Haskell Notes

Jason Sass

September 8, 2026

Haskell is

Definition 1. number
A **number** is an arithmetic value used to represent a quantity.
A number is a mathematical concept that is used to count and measure.

Construction of the natural number system

Definition 2. one
One is a quantity modeled as a vertical stroke |.

One is a **unit** of measure.

Definition 3. natural number
A **natural number** is a quantity that is modeled as a string of vertical strokes.

Let n be a natural number.
Then n can be viewed as a string of vertical strokes.
Since one can be viewed as a vertical stroke, then n can be viewed as a string of ones.
Therefore, any natural number can be viewed as a string of ones.
Observe that 1 is a natural number.

Definition 4. 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 $1, 2, 3, 4, 5, 6, 7, ...$
Note: The ellipses after 7, means 'continues in the same manner'.
It does not mean there are infinitely many natural numbers!

Since 1 measures each natural number exactly, the unit 1 is a factor of every natural number.

Therefore, 1 divides every natural number, so $1|n$ for every natural number n.

Definition 5. equal natural numbers

Let a and b be natural numbers.

Then a **equals** b, denoted $a = b$, if and only if all of the ones of a can be paired up with all of the ones of b via a one to one correspondence.

Theorem 6. ***Equality of natural numbers is an equivalence relation.***

Let a, b, and c be natural numbers.

1. Equality is reflexive.

For any natural number $n, n = n$.

2. Equality is symmetric.

For any natural numbers a and b, if $a = b$, then $b = a$.

3. Equality is transitive.

For any natural numbers a, b, and c, if $a = b$ and $b = c$, then $a = c$.

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

Definition 7. addition

Let a and b be natural numbers.

The **sum of** a **and** b, denoted $a + b$, is the concatenation of the ones of b to the ones of a.

The numbers that are added are called **addends**.

Therefore, a and b are addends of the sum $a + b$.

Theorem 8. ***laws of addition of natural numbers***

1. The natural numbers are closed under addition.

The sum of natural numbers is a natural number.

If a and b are any natural numbers, then $a + b$ is a natural number.

2. Addition is commutative.

For any natural numbers a and b, $a + b = b + a$.

3. Addition is associative.

For any natural numbers a, b, and c, $(a + b) + c = a + (b + c)$.

Multiplication is repeated addition.

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

Definition 9. multiplication

Let a and b be natural numbers.

The **product of** a **and** b, denoted ab, is the string formed by a copy of the ones of b for every vertical stroke of a.

Let a and b be natural numbers.

Then ab is a copies of b.

Theorem 10. ***laws of multiplication of natural numbers***

1. The natural numbers are closed under multiplication.
The product of natural numbers is a natural number.
If a and b are any natural numbers, then ab is a natural number.
2. Multiplication is commutative.
For any natural numbers a and b, $ab = ba$.
3. Multiplication is associative.
For any natural numbers a, b, and c, $(ab)c = a(bc)$.
4. One is multiplicative identity.
For any natural number n, $n \cdot 1 = n$.

Theorem 11. ***distributive law of multiplication over addition***

For any natural numbers a, b, and c, $a(b + c) = ab + ac$.

Definition 12. larger natural number

Take two natural numbers and pair the corresponding ones.
The natural number which has any left over ones is larger.

Definition 13. is less than

Let a and b be natural numbers.
Then a is less than b, denoted $a < b$, iff there are some left over ones in b when the ones in a are paired with the ones in b.

Let a and b be natural numbers.
Then a is less than b, denoted $a < b$, iff b is larger than a.

Definition 14. relation $<$ over the natural numbers

Let a and b be natural numbers.
Then 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 a and b be natural numbers.
Then $a < b$ indicates that a comes before b in the sequence of natural numbers.

Definition 15. relation $>$ over the natural numbers

Let a and b be natural numbers.
Then a **is greater than** b, denoted $a > b$, iff $b < a$.

Definition 16. relation $\leq$ over the natural numbers

Let a and b be natural numbers.
Then a **is less than or equal to** b, denoted $a \leq b$, iff either $a < b$ or $a = b$.

Definition 17. relation $\geq$ over the natural numbers

Let a and b be natural numbers.

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

Theorem 18. ***The relation $<$ over the natural numbers is transitive.***

For any natural numbers a, b, and c, if $a < b$ and $b < c$, then $a < c$.

Proposition 19. *There is no greatest natural number.*

Proposition 20. ***adding inequalities***

Let a, b, c, and d be natural numbers.

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

Proposition 21. ***multiplying inequalities***

Let a, b, c, and d be natural numbers.

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

Definition 22. subtraction

Let a and b be natural numbers and $a > b$.

The **difference between** a **and** b, denoted $a - b$, is the removal of the ones of b from the ones of a.

The number a is called the **minuend**.

The number b is called the **subtrahend**.

Subtraction of natural numbers is defined only if the minuend is larger than the subtrahend.

Theorem 23. ***Addition and subtraction are inverse operations.***

Let a, b, and c be natural numbers.

Then $a + b = c$ if and only if $c - b = a$.

Principle of Mathematical Induction

If n is any natural number, then $n + 1$ is a natural number.

Hence, we can always add one to any natural number, beginning with one. (counting)

Since 1 is a natural number, then $1+1 = 2$ is a natural number, and $2+1 = 3$ is a natural number, and $3 + 1 = 4$ is a natural number, and $4 + 1 = 5$ is a natural number, and $5 + 1 = 6$ is a natural number.

We may continue this process indefinitely in this manner.

The principle of mathematical induction formalizes this idea to prove statements about all natural numbers.

Theorem 24. ***Principle of Mathematical Induction***

Let $p(n)$ be a predicate defined over the natural numbers.

Suppose

1. $p(1)$ is true (basis), and

2. For any natural number k, if $p(k)$ is true, then $p(k+1)$ is true. (induction hypothesis)

Then $p(n)$ is true for any natural number n.

Theorem 25. ***Principle of Mathematical Induction(strong)***

Let $p(n)$ be a predicate defined over the natural numbers.

Suppose

1. $p(1)$ is true (basis), and

2. For any natural number k, if $p(1), p(2), ...,$ and $p(k)$ are all true, then $p(k+1)$ is true. (induction hypothesis)

Then $p(n)$ is true for any natural number n.

Construction of the integer number system

Let a and b be natural numbers.

If $a > b$, then the difference $a - b$ is a natural number.

If $a \leq b$, then $a - b$ is not a natural number.

Hence, if $a \leq b$, then $a - b$ is not defined for natural numbers.

Since we want to be able to subtract any two whole numbers, we extend the natural numbers to include new numbers zero and negative numbers.

This allows us to define subtraction to include zero and negative numbers.

The result is the system of integers.

TODO We must ensure the new larger system of integers is compatible with any old theorems of the natural numbers.

TODO We should define division of integers, too and that ties into the division algorithm.

Definition 26. zero

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

Observe that zero is not a natural number.

Proposition 27. *For any natural number n, $n - n = 0$.*

Proposition 28. *For any natural number n, $n - 0 = n$.*

Proposition 29. *For any natural number n, $n + 0 = n$.*

Proposition 30. *For any natural number n, $n \cdot 0 = 0$.*

Definition 31. negative of a natural number

Let n be a natural number.

The **negative of** n, denoted $-n$, is $0 - n$.

Let n be a natural number.

The negative of n is $-n$ and $-n = 0 - n$.

Definition 32. integer

An **integer** is defined to be exactly one of: a natural number, the negative of a natural number, or zero.

Let n be an integer.
Then n is exactly one of the following:
1. n is a natural number, or
2. n is the negative of a natural number, or
3. $n = 0$.
The integers are $..., -4, -3, -2, -1, 0, 1, 2, 3, 4, ...$

Observe that every natural number is an integer.

Let n be a natural number.
Since n is a natural number and 0 is not a natural number, then $n \neq 0$.
Since n is a natural number and $-n$ is not a natural number, then $n \neq -n$.
Since 1 is a natural number, then $1 \neq 0$.
Since 1 is a natural number and -1 is not a natural number, then $1 \neq -1$.

Definition 33. positive integer
A **positive integer** is a natural number.

Let n be a positive integer.
Then n is a natural number.
The positive integers are $1, 2, 3, 4, 5, ...$
Since zero is not a natural number, then zero is not a positive integer.

Definition 34. non-zero integer
A **non-zero integer** is an integer that is not zero.

Let n be a non-zero integer.
Then n is an integer and $n \neq 0$.
Therefore, either n is a natural number or n is the negative of a natural number.
The non-zero integers are $1, -1, 2, -2, 3, -3, 4, -4, 5, -5, ...$

Definition 35. 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 $0, 1, 2, 3, 4, 5, ...$

Definition 36. multiple of an integer
A **multiple of an integer** n is an integer nk for some integer k.

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

There are four integer arithmetic operations: addition, subtraction, multiplication, and division.

Since the natural numbers are closed under addition, to extend and ensure consistency of our number system, we also want the integers to be closed under addition.

Therefore, we assume the integers are closed under addition.

TODO We must define integer addition precisely!

Axiom 37. ***The integers are closed under addition.***

The sum of integers is an integer.

For any integers a and b, $a + b$ is an integer.

Let a and b be integers.

Then the sum $a + b$ is an integer and the sum $a + b$ is unique.

TODO Prove the sum of two integers is unique somewhere after we cover trichotomy property.

TODO We should prove the negative of a natural number is unique. This ties into the idea of additive inverse is unique, so combine these ideas.

Theorem 38. ***algebraic properties of integer addition***

1. Addition is associative.

For every integer a, b and c, $(a + b) + c = a + (b + c)$.

2. Addition is commutative.

For every integer a and b, $a + b = b + a$.

3. Additive identity is zero.

For every integer a, $a + 0 = 0 + a = a$.

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

For every integer a there is an integer $-a$ such that $a + (-a) = 0$.

Since $0 + 0 = 0$, then 0 is the additive inverse of 0.

Therefore, $-0 = 0$.

Lemma 39. *For any integer n, if n is the negative of a natural number, then $-n$ is a positive integer.*

Theorem 40. ***Trichotomy law***

For every integer n exactly one of the following statements is true:

i. n is a positive integer.

ii. $n = 0$.

iii. $-n$ is a positive integer.

Since 0 is an integer and $0 = 0$, then by trichotomy, 0 is not a positive integer.

Since 1 is a natural number, then 1 is a positive integer.

Theorem 41. ***The positive integers are closed under addition.***

A sum of positive integers is a positive integer.

If a and b are any positive integers, then $a + b$ is a positive integer.

Definition 42. integer subtraction

Let a and b be integers.

Define $a - b = a + (-b)$.

Then $a - b$ is the **difference** between a and b.

Theorem 43. ***The integers are closed under subtraction.***
For any integers a and b, $a - b$ is an integer.

Let a and b be integers.
Since the sum of two integers is unique, then $a + (-b) = a - b$ is unique.
Hence, the difference $a - b$ is unique.
Therefore, if a and b are any integers, then the difference $a - b$ is a unique integer.

Axiom 44. ***The integers are closed under multiplication.***
For any integers a and b, ab is an integer.

Let a and b be integers.
Then the product ab is an integer and the product ab is unique.
TODO Prove the product is unique.

Theorem 45. ***algebraic properties of integer multiplication***
1. Multiplication is associative.
For every integer $a, b,$ and c, $(ab)c = a(bc)$.
2. Multiplication is commutative.
For every integer a and b, $ab = ba$.
3. Multiplicative identity is one.
For every integer a, $a \cdot 1 = 1 \cdot a = a$.
4. Multiplication by zero.
For every integer a, $a0 = 0a = 0$.
5. Multiplication is distributive over addition.
For every integer $a, b,$ and c, $a(b + c) = ab + ac$. (left distributive law)
For every integer $a, b,$ and c, $(b + c)a = ba + ca$. (right distributive law)

Theorem 46. ***The positive integers are closed under multiplication.***
A product of positive integers is a positive integer.
If a and b are any positive integers, then ab is a positive integer.

Definition 47. relation $<$ over the integers
Let a and b be any integers.
Define a relation "is less than", denoted $<$, on the integers by $a < b$ iff $b - a$ is a positive integer.

Let a and b be any integers.
Then $a < b$ iff $b - a$ is a positive integer.

Proposition 48. ***Zero is less than one.***
$0 < 1$.

Definition 49. relation $\leq$ over the integers
Let a and b be any integers.
Then a **is less than or equal to** b, denoted $a \leq b$, iff either $a < b$ or $a = b$.

Definition 50. relation $>$ over the integers

Let a and b be any integers.

Then a **is greater than** b, denoted $a > b$, iff $b < a$.

Definition 51. relation $\geq$ over the integers

Let a and b be any integers.

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

Definition 52. negative integer

A **negative integer** is an integer that is less than zero.

Let n be a negative integer.

Then n is an integer and $n < 0$.

The negative integers are $-1, -2, -3, -4, -5, ...$

Proposition 53. ***positive integers and order relation***

1. For every integer n, $n > 0$ iff n is a positive integer.

2. For every integer n, $n < 0$ iff $-n$ is a positive integer.

3. For all integers a and b, $a < b$ iff $b - a > 0$.

Let n be a positive integer.

Then n is a natural number, and n is an integer and $n > 0$.

Let n be a negative integer.

Then n is an integer and $n < 0$, so $-n$ is a positive integer.

Therefore, if n is a negative integer, then $-n$ is a positive integer.

Theorem 54. ***The integers satisfy transitivity and trichotomy laws.***

1. $n < n$ is false for any integer n.

2. $<$ is transitive.

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

3. For any integer n, exactly one of the following is true (trichotomy):

i. $n > 0$

ii. $n = 0$

iii. $n < 0$

4. For any integers a and b, exactly one of the following is true (trichotomy):

i. $a > b$

ii. $a = b$

iii. $a < b$

Since $a < a$ is false for any integer a, then $<$ is not reflexive.

Let n be any integer.

Then exactly one of the following is true: $n > 0$ or $n = 0$ or $n < 0$.

Hence, exactly one of the following is true: n is a positive integer or n is zero or n is a negative integer.

Therefore, an integer is exactly one of the following: a positive integer, zero, or a negative integer.

Consequently, an integer can be classified as exactly one of : positive integer, zero, or negative integer.

Theorem 55. ***order relation rules with ring operations in the integers***

Let a and b be integers.
1. Addition preserves order.
If $a < b$, then $a + c < b + c$ for any integer c.
2. Subtraction preserves order.
If $a < b$, then $a - c < b - c$ for any integer c.
3. Multiplication by a positive integer preserves order.
If $a < b$, then $ac < bc$ for any positive integer c.
4. Multiplication by a negative integer reverses order.
If $a < b$, then $ac > bc$ for any negative integer c.

TODO Add some propositions to justify how to compute addition of integers, both positive and negative.

Theorem 56. ***multiplication with positive and negative integers***
Let a and b be integers.
1. The product of two positive integers is a positive integer.
If $a > 0$ and $b > 0$, then $ab > 0$.
2. The product of a positive and a negative integer is a negative integer.
If $a > 0$ and $b < 0$, then $ab < 0$.
3. The product of two negative integers is a positive integer.
If $a < 0$ and $b < 0$, then $ab > 0$.
4. If a product of two factors is positive, then the factors are both positive or both negative.
If $ab > 0$, then either $a > 0$ and $b > 0$, or $a < 0$ and $b < 0$.
5. If a product of two factors is negative, then one factor is positive and the other factor is negative.
If $ab < 0$, then either $a > 0$ and $b < 0$, or $a < 0$ and $b > 0$.

Theorem 57. ***multiplicative property of zero***
Let a and b be integers.
Then $ab = 0$ iff $a = 0$ or $b = 0$.

Let a and b be integers.
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 58. ***cancellation law for integers***
Let a, b, and k be integers.
If $ak = bk$ and $k \neq 0$, then $a = b$.

Theorem 59. *The relation $\leq$ is a partial order over the integers.*

Therefore,
1. $\leq$ is reflexive.
For any integer a, $a \leq a$.
2. $\leq$ is anti-symmetric.
For any integers a and b, if $a \leq b$ and $b \leq a$, then $a = b$.
3. $\leq$ is transitive.
For any integers a, b, and c, if $a \leq b$ and $b \leq c$, then $a \leq c$.

Since $\leq$ is a partial order over the integers, then the integers are partially ordered under the $\leq$ relation.

Corollary 60. *The relation $\leq$ is a total order over the integers.*

Since $\leq$ is a total order over the integers, then any two integers are comparable.
Therefore, either $a \leq b$ or $b \leq a$ for any integers a and b.

Since every positive integer is an integer, and the integers are totally ordered under the $\leq$ relation, then the positive integers are totally ordered under the $\leq$ relation.

Archimedean property of positive integers

Lemma 61. ***Any positive integer is greater than or equal to one.***
For any positive integer n, $n \geq 1$.

Since $n \geq 1$ for any positive integer n, then $1 \leq n$ for any positive integer n, so 1 is the least positive integer.
Therefore, there is no positive integer less than 1.

Lemma 62. *For any integers a and b, if $a > b$, then $a \geq b + 1$.*

Therefore, for any integers a and b, if $a < b + 1$, then $a \leq b$.

Theorem 63. ***well-ordering principle of natural numbers***
Every nonempty set of positive integers has a least element.

Let S be a nonempty set of positive integers.
Then S is a set of positive integers and S is not empty.
Hence, by WOP(well-ordering principle), S has a least element.
Therefore, $(\exists m \in S)(\forall s \in S)(m \leq s)$.
Consequently, any nonempty set of positive integers under the $\leq$ relation is well-ordered.
Therefore, every non-empty set of positive integers is well-ordered.

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

Corollary 64. *Every nonempty set of non-negative integers has a least element.*

Let S be a nonempty set of non-negative integers.
Then S is a set of non-negative integers and S is not empty.
Hence, S has a least element.
Therefore, $(\exists m \in S)(\forall s \in S)(m \leq s)$.
Consequently, any nonempty set of non-negative integers under the $\leq$ relation is well-ordered.
Therefore, every non-empty set of non-negative integers is well-ordered.

Theorem 65. ***Archimedean property of positive integers***
For any positive integers a and b, there exists a positive integer n such that $na > b$.

For any positive integers a and b, there exists a positive integer n such that $na > b$, so there exists a positive integer n such that $n > \frac{b}{a}$.
For any positive integers a and b, there exists a positive integer n such that $nb > a$, so there exists a positive integer n such that $n > \frac{a}{b}$.
Consequently, for any positive integers a and b, there exists a positive integer n such that $n > \frac{a}{b}$ or $n > \frac{b}{a}$.
Therefore, there is a positive integer n that is greater than a given positive rational number.

TODO Revise as needed to remove real number set and determine if laws of exponents should be a theorem that must be proved vs an assumption or axiom.

Axiom 66. ***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 67. consecutive integers
The integers n and $n + 1$ are said to be **consecutive**.

Lemma 68. ***There is no integer between zero and one.***
There is no integer n such that $0 < n < 1$.

Proposition 69. ***No integer exists between two consecutive integers.***
Let n be an integer.
There is no integer between n and $n + 1$.

Let n be an integer.
There is no integer m such that $n < m < n + 1$.

Definition 70. even number
Let n be an integer.
Then n is **even** iff there is an integer k such that $n = 2k$.

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 71. odd number
Let n be an integer.
Then n is **odd** iff there is an integer k such that $n = 2k + 1$.

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 the digit 1, 3, 5, 7, or 9.

Definition 72. 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

Natural Number Formulae

Proposition 73. *n^{th} triangular number as a sum*

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 any positive integer n.

Proposition 74. *n^{th} square number as a sum*

The sum of the first n odd positive integers is n^2.

Therefore, $\sum_{k=1}^{n}(2k-1) = n^2$ for any positive integer n.

Proposition 75. *sum of the first n squares*

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 any positive integer n.

Proposition 76. *sum of the first n cubes*

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 any positive integer n.

Definition 77. square number

Let n be a positive integer.

Then n is a **perfect square** iff $n = k^2$ for some positive integer k.

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

Definition 78. **n^{th} square number**

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

Let s_n be the number of dots in a square with n side dots.

We say s_n is the n^{th} **square number**.

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

Therefore, $s_1 = 1$, and $s_n = s_{n-1} + 2(n-1) + 1$ for any positive integer $n > 1$.

Proposition 79. *The n^{th} square number is the sum of the first n odd positive integers.*

Let (s_n) be a sequence of positive integers such that $s_1 = 1$ and $s_n = s_{n-1} + 2(n-1) + 1$ for any positive integer $n > 1$.

Then $s_n = \sum_{k=1}^{n}(2k-1)$ for any positive integer n.

Let (s_n) be a sequence of positive integers such that $s_1 = 1$ and $s_n = s_{n-1} + 2(n-1) + 1$ for any positive integer $n > 1$.

Then $s_n = \sum_{k=1}^{n}(2k-1)$ for any positive integer n.

Since $\sum_{k=1}^{n}(2k-1) = n^2$ for any positive integer n, then s_n is the sum of the first n odd positive integers.

Therefore, the n^{th} square number is $s_n = \sum_{k=1}^{n}(2k-1) = n^2$ for any positive integer n.

Let s be any positive integer.

Then s is a perfect square iff $s = n^2$ for some positive integer n.

Since $\sum_{k=1}^{n}(2k-1) = n^2$ for any positive integer n, then $s = \sum_{k=1}^{n}(2k-1)$.

Therefore, s is a perfect square iff $s = \sum_{k=1}^{n}(2k-1)$ for some positive integer n.

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

Definition 80. cube number

Let n be a positive integer.

Then n is a **perfect cube** iff $n = k^3$ for some positive integer k.

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

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

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

Definition 81. triangular number

Let t be a positive integer.

Then t is **triangular** iff $t = \sum_{k=1}^{n} k$ for some positive integer n.

A triangular number is visualized as an arrangement of dots in an equilateral triangle such that the first row has 1 dot and each subsequent row contains one more dot than the previous row.

Definition 82. n^{th} triangular number

Let n be the row in the triangular arrangement of dots with $n \geq 1$.

Let t_n be the number of all dots from row 1 to row n.

We say t_n is the n^{th} **triangular number**.

The n^{th} row has n dots.

The n^{th} triangular number is the $(n-1)$ triangular number + the number of dots in row n.

Therefore, $t_1 = 1$, and $t_n = t_{n-1} + n$ for any positive integer $n > 1$.

Since t_n is the sum of dots in all preceding rows up to row n, then

$t_n = 1 + 2 + 3 + ... + n = \sum_{k=1}^{n} k$.

Proposition 83. ***The n^{th} triangular number is the sum of the first n positive integers.***

Let (t_n) be a sequence of positive integers such that $t_1 = 1$ and $t_n = t_{n-1} + n$ for any positive integer $n > 1$.

Then $t_n = \sum_{k=1}^{n} k$ for any positive integer n.

Let (t_n) be a sequence of positive integers such that $t_1 = 1$ and $t_n = t_{n-1} + n$ for any positive integer $n > 1$.

Then $t_n = \sum_{k=1}^{n} k$ for any positive integer n.

Since $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$ for any positive integer n, then t_n is the sum of the first n positive integers.

Therefore, the n^{th} triangular number is $t_n = \sum_{k=1}^{n} k = \frac{n(n+1)}{2}$ for any positive integer n.

Let t be a positive integer.

Then t is triangular iff $t = \sum_{k=1}^{n} k$ for some positive integer n.

Since $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$ for any positive integer n, then $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$.

Therefore, t is triangular iff $t = \frac{n(n+1)}{2}$ for some positive integer n.

The sequence of triangular numbers is

$(t_n) = (\frac{n(n+1)}{2})_{n=1}^{\infty} = (1, 3, 6, 10, 15, 21, 28, 36, 45, 55, 66, 78, 91, ...)$.

Definition 84. 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 85. 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 the Integers

Definition 86. divides relation over the integers

Define the relation 'divides' for any integers a and b by $b \mid a$ iff there is some integer n such that $a = bn$.

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

Therefore, for any integers a and b, $b|a$ iff there is an integer n such that $a = bn$.

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 there does not exist an integer n such that $a = bn$.

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

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

Proposition 88. *The number 1 divides every integer.* $(\forall n \in \mathbb{Z})(1|n)$.

Therefore $1|1$ and $1|-1$.

Proposition 89. *Every integer divides itself.* $(\forall n \in \mathbb{Z})(n|n)$.

Therefore, the divides relation over the integers is reflexive.

Theorem 90. ***comparison property of divisibility***
A divisor of n is smaller than n.
Let d and n be positive integers.
If $d|n$, then $d \leq n$.

Let d and n be positive integers.
If $d|n$, then $d \leq n$.
Therefore, if $d > n$, then $d \not| n$.

Proposition 91. *Let a, b, and n be integers.*
1. If $a|b$, then $na|nb$. (multiplication property of divisibility)
2. If $na|nb$ and $n \neq 0$, then $a|b$. (cancellation property of divisibility)

Proposition 92. *Let a, b, c, and d be integers.*
If $a|b$ and $c|d$, then $ac|bd$.

Lemma 93. *Let a and b be integers.*
Then $a|b$ iff $-a|b$ iff $a|-b$ iff $-a|-b$.

Proposition 94. *1 and -1 are the only divisors of 1.*
Let n be an integer.
If $n|1$, then $n = \pm 1$.

Let n be an integer.
If $n|1$, then either $n = 1$ or $n = -1$.

Proposition 95. ***Zero divides only zero.***
The only integer that zero divides is zero.
Let n be an integer.
If $0|n$, then $n = 0$.

Let n be an integer.
If $0|n$, then $n = 0$.
Therefore, if $n \neq 0$, then $0 \not| n$.

Lemma 96. ***The only integers whose product is one are one and negative one.***
Let a and b be integers.
If $ab = 1$ then $a = b = 1$ or $a = b = -1$.

Proposition 97. *Let a and b be integers.*
If $a|b$ and $b|a$, then $a = \pm b$.

Let a and b be integers.
If $a|b$ and $b|a$, then $a = b$ or $a = -b$.

Theorem 98. ***The divides relation over the integers is transitive.***
For any integers a, b and c, if $a|b$ and $b|c$, then $a|c$.

Theorem 99. *The divides relation is a partial order over the positive integers.*

Therefore,
1. $|$ is reflexive. (reflexive property of divisibility)
For any positive integer a, $a|a$.
2. $|$ is anti-symmetric. (anti-symmetric property of divisibility)
For any positive integers a and b, if $a|b$ and $b|a$, then $a = b$.
3. $|$ is transitive. (transitive property of divisibility)
For any positive integers a, b, and c, if $a|b$ and $b|c$, then $a|c$.

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

Division Algorithm

Theorem 100. ***Division Algorithm***
Let a be an integer.
Let b be a positive integer.
Then there exist unique integers q and r such that $a = bq + r$ and $0 \leq r < b$.

This is 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.

Theorem 101. ***necessary and sufficient condition for*** $b|a$
Let a be an integer.
Let b be a positive integer.
Then $b|a$ iff the remainder is zero when a is divided by b.

Let a be an integer.
Let b be a positive integer.
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 a is divisible by b.
Hence, $b \nmid a$ iff $r \neq 0$ when a is divided by b. This means a is not divisible by b.

Lemma 102. ***One is not even.***

Proposition 103. *Every integer is either even or odd, but not both even and odd.*

Let n be any integer.
Then either n is even or n is odd, but n is not both even and odd.
Therefore, an integer is not both even and odd.

Proposition 104. ***A product of two consecutive integers is even.***
For any integer n, $n(n+1)$ is even.

Let n be an integer.
Then $n(n+1)$ is even.
Hence, $n(n+1) = 2k$ for some integer k, so 2 divides $n(n+1)$.
Hence, $n(n+1)$ is divisible by 2.
Therefore, a product of two consecutive integers is divisible by 2.

Greatest common divisor

Definition 105. positive divisor
Let n be an integer.
Then d is a **positive divisor of** n iff d is a positive integer and $d|n$.

Definition 106. divisors of an integer
Let n be an integer.
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 be a positive integer.
Let d be a positive divisor of n.
Then d is a positive integer and $d|n$.
Since d and n are positive integers and $d|n$, then $d \leq n$.
Since d is a positive integer, then $d \geq 1$, so $1 \leq d$.
Since $1 \leq d$ and $d \leq n$, then $1 \leq d \leq n$.
Therefore, any positive divisor of a positive integer n is bounded between 1 and n.

Definition 107. common divisor
Let a and b be integers.
Then d is a **common divisor** of a and b iff d is an integer and $d|a$ and $d|b$.

Definition 108. positive common divisor
Let a and b be integers.
Then d is a **positive common divisor** of a and b iff d is a positive integer and $d|a$ 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 integers.
Since the positive integer 1 divides every integer, then $1|a$ and $1|b$, so 1 is a positive common divisor of any integers a and b.

Proposition 109. ***A positive common divisor is bounded.***
Let a and b be positive distinct integers.
Let d be a positive common divisor of a and b.
Then $1 \leq d \leq \min(a, b)$.

Definition 110. 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, and 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 111. ***Any common divisor of*** a ***and*** b ***divides their sum and difference.***
Let a, b, *and* d *be integers.*
If $d|a$ *and* $d|b$, *then* $d|(a + b)$ *and* $d|(a - b)$.

Lemma 112. ***If*** d ***divides*** a***, then*** d ***divides any multiple of*** a***.***
Let a *and* d *be integers.*
If $d \mid a$, *then* $d \mid ma$ *for any integer* m.

Theorem 113. ***Linearity property of divisibility***
Any common divisor of a ***and*** b ***divides any linear combination of*** a ***and*** b***.***
Let a, b, *and* d *be integers.*
If $d|a$ *and* $d|b$, *then* $d|(ma + nb)$ *for all integers* m *and* n.

Corollary 114. ***Any common divisor of a finite number of integers divides any linear combination of those integers.***
Let $a_1, a_2, ..., a_n$ *be* n *integers with* $n \geq 1$.
Let d *be an integer.*
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 115. 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 116. ***existence and uniqueness of greatest common divisor***
Let a *and* b *be integers 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 and b be integers 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 if a positive integer n divides 0, then $n+1$ divides 0.

Hence, there is no greatest positive common divisor 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 be any set of positive linear combinations of a and b.

Then $x \in S$ iff $x = ma + nb$ and $ma + nb > 0$ for some integers m and n.

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 and b be positive integers.

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 any positive integers a and b.

Theorem 117. ***properties of gcd***

1. $\gcd(a,0) = a$ *for any positive integer* a.

2. $\gcd(a,1) = 1$ *for any integer* a.

3. $\gcd(a,a) = a$ *for any positive integer* a.

4. $\gcd(a,b) = \gcd(b,a)$ *for any integers* a *and* b *not both zero.*

5. $\gcd(a,b) = \gcd(-a,b) = \gcd(a,-b) = \gcd(-a,-b)$ *for any integers* a *and* b *not both zero.*

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

Then $\gcd(ka,kb) = k \cdot \gcd(a,b)$ *for any positive integer* k.

Lemma 118. *The only positive divisor of* 1 *is* 1.

Theorem 119. *Let* a *and* b *be integers.*

For any integer c, 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 120. ***The greatest common divisor of two integers is one iff one is a linear combination of those integers.***

Let a *and* b *be integers.*

Then $\gcd(a,b) = 1$ *iff there exist integers* m *and* n *such that* $ma + nb = 1$.

Let a and b be integers.

Then $\gcd(a,b) = 1$ iff there exist integers m and n such that $ma + nb = 1$.

Therefore, $\gcd(a,b) = 1$ iff 1 is a linear combination of a and b.

Corollary 121. *Let a and b be integers.*
If $d = \gcd(a, b)$, then $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$.

Definition 122. relatively prime integers
Two integers are relatively prime (or **coprime**) iff their only positive common divisor is 1.
Let a and b be integers.
Then a and b are **relatively prime** iff $\gcd(a, b) = 1$.

Let a and b be integers.
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 positive common divisor.
Therefore, there is no integer greater than one that divides them both.
Therefore, relatively prime numbers have no positive common divisor other than 1.

Let a and b be integers.
Then a and b are relatively prime iff $\gcd(a, b) = 1$ iff there exist integers m and n such that $ma + nb = 1$ iff 1 is a linear combination of a and b.

Theorem 123. ***If d is a divisor of ab and is relatively prime to a, then d is a divisor of b.***
Let $a, b,$ and d be integers.
If $d|ab$ and $\gcd(d, a) = 1$, then $d|b$.

Theorem 124. ***If m is a multiple of a and b, and a and b are relatively prime, then m is a multiple of ab.***
Let $a, b,$ and m be integers.
If $a|m$ and $b|m$ and $\gcd(a, b) = 1$, then $ab|m$.

Euclidean Algorithm

The Euclidean algorithm appears in Euclid's Elements Book VII proposition 2.

Let a and b be 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 125. ***Euclidean Algorithm lemma***
Let a be an integer.
Let b be a positive integer.
If r is the remainder when a is divided by b, then $\gcd(a, b) = \gcd(b, r)$.

Theorem 126. ***Euclidean Algorithm***

Let a be an integer.

Let b be a positive integer.

Let n be the number of iterative steps and

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

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

Let a be an integer.

Let b be a positive integer.

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

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 repeated 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 127. multiple

Let n be an integer.

Then m is a **multiple of** n iff m is an integer and $m = nk$ for some integer k.

Let n be an integer.

Then m is a multiple of n iff m is an integer and $m = nk$ for some integer k.

Therefore, m is a multiple of n iff m is an integer and $n|m$.

Definition 128. positive multiple

Let n be an integer.

Then m is a **positive multiple of** n iff m is a positive integer and $m = nk$ for some integer k.

Definition 129. multiples of an integer

Let n be an integer.

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

Let n be an integer.
Then $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\} = \{0, \pm n, \pm 2n, \pm 3n, \pm 4n, \pm 5n, ...\}$.

Definition 130. positive multiples of an integer
Let n be a positive integer.
The set of all positive multiples of n is $\{nk : k \in \mathbb{Z}^+\}$.

Let n be a positive integer.
The set of all positive multiples of n is $\{nk : k \in \mathbb{Z}^+\} = \{n, 2n, 3n, 4n, 5n, ...\}$.

Definition 131. common multiple
Let a and b be integers.
Then m is a **common multiple** of a and b iff m is an integer and $a|m$ 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.

Definition 132. positive common multiple
Let a and b be integers.
Then m is a **positive common multiple** of a and b iff m is a positive integer and $a|m$ and $b|m$.

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

Definition 133. 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 $m|c$.

Theorem 134. ***existence and uniqueness of least common multiple***
Let a and b be positive integers.
The least common multiple of a and b exists and is unique.

Let a and b be positive integers.
The least common multiple of a and b is denoted by $lcm(a, b)$.
Since a and b are positive integers, then $a > 0$ and $b > 0$, so $a \neq 0$ and $b \neq 0$.
Therefore, $lcm(0, 0)$ is undefined.

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.

Proposition 135. *For any positive integers a and b, $lcm(a, b)$ divides ab.*

Let a and b be positive integers.

Then ab and $lcm(a, b)$ are positive integers.

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

Since $lcm(a, b)$ is a positive integer, then $lcm(a, b) \geq 1$, so $1 \leq lcm(a, b)$.

Since $1 \leq lcm(a, b)$ and $lcm(a, b) \leq ab$, then $1 \leq lcm(a, b) \leq ab$.

Therefore, $1 \leq lcm(a, b) \leq ab$ for any positive integers a and b.

Theorem 136. ***lcm and gcd relationship***

For any positive integers a and b, $\gcd(a, b) \cdot lcm(a, b) = ab$.

Corollary 137. *For any positive integers a and b, $lcm(a, b) = ab$ iff $\gcd(a, b) = 1$.*

Theorem 138. ***properties of lcm***

1. *$lcm(a, 1) = a$ for any positive integer a.*
2. *$lcm(a, a) = a$ for any positive integer a.*
3. *$lcm(a, b) = lcm(b, a)$ for any positive integers a and b.*
4. *Let a and b be positive integers.*
   Then $lcm(ka, kb) = k \cdot lcm(a, b)$ for any positive integer k.
5. *$\gcd(a, b)$ divides $lcm(a, b)$ for any positive integers a and b.*
6. *$\gcd(a, b) = lcm(a, b)$ iff $a = b$ for any positive integers a and b.*
7. *$a|b$ iff $\gcd(a, b) = a$ iff $lcm(a, b) = b$ for any positive integers a and b.*

Let a and b be positive integers.

Then $\gcd(a, b)$ divides $lcm(a, b)$, and $lcm(a, b)$ divides ab.

Linear Diophantine Equations

Definition 139. diophantine equation

A **diophantine equation** is a polynomial equation in one or more unknowns whose solutions are integers or rational numbers.

Definition 140. linear diophantine equation

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

A **linear diophantine equation in two unknowns** is the equation $ax + by = c$ with unknowns x and y.

A **solution** of the equation $ax + by = c$ is a pair of numbers (x_0, y_0) such that $ax_0 + by_0 = c$.

We say that the equation $ax + by = c$ is **solvable in the rationals** iff there is a pair of rational numbers (x_0, y_0) such that $ax_0 + by_0 = c$.

We say that the equation $ax + by = c$ is **solvable in the integers** iff there is a pair of integers (x_0, y_0) such that $ax_0 + by_0 = c$.

Proposition 141. ***A linear diophantine equation is solvable in the rationals.***

Let a, b, and c be integers and $a \neq 0$ and $b \neq 0$.

All rational solutions of the equation $ax + by = c$ are given by $x = t$ and $y = \dfrac{c - at}{b}$ for any rational number t.

Let a, b, and c be integers and $a \neq 0$ and $b \neq 0$.

All rational solutions of the equation $ax + by = c$ are given by $x = t$ and $y = \dfrac{c - at}{b}$ for any rational number t.

Therefore, the equation $ax + by = c$ has infinitely many rational number solutions.

Theorem 142. ***existence of an integer solution of a linear diophantine equation***

Let a, b, and c be integers and $a \neq 0$ and $b \neq 0$.

The equation $ax + by = c$ is solvable in the integers if and only if $\gcd(a, b)$ divides c.

Let a, b, and c be integers and $a \neq 0$ and $b \neq 0$.

The equation $ax + by = c$ is solvable in the integers if and only if $\gcd(a, b)$ divides c.

If $\gcd(a, b)$ divides c, then $ax + by = c$ is solvable in the integers.

If $\gcd(a, b)$ does not divide c, then $ax + by = c$ is not solvable in the integers.

Lemma 143. ***There are infinitely many integer solutions of a solvable linear diophantine equation.***

Let a, b, and c be integers.

If a pair of integers (x_0, y_0) is a particular solution of the equation $ax + by = c$, then the pair of integers $x_0 + bt$ and $y_0 - at$ is an integer solution for any integer t.

Theorem 144. ***all integer solutions of a linear diophantine equation***
Let a, b, and c be integers and $a \neq 0$ and $b \neq 0$.
If a pair of integers (x_0, y_0) is a particular solution of the equation $ax+by = c$, then all integer solutions are given by $x = x_0 + \frac{bt}{d}$ and $y = y_0 - \frac{at}{d}$ for any integer t, where $d = \gcd(a, b)$.

Let a, b, and c be integers and $a \neq 0$ and $b \neq 0$.
The equation $ax + by = c$ is solvable in the integers if and only if d divides c, where $d = \gcd(a, b)$.
If a pair of integers (x_0, y_0) is a particular solution, then all integer solutions are given by $x = x_0 + \frac{bt}{d}$ and $y = y_0 - \frac{at}{d}$ for any integer t.

Corollary 145. ***all integer solutions of a linear diophantine equation***
Let a, b, and c be integers and $a \neq 0$ and $b \neq 0$.
If a pair of integers (x_0, y_0) is a particular solution of the equation $ax+by = c$ and $\gcd(a, b) = 1$, then all integer solutions are given by $x = x_0 + bt$ and $y = y_0 - at$ for any integer t.

Fundamental Theorem of Arithmetic

The fundamental theorem of arithmetic appears in Euclid's Elements Book VII proposition 32 and Book IX proposition 14.

Let n be a positive integer.
Then $1|n$ and $n|n$, so 1 and n are positive divisors of n.
Therefore, 1 and n are positive divisors of any positive integer n.
A prime number has no positive factors other than one and itself.

Definition 146. 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 and p.
By definition of prime, 1 is not prime.

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 other than 1.
If the only positive divisors of p are 1 and p, then p is a prime number.

Lemma 147. *The number 2 is prime.*

Let p be any prime number.
Then p is a positive integer and $p \neq 1$.
Since p is a positive integer, then $p \geq 1$.
Since $p \geq 1$ and $p \neq 1$, then $p > 1$.
Since p is an integer and $p > 1$, then $p \geq 2$.
Therefore, any prime number is greater than or equal to 2, so 2 is the smallest prime.

The prime numbers are $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, ...$

Lemma 148. *A prime is odd iff it is greater than* 2*.*

Let p be any prime.
Then p is odd iff $p > 2$.

If p is odd, then $p > 2$.
Therefore, any odd prime is greater than 2.

If $p > 2$, then p is odd.
Therefore, any prime greater than 2 is odd.

Proposition 149. *The only even prime is* 2*.*

Proposition 150. *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 $\gcd(p, q) = 1$.

A composite number is composed of smaller positive factors.

Definition 151. composite number
Let n be a positive integer.
Then n is **composite** iff there exist positive integers a and b such that $n = ab$ and $1 < a < n$ and $1 < b < n$.

The composite numbers are $4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, 21, 22, 24, 25, 26, 27, 28, 30, ...$

Lemma 152. ***A composite number has a positive factor other than one and itself.***
Let n be a positive integer.
Then n is composite iff there exists an integer d such that $d|n$ and $1 < d < n$.

Proposition 153. *A positive integer other than* 1 *is composite iff it is not prime.*

Therefore, a positive integer other than 1 is not composite iff it is prime.

Lemma 154. *The number* 1 *is not composite.*

Theorem 155. ***classification of positive integers by divisibility***
A positive integer n *is exactly one of the following:*
1. $n = 1$.
2. n *is prime.*
3. n *is composite.*

Corollary 156. ***A positive integer is composite iff it is neither*** 1 ***nor prime.***
Let n *be a positive integer.*
Then n *is composite if and only if* n *is neither* 1 *nor prime.*

Let n be a positive integer.
Then n is composite if and only if n is neither 1 nor prime.
Therefore, n is composite if and only if $n \neq 1$ and n is not prime.

Since 1 is not prime, and 1 is not composite, then 1 is neither prime nor composite. We say that 1 is a unit of the integers.

Theorem 157. ***Euclid's Lemma***
Let a *and* b *be integers.*
Let p *be a positive integer.*
If p *is prime and* $p|ab$*, then either* $p|a$ *or* $p|b$.

Corollary 158. ***If prime*** p ***divides a product of integers, then*** p ***divides one of those integers.***
Let $a_1, a_2, ..., a_n$ *be integers.*
Let p *be a positive integer.*
If p *is prime and* p *divides* $a_1 a_2 \cdots a_n$*, 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.

Corollary 159. ***If prime*** p ***divides a product of primes, then*** p ***is one of those primes.***
Let $p, q_1, q_2, ..., q_n$ *be positive integers.*
If $p, q_1, q_2, ..., q_n$ *are all prime and* p *divides* $q_1 q_2 \cdots q_n$*, 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.

Lemma 160. *Every integer greater than* 1 *is divisible by a prime.*

Let n be any integer greater than 1.
Then n is divisible by a prime.
Therefore, there exists a prime p such that $p|n$.

Definition 161. prime factorization of an integer

A **prime factorization of an integer** $n > 1$ is a representation of n as a product of one or more primes.

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

Theorem 162. ***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 163. ***A product of primes is greater than one.***

Let n be any positive integer.

If $p_1, p_2, ..., p_n$ are all primes, then $p_1 p_2 \cdots p_n > 1$.

The fundamental theorem of arithmetic states that every integer greater than one is a unique product of primes.

Theorem 164. ***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 any integer greater than 1.

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

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

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

Corollary 165. ***Every integer greater than one has a unique prime power factorization.***

Every integer $n > 1$ can be written uniquely in a canonical form $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, 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 any integer greater than 1.

Then $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ 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, all the positive integers greater than one.

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

Theorem 166. *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.

TODO: Revise the below proof as needed. .

Theorem 167. ***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.

TODO: Revise the below proof as needed.

Theorem 168. ***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.

Sieve of Eratosthenes

Lemma 169. *Let n be a positive integer.*

If n is composite, then there is an integer d such that $d|n$ and $1 < d \leq \sqrt{n}$.

Proposition 170. ***Any composite number has a prime factor that does not exceed its square root.***

Let n be a positive integer.

If n is composite, then n has a prime factor less than or equal to $\sqrt{n}$.

Let n be a positive integer.

If n is composite, then there is a prime p such that $p|n$ and $p \leq \sqrt{n}$.

Corollary 171. ***sieve of Eratosthenes fact***

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.

Proposition 172. ***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. Eliminate all composite numbers by removing all multiples of p greater than p for each prime $p \leq \sqrt{n}$.

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

Distribution of Primes

Theorem 173. ***Euclid's Theorem***

There are more prime numbers than in any given list of them.

Let $p_1, p_2, ..., p_n$ be a finite list of primes for some positive integer n.
Then there is a prime that is not in the list.
Therefore, there is a prime q such that q is not in the list.

Euclid's theorem is interpreted to mean 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.'

Corollary 174. *For any positive integer n, there is a prime greater than n.*

For any positive integer n, there is a prime p such that $p > n$.

Definition 175. sequence of prime numbers

The **sequence of prime numbers** in increasing order is $2, 3, 5, 7, 11, 13, 17, 19, 23, ...$

Let p_n denote the n^{th} term in the sequence of prime numbers.

Then n is a positive integer and $p_1 = 2$ and $p_2 = 3$ and $p_3 = 5$ and $p_4 = 7$ and ...

The sequence of prime numbers is denoted (p_n).

Since $2 < 3 < 5 < 7 < ...$, then $p_1 < p_2 < p_3 < p_4 < ... < p_n < ....$
Therefore, the sequence of prime numbers is a strictly increasing sequence.
Observe that $1 < p_1 < p_2 < p_3 < ... < p_n < p_{n+1} < ....$

Lemma 176. ***upper growth bound on a prime***

Let p_n be the n^{th} prime number in the sequence of primes.
Then $p_{n+1} \leq p_1 p_2 \cdots p_n + 1$ for any positive integer n.

Lemma 177. ***lower growth bound on a prime***

Let p_n be the n^{th} prime number in the sequence of primes.
Then $p_1 p_2 \cdots p_n < {p_n}^n$ for any positive integer $n > 1$.

Proposition 178. ***bound on the size of a prime***
Let p_n be the n^{th} prime number in the sequence of primes.
Then $p_{n+1} < {p_n}^n + 1$ for any positive integer $n > 1$.

Proposition 179. ***another bound on the size of a prime***
Let p_n be the n^{th} prime number in the sequence of primes.
Then $p_n < 2^{2^{n-1}}$ for any positive integer $n > 1$.

Corollary 180. *For any positive integer n, there are at least $n+1$ primes less than 2^{2^n}.*

Goldbach Conjecture

Definition 181. twin primes
A **twin prime** is a pair of primes which differ by 2.

Let p and $p+2$ be primes.
Since $(p+2) - p = 2$, then p and $p+2$ are twin primes.
We say that $(p, p+2)$ is a **twin prime pair**.

Proposition 182. ***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 prime gap is the difference between two distinct primes.

Definition 183. prime gap
Let p and q be distinct primes.
The **prime gap** is the difference $|q - p|$.

Let p and q be distinct primes.
Then p and q are primes and $p \neq q$, so either $p < q$ or $p > q$.
Suppose $p < q$.
Then $q - p > 0$, so the prime gap is $|q - p| = q - p$.
Therefore, if p and q are primes and $p < q$, then the prime gap is $q - p$.

Let p and $p+2$ be twin primes.
Then p and $p+2$ are prime.
Since p and $p+2$ are prime and $p < p+2$, then the prime gap is $(p+2)-p = 2$.
Therefore, the prime gap of twin primes is 2.

Conjecture 184. ***twin prime conjecture***
There are infinitely many pairs of twin primes.

Therefore, the twin prime conjecture states there are infinitely many pairs of primes which differ by 2.

An equivalent statement of the twin prime conjecture is: there are infinitely many primes p such that $p+2$ is also prime.

Theorem 185. ***Arbitrarily large gaps can exist between consecutive primes.***

For any positive integer $n > 1$, there are n consecutive composite integers.

Conjecture 186. ***binary Goldbach conjecture***

Every even integer greater than 2 is the sum of two primes.

Let n be any even integer greater than 2.
Then n is an even integer and $n > 2$, so n is the sum of two primes.
Therefore, there are primes p and q such that $n = p + q$.

Theodor Estermann proved that almost every positive even integer is the sum of two primes. (Proc. London Math. Soc. Ser.2 44, 307-314, 1938).

Chen Jingrun proved that every sufficiently large integer is the sum of a prime and a number with at most two prime factors. This is Chen's theorem.

Corollary 187. ***binary Goldbach conjecture corollary***

Every even integer greater than 4 is the sum of two odd primes.

If the binary Goldbach conjecture is true, then the binary Goldbach conjecture corollary is true, so the binary Goldbach conjecture implies the binary Goldbach conjecture corollary.

Conjecture 188. ***ternary Goldbach conjecture***

Every odd integer greater than 5 is the sum of three primes.

Let n be any odd integer greater than 5.
Then n is an odd integer and $n > 5$, so n is the sum of three primes.
Therefore, there are primes p, q, and r such that $n = p + q + r$.

Proposition 189. *The binary Goldbach conjecture implies the ternary Goldbach conjecture.*

If the binary Goldbach conjecture is true, then the ternary Goldbach conjecture is true.

Ivan Matveevich Vinogradov's three primes theorem states that every sufficiently large odd integer is the sum of three primes. (Dokl. Akad. Nauk. SSSR, 15:169-172, 'Some theorems concerning the theory of prime numbers', 1937).

Harald Andres Helfgott submitted a paper for publication in 2015 in Annals of Mathematics Studies that claims every odd integer greater than 5 is the sum of three primes.

Conjecture 190. ***odd ternary Goldbach conjecture***

Every odd integer greater than 7 is the sum of three odd primes.

Let n be any odd integer greater than 7.
Then n is an odd integer and $n > 7$, so n is the sum of three odd primes.
Therefore, there are odd primes p, q, and r such that $n = p + q + r$.

Proposition 191. *The binary Goldbach conjecture implies the odd ternary Goldbach conjecture.*

If the binary Goldbach conjecture is true, then the odd ternary Goldbach conjecture is true.

Proposition 192. *Every odd integer is of the form $4n+1$ or $4n+3$, where n is an integer.*

Therefore, all positive odd integers are in one of two sequences:
$(4n+1)$ contains $1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61, 65, 69, 73, 77, ...$
$(4n+3)$ contains $3, 7, 11, 15, 19, 23, 27, 31, 35, 39, 43, 47, 51, 55, 59, 63, 67, 71, 75, 79, ...$

Lemma 193. *The product of two or more integers of the form $4a+1$ is of the same form, where a is an integer.*

Proposition 194. *There are infinitely many primes of the form $4n+3$, where n is an integer.*

The sequence $(4n+3)$ contains the primes
$3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79, 83, 103, 107, 127, 131, 139, 151, 163, ...$

Theorem 195. ***Dirichlet's theorem on primes in arithmetic progressions***

There are infinitely many prime numbers in all arithmetic progressions with initial term and common difference coprime.

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

Let (a_n) be an arithmetic sequence with common difference d and initial term a, where d and a are positive integers.
Suppose a and d are relatively prime.
Then $\gcd(a, d) = 1$.
Therefore, (a_n) contains infinitely many primes.

Peter Gustav Lejeune Dirichlet's theorem is found in Abhandlungen der Koniglich Preussischen Akademie der Wissenschaften von 1837, pp. 45-81 titled Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, Berliner Abh., (1837), pp. 45–81.

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

Proposition 196. ***sufficient condition for an arithmetic sequence to contain only composite numbers***

Let a and m be positive integers.

If $\gcd(a, m) > 1$ and a is composite, then the arithmetic sequence $a, a+m, a+2m, a+3m, ...$ contains only composite numbers.

Proposition 197. *No arithmetic sequence contains only prime numbers.*

Suppose the prime numbers are equally spaced in the sequence of positive integers.

Then the gap between consecutive primes is constant, so the sequence of primes $p_1, p_2, p_3, ...$ is an arithmetic sequence.

Hence, there is an arithmetic sequence that contains only prime numbers.

But, this contradicts there is no arithmetic sequence that contains only prime numbers.

Therefore, the prime numbers are not equally spaced in the sequence of positive integers.

Congruences

Definition 198. congruence modulo relation over the integers

Let m be a fixed positive integer.

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

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

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

Define the relation 'is congruent to modulo m' for any integers a and b by $a \equiv b \pmod{m}$ iff $m|(a - b)$.

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

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

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

Let m be a fixed positive integer.

Let a and b be any two integers.

Then $a \equiv b \pmod{m}$ iff $m|(a - b)$.

Therefore, a is congruent to b modulo m iff a and b differ by a multiple of m.

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

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

Proposition 199. *a is congruent to b modulo m if and only if a equals b plus some multiple of m.*

Let m be a fixed positive integer.

Let a and b be any integers.

Then $a \equiv b \pmod{m}$ iff $a = b + km$ for some integer k.

Theorem 200. *Congruent integers leave the same remainder when divided by the modulus.*

Let m be a fixed positive integer.

Let a and b be any integers.

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

Theorem 201. *The congruence modulo relation is an equivalence relation on $\mathbb{Z}$.*

Let m be a fixed positive integer.
Then
1. $\equiv$ is reflexive
For any integer a, $a \equiv a \pmod{m}$.
2. $\equiv$ is symmetric
For any integers a and b, if $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$.
3. $\equiv$ is transitive
For any integers a, b, and c, if $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

Theorem 202. ***arithmetic operations on congruences***
Let m be a fixed positive integer.
Let a, b, c, and d be any integers.
If $a \equiv c \pmod{m}$ and $b \equiv d \pmod{m}$, then
1. $a + b \equiv c + d \pmod{m}$ (addition of congruences is well defined)
2. $a - b \equiv c - d \pmod{m}$ (subtraction of congruences is well defined)
3. $ab \equiv cd \pmod{m}$. (multiplication of congruences is well defined)

Theorem 203. ***operations that preserve congruences***
Let m be a fixed positive integer.
Let a and b be any integers.
1. Addition preserves congruence.
If $a \equiv b \pmod{m}$, then $a + k \equiv b + k \pmod{m}$ for any integer k.
2. Subtraction preserves congruence.
If $a \equiv b \pmod{m}$, then $a - k \equiv b - k \pmod{m}$ for any integer k.
3. Multiplication preserves congruence.
If $a \equiv b \pmod{m}$, then $ak \equiv bk \pmod{m}$ for any integer k.
4. Exponentiation preserves congruence.
If $a \equiv b \pmod{m}$, then $a^k \equiv b^k \pmod{m}$ for any positive integer k.

Theorem 204. ***cancellation laws for congruences***
Let m be a fixed positive integer.
Let a, b, and k be any integers.
1. Addition cancellation law
If $a + k \equiv b + k \pmod{m}$, then $a \equiv b \pmod{m}$.
2. Multiplication cancellation law
If $ak \equiv bk \pmod{m}$, then $a \equiv b \pmod{\frac{m}{\gcd(k, m)}}$.

Corollary 205. ***cancellation multiplication relatively prime to modulus***

Let m be a fixed positive integer.

Let a, b, and k be any integers.
If $ak \equiv bk \pmod{m}$ and $\gcd(k, m) = 1$, then $a \equiv b \pmod{m}$.

Lemma 206. *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 207. ***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 $a \equiv b \pmod{p}$.

Residues

Proposition 208. *Let m be a positive integer.*
Every integer is congruent modulo m to exactly one of $0, 1, ..., m - 1$.

Let m be a positive integer.
Let a be any integer.
Then a is congruent modulo m to exactly one of the integers $0, 1, ..., m - 1$, so exactly one of the following holds:
$a \equiv 0 \pmod{m}$, $a \equiv 1 \pmod{m}$, ... , $a \equiv m - 1 \pmod{m}$.

Proposition 209. *Let m be a positive integer.*
No two distinct integers in the set $\{0, 1, ..., m - 1\}$ are congruent modulo m.

Let m be a positive integer.
Let $S = \{0, 1, ..., m - 1\}$.
Then no two distinct integers in the set S are congruent modulo m.
Therefore, there are no distinct integers $a \in S$ and $b \in S$ such that $a \equiv b \pmod{m}$.
Equivalently, for any distinct integers $a \in S$ and $b \in S$, $a \not\equiv b \pmod{m}$.

Definition 210. residue of an integer modulo m
Let m be a fixed positive integer.
Let a be any integer.
An integer b is a **residue of** a **modulo** m if and only if $a \equiv b \pmod{m}$.

Definition 211. least residue of an integer modulo m
Let m be a fixed positive integer.
Let a be any integer.
The **least residue of** a **modulo** m is the remainder when a is divided by m.

Let m be a fixed positive integer.
Let a be any integer.
Let r be the least residue of a modulo m.
Then r is the remainder when a is divided by m, so r is unique, by the division algorithm.
Therefore, the least residue of an integer modulo m is unique.

A complete system of residues modulo m is a set of m integers such that every integer is congruent modulo m to exactly one of them.

Definition 212. complete system of residues modulo m

Let m be a fixed positive integer.

A set of m integers $a_1, a_2, ..., a_m$ is a **complete system of residues modulo** m if and only if every integer is congruent modulo m to exactly one of the a_i.

Let m be a fixed positive integer.

Let $\{a_1, a_2, ..., a_m\}$ be a set of m integers.

Then $\{a_1, a_2, ..., a_m\}$ is a complete system of residues modulo m if and only if for every integer b there is exactly one a_i such that $b \equiv a_i \pmod{m}$.

Theorem 213. ***properties of a complete residue system modulo*** m

Let m be a fixed positive integer.

Let $\{a_1, a_2, ..., a_m\}$ be a complete system of residues modulo m.

1. Every integer is congruent modulo m to exactly one of the values $a_1, a_2, ..., a_m$.

For every integer b, there is a unique index i with $1 \leq i \leq m$ such that $b \equiv a_i \pmod{m}$.

2. No two of the integers $a_1, a_2, ..., a_m$ are congruent modulo m.

If $i \neq j$, then $a_i \not\equiv a_j \pmod{m}$.

Proposition 214. *Let m be a fixed positive integer.*

A set of m integers is a complete system of residues modulo m if and only if no two of the integers in the set are congruent modulo m.

Let m be a fixed positive integer.

Let $\{a_1, a_2, ..., a_m\}$ be a set of integers.

Then $\{a_1, a_2, ..., a_m\}$ is a complete system of residues modulo m if and only if for any integers i and j if $i \neq j$, then $a_i \neq a_j \pmod{m}$.

TODO The proof of the prop is in theorem of ch4-1.pdf page 2 under residue classes. Look over its proof.

Linear Congruences

Definition 215. linear congruence

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

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

A **linear congruence in one unknown** is the equation $ax \equiv b \pmod{n}$ with unknown x.

A **solution** of the equation $ax \equiv b \pmod{n}$ is an integer x_0 such that $ax_0 \equiv b \pmod{n}$.

TODO: Decide if the solution set notes are needed or not. If not, then delete the notes about solution sets.

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 216. *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 217. 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 218. ***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.

Theorem 219. ***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 220. 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 221. *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 222. *Let $n \in \mathbb{Z}^+$.*
Then $[n] = [0]$.

Proposition 223. *Let $n \in \mathbb{Z}^+$.*
Then $[-a] = [n-a]$ for all $[a] \in \mathbb{Z}_n$.

Definition 224. 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 225. *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 226. ***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 227. ***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 228. 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 229. ***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 230. 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 231. ***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 232. ***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 233. 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 234. ***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 235. 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 236. ***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 237. *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 238. 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 239. *Let* $n \in \mathbb{Z}^+$.
A nonzero element of $\mathbb{Z}_n$ *either has a multiplicative inverse or is a divisor of zero.*

Proposition 240. *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 241. 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 242. *If p is prime, then $\phi(p) = p - 1$.*

Definition 243. 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 244. 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 245. ***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 246. ***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 247. ***Fermat's Little Theorem***
Let $a \in \mathbb{Z}$.
If p is prime, then $a^p \equiv a \pmod{p}$.

Miscellaneous Stuff

Proposition 248. ***Every integer is congruent modulo n to exactly one of the integers $0, 1, 2, ..., n-1$.***

Definition 249. 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 250. 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 251. The set $\{-12, -4, 11, 13, 22, 82, 91\}$ is a complete set of residues modulo 7.

Proposition 252. ***Any set of n integers is a complete set of residues modulo n iff no two of the integers are congruent modulo n.***

Definition 253. 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.