Monday November 22

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 $f_{TF} : A \times B \to \{T, F\}$ 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 $f_{\mathcal{P}} : A \to \mathcal{P}(B)$ 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 relation R on a set A, we can represent this relation as a **graph**: a collection of nodes (vertices) and edges (arrows). The nodes of the graph are the elements of A and there is an edge from a to b exactly when $(a,b) \in R$.

Example: For $A = \mathcal{P}(\mathbb{R})$, we can define the relation $EQ_{\mathbb{R}}$ on A as

$$\{(X_1, X_2) \in \mathcal{P}(\mathbb{R}) \times \mathcal{P}(\mathbb{R}) \mid |X_1| = |X_2|\}$$

Example: Let $R_{(\textbf{mod } n)}$ be the set of all pairs of integers (a,b) such that $(a \textbf{ mod } n = b \textbf{ mod } n)$. Then a is **congruent to** b **mod** n means $(a,b) \in R_{(\textbf{mod } n)}$. A common notation is to write this as $a \equiv b(\textbf{mod } n)$.

$R_{(\textbf{mod } n)}$ is a relation on the set ______________________________

Some example elements of $R_{(\textbf{mod } 4)}$ are:

A relation R on a set A is called **reflexive** means $(a, a) \in R$ for every element $a \in A$.

Informally, every element is related to itself.

Graphically, there are self-loops (edge from a node back to itself) at every node.

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

Informally, order doesn't matter for this relation.

Graphically, every edge has a paired "backwards" edge so we might as well drop the arrows and think of edges as undirected.

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 $a, b, c \in A$.

Informally, chains of relations collapse.

Graphically, there's a shortcut between any endpoints of a chain of edges.

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

Informally: the relation has directionality.

Graphically, can organize the nodes of the graph so that all non-self loop edges go up.

When the domain is $\{a, b, c, d, e, f, g, h\}$ define a relation that is **not reflexive** and is **not symmetric** and is **not transitive**.

When the domain is $\{a, b, c, d, e, f, g, h\}$ define a relation that is **not reflexive** but is **symmetric** and is **transitive**.

When the domain is $\{a, b, c, d, e, f, g, h\}$ define a relation that is **symmetric** and is **antisymmetric**.

Is the relation $EQ_{\mathbb{R}}$ reflexive? symmetric? transitive? antisymmetric?

Is the relation $R_{(\textbf{mod } 4)}$ reflexive? symmetric? transitive? antisymmetric?

Is the relation Sub on $W = \mathcal{P}(\{1, 2, 3, 4, 5\})$ given by $Sub = \{(X, Y) \mid X \subseteq Y\}$ reflexive? symmetric? transitive? antisymmetric?

A relation is an **equivalence relation** means it is reflexive, symmetric, and transitive.

A relation is a **partial ordering** (or partial order) means it is reflexive, antisymmetric, and transitive.

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.

Draw the Hasse diagram of the partial order on the set $\{a, b, c, d, e, f, g\}$ defined as

$$\begin{gathered}\{(a,a),(b,b),(c,c),(d,d),(e,e),(f,f),(g,g),\\ (a,c),(a,d),(d,g),(a,g),(b,f),(b,e),(e,g),(b,g)\}\end{gathered}$$

Summary: binary relations can be useful for organizing elements in a domain. Some binary relations have special properties that make them act like some familiar relations. Equivalence relations (reflexive, symmetric, transitive binary relations) "act like" equals. Partial orders (reflexive, antisymmetric, transitive binary relations) "act like" less than or equals to.

Review

1.

Recall that the binary relation $EQ_{\mathbb{R}}$ on $\mathcal{P}(\mathbb{R})$ is

$$\{(X_1, X_2) \in \mathcal{P}(\mathbb{R}) \times \mathcal{P}(\mathbb{R}) \mid |X_1| = |X_2|\}$$

and $R_{(\textbf{mod } n)}$ is the set of all pairs of integers (a, b) such that $(a \textbf{ mod } n = b \textbf{ mod } n)$.

Select all and only the correct items.

(a) $(\mathbb{Z}, \mathbb{R}) \in EQ_{\mathbb{R}}$

(b) $(0, 1) \in EQ_{\mathbb{R}}$

(c) $(\emptyset, \emptyset) \in EQ_{\mathbb{R}}$

(d) $(-1, 1) \in R_{(\textbf{mod } 2)}$

(e) $(1, -1) \in R_{(\textbf{mod } 3)}$

(f) $(4, 16, 0) \in R_{(\textbf{mod } 4)}$

2.

Consider the binary relation on $\mathbb{Z}^+$ defined by $\{(a, b) \mid \exists c \in \mathbb{Z}(b = ac)\}$. Select all and only the properties that this binary relation has.

(a) It is reflexive.

(b) It is symmetric.

(c) It is transitive.

(d) It is antisymmetric.

3.

(a) Consider the partial order on the set $\mathcal{P}(\{1, 2, 3\})$ given by the binary relation $\{(X, Y) \mid X \subseteq Y\}$

i. How many nodes are in the Hasse diagram of this partial order?

ii. How many edges are in the Hasse diagram of this partial order?

(b) Consider the binary relation on $\{1, 2, 4, 5, 10, 20\}$ defined by $\{(a, b) \mid \exists c \in \mathbb{Z}(b = ac)\}$.

i. How many nodes are in the Hasse diagram of this partial order?

ii. How many edges are in the Hasse diagram of this partial order?

Wednesday November 24

Exploring equivalence relations

A **partition** of a set A is a set of non-empty, disjoint subsets $A_1, A_2, \cdots, A_n$ such that

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

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

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

We write $[a]_R$ for this set, which is the equivalence class of a with respect to R.

Fact: When R is an equivalence relation on a nonempty set A, the collection of equivalence classes of R is a partition of A.

Also, given a partition P of A, the relation R_P on A given by

$$R_P = \{(x,y) \in A \times A \mid x \text{ and } y \text{ are in the same part of the partition } P\}$$

is an equivalence relation on A.

Recall: We say a is **congruent to** b **mod** n means $(a,b) \in R_{(\textbf{mod } n)}$. A common notation is to write this as $a \equiv b(\textbf{mod } n)$.

We can partition the set of integers using equivalence classes of $R_{(\textbf{mod } 4)}$

$$\begin{aligned}
[0]_{R_{(\textbf{mod } 4)}} &= \\
[1]_{R_{(\textbf{mod } 4)}} &= \\
[2]_{R_{(\textbf{mod } 4)}} &= \\
[3]_{R_{(\textbf{mod } 4)}} &= \\
[4]_{R_{(\textbf{mod } 4)}} &= \\
[5]_{R_{(\textbf{mod } 4)}} &= \\
[-1]_{R_{(\textbf{mod } 4)}} &=
\end{aligned}$$

$$\mathbb{Z} = [0]_{R_{(\textbf{mod } 4)}} \cup [1]_{R_{(\textbf{mod } 4)}} \cup [2]_{R_{(\textbf{mod } 4)}} \cup [3]_{R_{(\textbf{mod } 4)}}$$

Integers are useful because they can be used to encode other objects and have multiple representations. However, infinite sets are sometimes expensive to work with computationally. Reducing our attention to a *partition of the integers* based on congrunce mod n, where each part is represented by a (not too large) integer gives a useful compromise where many algebraic properties of the integers are preserved, and we also get the benefits of a finite domain. Moreover, modular arithmetic is well-suited to model any cyclic behavior.

Lemma : For $a, b \in \mathbb{Z}$ and positive integer n, $(a, b) \in R_{(\textbf{mod } n)}$ if and only if $n | a - b$.

Proof:

Application: Cycling

How many minutes past the hour are we at? *Model with* $+15$ **mod** 60

Time:	12:00pm	12:15pm	12:30pm	12:45pm	1:00pm	1:15pm	1:30pm	1:45pm	2:00pm
"Minutes past":	0	15	30	45	0	15	30	45	0

Replace each English letter by a letter that's fifteen ahead of it in the alphabet *Model with* $+15$ **mod** 26

Original index:	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
Original letter:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Shifted letter:	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Shifted index:	15	16	17	18	19	20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14

Modular arithmetic:

Lemma: For $a, b, c, d \in \mathbb{Z}$ and positive integer n, if $a \equiv b$ (**mod** n) and $c \equiv d$ (**mod** n) then $a + c \equiv b + d$ (**mod** n) and $ac \equiv bd$ (**mod** n). **Informally**: can bring mod "inside" and do it first, for addition and for multiplication.

$(102 + 48)$ **mod** $10 =$ ____________________________________

$(7 \cdot 10)$ **mod** $5 =$ ____

(2^5) **mod** $3 =$ ____

Application: Cryptography

Definition: Let a be a positive integer and p be a large[1] prime number, both known to everyone. Let k_1 be a secret large number known only to person P_1 (Alice) and k_2 be a secret large number known only to person P_2 (Bob). Let the **Diffie-Helman shared key** for a, p, k_1, k_2 be $(a^{k_1 \cdot k_2} \textbf{ mod } p)$.

Idea: P_1 can quickly compute the Diffie-Helman shared key knowing only a, p, k_1 and the result of $a^{k_2} \textbf{ mod } p$ (that is, P_1 can compute the shared key without knowing k_2, only $a^{k_2} \textbf{ mod } p$). Similarly, P_2 can quickly compute the Diffie-Helman shared key knowing only a, p, k_2 and the result of $a^{k_1} \textbf{ mod } p$ (that is, P_2 can compute the shared key without knowing k_1, only $a^{k_1} \textbf{ mod } p$). But, any person P_3 who knows neither k_1 nor k_2 (but may know any and all of the other values) cannot compute the shared secret efficiently.

Key property for *shared* secret:

$$\forall a \in \mathbb{Z}\, \forall b \in \mathbb{Z}\, \forall g \in \mathbb{Z}^+\, \forall n \in \mathbb{Z}^+ ((g^a \textbf{ mod } n)^b, (g^b \textbf{ mod } n)^a) \in R_{(\textbf{mod } n)}$$

Key property for shared *secret*:

There are efficient algorithms to calculate the result of modular exponentiation but there are no (known) efficient algorithms to calculate discrete logarithm.

[1] We leave the definition of "large" vague here, but think hundreds of digits for practical applications. In practice, we also need a particular relationship between a and p to hold, which we leave out here.

Review

1.

Fill in the blanks in the following proof that, for any equivalence relation R on a set A,

$$\forall a \in A\ \forall b \in A\ \ ((a,b) \in R \leftrightarrow [a]_R \cap [b]_R \neq \emptyset)$$

Proof: Towards a **(a)**________________, consider arbitrary elements a, b in A. We will prove the biconditional statement by proving each direction of the conditional in turn.

Goal 1: we need to show $(a,b) \in R \to [a]_R \cap [b]_R \neq \emptyset$ *Proof of Goal 1*: Assume towards a **(b)**________________ that $(a,b) \in R$. We will work to show that $[a]_R \cap [b]_R \neq \emptyset$. Namely, we need an element that is in both equivalence classes, that is, we need to prove the existential claim $\exists x \in A\ (x \in [a]_R \wedge x \in [b]_R)$. Towards a **(c)**________________, consider $x = b$, an element of A by definition. By **(d)**________________ of R, we know that $(b,b) \in R$ and thus, $b \in [b]_R$. By assumption in this proof, we have that $(a,b) \in R$, and so by definition of equivalence classes, $b \in [a]_R$. Thus, we have proved both conjuncts and this part of the proof is complete.

Goal 2: we need to show $[a]_R \cap [b]_R \neq \emptyset \to (a,b) \in R$ *Proof of Goal 2*: Assume towards a **(e)**________________ that $[a]_R \cap [b]_R \neq \emptyset$. We will work to show that $(a,b) \in R$. By our assumption, the existential claim $\exists x \in A\ (x \in [a]_R \wedge x \in [b]_R)$ is true. Call w a witness; thus, $w \in [a]_R$ and $w \in [b]_R$. By definition of equivalence classes, $w \in [a]_R$ means $(a,w) \in R$ and $w \in [b]_R$ means $(b,w) \in R$. By **(f)**________________ of R, $(w,b) \in R$. By **(g)**________________ of R, since $(a,w) \in R$ and $(w,b) \in R$, we have that $(a,b) \in R$, as required for this part of the proof.

Consider the following expressions as options to fill in the two proofs above. Give your answer as one of the numbers below for each blank a-c. You may use some numbers for more than one blank, but each letter only uses one of the expressions below.

i exhaustive proof

ii proof by universal generalization

iii proof of existential using a witness

iv proof by cases

v direct proof

vi proof by contrapositive

vii proof by contradiction

viii reflexivity

ix symmetry

x transitivity

2.

Modular exponentiation is required to carry out the Diffie-Helman protocol for computing a shared secret over an unsecure channel.

Consider the following algorithm for fast exponentiation (based on binary expansion of the exponent).

Modular Exponentation

```
procedure modular exponentiation(b: integer;
            $n = (a_{k-1}a_{k-2}\ldots a_1a_0)_2$, m: positive integers)
$x$ := 1
power := $b$ mod $m$
for $i$ := 0 to $k-1$
    if $a_i = 1$ then $x$ := ($x \cdot$ power) mod $m$
    power := (power $\cdot$ power) mod $m$
return $x$ {$x$ equals $b^n$ mod $m$}
```

(a) If we wanted to calculate 3^8 **mod** 7 using the modular exponentation algorithm above, what are the values of the parameters b, n, and m? (Write these values in usual, decimal-like, mathematical notation.)

(b) Give the output of the *modular exponentiation* algorithm with these parameters, i.e. calculate 3^8 **mod** 7. (Write these values in usual, decimal-like, mathematical notation.)

Friday November 26

No class, in observance of Thanksgiving holiday.