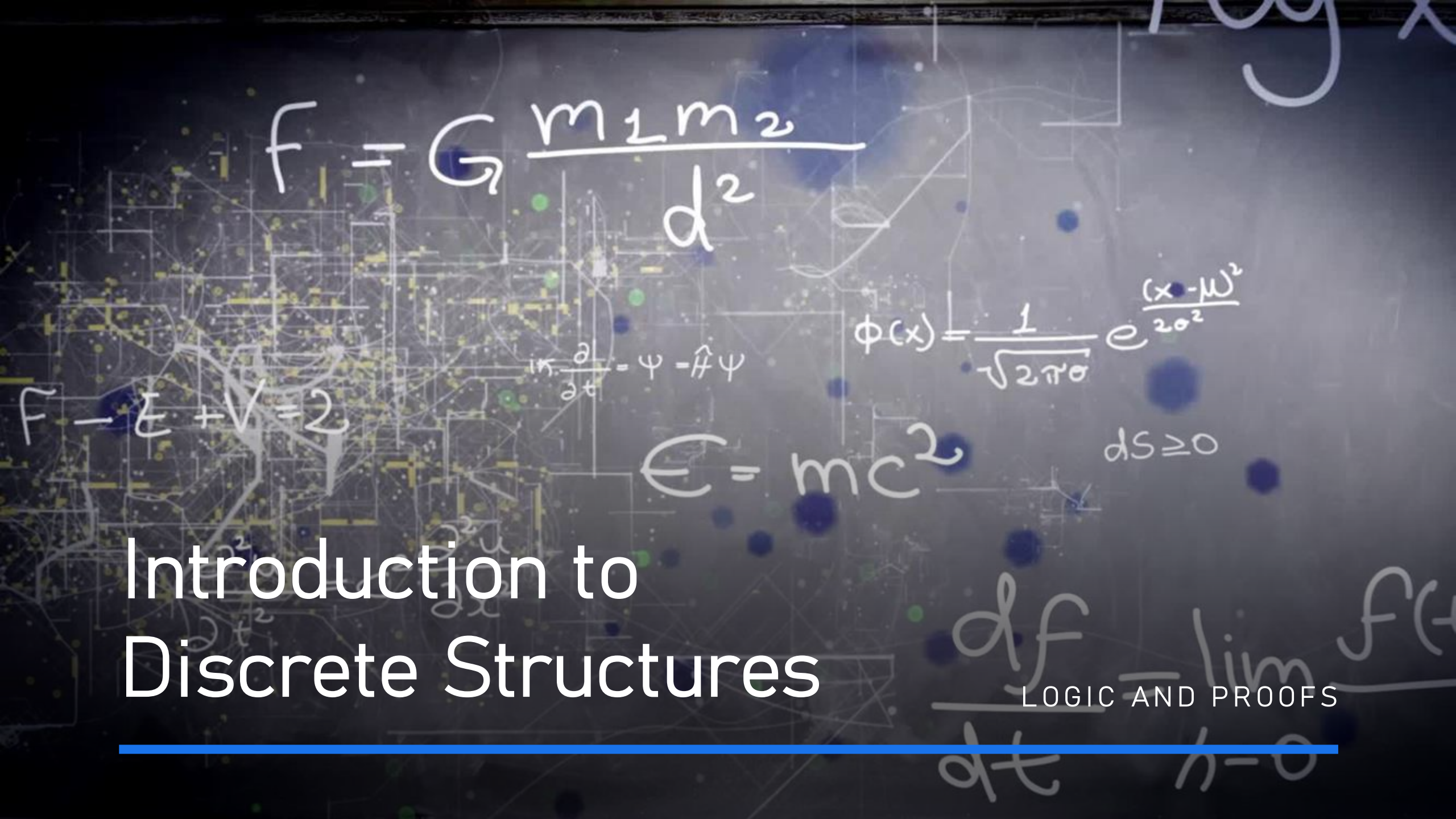
OL Academy

ITCS254/258
Discrete Structures I

T.Adnan Hashim



Introduction to Discrete Structures

LOGIC AND PROOFS

Session Roadmap

Motivating Questions

Teaching Style

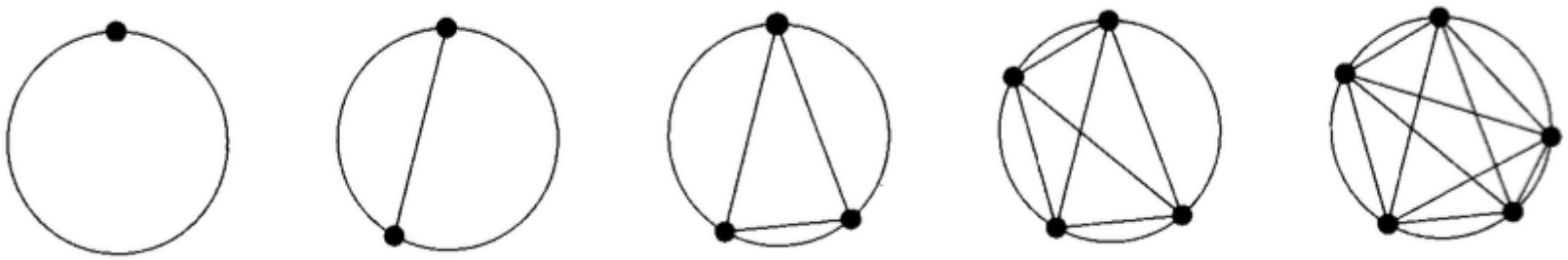
Overview of Discrete Math (also called Discrete Structures)

Propositional Logic Exercises

Fun Question: Guess the number

- Without telling me, choose a number from {1, 2, 3, ..., n}, where n is any Natural number.
- I will guess the number in "few" steps only by asking you:
  - Is the number you chose less than x (where x a number I will choose each time differently)?
- I will only need a maximum of ceil($\log_2(n)$) steps.
  - Ex. If n = 1000, and you choose any number in {1, 2, 3, ..., 1000}, I will guess it in at most 10 steps.

Observe the following and guess the next



$n = 1$
1 region

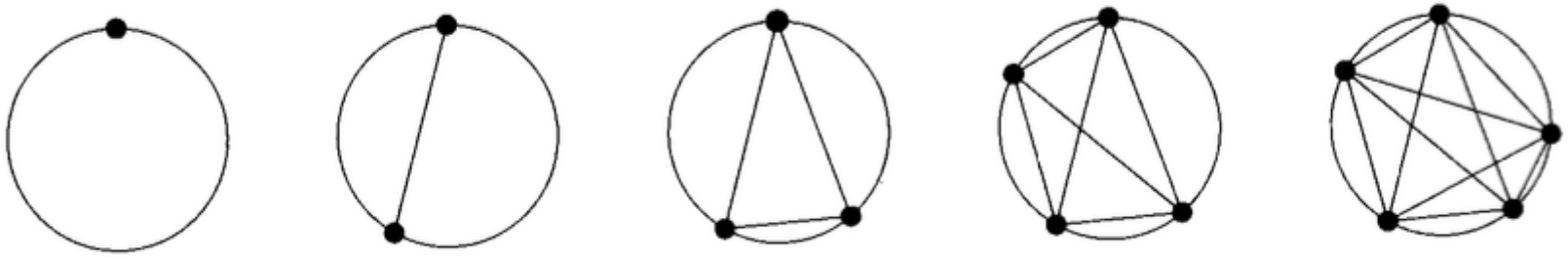
$n = 2$
2 regions

$n = 3$
4 regions

$n = 4$
8 regions

$n = 5$
16 regions

Claim: # regions = 2^n ? Examples are proof?



$n = 1$
1 region

$n = 2$
2 regions

$n = 3$
4 regions

$n = 4$
8 regions

$n = 5$
16 regions

Teaching Style

Focus on teaching you how to think, not just how to get high grades.

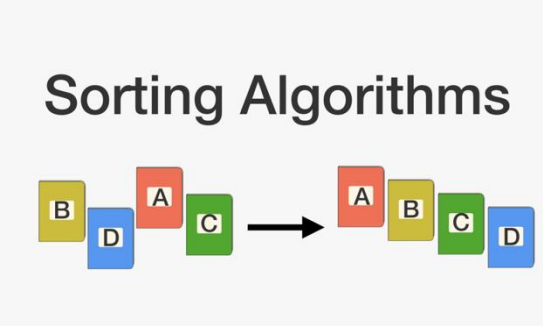
Demonstrate how beautiful the subject is.

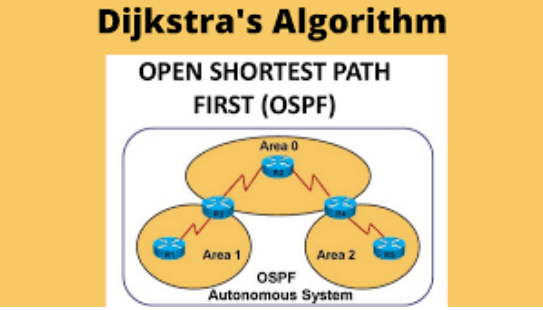
Interactive (e.g. We both solve questions, and compare our answers)

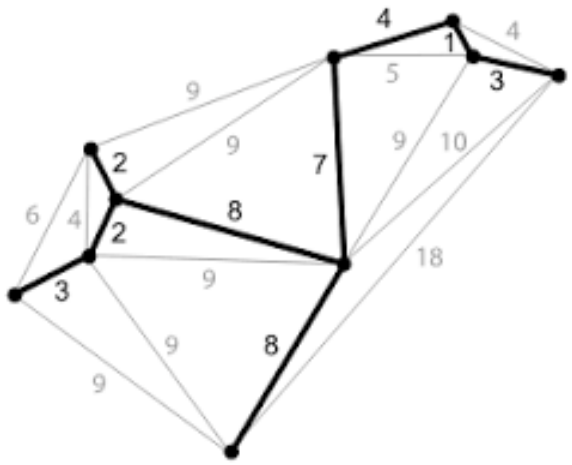
Assume minimum background knowledge.

I love being challenged and asked questions.

Discrete Math Applications: Analysis of Algorithms







- Insertion Sort, Merge Sort, Quick Sort, etc.
- Dijkstra's Algorithm (for shortest path)
- Minimum Spanning Tree Algorithms

Theorem 10.6.4 Correctness of Dijkstra's Algorithm

When a connected, simple graph with a positive weight for every edge is input to Dijkstra's algorithm with starting vertex a and ending vertex z, the output is the length of a shortest path from a to z.

Proof:

Let G be a connected, weighted graph with no loops or parallel edges and with a positive weight for every edge. Let T be the graph built up by Dijkstra's algorithm, and for each vertex u in G, let $L(u)$ be the label given by the algorithm to vertex u. For each integer $n \geq 0$, let the property $P(n)$ be the sentence

> After the nth iteration of the while loop in Dijkstra's algorithm, (1) T is a tree, and (2) for every vertex v in T, $L(v)$ is the length of a shortest path in G from a to v. ←$P(n)$

We will show by mathematical induction that $P(n)$ is true for each integer n from 0 through the termination of the algorithm.

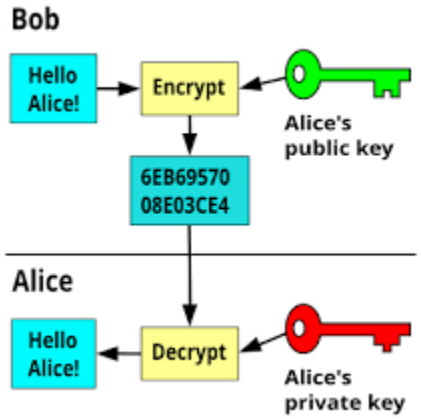
Show that P(0) is true: When $n = 0$, the graph T is a tree because it is defined to consist only of the vertex a and no edges. In addition, $L(a)$ is the length of the shortest path from a to a because the initial value of $L(a)$ is 0.

Show that for every integer k ≥ 0, if P(k) is true then P(k +1) is also true: Let k be any integer with $k \geq 0$ and suppose that

> After the kth iteration of the while loop in Dijkstra's algorithm, (1) T is a tree, and (2) for every vertex v in T, $L(v)$ is the length of a shortest path in G from a to v. ←$P(k)$ inductive hypothesis

Dijkstra's proof of correctness snippet

Discrete Math Applications: Cryptography



RSA Algorithm

Blockchains

Cryptocurrencies

The RSA cryptosystem

In the ***RSA public-key cryptosystem***, a participant creates his or her public and secret keys with the following procedure:

1. Select at random two large prime numbers p and q such that $p \neq q$. The primes p and q might be, say, 1024 bits each.
2. Compute $n = pq$.
3. Select a small odd integer e that is relatively prime to $\phi(n)$, which, by equation (31.20), equals $(p-1)(q-1)$.
4. Compute d as the multiplicative inverse of e, modulo $\phi(n)$. (Corollary 31.26 guarantees that d exists and is uniquely defined. We can use the technique of Section 31.4 to compute d, given e and $\phi(n)$.)
5. Publish the pair $P = (e, n)$ as the participant's ***RSA public key***.
6. Keep secret the pair $S = (d, n)$ as the participant's ***RSA secret key***.

For this scheme, the domain $\mathcal{D}$ is the set $\mathbb{Z}_n$. To transform a message M associated with a public key $P = (e, n)$, compute

$$P(M) = M^e \bmod n \ . \tag{31.37}$$

To transform a ciphertext C associated with a secret key $S = (d, n)$, compute

$$S(C) = C^d \bmod n \ . \tag{31.38}$$

These equations apply to both encryption and signatures. To create a signature, the signer applies his or her secret key to the message to be signed, rather than to a ciphertext. To verify a signature, the public key of the signer is applied to it, rather than to a message to be encrypted.

Theorem 31.36 (Correctness of RSA)
The RSA equations (31.37) and (31.38) define inverse transformations of $\mathbb{Z}_n$ satisfying equations (31.35) and (31.36).

Proof From equations (31.37) and (31.38), we have that for any $M \in \mathbb{Z}_n$,

$$P(S(M)) = S(P(M)) = M^{ed} \pmod{n} .$$

Since e and d are multiplicative inverses modulo $\phi(n) = (p-1)(q-1)$,

$$ed = 1 + k(p-1)(q-1)$$

for some integer k. But then, if $M \not\equiv 0 \pmod{p}$, we have

$$\begin{aligned}
M^{ed} &\equiv M(M^{p-1})^{k(q-1)} && \pmod{p} \\
&\equiv M((M \bmod p)^{p-1})^{k(q-1)} && \pmod{p} \\
&\equiv M(1)^{k(q-1)} && \pmod{p} \qquad \text{(by Theorem 31.31)} \\
&\equiv M && \pmod{p} .
\end{aligned}$$

Also, $M^{ed} \equiv M \pmod{p}$ if $M \equiv 0 \pmod{p}$. Thus,

$$M^{ed} \equiv M \pmod{p}$$

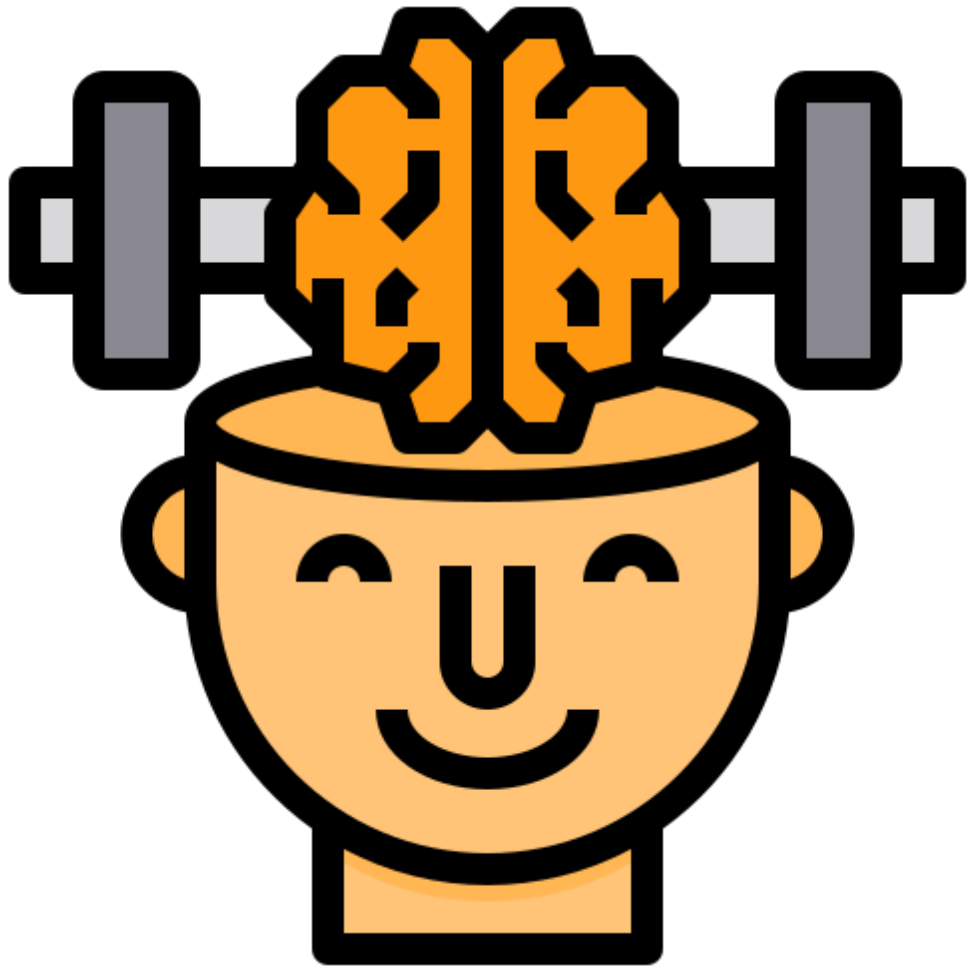
for all M. Similarly,

$$M^{ed} \equiv M \pmod{q}$$

for all M. Thus, by Corollary 31.29 to the Chinese remainder theorem,

$$M^{ed} \equiv M \pmod{n}$$

for all M. ■



Exercises

Which of these sentences are propositions? What are the truth values of those that are propositions?

a) Boston is the capital of Massachusetts.
b) Miami is the capital of Florida.
c) $2 + 3 = 5$.
d) $5 + 7 = 10$.
e) $x + 2 = 11$.
f) Answer this question.

Hint: Review what "proposition" mean.

Def (Proposition): A proposition is a declarative sentence (that is, a sentence that declares a fact) that is either true or false, but not both.

What is the negation of each of these propositions?

a) Linda is younger than Sanjay.
b) Mei makes more money than Isabella.
c) Moshe is taller than Monica.
d) Abby is richer than Ricardo.

Hint: Review what "negation" means.

Let p be a proposition. The *negation of* p, denoted by $\neg p$ (also denoted by $\overline{p}$), is the statement

"It is not the case that p."

The proposition $\neg p$ is read "not p." The truth value of the negation of p, $\neg p$, is the opposite of the truth value of p.

7. What is the negation of each of these propositions?

a) Steve has more than 100 GB free disk space on his laptop.

b) Zach blocks e-mails and texts from Jennifer.

c) $7 \cdot 11 \cdot 13 = 999$.

d) Diane rode her bicycle 100 miles on Sunday.

Hint: Review what "negation" means.

Let p be a proposition. The *negation of* p, denoted by $\neg p$ (also denoted by $\overline{p}$), is the statement

"It is not the case that p."

The proposition $\neg p$ is read "not p." The truth value of the negation of p, $\neg p$, is the opposite of the truth value of p.

11. Let p and q be the propositions "Swimming at the New Jersey shore is allowed" and "Sharks have been spotted near the shore," respectively. Express each of these compound propositions as an English sentence.

a) $\neg q$ **b)** $p \wedge q$ **c)** $\neg p \vee q$

d) $p \rightarrow \neg q$ **e)** $\neg q \rightarrow p$ **f)** $\neg p \rightarrow \neg q$

g) $p \leftrightarrow \neg q$ **h)** $\neg p \wedge (p \vee \neg q)$

Hint: Review what the following mean:

- Disjunction (∨)
- Conjunction (∧)
- Implication (→)
- Biconditional (↔)

See the next pages for the full definitions.

Def (Conjunction (∧))

Let p and q be propositions. The *conjunction* of p and q, denoted by $p \wedge q$, is the proposition "p and q." The conjunction $p \wedge q$ is true when both p and q are true and is false otherwise.

TABLE 2 The Truth Table for the Conjunction of Two Propositions.

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

Def (Disjunction (∨))

Let p and q be propositions. The *disjunction* of p and q, denoted by $p \vee q$, is the proposition "p or q." The disjunction $p \vee q$ is false when both p and q are false and is true otherwise.

TABLE 3 The Truth Table for the Disjunction of Two Propositions.

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

Def (Implication (p→q))

Let p and q be propositions. The *conditional statement* $p \rightarrow q$ is the proposition "if p, then q." The conditional statement $p \rightarrow q$ is false when p is true and q is false, and true otherwise. In the conditional statement $p \rightarrow q$, p is called the *hypothesis* (or *antecedent* or *premise*) and q is called the *conclusion* (or *consequence*).

TABLE 5 The Truth Table for the Conditional Statement $p \rightarrow q$.

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

Def (Biconditional (p↔q))

Let p and q be propositions. The *biconditional statement* $p \leftrightarrow q$ is the proposition "p if and only if q." The biconditional statement $p \leftrightarrow q$ is true when p and q have the same truth values, and is false otherwise. Biconditional statements are also called *bi-implications*.

TABLE 6 The Truth Table for the Biconditional $p \leftrightarrow q$.

p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

Different ways of saying "p → q"

- “if p, then q”
- “p implies q”
- “if p, q”
- “p only if q”
- “p is sufficient for q”
- “a sufficient condition for q is p”
- “q if p”
- “q whenever p”
- “q when p”
- “q is necessary for p”
- “a necessary condition for p is q ”
- “q follows from p”
- “q unless ¬p”
- “q provided that p”

15. Let p and q be the propositions

p: You drive over 65 miles per hour.
q: You get a speeding ticket.

Write these propositions using p and q and logical connectives (including negations).

a) You do not drive over 65 miles per hour.
b) You drive over 65 miles per hour, but you do not get a speeding ticket.
c) You will get a speeding ticket if you drive over 65 miles per hour.
d) If you do not drive over 65 miles per hour, then you will not get a speeding ticket.
e) Driving over 65 miles per hour is sufficient for getting a speeding ticket.
f) You get a speeding ticket, but you do not drive over 65 miles per hour.
g) Whenever you get a speeding ticket, you are driving over 65 miles per hour.

19. Determine whether each of these conditional statements is true or false.

a) If $1 + 1 = 2$, then $2 + 2 = 5$.

b) If $1 + 1 = 3$, then $2 + 2 = 4$.

c) If $1 + 1 = 3$, then $2 + 2 = 5$.

d) If monkeys can fly, then $1 + 1 = 3$.

25. Write each of these statements in the form "if p, then q" in English. [*Hint:* Refer to the list of common ways to express conditional statements.]

a) It snows whenever the wind blows from the northeast.
b) The apple trees will bloom if it stays warm for a week.
c) That the Pistons win the championship implies that they beat the Lakers.
d) It is necessary to walk eight miles to get to the top of Long's Peak.
e) To get tenure as a professor, it is sufficient to be world famous.
f) If you drive more than 400 miles, you will need to buy gasoline.
g) Your guarantee is good only if you bought your CD player less than 90 days ago.
h) Jan will go swimming unless the water is too cold.
i) We will have a future, provided that people believe in science.

27. Write each of these propositions in the form "p if and only if q" in English.

a) If it is hot outside you buy an ice cream cone, and if you buy an ice cream cone it is hot outside.

b) For you to win the contest it is necessary and sufficient that you have the only winning ticket.

c) You get promoted only if you have connections, and you have connections only if you get promoted.

d) If you watch television your mind will decay, and conversely.

e) The trains run late on exactly those days when I take it.

29. State the converse, contrapositive, and inverse of each of these conditional statements.

a) If it snows today, I will ski tomorrow.

b) I come to class whenever there is going to be a quiz.

c) A positive integer is a prime only if it has no divisors other than 1 and itself.

Hint: Review what "converse", "contrapositive", and "inverse" means.

Def (Converse): The proposition $q \rightarrow p$ is called the converse of $p \rightarrow q$.

Def (Contrapositive): The contrapositive of $p \rightarrow q$ is the proposition $\neg q \rightarrow \neg p$.

Def (Inverse): The proposition $\neg p \rightarrow \neg q$ is called the inverse of $p \rightarrow q$.

Important Note: only the **contrapositive** always has the same truth value as $p \rightarrow q$. Why?