BBM 205 LOGICAL RULES

· proposition

statement = ifade

proposition = önerme

$2+2=4$ ✓ prop.

it may rain today. (not a prop.)

Our midterm exam is on Nov. 23. (not a prop.)

p, q, r typical names for prop's.

$p \rightarrow q$: read as "p implies q" (sebebi olmak) ise

T = true
F = false

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

p: $n=12$

q: n is even.

even = gift

odd = ~~gift~~ tek

p	q	$p \rightarrow q$
$n=12$	n, even	T
$n=12$	n, odd	F
$n \neq 12$	n, even	T (n can be still an even number)
$n \neq 12$	n, odd	T

$\Longleftrightarrow$ (Favorite for BBM 205)

$p \Longleftrightarrow q$ means $(p \rightarrow q) \wedge (q \rightarrow p)$

p	q	$p \rightarrow q$	$q \rightarrow p$	$p \leftrightarrow q$
0	0	1	1	1
0	1	1	0	0
1	0	0	1	0
1	1	1	1	1

$\Longleftrightarrow$ read as "$\underbrace{\text{if and only if}}_{\text{iff}}$"

② $p \Longleftrightarrow q$ is true only when p and q have the same value EQUIVALENCE!

- if p & q are EQUIVALENT that means that they are both correct or they are both false.

! EQUIVALENT does not mean EQUAL, EQUIVALENT, "$\equiv$" is ~~the~~ a logical term.

<u>Ex:</u>

$$\left.\begin{array}{l} p: x^2-4 \geq 0 \\ q: |x| \geq 2 \end{array}\right\} \text{mathematically, } p \Longleftrightarrow q$$

'iff'

Other favorite terms for BBM 205:

For $p \to q$

♥ · contrapositive : $\neg q \to \neg p$

· converse : $q \to p$

· inverse : $\neg p \to \neg q$

Ex: $p: n=12$, $q: n$, even $\quad p \to q$, T

contrap. $\neg q \to \neg p$: If n, odd then $n \neq 12$

conv. $q \to p$: If n, even then $n=12$? TRUE

inv. $\neg p \to \neg q$: If $n \neq 12$, then n, odd ?

③ observe:

If $p \to q$ true, converse and inverse may not be true

p	q	$\neg p$	$\neg q$	$p \to q$	$\neg q \to \neg p$
0	0	1	1	1	1
0	1	1	0	1	1
1	0	0	1	0	0
1	1	0	0	1	1

Shows $p \to q$ is EQUIVALENT to $\neg q \to \neg p$

$$\boxed{p \to q \equiv \neg q \to \neg p}$$

Preview for next week: coming....

<u>Predicates:</u>

<u>Prop</u>: $p(n) = n^2 + n + 41$ is prime (asa) for every nonnegative integer n.

<u>Claim</u>: Prop. is False. $n \in \mathbb{Z}^+ \cup \{0\}$

True or False?

$$p(40) = 40^2 + 40 + 41 = \underbrace{40(40+1)}_{41^2} + 41$$

$$\underbrace{41(40+1)}_{41}$$

Four Color Thm. (1976): <u>Every</u> map can be colored by using four color s.t. no two neighbor regions get the same color.

such that

Goldbach's Conjecture (1742): Every even integer greater than 2 is the sum of two primes.

Conjecture means no one knows its truth value (if it is T or F).

$$4 = 2+2,\ 6 = 3+3,\ 8 = 3+5, \ldots$$

<u>Some Logical Notation</u> (symbols)

$\forall$: "for all" $\in$: "is in"

$\exists$: "there exists"

$\forall x \in D, P(x)$: For all x in D, P(x) is true.

such that (öyle ki) such that

Domain

$\exists x \in D, P(x)$: There exists (some) an x in D such that P(x) is true.

Goldbach's Conj. in Logical Notation:

$D := \{$All even integers $> 2\}$.

P := set of primes

$$\forall n \in D, \underbrace{\exists p, q \in P \text{ s.t. } n = p + q}_{\text{little } p \text{ not } P \quad p(n)}.$$

Note: $\forall$, $\exists$ are called Quantifiers.

$\forall$: Universal Quantifier

$\exists$: Existential Quantifier

Discussion: How would you show $\forall x \in D, P(x)$? You need some mathematical arguments, esp. if D is an infinite set.

esp. = especially

Ex: $\forall x \in \mathbb{R}$, $x + 1 > x$. Show this.

$\mathbb{R}$ = real

- Subtract x from both sides

$$\left.\begin{array}{r} x+1 > x \\ -x \quad\quad -x \end{array}\right\} 1 > 0 \text{ True.}$$

Predicate:	Its negation:
$\forall x \in D, P(x)$	$\exists x \in D, \neg P(x)$
$\exists x \in D, P(x)$	$\forall x \in D, \neg P(x)$

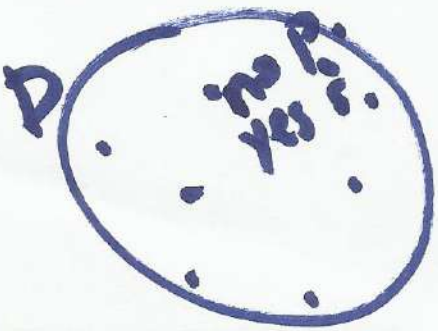
$\neg P(x)$: not $P(x)$ (if $P(x)$, T
$\neg P(x)$, F vice versa)

Ex: $D = \mathbb{R}$
$P(x): x > 0$

Question: $\forall x \in \mathbb{R}, P(x)$? T or F
(if answer is F, then show that the negation of this is T.)

Answer: F
To show neg., give one x for which $p(x)$ is false, e.g. $x = -1$.
$P(-1)$ is F, thus $\forall x \in \mathbb{R}, P(x)$ is F.

<u>Ex</u>: $\forall x \in D, (\neg C(x) \wedge TS(x)) \overset{?}{\equiv} \neg \exists x \in D, (C(x) \wedge S(x))$
?NO!!



<u>Ex:</u> $\forall x \in D, \neg(C(x) \wedge S(x)) \overset{?}{\equiv} \neg \exists x \in D, C(x) \wedge S(x).$

NO QUIZ TODAY.

Recall proof by contradiction:

$$\begin{array}{c} p \\ \neg q \\ \hline F \end{array}$$

If $\neg q \wedge p \rightarrow F$, then only possible if $\neg q = F$. So, we get $q = T$.

Today: Proof by induction.

We want to show that $P(n)$ is true, for all $n \geq 0$ (or sometimes for all $n \geq k$).

Then, all we need is to show:

1) $P(0)$ is true

2) $P(n) \rightarrow P(n+1)$ is true for all $n \geq 0$.

$P(n)$, True for all $n \geq 0$.

This means:

$n=0$

$$\begin{array}{c} P(0), \text{True} \\ P(0) \rightarrow P(1) \\ \hline P(1), T \end{array} \qquad \begin{array}{c} P(1), T \\ P(1) \rightarrow P(2) \\ \hline P(2), T \end{array} \quad \cdots\cdots \quad \begin{array}{c} P(n), T \\ P(n) \rightarrow P(n+1) \\ \hline P(n+1), T \end{array} \quad \cdots$$

By Modus Ponens Rule

To show $P(n), T \ \forall n \geq 0$, we prove two things: 1) $P(0), T$ - Base Case

2) $(P(n) \rightarrow P(n+1)), T$ Inductive Case

<u>Ex:</u> Show that $1+2+\ldots+n = \frac{n(n+1)}{2}, \forall n \geq 0.$

- predicate

0) $P(n)$: $1+2+\ldots+n = \frac{n(n+1)}{2}$.

want to show $P(n), T \ \forall n \geq 0$:

✓ 1) Base Case: Show that $P(0), T$: $\sum_{i=1}^{0} i = 0$

Remark: $\sum_{i=a}^{b} f(i) = 0$ $\quad b<a$

Formula works $\frac{0 \cdot (0+1)}{2} = 0$

✓ 2) To show $P(n) \rightarrow P(n+1)$ means

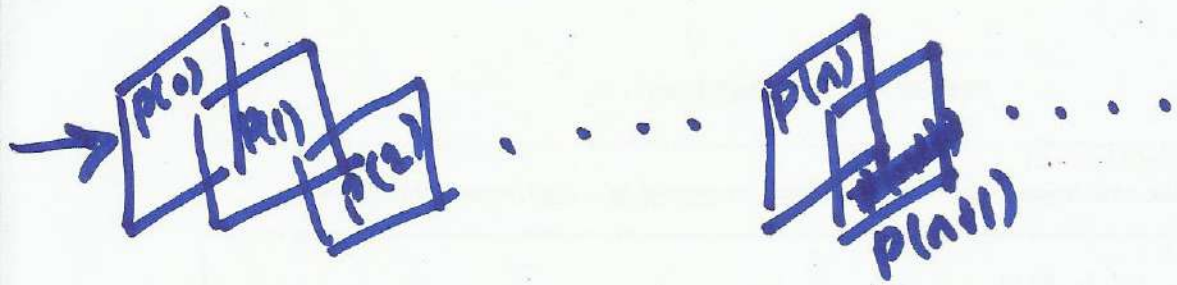
$$1+2+\ldots+n = \frac{n(n+1)}{2} \xrightarrow{\text{Show}} 1+2+\ldots+n+(n+1) = \frac{(n+1)(n+2)}{2}$$

$\therefore$ Let's add $n+1$ to each side on RHS (Right-hand side)

$$\begin{array}{rcl} 1+2+\ldots+n & = & n(n+1)/2 \\ +\,n+1 & & n+1 \\ \hline 1+2+\ldots+n+n+1 & = & (n+1)\left[\frac{n}{2}+1\right] \end{array}$$

Actually, this is $\frac{(n+1)(n+2)}{2}$. DONE

2)



Domino Tiles: You need to push P(0) first.

<u>Ex</u>: $3 \mid n^3 - n$, $\forall n \geq 0$.

Prove this by induction <u>on n</u>.

skip 0) $P(n)$: $3 \mid n^3 - n$, ~~$\forall n \geq 0$~~

1) Base case: Show $P(0)$, T meaning show $3 \mid 0^3 - 0$. of course!

2) Inductive case: Prove $\underbrace{P(n)}_{} \rightarrow P(n+1)$

$$3 \mid n^3 - n \rightarrow 3 \mid (n+1)^3 - (n+1)$$

Idea: Simplify (serkan) $(n+1)^3 - (n+1)$

$$(n+1)^3 - (n+1) = \underbrace{n^3 + 3n^2 + 3n + 1}_{\text{By Binomial Expansion}} - (n+1) =$$

$= \cancel{n^3 + 3n^2 + 2n}$ not a good idea

See next page.

$$n^3 + \underbrace{3n^2 + 3n}_{\text{divisible by } 3} + \cancel{1} - (n + \cancel{1})$$

$3 \mid n^3 - n$
Because we assume $P(n)$, T.

Conclusion:

$$\left.\begin{array}{l} 3 \mid n^3 - n \\ 3 \mid 3n^2 + 3n \end{array}\right\} 3 \mid (n^3 + 3n^2 + 3n + 1) - (n+1)$$

Thus, $P(n+1)$, T.

DONE.

Atakan suggested:

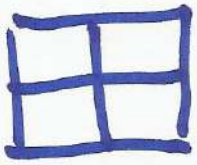
$$n^3 - n = n(n-1)(n+1)$$

3 consecutive integers
Exactly one of them is divisible by 3.

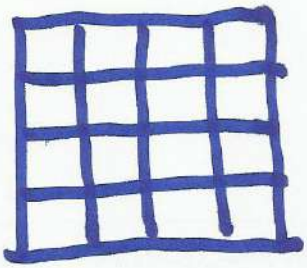
This is direct proof of $P(n)$, $\forall n \geq 0$.

Ex: Claim: Every $2^n \times 2^n$ grid of squares can be tiled (döşenmek) by domino tiles when one square is removed (from anywhere you want)

$2^1 \times 2^1$



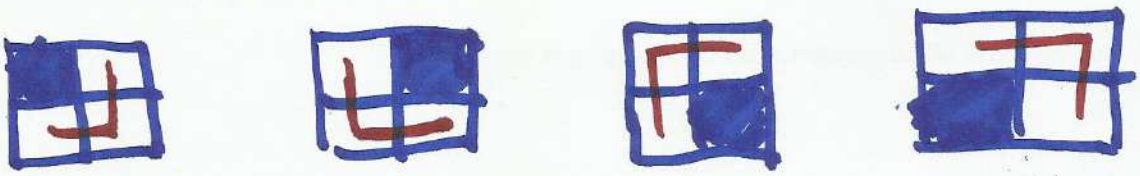
$2^2 \times 2^2$



$P(n)$: $2^n \times 2^n$ grid can be tiled with when one square is removed

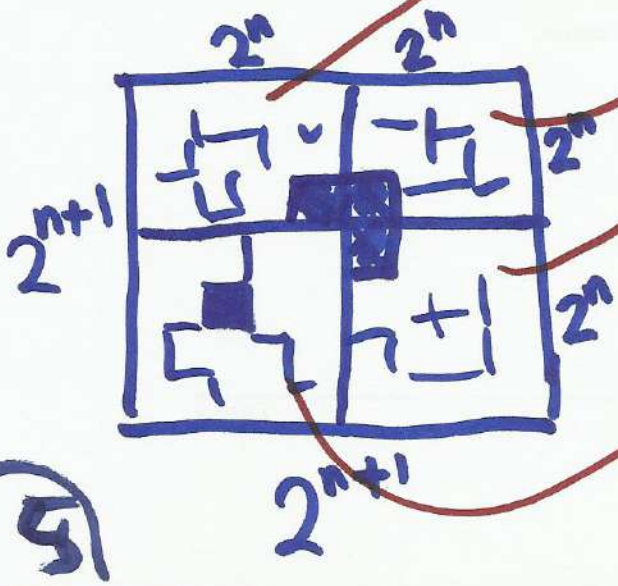
You can pick

Base Case: Show $P(n)$, T for $n = 1$.



$P(1)$, True ✓

Inductive Case: $P(n) \rightarrow P(n+1)$



We know, we can tile this, because $P(n)$ is true (This is inductive hypothesis)

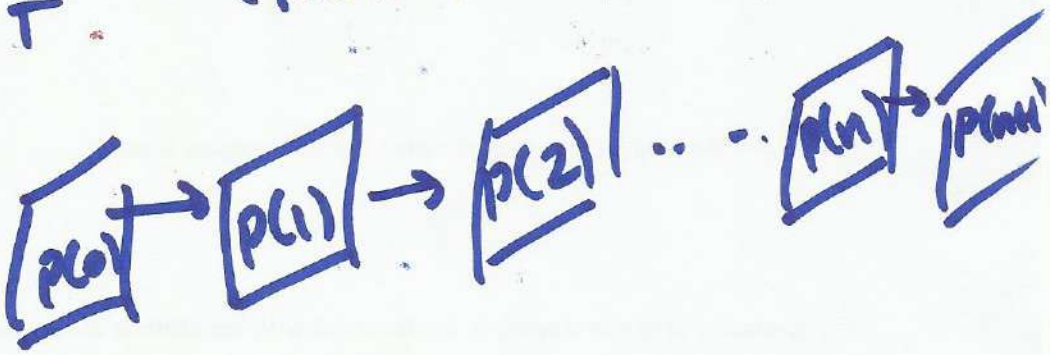
Strong Induction:

$$\frac{\begin{array}{c} P(0), T \\ P(1) \wedge P(2) \wedge \ldots \wedge P(n), T \end{array}}{P(n+1)}$$

Now, we can use more information:

$$\frac{\begin{array}{c} P(1), T \\ P(2), T \\ \vdots \\ P(n), T \end{array}}{P(n+1), T}$$

(Recall the dominoes:



Base Case: ?

Ind Case: $23 < n-5$

$P(n-5)$, True (by Inductive Hypo.) because Strong Induction.

$\exists a, b \in \mathbb{N}^+$

$n-5 = 5 \cdot a + 7b$

$n = 5a + 7b + 5$

$= 5(a+1) + 7b$

$\therefore$ $P(n)$, True.

If $n-5 \leq 23$, then

means $n \leq 28$

Base case

$$\begin{cases} 24 = 7+7+5+5 \\ 25 = 5 \cdot 5 \\ 26 = 7+7+7+5 \\ 27 = 7+5+5+5 \\ 28 = 7+7+7+7 \end{cases}$$

7)

~~Deneme~~ (No quiz today)

- Fermat's Last Theorem:

$\nexists\ x, y, z > 0$ such that (öyle ki)

$$x^n + y^n = z^n \qquad n > 2.$$

conjectured around 1630.

In 1994, Wiles gave a proof of this theorem.
(after working on it for 7 years)

- Twin Prime Conjecture:
(Sanı)

$\exists$ infinitely many primes p such that $p+2$ is also prime.

- Primality Testing:

Some progress in 2002, Agarwal, Kayal, Saxena that algo finishes in polynomial time.

- Factoring: (Factor = Çarpan
Factoring = çarpanlarına ayırma)

Given $n = p \cdot q$ (say n is 100 digit number)

$\Rightarrow$ not so easy to recover p & q.

Division Theorem: $\forall n \in \mathbb{Z}$, $\forall d \in \mathbb{Z}^+$, there exist a <u>unique</u> pair of integers q and r such that

$$n = q \cdot d + r \qquad 0 \leq r < d$$

q, quotient (bölüm) $\qquad$ r, remainder (kalan)

Let $q := \text{qcnt}(n, d)$

$r := \text{rem}(n, d)$

Ex: $\text{qcnt}(2716, 10) = 271$

$\text{rem}(2716, 10) = 6$

Ex: $\text{qcnt}(-11, 7) = -2$

$\text{rem}(-11, 7) = 3$

Water jug Problem
(domeccana)

Tools:

- Fill the jug with water to the top
- Pour the water in the smaller jug to the bigger jug
- Empty the jugs you want

1 (5kg)	2 (3kg)	
+5	0	(Fill Jug 1)
5-3=2	3	(Pour from Jug 1 to Jug 2)
2	0	(Empty Jug 2)
0	2	
+5	2	
5-1=4	2+1	(Fill 2nd Jug from the by pouring from Jug 1)

Saved the world
(by Ismet & Mehmet Ali)

Note: If our jugs could take 3kg & 6kg. Could we still get 4kg?

Thm.: Suppose that we have water jugs with capacities a and b. Then, (by using the tools) the amount of water in each jugs is always a linear combination of a and b.

$$\textcircled{3/4} \quad s \cdot \overset{3}{a} + t \cdot \overset{6}{b} \text{ where } s,t \in \mathbb{Z}$$

Recall the Die Hard Solution: $(b \geq a)$

$(0,0) \longrightarrow (a,0)$ fill the first jug

$\longrightarrow (0,a)$ pour first into second

$\longrightarrow (a,a)$

$\longrightarrow (\underbrace{a-(b-a)}_{2a-b}, \underbrace{a+(b-a)}_{b})$ pour first into second

$\longrightarrow (2a-b, 0)$

$\longrightarrow (0, 2a-b)$

$\longrightarrow (a^3, 2a-b) \longrightarrow (0, 3a-b)$

$\cancel{\longrightarrow (\underbrace{a-[b-(2a-b)]}_{3a-2b}, b)}$ ~~Pour first into second~~

Ex:
$a=3$
$b=5$

$\cancel{3 \cdot 3 - 2 \cdot 5}$

$3 \cdot 3 - 5 = 4$

= Greatest Common Divisor (GCD) =
(OBEB: Ortak Bölenlerin En Büyüğü)

<u>Thm</u>. The g.c.d. of the numbers a and b, denoted as $\gcd(a,b)$, is the smallest positive linear combination of a and b.

<u>Proof</u>: In two steps.

$m :=$ smallest positive lin. combin. of a & b

<u>Step 1</u>: $\gcd(a,b) \leq m$ <u>Step 2</u>: $m \leq \gcd(a,b)$

imply

$\gcd(a,b) = m$

<u>Proof of Step 1:</u>

$\gcd(a,b) \mid m$?

Write m with a formula:

$$m = s \cdot a + t \cdot b \quad , s,t \in \mathbb{Z}$$

$$\gcd(a,b) \mid s \cdot a$$

$$\gcd(a,b) \mid t \cdot b$$

$$\therefore \gcd(a,b) \mid m = sa + tb.$$

Since, $\gcd(a,b) \mid m$, we have $\gcd(a,b) \leq m$.

Step 2: Show $m \leq \gcd(a,b)$.

Step 2.a: Show $m|a$

Step 2.b: Show $m|b$.

imply

m is a common divisor of a & b, therefore $m \leq \gcd(a,b)$.

Let us divide a by m:

$$a = q \cdot m + r \quad (0 \leq r < m)$$

Let us substitute m:
(yerine/ikine koymak)

$$a = q \cdot (s \cdot a + t b) + r$$

We get:

$$r = (1 - qs)a + (-qt)b$$

we notice, r is also a linear combination of a and b.

Compare r & m

This is only possible if $r = \underline{0}$.

$\therefore$ Yes, $m|a$.

Step 2.b can be proved similarly.

Corollary (a direct result of a theorem):

An integer is linear combin of a and b $\iff$ it is a multiple of $\gcd(a,b)$.

if and only if "iff"

Corollary: Spps. (suppose) that we have water jugs with capacities a and b. The amount of water in each jug is <u>always</u> a multiple of $\gcd(a,b)$.

Observation: $(a \geq b)$

$$\gcd(a,b) = \gcd(b, \text{rem}(a,b))$$

remainder when you divide a by b.

Ex: Find $\gcd(1147, 899)$. Write an algo. to calculate this "quickly". You are allowed to divide and find remainder & quotients.

$1147 \lfloor 899$ $-899 \quad 1$ 248	$899 \lfloor 248$ 3 155	$248 \lfloor 155$ 1 93	....
$\gcd(1147,899) =$ $= \gcd(899, 248)$	$\gcd(899, 248) =$ $= \gcd(248, 155)$	$\gcd(248, 155)$ $= \gcd(155, 93)$	until the remainder is 0

Encrypt a message:

$$\left.\begin{array}{l} A = 00 \\ B = 01 \\ C = 02 \\ \vdots \\ Z = 23 \end{array}\right\} \quad \begin{array}{l} m: \\ \text{victory} \\ 22\ 09\ 03\ 20\ 15\ 18 \\ \qquad\qquad\qquad 25 \end{array}$$

$m :=$ our message

$m^* :=$ encryption of m (encrypted message)

m, prime (Attach 13 to the end)

k, key (to encode / decode the message)

$m: 2209032015182513$ prime (Don't ask why)

Algo. for encrypting: $m^* = m \cdot k$

$m^* = 503698\ldots$

1) Problem: To make m a prime number.

8 2) Problem: Is it really secure?

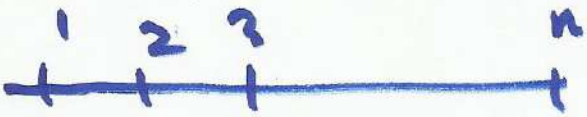
$15 = 3 \cdot 5$ (only one way)

If 1 were a prime number, then

$$\left.\begin{array}{l} 15 = 1 \cdot 3 \cdot 5 \\ 15 = 1^2 \cdot 3 \cdot 5 \end{array}\right\} \text{not unique!!!}$$

<u>Lemma:</u> p, prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.

Proof by F.T.A. (Fund. Thm. of Arithmetic)



How many primes in $[1, n]$?

Call $\pi(n)$.

Answer (Legendre, 1798): $\sim \dfrac{n}{\ln n}$

m_1^* $\qquad$ m_2^*

(m_1, prime) $\qquad$ (m_2, prime)

message 1 $\qquad$ message 2

$$\gcd(m_1^*, m_2^*) = ?\ k$$

$$m_1^* = m_1 \cdot k \qquad m_2^* = m_2 \cdot k$$

prime $\qquad$ prime

<u>New idea</u>: Let us not make m prime.

- p, large prime that the sender and the receiver ~~know~~ agree. (public) ununi
- k, let $k \in \{0, 1, \ldots p-1\}$
  k is secret

Encryption: $\quad m^* = \text{rem}(mk, p)$

Here, the message m can be any integer in the set $\{0, 1, \ldots, p-1\}$

Decryption: How? (As a receiver, I just have k, p, m^*)

$$7 \cdot 8 \equiv 1 \mod 5$$

No division in modular arithmetic.

You multiply by inverse:

To remove 7 from LHS,

multiply by inverse of 7 both sides.

inverse: multiplicative inverse:

x^{-1} denotes the inv. of x

If $x \cdot x^{-1} \equiv 1 \mod n$, then x^{-1} is the mult. inverse of x modulo n.

<u>Lemma 1</u>: If p is a prime and k is not a multiple of p, then k has a mult. inv. modulo p.

<u>Proof:</u> Obs. 1: $\gcd(k,p) = 1$

Obs. 2: $1 = s \cdot p + t \cdot k$ for some $s, t \in \mathbb{Z}$

(from last week)

$$\Downarrow$$

$$sp = 1 - tk$$

$$\Downarrow$$

$$p \mid 1 - tk$$

$$\Downarrow$$

$$tk \equiv 1 \mod p$$

So, $t \equiv k^{-1} \mod p$.

Lemma. 2: If p, prime and k is not a multiple of p then

$$ak \equiv bk \mod p \quad \text{implies}$$

$$a \equiv b \mod p \quad \text{because} \quad a\overbrace{kk^{-1}}^{=1} \equiv b\overbrace{kk^{-1}}^{=1} \mod p \quad \mod p$$

Lemma-3: If p, prime and k is not a multiple of p, then

$$\overbrace{\text{rem}((1\cdot k),p), \text{rem}((2k),p), \text{rem}((3k),p) \ldots \text{rem}((p-1)k,p)}^{p-1 \text{ numbers}}$$

is a set that is equal to $\{1, 2, \ldots, p-1\}$.

Proof: (By contradiction)

if for $i \neq j$, $\underbrace{\text{rem}(ik,p) = \text{rem}(jk,p)}_{(*)}$

$i, j \in \{1, \ldots p-1\}$

$(*)$ means $ik \equiv jk \mod p$

$$ik \cdot k^{-1} \equiv jkk^{-1} \mod p$$

$$i \equiv j \mod p$$

Contradiction!

Because $i \neq j$, $i, j \in \{1, \ldots p-1\}$

Therefore,

$\text{rem}(1k,p), \text{rem}(2k,p) \ldots, \text{rem}((p-1)k,p)$ must be different.

Fermat's Little Theorem: If p is a prime and k is not a multiple of p, then

$$k^{p-1} \equiv 1 \mod p.$$

Proof: (Direct proof)

$$(p-1)! = 1 \cdot 2 \cdot \dots \cdot (p-1)$$

read as "(p-1) factorial"

$$(p-1)! := 1 \cdot 2 \cdots (p-1) \overset{\text{by Lemma 3}}{=}$$

$$= \text{rem}(k,p) \cdot \text{rem}(2k,p) \dots \text{rem}((p-1)k,p)$$

(order may be different, we do not mean $1 = \text{rem}(k,p)$, $2 = \text{rem}(2k,p)$, $\vdots$)

$$\equiv k \cdot 2k \cdot 3k \dots (p-1)k \mod p$$

$$\equiv (p-1)!\, k^{p-1} \mod p$$

This means $(p-1)! \equiv (p-1)!\, k^{p-1} \mod p$

is this number a multiple of p?

NO.

By Lemma 1, $(p-1)!$ has a mult. inverse mod p.

$$\underbrace{(p-1)!^{-1} \cdot (p-1)!}_{=1} \equiv \underbrace{((p-1)!)^{-1} \cdot (p-1)!}_{=1}\, k^{p-1} \mod p$$

DONE.

By F.L.T., we see

$$\underbrace{k^{p-2}}_{k^{-1}} \cdot k \equiv 1 \mod p$$

<u>Ex:</u> $p = 23$, $k = 19$

$$\underbrace{19^{21}}_{19^{-1}} \cdot 19 \equiv 1 \mod 23$$

<u>Ex:</u> $p = 23$

$$7^{100} \mod 23$$

$23 \nmid 7$, so use F.L.T: $7^{22} \equiv 1 \mod 23$

$$7^{100} \equiv \underbrace{7^{22}}_{1} \cdot \underbrace{7^{22}}_{1} \cdot \underbrace{7^{22}}_{1} \cdot \underbrace{7^{22}}_{1} \cdot 7^{12} \mod 23$$

$$\equiv 7^{12} \mod 23$$

$$\equiv (7^2)^6 \mod 23 \qquad 7^2 \equiv 49 \equiv 3 \mod 23$$

$$\equiv 3^6 \mod 23 \ \ldots$$

Breaking Turing's Code:

Say we have m and m^* and p,

where $m^* \equiv mk \mod p$

$$m^{p-2} m^* = ? \mod p$$

$$\equiv m^{p-2} mk \mod p$$

$$\equiv m^{p-1} k \mod p$$

$$p \nmid m \longrightarrow \equiv 1 \cdot k \mod p$$

secret key recovered.

RSA - method, got Turing award in 1977

Rivest
Shamir
Adleman

Relatively Prime: If $\gcd(a,b)=1$ then a and b are rel. prime.

Lemma 4: If $n \in \mathbb{Z}^+$ and $\gcd(k,n)=1$, i.e. k and n are r.p., then k has mult. inv. mod n.

$(\exists k^{-1} \text{ s.t. } k k^{-1} \equiv 1 \bmod n)$

Corollary ~~Lemma~~ 5: If k and n are rel. prime, $n \in \mathbb{Z}^+$, then $ak \equiv bk \bmod n$ implies

$$a \equiv b \bmod n.$$

Lemma 6: If k and n are rel. prime, $n \in \mathbb{Z}^+$, and $k_1, k_2, \ldots, k_r$ are integers rel. prime to n in the range 1 to $n-1$. Then

$$\{\text{rem}(k_1 \cdot k, n), \text{rem}(k_2 \cdot k, n), \ldots, \text{rem}(k_r \cdot k, n)\} = \{k_1, k_2, \ldots, k_r\}$$

Euler Totient Function: ϕ

For $n \in \mathbb{Z}^+$, $\phi(n)$ = the number of numbers rel. prime to n in the range $1 \ldots n-1$.

Ex: $\phi(12)=4$

The numbers $1, 5, 7, 11$ are rel. prime to 12.

Information: If n is prime, $\phi(n)=n-1$.

Theorem: For any number n, if $p_1, p_2, \ldots, p_j$ are the distinct prime factors of n,

$$\phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_j}\right)$$

Ex: $\phi(300) = \phi(2^2 \cdot 3 \cdot 5^2) =$

$$= 300\left(1-\frac{1}{2}\right)\cdot\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)$$

$$= 80$$

so many numbers rel. prime to 300 from 1 to 299.

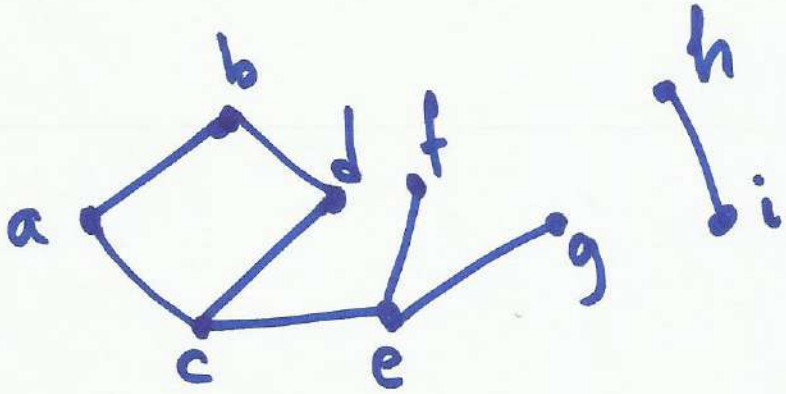
Corollary: If $n = pq$, then

$$\phi(n) = pq\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right) =$$

$$= (p-1)(q-1).$$

Euler's Theorem: If $n \in \mathbb{Z}^+$ and k is rel. prime to n, then

$$k^{\phi(n)} \equiv 1 \mod n.$$



- vertex set of this graph $= \{a, b, c, d, e, f, g, h, i\}$
  (pl. vertices)

- edge set of this graph =
  $\{\{a,b\}, \{b,d\}, \{a,c\}, \{c,d\}, \{c,e\}, \{e,f\}, \{e,g\}, \{h,i\}\}$

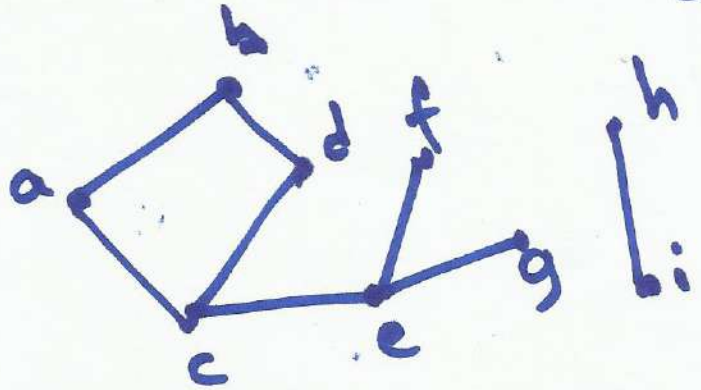
- Let's use a $\boxed{\text{shorter notation}}$ for every edge, Let's call
  ab for $\{a,b\}$
  bd for $\{b,d\}$
  ac for $\{a,c\}$
  ⋮

So, to define a graph $G = (V, E)$, we need to define two sets: vertex set V and edge set E.

- adjacent: Two vxs (short for vertices) a and b are adjacent in G if ab is an edge in G.
- incident: If ab is an edge in G, then we say the edge ab is incident to a and incident to b.

- **degree of a vertex:** The number of edges incident to that vertex in a graph.

We denote the degree of v by $\deg(v)$.



$\deg(a) = 2$

$\deg(c) = 3$

$\deg(i) = 1 \ldots$

Ex: The vxs e and f are adjacent.

We can also say that **e and f are neighbors** of each other.

$N(v)$: denotes the set of neighbors of v in the graph. So, **$\deg(v)$** is equal to $|N(v)|$ which is the number of vertices in the set $N(v)$.

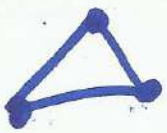
Some Important Graphs:

- Complete Graphs:

A complete graph on n vxs, has every vx pair as an edge in the graph. We write this graph as K_n.

K_2:

K_3:



K_4:

K_5:

...

- How many edges are there in K_n?

$$\binom{n}{2} = \frac{n\cdot(n-1)}{2}$$

read as "n choose 2"

- Paths : (LLM book calls this L_n)

P_n : A graph with vertex set $\{v_1, v_2, \ldots, v_n\}$ with edge set $\{v_1v_2, v_2v_3, \ldots, v_{n-1}v_n\}$.

P_2 :

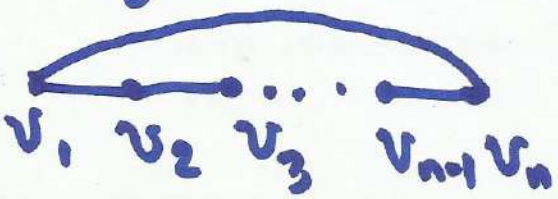
P_3 :

P_4 :

$\vdots$

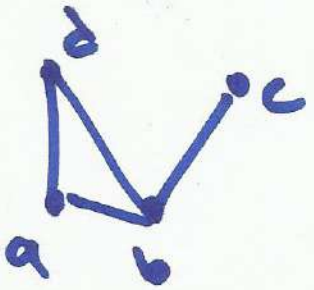
- Cycles :

C_n : A graph with vertex set $\{v_1, v_2, \ldots, v_n\}$ with edge set $\{v_1v_2, v_2v_3, \ldots, v_{n-1}v_n, v_nv_1\}$



Representation of a graph mathematically:
(computationally)

Adjacency Matrix of a graph:
(Komşuluk)



$$A = \begin{array}{c|cccc} & a & b & c & d \\ \hline a & 0 & 1 & 0 & 1 \\ b & 1 & 0 & 1 & 1 \\ c & 0 & 1 & 0 & 0 \\ d & 1 & 1 & 0 & 0 \end{array}$$

(symmetric matrix)

Definition of adjacency matrix A:

$$a_{ij} = \begin{cases} 1 & \text{if } ij \text{ is an edge} \\ 0 & \text{o/w} \end{cases}$$

<u>Remark:</u> The entries of A are 0 or 1 and the diagonal (hane) is 0. Because there are no multiple edges and no loops.

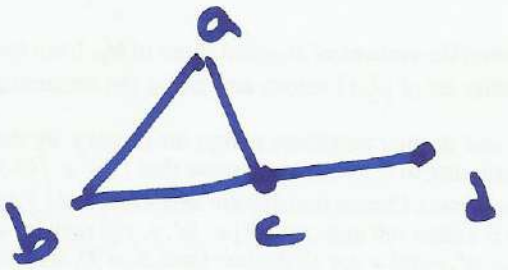
more than one edge between a pair

edge w/ two endpoints being the same vertex

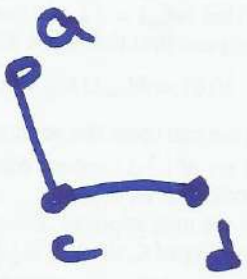
Last week:

- incident
- adjacent
- neighbor
- complete graph
- cycle
- path
- adjacency matrix
- vertex
- edge
- multiple edges
- loop
- simple

Subgraph H in a graph G:



G



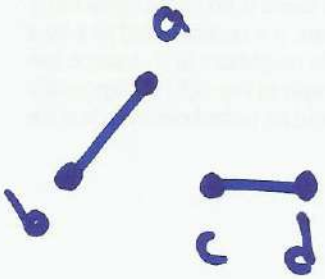
H

<u>Defn.</u>: H is a subgr. of G if and only if

$$V(H) \subseteq V(G)$$

and

$$E(H) \subseteq E(G).$$



H_1

H_1 is a subgraph of G.

denoted by

$H_1 \subseteq G$

a subgraph of

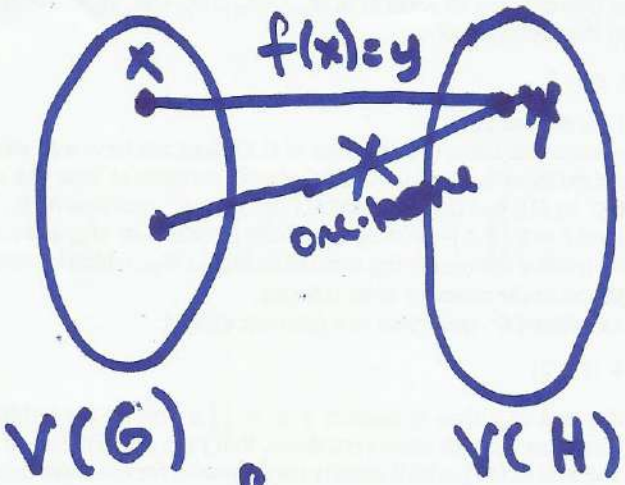
Isomorphism of two Graphs:

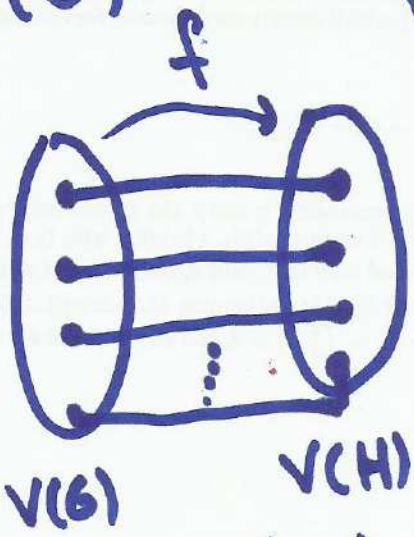
We say the graphs G and H isomorphic (to each other) if ~~and only if~~ there is a function f such that $f: V(G) \to V(H)$ one-to-one and onto

and

$$\forall u,v \in V(G),\ uv \in E(G) \Longleftrightarrow f(u)f(v) \in E(H)$$

Remark: How does a one-to-one (birebir) and onto (örten) function look like?



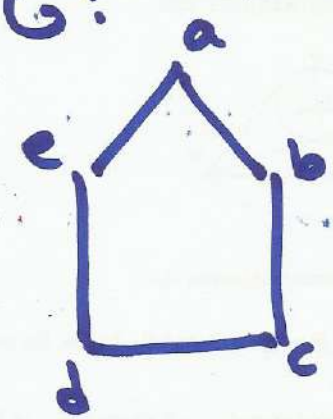


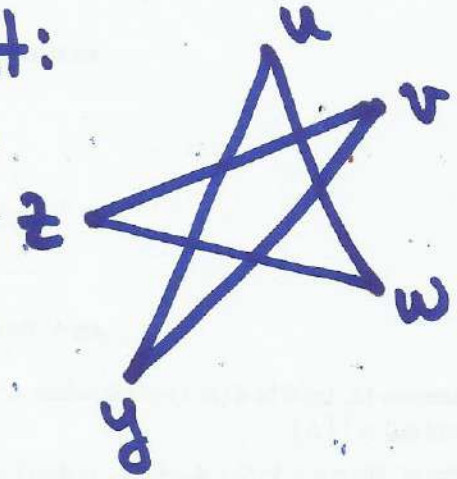
One-to-one & onto

"bijection"

$$|V(G)| = |V(H)|$$

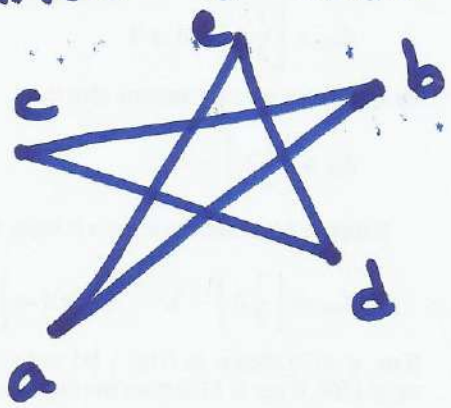
Ex: G: H:





Are G and H isomorphic?

In other words, can you DRAW G such that it looks like H:



Yes.

This is G.

Now, what should be f? (isomorphism function)

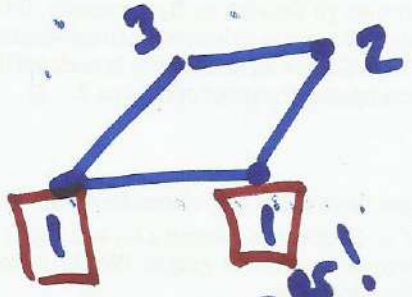
$$\left.\begin{aligned} f(a) &= y \\ f(b) &= v \\ f(c) &= z \\ f(d) &= w \\ f(e) &= u \end{aligned}\right\}$$

Since we could find an isomorphism fn., G and H are isomorphic.

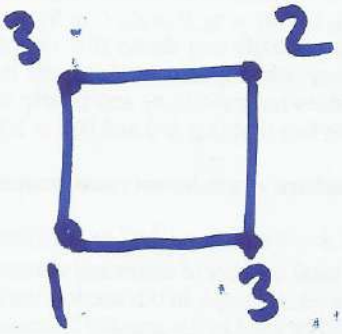
Graph Coloring: $f: V(G) \to \{1, 2, \dots, k\}$

- proper (uygun): Any two neighbor vxs (adjacent) should get different colors.

Ex:



not proper!

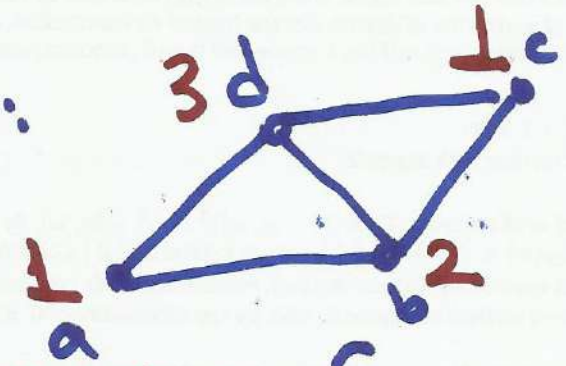


proper

Chromatic Number of a graph G: $\chi(G)$ - chi (read 'kay' in Turkish)

This is the minimum number of colors that we need to color $V(G)$ <u>properly.</u>

Ex:



$\chi(G) = 3$ G

$f: \{a, b, c, d\} \to \{1, 2, \dots k\}$

minimum k for a proper coloring?

We say this graph is 3-colorable.

<u>not</u> 2-colorable.

<u>not</u> 1-colorable.

4-colorable

5-colorable

6-colorable

⋮

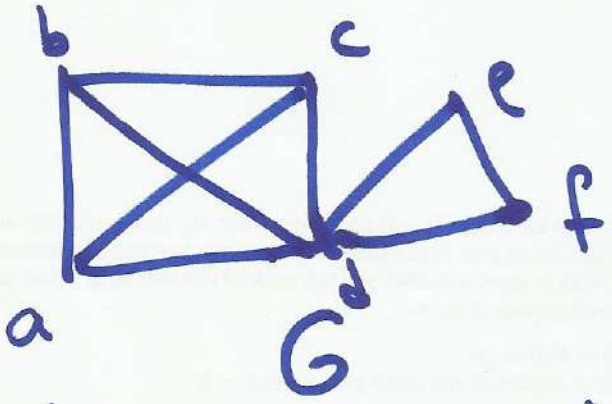
$\boxed{\chi(G) = 3}$

Parameters related to the degrees of vxs:

- maximum degree of G: $\Delta(G)$ big delta
- minimum degree of G: $\delta(G)$ small delta
- average degree of G: $d_{avg}(G)$

- Hand-shaking Lemma
  (also known as degree-sum formula)

Ex:



$\deg(a) = 3$
$\deg(b) = 3$
$\deg(c) = 3$
$\deg(d) = 5$
$\deg(e) = 2$
$\deg(f) = 2$

multiset (elements may repeat) containing all degrees in G:

$\{2, 2, 3, 3, 3, 5\}$

$\delta(G)$ $\Delta(G)$

$$d_{avg}(G) = \frac{2+2+3+3+3+5}{6}$$

$$\boxed{d_{avg}(G) = 3} = \frac{\sum_{v \in V(G)} \deg(v)}{|V(G)|}$$

. Degree-sum of $G = \sum_{v \in V(G)} \deg(v) = 2+2+3+3+3+5 = 18$

. Number of edges of $G = |E(G)| = 9$

$$\boxed{\sum_{v \in V(G)} \deg(v) = 2 \cdot \sum_{e \in E(G)} 1}$$

— Degree-Sum Formula (or H.S. Lemma)

e contributes +1 to deg(u) and +1 to deg(v)

· <u>Walks</u>, · Paths, · Cycles, · <u>Tours</u>

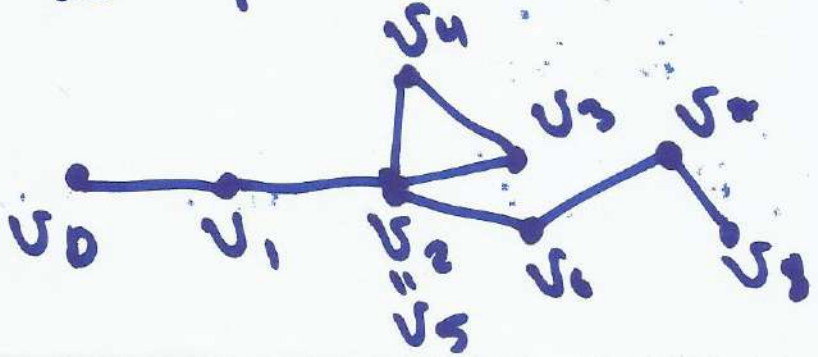
Walk: Just a sequence looking like this:

$$W = v_0, v_0v_1, v_1, v_1v_2, v_2, \ldots, v_{k-1}v_k, v_k$$

a vertex an edge

- starts and ends w/ a vx
- alternating between vxs and edges
- has length $|W| = k$, the number of edges used in W.
- different than the path, there may be repeated vxs in W.

Ex:



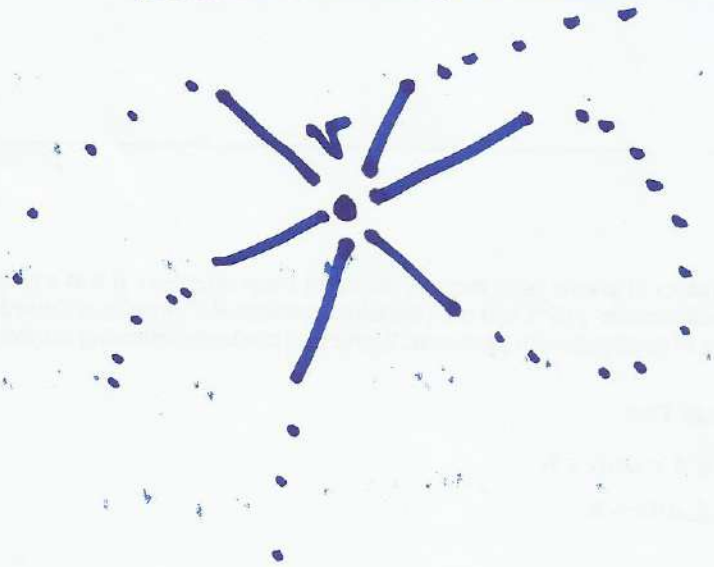
$|W| = 8$

W has length 8.

- closed walk: If $v_0 = v_k$, then W is a closed walk.
- open walk: ~~Tour~~: If $v_0 \neq v_k$, W is called a tour.

· Euler Walk , · Euler Tour

: Euler Tour of a graph G is a closed walk that includes <u>every edge of G.</u>



Every time a vertex v appears in W, since W is closed, this visit looks like

$$\ldots\ldots, v_{i-1}\, v,\, v_i, v_i\, v_{i+1} \ldots\ldots$$

it has two edges (one before and one after) in W.

This graph has an Euler Tour:

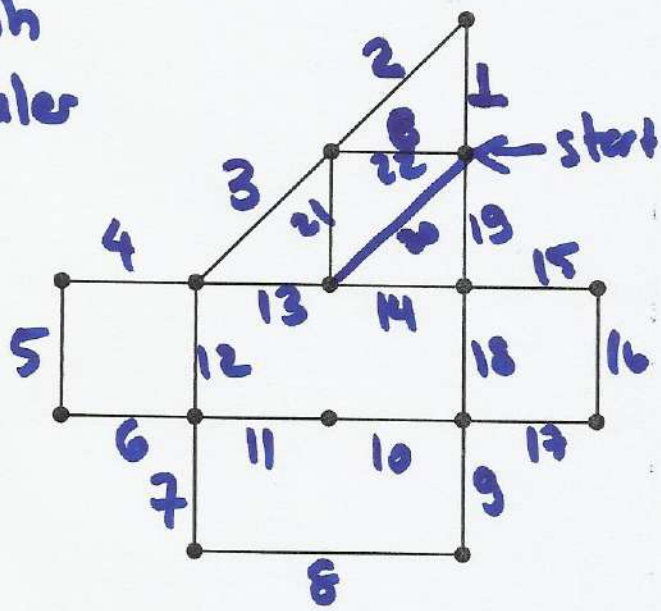


Figure 5.23 A possible floor plan for a museum. Can you
verses every edge exactly once?

Theorem 5.6.2 turns out to be useful since bipartite graphs
in practice. We'll see examples when we talk about planar
and when we talk about packet routing in communication net

5.6.3 Euler Tours

Can you walk every hallway in the Museum of Fine Arts
represent hallways and intersections with edges and vertices,
question about graphs. For example, could you visit every ha
a museum with the floor plan in Figure 5.23?

The entire field of graph theory began when Euler aske
bridges of Königsberg could all be traversed exactly once–
question we asked about the Museum of Fine Arts. In his h
a defined to be a walk that traverses every edge in a graph ex
an *Euler tour* is an Euler walk that starts and finishes at the
with Euler tours and Euler walks both have simple characteri

Thm.: A graph G has an Euler tour $\Longleftrightarrow$ every degree of G even

iff "if and only if"

Proof:

$\Longrightarrow$ trivial (See previous page)

$\Longleftarrow$ Knowing that all degrees are even, show that G has Euler tour.

Proof by maximality:

Let's say we write an algorithm that finds a walk W that cannot be made any longer:

algo. stops if v has no more incident edge outside W, and no more edge incident to u outside W.

W: — Blue (used)

$\bar{W}$: — Red (unused)

Obs. 1: ~~If we could~~

Since W is <u>maximal</u> (cannot be made longer)

every edge incident to u has color blue

—— " —— v has color blue

Therefore, W is closed!