23/11/2018

Integers, divisors, primes

Set of integers $\mathbb{Z} = \{-3, -2, -1, 0, 1, 2, \dots\}$

Let a, b be two integers. We say a divides b if a is a diviser of b, if b is a multiple of a, if there exists an integer m such that $b = a \cdot m$

We notate this as a/b

Ex $2/6$

If a doesn't divide b then we write $a \nmid b$. Then, a will divide b with a remainder. The remainder r of the division $b:a$ is an integer that satisfies $0 \leq r \leq a$.
If the quotient of the division with remainder is q, we have $b = a \cdot q + r$

Results $\forall a \in \mathbb{Z}$, $1/a$, $-1/a$
a/a and $-a/a$

2) $\forall a \in \mathbb{Z}$ $2/a \rightarrow a \rightarrow$ even
$2 \nmid a \rightarrow a \rightarrow$ odd

Prove that if a/b and b/c then a/c

If a/b then $b = a \cdot m$, $m \in \mathbb{Z}$

If b/c then $c = b \cdot n$, $n \in \mathbb{Z}$

$c = a \cdot m \cdot n$

Then a/c

② Prove that every integer a and for any positive integer n, $a-1 / a^n - 1$

Using induction on n,

<u>Base case</u> $n = 1$ $\quad a-1/a-1$ YES!

<u>Inductive step</u> Assume $a-1/a^k-1$. Show that $a-1/a^{k+1}-1$

If $a-1/a^k-1$ then $a^k-1=(a-1)\cdot c \quad c\in\mathbb{Z}$

$$a^{k+1}-1 = (a^k-1)a+a-1$$
$$= (a^k-1)a+(a-1)$$
$$= \underbrace{(a-1).c}_{a^k-1}.a+(a-1)$$

$$a^{k+1}-2=(a-1)(ca+1)$$

$$a-1/a^{k+1}-1$$

23/11/2018

ER-BAKIR

~PRIME NUMBERS~

An integer $p>1$ is called a prime if it is NOT divisable by any integer other than 1 and p.

2, 3, 5, 7, 11, 13 are prime numbers.

$24 = 2 \cdot 2 \cdot 2 \cdot 3$

THM 8.1 Every positive integer can be written as the product of primes, and this factorization is unique.

Proof Proof by contradiction

Assume $n \in \mathbb{Z}^+$, and n can be written as a product of primes in two different ways

(1) $n = p_1 \cdot p_2 \cdots p_n = q_1 \cdot q_2 \cdots q_n$

$$\prod_{i=1}^{m} p_i = \prod_{j=1}^{m} q_i$$

$p_i \neq q_i$ are primes

$p_i = q_j$
for all i, j

(2) $n = p_1 \cdot p_2 \cdots p_m = q_1 \cdot q_2 \cdots q_n$

$p_1 = \dfrac{q_1 \cdot q_2 \cdots q_n}{p_2 \cdot p_3 \cdot p_m}$ since $\dfrac{q_1 \cdot q_2 \cdot q_n}{p_2 \cdot p_3 \cdot p_m}$

ER-BAKIR

23 / 11 / 2018

Prove that if p is a prime, a, b are integers, and p / ab then either p / a or p / b

If p/ab then p/a or p/b p is prime a, b

Ex Suppose $a, b \in \mathbb{Z}$ and a/b and also p is a prime and p/b but $p \not| a$. Show that p is a divisor of b/a

If p/b then $b = p \cdot x$, $x \in \mathbb{Z}$
If a/b then $b = a \cdot y$, $y \in \mathbb{Z}$

Assume $b = p \cdot \underbrace{q_1 \cdot q_2 \cdots q_J}_{x}$ where $\forall i \geq 1$, q_i is a prime

If $p \not| a$ then $a = r_1 \cdot r_2 \cdots r_s$ where $\forall i$, $r_i \neq p$ and r_i is a prime

Now consider $\dfrac{b}{a} = \dfrac{p \cdot q_1 \cdot q_2 \cdots q_J}{r_1 \cdot r_2 \cdots r_s}$

If $p \not| a$ then $a = q_{i_1} \cdot q_{i_2} \cdots q_{i_k}$ where $q_{i_J} = q_\ell$ and $k \leq J$

Now consider $\dfrac{b}{a} = p \dfrac{q_1 \cdot q_2 \cdots q_J}{q_{i_1} \cdot q_{i_2} \cdots q_{i_k}} = p \cdot M$, $M \in \mathbb{Z}^+$

$p / \dfrac{a}{b}$

ER-BAKIR

30 / 11 / 2018

THEOREM There are infinetely many primes. (For any positive integer n, there is a prime larger than n.)

1st way Let $n \in \mathbb{Z}^+$ Consider $n!+1$. Let p be a prime divisor of $n!+1$, we will show that $p>n$.

Proof by Contradiction Assume $p \leq n$. If $p \leq n$ then $p / n!$

But we also know that $p / n!+1$

If $p/n!+1$ and $p/n!$ then $n!+1 = p.k \quad k \in \mathbb{Z}^+$

$$\begin{array}{rl} & n! = p.\ell \quad \ell \in \mathbb{Z}^+ \\ - & \\ \hline & 1 = p(k-\ell) \end{array}$$

Therefore our assumption that $p<n$ is $1=p(k-\ell)$ which cannot be true. false. Therefore, $p>n$.

2nd way Consider $n!+1$.

1. If $n!+1$ is prime then, we have found a prime larger than n.
2. If $n!+1$ is composite (i.e. is NOT prime) show that it is not divisable to any number from 2 to n.

Consider $n!+1 \equiv 1 \pmod 2$

Consider $n!+1 \equiv 1 \pmod 3$

$\vdots$

$n!+1 \equiv 1 \pmod n$

* $n!+1$ has a prime factor larger than n.

ER-BAKIR

* Ardışık Asal olmayan seri

30 / 11 / 2018

THEOREM for any positive integer k, there exists k consecutive composite integers

$\underbrace{\text{consecutive}}_{\text{ardışık}}$ $\underbrace{\text{composite}}_{\text{non-prime}}$

$2, 3, 4, 5, 6, 7, \underline{8}, \underline{9}, \underline{10}, 11$

$k=3$

$\underbrace{24, 25, 26, 27, 28}_{k=5}, 29, 30$

Let $n = k+1$

Consider $\underbrace{n!+2, n!+3, n!+4, \ldots, n!+n}_{n-1 \text{ numbers}}$

we will show that none of the above $n-1$ numbers are prime.

Is $n!+2$ a prime number? No! because $2 / n!+2$

Is $n!+3$ a prime number? NO!

Is $n!+n$ a prime number? NO! $n / n!+n$

$n=2 \quad k=1 \quad n!+2 = 4$

$n=3 \quad n!+2, n!+3 = \underline{8}, \underline{9}$

30 / 11 / 2018

~ FERMAT'S LITTLE THEOREM ~

French mathematician Pierre de Fermat (1601-1655)

Theorem If p is prime and a is an integer, then $p \mid a^p - a$

Before proouing the above theorem

$a = 4$

$p = 3$

LEMMA: If p is prime and $1 < k < p$ than $p \mid \binom{p}{k}$

$3 \mid 4^3 - 4$

Proof of lemma: Consider $\binom{p}{k} = \frac{p!}{(p-k)! \cdot k!} = \frac{p(p-1)\cdots(p-k+1)}{k(k-1)\cdots 2 \cdot 1}$ $\quad 3 \mid 60$

$$\binom{p}{k} = p \cdot \underbrace{\frac{(p-1)(p-2)\cdots(p-k+1)}{k(k-1)\cdots 2 \cdot 1}}_{(A)}$$

$$\therefore p \mid \binom{p}{k}$$

* None of the integers in the denominator of A is divisable by p, because p is prime. But A is an integer. Therefore all integers in the denominator of A are divisable by integers in the numerator. A is the product of all prime factors of $\binom{p}{k}$ other than "p". Thus $p \mid \binom{p}{k}$

30/11/2018

Proof by induction on a: Base case $a=0$

$$p \mid 0^p - 0$$

$$0^p - 0 = 0$$

$$p \mid 0 \checkmark$$

Inductive Step: Assume $p \mid k^p - k$. Show that $p \mid (k+1)^p - (k+1)$

Consider $(k+1)^p - (k+1) = \underbrace{k^p + \binom{p}{2} k^{p-1} + \binom{p}{3} k^{p-2} + \dots \binom{p}{p-1} k + 1}_{(k+1)^p} - k - 1$

$$= k^p - k + \binom{p}{2} k^{p-1} + \dots + \binom{p}{p-1} k$$

We know that $p \mid k^p - k$

From lemma we've just proved, we know that $\binom{p}{2}, \binom{p}{3}, \dots \binom{p}{p-1}$ are all divisable by p. Therefore $p \mid (k+1)^p - (k+1)$

RSA public-key cryptosystem (created in 1970's.

30/11/2018

ER-BAKIR
elektrolitik bakır mamulleri a.ş.

Euclidean Algorithm

① Greatest common divisor of two integers a,b is the largest integer that divides both a and b.

$gcd(6,8) = 2$
$gcd(3,6) = 3$

② Two integers a,b are relatively prime if $gcd(a,b)=1$

③ Least common multiple of a,b is the smallest integer which is a multiple of both a and b.

$lcm(6,8) = 24$
$lcm(3,6) = 6$

$gcd(12,18) = 6$

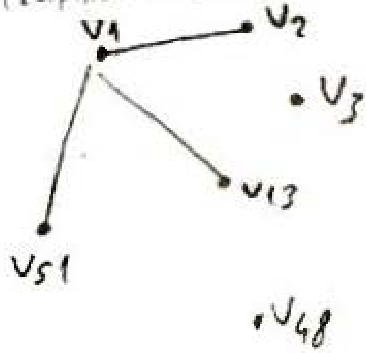
$lcm(12,18) = 2 \cdot 3 \cdot 2 \cdot 3 = 36$

12	18	2
6	9	3
2	3	2
1	1	3

> 6

~ GRAPH THEORY ~

Prove that at a party with 51 people, there is always a person who knows an even number of others. (Assume that acquitance is mutual)
(karşılıklı tanışıklık)



PROOF Assume every person in the party knows an odd number of other people.

degree(v_i) is the # of edges v_i has.

degree(v_{1i}) is the # of people v_i knows.

$$\sum_{i=1}^{51} \text{degree}(v_i) \text{ is an odd number}$$

Now, consider the # of edges in the graph.

$$2\sum \text{edges} = \sum_{i=1}^{51} \text{degree}(v_i)$$

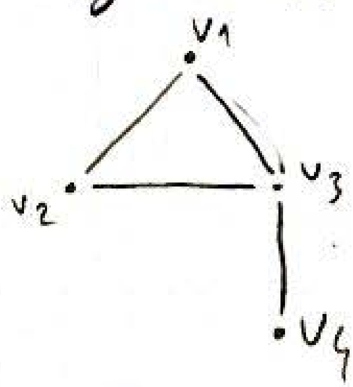
Therefore, we readed a contradiction

$\therefore$ Our assumption that every person in the party knows an odd # of other people is FALSE!

07 / 12 / 2018

A graph is a set of nodes (vertices) and some pairs of these vertices might be connected by edges. Thus, $G = (V, E)$ where V is the set of vertices and E is the set of edges.

Edges can be denoted by two elements vertex sets, if they are not directed.



$G = (V, E) \quad V = \{v_1, v_2, v_3, v_4\}$

$E = (\{v_1, v_2\}, \{v_2, v_3\}, \{v_3, v_4\}, \{v_1, v_3\})$

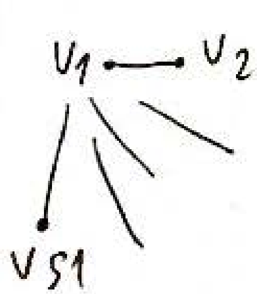
$d(v_1) = 2 \quad d(v_3) = 3$

$d(v_2) = 2 \quad d(v_4) = 1$

The # of outgoing edges in the degree of a node.

Question

Assume in the group of 51 people.
Everyone knows each other. what would be the sum of degree?



$\underbrace{50 + 50 + 50 + \cdots + 50}_{51} \qquad 51 \times 50 = 2550$

$$\sum_{i=1}^{51} d(v_i) = 51 \times 50$$

$$\text{Number of edges} = \frac{1}{2} \cdot \sum_{i=1}^{51} 51 \times 50$$

$$\frac{51 \times 50}{2} = 1275$$

07/12/2018

Question If a graph has an odd number of vertices, then the # of nodes with an odd degree is even.

Let V_{even} be the vertices with an even degree.
Let V_{odd} be the vertices with an odd degree.

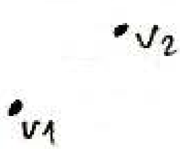
$$V = V_{even} \cup V_{odd}$$

$$\sum_{v \in V_{even}} d(v) \text{ is even}$$

$$\sum_{v \in V} d(v) \text{ is even} \qquad \underbrace{\sum_{v \in V} d(v)}_{\text{even}} = \underbrace{\sum_{v \in V_{even}} d(v)}_{\text{even}} + \underbrace{\sum_{v \in V_{odd}} d(v)}_{\text{even}}$$

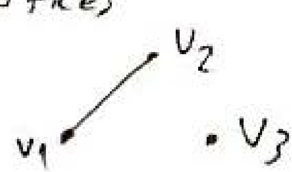
$$\sum_{v \in V_{odd}} d(v) \text{ is even}$$

1 All graphs with 2 vertices



$G = \{v_1, v_2\}, \emptyset$ $\qquad$ $G = \{v_1, v_2\}, \{v_1, v_2\}$

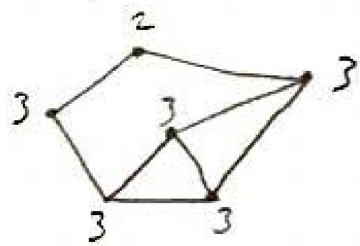
2 All graphs with 3 vertices



$G = \{v_1, v_2, v_3\}, \emptyset$ $\qquad$ $G = \{v_1, v_2, v_3\}, \{v_1, v_2\}$

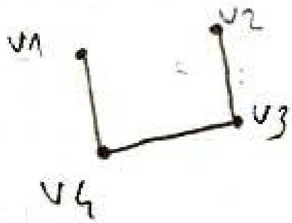
07 / 12 / 2018

* Is there a graph on 6 vertices, with degrees 2, 3, 3, 3, 3, 3 ? NO!



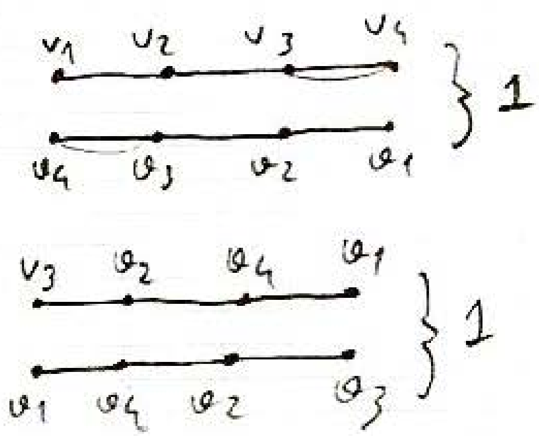
Because sum of all degrees should be even number

* How many graphs are there on 4 vertices with degrees 1, 1, 2, 2 ?



$V = \{v_1, v_2, v_3, v_4\}$

$G_2 = (V, \{v_1, v_4\}, \{v_4, v_3\}, \{v_2, v_3\})$

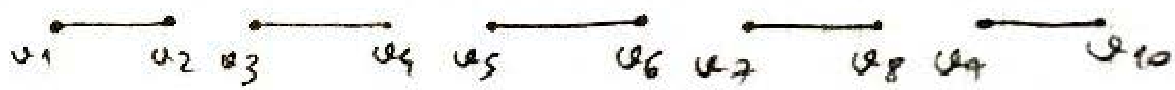


$4! = 24$

$\frac{24}{2} = 12$ //

07/12/2018

* How many graphs are there with 10 vertices, with degrees 1, 1, 1, 1, 1, 1, 1, 1, 1, 1 ?



$$9 \times 7 \times 5 \times 3 \times 1 = 945$$

1, 1, 1, 1

$3 \times 1 = 3$

* An <u>empty graph</u> is a graph with no edges.

* A <u>complete graph</u> (or a clique) with n vertices has $\binom{n}{2}$ edges. $\binom{n}{2} = \frac{n(n-1)}{2}$

<u>Proof</u> $V = \{v_1, \ldots, v_n\}$

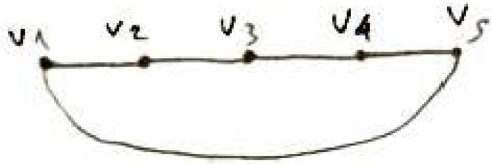
	degree
v_1	$n-1$
v_2	$n-1$
$\vdots$	
v_n	$n-1$
	$n(n-1)$

v_1 will have $n-1$ new edges incident

$$\frac{n(n-1)}{2}$$

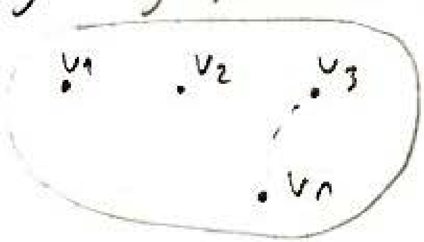
14 / 12 / 2018

* Let us draw n nodes in a row and connect the consecutive ones by an edge. The graph has $n-1$ edges and is called a <u>path</u>. The first and last nodes (vertices) are the end points of the path. If we connect the endpoints as well, we get a <u>cycle.</u>

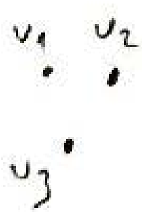


* A graph H is called a subgraph of G if it can be obtained from G by deleting some of its edges and nodes.

<u>Ex</u> How many subgraphs does an empty graph on n nodes are there?



$2^n - 1$



v_1
v_2
v_3
$v_1 - v_2$
$v_1 - v_3$
$v_2 - v_3$
ϕ
$v_1 - v_2 - v_3$

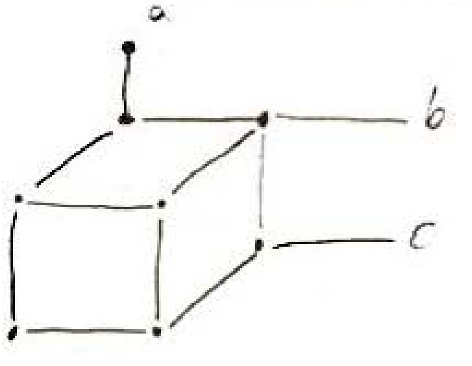
$2^3 - 1$

14/12/2018

* A graph G is connected if every two nodes of the graph can be connected by a.

* A graph G is connected if for every two nodes u and v, path in G there exists a path with end points u and v that is a subgraph of G.

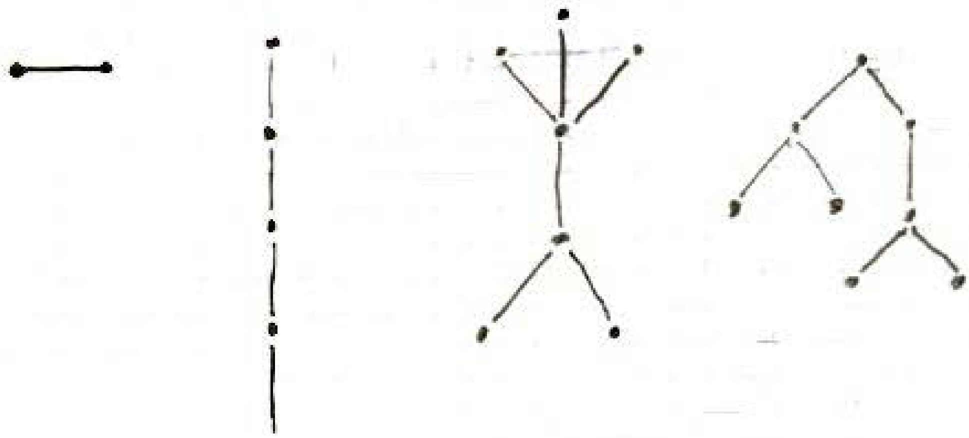
Ex Assume in a graph vertices a, b are connected with a path P. And vertices b, c are connected with a path Q. How to find the path that connects a to c?



14/12/2018

~ TREES ~

A graph $G=(V,E)$ is called a TREE if it is not connected and contains no <u>cycle</u> as a subgraph



Note that <u>connectedness</u> imply not too few edges, while having no cycle implies not too many edges.

THEOREM

A graph G is a tree <u>if and only if</u> it's connected but deleting only of its edges results in a disconnected graph.

→ If G is a tree then deleting any edge in G results in a disconnected graph ($p \to q \equiv \neg q \to \neg p$)

Assume I delete the edge (v,w) in G but G is still connected. This means there is a path with endpoints v and w other than the edge that I had just deleted. This means there is a cycle in G (which edge $\{v,w\}$ is part of). Then G is not a tree.