $ac \equiv bc \pmod{nc}$ iff $a \equiv b \pmod{n}$.

Definition 135. Inverse modulo
Let $n \in \mathbb{Z}^+$ be the modulus.
Let $a \in \mathbb{Z}^+$.
Then a is invertible modulo n iff $(\exists b \in \mathbb{Z})(ab \equiv 1 \pmod{n})$.

Let $a \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$.
Then a is invertible modulo n iff there exists $b \in \mathbb{Z}$ such that $ab \equiv 1 \pmod{n}$ and we say that b is a (multiplicative) inverse of a.

Proposition 136. *Let $n \in \mathbb{Z}^+$.*
Let $a \in \mathbb{Z}^+$.
Then a is invertible modulo n iff $\gcd(a, n) = 1$.

Let $a \in \mathbb{Z}$ and $n \in \mathbb{N}$.
The multiplicative inverse of a modulo n exists if and only if $\gcd(a, n) = 1$.
The inverse of a is unique modulo n.

Linear Congruences

Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$.
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 137. *Let $a, b, x, x_0 \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$.*
If x_0 is a solution to $ax \equiv b \pmod{n}$, then so is $x_0 + nk$ for any integer k.

Definition 138. A solution x of a congruence is **unique modulo** n iff any solution x' is congruent to x modulo n.

Theorem 139. ***Existence of solution to linear congruence***
Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$.
A solution exists to the linear congruence $ax \equiv b \pmod{n}$ if and only if $d|b$, where $d = \gcd(a, n)$.
Moreover, if a solution exists, then there are d distinct solutions modulo n and these solutions are congruent modulo $\frac{n}{d}$.

Corollary 140. *Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$.*
There exists an integer b such that $ab \equiv 1 \pmod{n}$ if and only if $\gcd(a, n) = 1$.
Moreover, b is the inverse of a and the inverse of a is unique modulo n.

Integers Modulo n

Definition 141. Congruence class
Let $n \in \mathbb{Z}^+$.
Let $a \in \mathbb{Z}$.
The **congruence class containing** a, denoted $[a]$, is the set of all integers congruent to a modulo n.
Therefore $[a] = \{x \in \mathbb{Z} : x \equiv a \pmod{n}\}$.

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

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.

Since the remainders upon dividing by n are $0, 1, ..., n-1$, then every integer must be congruent to exactly one of the remainders: 0,1,.., n-1.

Definition 142. Integers Modulo n

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

The collection of all congruence classes modulo n is the **set of integers modulo** n, denoted $\frac{\mathbb{Z}}{n\mathbb{Z}}$ or $\mathbb{Z}_n$.

Therefore, $\mathbb{Z}_n = \frac{\mathbb{Z}}{n\mathbb{Z}} = \{[a]_n : a \in \mathbb{Z}\} = \{[0], [1], [2], ..., [n-1]\}$.

The set $\frac{\mathbb{Z}}{n\mathbb{Z}}$ is a partition of $\mathbb{Z}$ under the congruence modulo relation.

The number of congruence classes is $|\mathbb{Z}_n| = |\frac{\mathbb{Z}}{n\mathbb{Z}}| = n$.

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, k and a are unique integers such that $0 \leq a < n$.

Thus, a is the remainder when x is divided by n.

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.

In $\frac{\mathbb{Z}}{n\mathbb{Z}}$:

additive identity is $[0]$.

additive inverse of $[a]$ is $-[a] = [n-a]$.

multiplicative identity is $[1]$.

$[n] = [0]$.

$(\frac{\mathbb{Z}}{n\mathbb{Z}}, +)$ is an abelian group.
$(\frac{\mathbb{Z}}{n\mathbb{Z}}, +, \cdot)$ is a commutative ring with unity $[1]$.

Lemma 143. ***addition modulo n is well-defined***
Let $[a], [b] \in \mathbb{Z}_n$.
Let $x, x' \in [a]_n$ and $y, y' \in [b]_n$.
Then $[x + y] = [x' + y']$.

Proposition 144. ***Addition modulo n is a binary operation.***
Let $+_n : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ be a binary relation defined by $[a] + [b] = [a + b]$ for all $[a], [b] \in \mathbb{Z}_n$.
Then $+_n$ is a binary operation on $\mathbb{Z}_n$.

Definition 145. Addition modulo n
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 146. ***algebraic properties of addition modulo n***
1. $[a] + ([b] + [c]) = ([a] + [b]) + [c]$ for all $[a], [b], [c] \in \mathbb{Z}_n$.(associative)
2. $[a] + [b] = [b] + [a]$ for all $[a], [b] \in \mathbb{Z}_n$.(commutative)
3. $[a] + [0] = [0] + [a] = [a]$ for all $[a] \in \mathbb{Z}_n$. (additive identity)
4. $[a] + [-a] = [-a] + [a] = [0]$ for all $[a] \in \mathbb{Z}_n$. (additive inverses)

Definition 147. 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 $[a]$.

Proposition 148. ***Multiplication modulo n is a binary operation.***
Let $*_n : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ be a binary relation defined by $[a][b] = [ab]$ for all $[a], [b] \in \mathbb{Z}_n$.
Then $*_n$ is a binary operation on $\mathbb{Z}_n$.

Definition 149. Multiplication modulo n

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 150. ***algebraic properties of multiplication modulo*** n

1. *$[a]([b][c]) = ([a][b])[c]$ for all $[a], [b], [c] \in \mathbb{Z}_n$. (associative)*
2. *$[a][b] = [b][a]$ for all $[a], [b] \in \mathbb{Z}_n$. (commutative)*
3. *$[a][1] = [1][a] = [a]$ for all $[a] \in \mathbb{Z}_n$. (multiplicative identity)*
4. *$[a][0] = [0][a] = [0]$ for all $[a] \in \mathbb{Z}_n$.*
5. *$[a]([b] + [c]) = [a][b] + [a][c]$ for all $[a], [b], [c] \in \mathbb{Z}_n$. (left distributive)*
6. *$([a] + [b])[c] = [a][c] + [b][c]$ for all $[a], [b], [c] \in \mathbb{Z}_n$. (right distributive)*

Definition 151. 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 152. ***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 $\gcd(a, n) = 1$.

Corollary 153. *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 154. 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 155. *Let $n \in \mathbb{Z}^+$.*
A nonzero element of $\mathbb{Z}_n$ either has a multiplicative inverse or is a divisor of zero.

Definition 156. 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 157. *If p is prime, then $\phi(p) = p - 1$.*

Definition 158. 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 159. 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 160. ***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 161. *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 162. *Fermat's Little Theorem*
Let $a \in \mathbb{Z}$.
If p is prime, then $a^p \equiv a \pmod{p}$.

Miscellaneous Stuff

Proposition 163. *Every integer is congruent modulo n to exactly one of the integers $0, 1, 2, ..., n-1$.*

Definition 164. 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 165. 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 166. The set $\{-12, -4, 11, 13, 22, 82, 91\}$ is a complete set of residues modulo 7.

Proposition 167. *Any set of n integers is a complete set of residues modulo n iff no two of the integers are congruent modulo n.*

Definition 168. 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**.