New! An algorithm is a finite sequence of precise instructions for solving a problem.

A relation R on a set A is called **antisymmetric** means $\forall a \in A\, \forall b \in A\ (\ (\ (a,b) \in R \wedge (b,a) \in R\ ) \rightarrow a = b\ )$

Definition For b an integer greater than 1 and n a positive integer, the **base** b **expansion of** n is

$$(a_{k-1} \cdots a_1 a_0)_b$$

where k is a positive integer, $a_0, a_1, \ldots, a_{k-1}$ are nonnegative integers less than b, $a_{k-1} \neq 0$, and

$$n = \sum_{i=0}^{k-1} a_i b^i$$

Notice: *The base b expansion of a positive integer n is a string over the alphabet $\{x \in \mathbb{N} \mid x < b\}$ whose leftmost character is nonzero.*

Base b	Collection of possible coefficients in base b expansion of a positive integer
Binary ($b = 2$)	$\{0, 1\}$
Ternary ($b = 3$)	$\{0, 1, 2\}$
Octal ($b = 8$)	$\{0, 1, 2, 3, 4, 5, 6, 7\}$
Decimal ($b = 10$)	$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$
Hexadecimal ($b = 16$)	$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F\}$ letter coefficient symbols represent numerical values $(A)_{16} = (10)_{10}$ $(B)_{16} = (11)_{10}$ $(C)_{16} = (12)_{10}$ $(D)_{16} = (13)_{10}$ $(E)_{16} = (14)_{10}$ $(F)_{16} = (15)_{10}$

Definition : A function $f : D \rightarrow C$ is a **bijection** means that it is both one-to-one and onto. The **inverse** of a bijection $f : D \rightarrow C$ is the function $g : C \rightarrow D$ such that $g(b) = a$ iff $f(a) = b$.

Definition: When A and B are sets, we say any subset of $A \times B$ is a **binary relation**. A relation R can also be represented as

- A function $f_{TF} : A \times B \rightarrow \{T, F\}$ where, for $a \in A$ and $b \in B$, $f_{TF}(\ (a,b)\ ) = \begin{cases} T & \text{when } (a,b) \in R \\ F & \text{when } (a,b) \notin R \end{cases}$
- A function $f_{\mathcal{P}} : A \rightarrow \mathcal{P}(B)$ where, for $a \in A$, $f_{\mathcal{P}}(a) = \{b \in B \mid (a,b) \in R\}$

When A is a set, we say any subset of $A \times A$ is a (binary) **relation** on A.

For nonempty sets A, B we say

$|A| \leq |B|$ means there is a one-to-one function with domain A, codomain B
$|A| \geq |B|$ means there is an onto function with domain A, codomain B
$|A| = |B|$ means there is a bijection with domain A, codomain B

For all sets A, we say $|A| = |\emptyset|$, $|\emptyset| = |A|$ if and only if $A = \emptyset$. **Definition**: For nonempty sets A, B, we say that **the cardinality of A is no bigger than the cardinality of** B, and write $|A| \leq |B|$, to mean there is a one-to-one function with domain A and codomain B. Also, we define $|\emptyset| \leq |B|$ for all sets B. **Definition**: For nonempty sets A, B, we say that **the cardinality of A is no smaller than the cardinality of** B, and write $|A| \geq |B|$, to mean there is an onto function with domain A and codomain B. Also, we define $|A| \geq |\emptyset|$ for all sets A.

Definition: The **Cartesian product** of the sets A and B, $A \times B$, is the set of all ordered pairs (a, b), where $a \in A$ and $b \in B$. That is: $A \times B = \{(a, b) \mid (a \in A) \wedge (b \in B)\}$. The Cartesian product of the sets $A_1, A_2, \ldots, A_n$, denoted by $A_1 \times A_2 \times \cdots \times A_n$, is the set of ordered n-tuples $(a_1, a_2, ..., a_n)$, where a_i belongs to A_i for $i = 1, 2, \ldots, n$. That is,

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in A_i \text{ for } i = 1, 2, \ldots, n\}$$

Proposition: Declarative sentence that is true or false (not both). **Propositional variable**: Variable that represents a proposition. **Compound proposition**: New proposition formed from existing propositions (potentially) using logical operators. *Note*: A propositional variable is one example of a compound proposition. **Truth table**: Table with one row for each of the possible combinations of truth values of the input and an additional column that shows the truth value of the result of the operation corresponding to a particular row.

We can use a recursive definition to describe all compound propositions that use propositional variables from a specified collection. Here's the definition for all compound propositions whose propositional variables are in $\{p, q\}$.

Basis Step:	p and q are each a compound proposition
Recursive Step:	If x is a compound proposition then so is $(\neg x)$ and if x and y are both compound propositions then so is each of $(x \wedge y), (x \oplus y), (x \vee y), (x \rightarrow y), (x \leftrightarrow y)$

Definition: A set A is **countably infinite** means it is the same size as $\mathbb{N}$.

Term	Notation Example(s)	We say in English ...
sequence	$x_1, \ldots, x_n$	A sequence x_1 to x_n
summation	$\sum_{i=1}^{n} x_i$ or $\sum_{i=1}^{n} x_i$	The sum of the terms of the sequence x_1 to x_n
all reals	$\mathbb{R}$	The (set of all) real numbers (numbers on the number line)
all integers	$\mathbb{Z}$	The (set of all) integers (whole numbers including negatives, zero, and positives)
all positive integers	$\mathbb{Z}^+$	The (set of all) strictly positive integers
all natural numbers	$\mathbb{N}$	The (set of all) natural numbers. **Note**: we use the convention that 0 is a natural number.
piecewise rule definition	$f(x) = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0 \end{cases}$	Define f of x to be x when x is nonnegative and to be $-x$ when x is negative
function application	$f(7)$	f of 7 **or** f applied to 7 **or** the image of 7 under f
	$f(z)$	f of z **or** f applied to z **or** the image of z under f
	$f(g(z))$	f of g of z **or** f applied to the result of g applied to z
absolute value	$\lvert -3 \rvert$	The absolute value of -3
square root	$\sqrt{9}$	The non-negative square root of 9

Definition An expression built of variables and logical operators is in **disjunctive normal form** (DNF) means that it is an OR of ANDs of variables and their negations. **Definition** An expression built of variables and logical operators is in **conjunctive normal form** (CNF) means that it is an AND of ORs of variables and their negations.

An **equivalence class** of an element $a \in A$ with respect to an equivalence relation R on the set A is the set

$$\{s \in A \mid (a, s) \in R\}$$

We write $[a]_R$ for this set, which is the equivalence class of a with respect to R. A relation is an **equivalence relation** means it is reflexive, symmetric, and transitive. **Definition**: When a and b are integers and a is nonzero, a **divides** b means there is an integer c such that $b = ac$. Symbolically, $F(\ (a, b)\ ) =$ and is a predicate over the domain _____ Other (synonymous) ways to say that $F(\ (a, b)\ )$ is true:

a is a **factor** of b $\quad$ a is a **divisor** of b $\quad$ b is a **multiple** of a $\quad$ $a|b$

When a is a positive integer and b is any integer, $a|b$ exactly when b **mod** $a = 0$ When a is a positive integer and b is any integer, $a|b$ exactly $b = a \cdot (b$ **div** $a)$ **Definition**: A **finite** set is one whose distinct elements can be counted by a natural number.

Definition For b an integer greater than 1, w a positive integer, and n a nonnegative integer _____, the **base** b **fixed-width** w **expansion of** n is

$$(a_{w-1} \cdots a_1 a_0)_{b,w}$$

where $a_0, a_1, \ldots, a_{w-1}$ are nonnegative integers less than b and

$$n = \sum_{i=0}^{w-1} a_i b^i$$

Definition For b an integer greater than 1, w a positive integer, w' a positive integer, and x a real number the **base b fixed-width expansion of x with integer part width w and fractional part width w'** is $(a_{w-1} \cdots a_1 a_0 . c_1 \cdots c_{w'})_{b,w,w'}$ where $a_0, a_1, \ldots, a_{w-1}, c_1, \ldots, c_{w'}$ are nonnegative integers less than b and

$$x \geq \sum_{i=0}^{w-1} a_i b^i + \sum_{j=1}^{w'} c_j b^{-j} \qquad \text{and} \qquad x < \sum_{i=0}^{w-1} a_i b^i + \sum_{j=1}^{w'} c_j b^{-j} + b^{-w'}$$

3.75 in fixed-width binary, integer part width 2, fractional part width 8	
0.1 in fixed-width binary, integer part width 2, fractional part width 8	

```
|welcome $jshell
|  Welcome to JShell -- Version 10.0.1
|  For an introduction type: /help intro

jshell> 0.1
$1 ==>

jshell> 0.2
$2 ==>

jshell> 0.1 + 0.2
$3 ==>

jshell> Math.sqrt(2)
$4 ==>

jshell> Math.sqrt(2)*Math.sqrt(2)
$5 ==>

jshell>
```

Note: Java uses floating point, not fixed width representation, but similar rounding errors appear in both.

Definition: **Greatest common divisor** Let a and b be integers, not both zero. The largest integer d such that d is a factor of a and d is a factor of b is called the greatest common divisor of a and b and is denoted by $gcd(\ (a, b)\ )$. For a partial ordering, its **Hasse diagram** is a graph whose nodes (vertices) are the elements of the domain of the binary relation and which are located such that nodes connected to nodes above them by (undirected) edges indicate that the relation holds between the lower node and the higher node. Moreover, the diagram omits self-loops and omits edges that are guaranteed by transitivity.

Definition : A function $f : D \to C$ is **one-to-one** (or injective) means for every a, b in the domain D, if $f(a) = f(b)$ then $a = b$. Formally, $f : D \to C$ is one-to-one means _____.

Definition The function $append : L \times \mathbb{N} \to L$ that adds an element at the end of a linked list is defined by

Basis Step: If $m \in \mathbb{N}$ then
Recursive Step: If $l \in L$ and $n \in \mathbb{N}$ and $m \in \mathbb{N}$, then

Definition: The length of a linked list of natural numbers L, $length : L \to \mathbb{N}$ is defined by

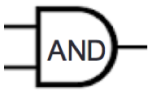
Basis Step:		$length(\ [])$	$= 0$
Recursive Step:	If $l \in L$ and $n \in \mathbb{N}$, then	$length(\ (n, l)\ )$	$= 1 + length(l)$

Definition The set of linked lists of natural numbers L is defined recursively by

Basis Step:	$[] \in L$
Recursive Step:	If $l \in L$ and $n \in \mathbb{N}$, then $(n, l) \in L$

Definition: The function $prepend : L \times \mathbb{N} \to L$ that adds an element at the front of a linked list is defined by

Inputs		Output
x	y	x AND y
1	1	1
1	0	0
0	1	0
0	0	0



Inputs		Output
x	y	x XOR y
1	1	0
1	0	1
0	1	1
0	0	0

Input	Output
x	NOT x
1	0
0	1

A relation is a **partial ordering** (or partial order) means it is reflexive, antisymmetric, and transitive. A **partition** of a set A is a set of non-empty, disjoint subsets $A_1, A_2, \cdots, A_n$ such that

$$A = \bigcup_{i=1}^{n} A_i = \{x \mid \exists i(x \in A_i)\}$$

Definition: A **predicate** is a function from a given set (domain) to $\{T, F\}$. A predicate can be applied, or **evaluated** at, an element of the domain. Usually, a predicate *describes a property* that domain elements may or may not have. Two predicates over the same domain are **equivalent** means they evaluate to the same truth values for all possible assignments of domain elements to the input. In other words, they are equivalent means that they are equal as functions. To define a predicate, we must specify its domain and its value at each domain element. The rule assigning truth values to domain elements can be specified using a formula, English description, in a table (if the domain is finite), or recursively (if the domain is recursively defined). **Definition**: The **truth set** of a predicate is the collection of all elements in its domain where the predicate evaluates to T. Notice that specifying the domain and the truth set is sufficient for defining a predicate. **Definition**: An integer p greater than 1 is called **prime** means the only positive factors of p are 1 and p. A positive integer that is greater than 1 and is not prime is called composite. The **universal**

quantification of predicate $P(x)$ over domain U is the statement "$P(x)$ for all values of x in the domain U" and is written $\forall x P(x)$ or $\forall x \in U\ P(x)$. When the domain is finite, universal quantification over the domain is equivalent to iterated *conjunction* (ands). The **existential quantification** of predicate $P(x)$ over domain U is the statement "There exists an element x in the domain U such that $P(x)$" and is written $\exists x P(x)$ for $\exists x \in U\ P(x)$. When the domain is finite, existential quantification over the domain is equivalent to iterated *disjunction* (ors). An element for which $P(x) = F$ is called a **counterexample** of $\forall x P(x)$. An element for which $P(x) = T$ is called a **witness** of $\exists x P(x)$.

Colors can be described as amounts of red, green, and blue mixed together[1] Mathematically, a color can be represented as a 3-tuple (r, g, b) where r represents the red component, g the green component, b the blue component and where each of r, g, b must be a value from this collection of numbers:

{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148, 149, 150, 151, 152, 153, 154, 155, 156, 157, 158, 159, 160, 161, 162, 163, 164, 165, 166, 167, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 178, 179, 180, 181, 182, 183, 184, 185, 186, 187, 188, 189, 190, 191, 192, 193, 194, 195, 196, 197, 198, 199, 200, 201, 202, 203, 204, 205, 206, 207, 208, 209, 210, 211, 212, 213, 214, 215, 216, 217, 218, 219, 220, 221, 222, 223, 224, 225, 226, 227, 228, 229, 230, 231, 232, 233, 234, 235, 236, 237, 238, 239, 240, 241, 242, 243, 244, 245, 246, 247, 248, 249, 250, 251, 252, 253, 254, 255}

1. **True** or **False**: $(1, 3, 4)$ fits the definition of a color above.
2. **True** or **False**: $(1, 100, 200, 0)$ fits the definition of a color above.
3. **True** or **False**: $(510, 255)$ fits the definition of a color above.
4. **True** or **False**: There is a color (r_1, g_1, b_1) where $r_1 + g_1 + b_1$ is greater than 765.
5. **True** or **False**: There is a color (r_2, g_2, b_2) where $r_2 + g_2 + b_2$ is equal to 1.
6. **True** or **False**: Another way to write the collection of allowed values for red, green, and blue components is
$$\{x \in \mathbb{N} \mid 0 \leq x \leq 255\}$$
.
7. **True** or **False**: Another way to write the collection of allowed values for red, green, and blue components is
$$\{n \in \mathbb{Z} \mid 0 \leq n \leq 255\}$$
.

[1] This RGB representation is common in web applications. Many online tools are available to play around with mixing these colors, e.g. `https://www.w3schools.com/colors/colors_rgb.asp`.

8. **True** or **False**: Another way to write the collection of allowed values for red, green, and blue components is

$$\{y \in \mathbb{Z} \mid -1 < y \leq 255\}$$

.

Recall the definition of linked lists from class. Consider this (incomplete) definition: **Definition** The function *increment* : _____ that adds 1 to the data in each node of a linked list is defined by:

		increment : _____	$\to$ _____
Basis Step:		*increment*([])	$= []$
Recursive Step:	If $l \in L, n \in \mathbb{N}$	*increment*$((n, l))$	$= (1 + n,$ *increment*$(l))$

Consider this (incomplete) definition: **Definition** The function $sum : L \to \mathbb{N}$ that adds together all the data in nodes of the list is defined by:

		$sum : L$	$\to \mathbb{N}$
Basis Step:		$sum([])$	$= 0$
Recursive Step:	If $l \in L, n \in \mathbb{N}$	$sum((n, l))$	$=$ _____

You will compute a sample function application and then fill in the blanks for the domain and codomain of each of these functions.

1. Based on the definition, what is the result of *increment*$((4, (2, (7, []))))$? Write your answer directly with no spaces.

2. Which of the following describes the domain and codomain of *increment*?

   (a) The domain is L and the codomain is $\mathbb{N}$
   (b) The domain is L and the codomain is $\mathbb{N} \times L$
   (c) The domain is $L \times \mathbb{N}$ and the codomain is L
   (d) The domain is $L \times \mathbb{N}$ and the codomain is $\mathbb{N}$
   (e) The domain is L and the codomain is L
   (f) None of the above

3. Assuming we would like $sum((5, (6, [])))$ to evaluate to 11 and $sum((3, (1, (8, []))))$ to evaluate to 12, which of the following could be used to fill in the definition of the recursive case of *sum*?

   (a) $\begin{cases} 1 + sum(l) & \text{when } n \neq 0 \\ sum(l) & \text{when } n = 0 \end{cases}$
   (b) $1 + sum(l)$
   (c) $n +$ *increment*(l)
   (d) $n + sum(l)$
   (e) None of the above

4. Choose only and all of the following statements that are **well-defined**; that is, they correctly reflect the domains and codomains of the functions and quantifiers, and respect the notational conventions we use in this class. Note that a well-defined statement may be true or false.

   (a) $\forall l \in L\,(sum(l))$
   (b) $\exists l \in L\,(sum(l) \wedge length(l))$
   (c) $\forall l \in L\,(sum(increment(l)) = 10)$
   (d) $\exists l \in L\,(sum(increment(l)) = 10)$
   (e) $\forall l \in L\,\forall n \in \mathbb{N}\,((n \times l) \subseteq L)$
   (f) $\forall l_1 \in L\,\exists l_2 \in L\,(increment(sum(l_1)) = l_2)$
   (g) $\forall l \in L\,(length(increment(l)) = length(l))$

5. Choose only and all of the statements in the previous part that are both well-defined and true.

Which of the following formalizes the definition of the predicate $Pr(x)$ over the set of integers, and evaluates to T exactly when x is prime. (Select all and only correct options.)

1. $\forall a \in \mathbb{Z}^{\neq 0}\ (\ (x > 1 \wedge a > 0) \rightarrow F(\ (a, x)\ ))$
2. $\neg\exists a \in \mathbb{Z}^{\neq 0}\ (x > 1 \wedge (a = 1 \vee a = x) \wedge F(\ (a, x)\ ))$
3. $(x > 1) \wedge \forall a \in \mathbb{Z}^{\neq 0}\ (\ (\ a > 0 \wedge F(\ (a, x)\ )\ ) \rightarrow (a = 1 \vee a = x)\ )$
4. $(x > 1) \wedge \forall a \in \mathbb{Z}^{\neq 0}\ (\ (\ a > 1 \wedge \neg(a = x)\ ) \rightarrow \neg F(\ (a, x)\ )\ )$

Which of the following are (recursive) definitions of the set of integers $\mathbb{Z}$? (Select True/False for each one.)

1.
   Basis Step: $5 \in \mathbb{Z}$
   Recursive Step: If $x \in \mathbb{Z}$, then $x + 1 \in \mathbb{Z}$ and $x - 1 \in \mathbb{Z}$

2.
   Basis Step: $0 \in \mathbb{Z}$
   Recursive Step: If $x \in \mathbb{Z}$, then $x + 1 \in \mathbb{Z}$ and $x - 1 \in \mathbb{Z}$ and $x + 2 \in \mathbb{Z}$ and $x - 2 \in \mathbb{Z}$

3.
   Basis Step: $0 \in \mathbb{Z}$
   Recursive Step: If $x \in \mathbb{Z}$, then $x + 2 \in \mathbb{Z}$ and $x - 1 \in \mathbb{Z}$

4.
   Basis Step: $0 \in \mathbb{Z}$
   Recursive Step: If $x \in \mathbb{Z}$, then $x + 1 \in \mathbb{Z}$ and $x + 2 \in \mathbb{Z}$

The **set of rational numbers**, $\mathbb{Q}$ is defined as

$$\left\{\frac{p}{q} \mid p \in \mathbb{Z} \text{ and } q \in \mathbb{Z} \text{ and } q \neq 0\right\} \quad \text{or, equivalently,} \quad \{x \in \mathbb{R} \mid \exists p \in \mathbb{Z} \exists q \in \mathbb{Z}^{+}(p = x \cdot q)\}$$

Extra practice: Use the definition of set equality to prove that the definitions above give the same set.

New! Recursive Definitions of Sets: The set S (pick a name) is defined by:

Basis Step: Specify finitely many elements of S
Recursive Step: Give rule(s) for creating a new element of S from known values existing in S, and potentially other values.

The set S then consists of all and only elements that are put in S by finitely many (a nonnegative integer number) of applications of the recursive step after the basis step. A relation R on a set A is called **reflexive** means $(a, a) \in R$ for every element $a \in A$.

Recall the definitions: The set of RNA strands S is defined (recursively) by:

Basis Step:	$\mathtt{A} \in S, \mathtt{C} \in S, \mathtt{U} \in S, \mathtt{G} \in S$
Recursive Step:	If $s \in S$ and $b \in B$, then $sb \in S$

where sb is string concatenation. The function *rnalen* that computes the length of RNA strands in S is defined recursively by:

		$rnalen : S$	$\to \mathbb{Z}^+$
Basis Step:	If $b \in B$ then	$rnalen(b)$	$= 1$
Recursive Step:	If $s \in S$ and $b \in B$, then	$rnalen(sb)$	$= 1 + rnalen(s)$

The function *basecount* that computes the number of a given base b appearing in a RNA strand s is defined recursively by:

		$basecount : S \times B$	$\to \mathbb{N}$	
Basis Step:	If $b_1 \in B, b_2 \in B$	$basecount(\ (b_1, b_2)\ )$	$= \begin{cases} 1 & \text{when } b_1 = b_2 \\ 0 & \text{when } b_1 \neq b_2 \end{cases}$	
Recursive Step:	If $s \in S, b_1 \in B, b_2 \in B$	$basecount(\ (sb_1, b_2)\ )$	$= \begin{cases} 1 + basecount(\ (s, b_2)\ ) & \text{when } b_1 = b_2 \\ basecount(\ (s, b_2)\ ) & \text{when } b_1 \neq b_2 \end{cases}$	

Definitions: A **set** is an unordered collection of elements. When A and B are sets, $A = B$ (set equality) means

$$\forall x(x \in A \leftrightarrow x \in B)$$

When A and B are sets, $A \subseteq B$ ("A is a **subset** of B") means

$$\forall x(x \in A \to x \in B)$$

When A and B are sets, $A \subsetneq B$ ("A is a **proper subset** of B") means

$$(A \subseteq B) \wedge (A \neq B)$$

Definition: A function $f : D \to C$ is **onto** (or surjective) means for every b in the codomain, there is an element a in the domain with $f(a) = b$. Formally, $f : D \to C$ is onto means _____.

A relation R on a set A is called **symmetric** means $(b, a) \in R$ whenever $(a, b) \in R$, for all $a, b \in A$.

A relation R on a set A is called **transitive** means whenever $(a, b) \in R$ and $(b, c) \in R$, then $(a, c) \in R$, for all $a, b, c \in A$.