Topics:

Congruences
induction / well-ordering
rationality / contradiction
graphs
~~sets (products ...)~~ - not on exam
proof by cases

~~Euclid's proof~~ - not on exam

I. Graphs.

- degrees of vertices. sum of degrees of the vertices = 2 # edges.

- connected components, connectedness.

example problem:

country with 20 cities
each city had 10 roads from it.

a) How many roads?

(a) Prove that you can get from every city to every other city with ≤ 1 connection.

(b) One road got closed. Prove that you can still get from any city to any other city.

Solution: (a): How many roads?
sum of degrees of the vertices:

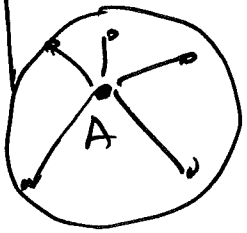
$$\frac{20 \cdot 10}{2} = 100$$

20 vertices, 10 edges from each. (each has degree 10)

cities = vertices
roads = edges.

(a) Prove by contradiction.

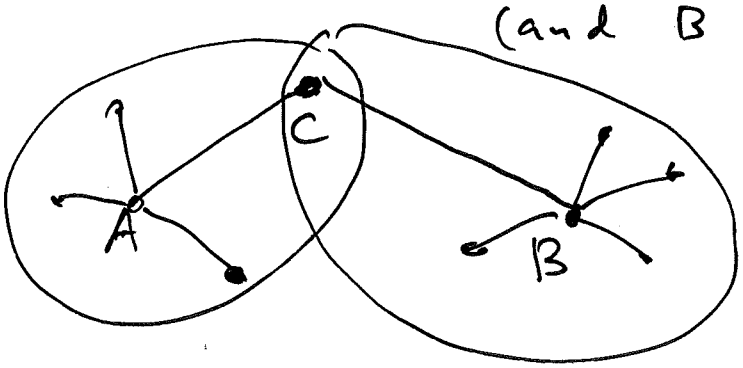
Let A, B be cities.



suppose we could not get from A to B.

11 cities:

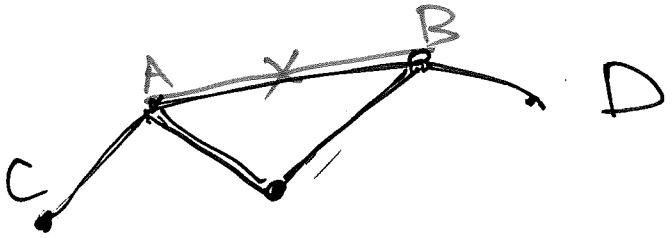
If we cannot get from A to B,
then we have 10 cities connected by
direct road to A, and A
and 10 cities connected by road to B
(and B itself)



since we cannot get
from A to B,
there are no
common cities!
But then we get 22
cities!
Contradiction!

(b) Suppose the road from A to B got closed.
~~If our statement is false then~~ ~~can no longer get from A to B.~~
~~Contradiction.~~
We still need to prove that we can get
from A to B.

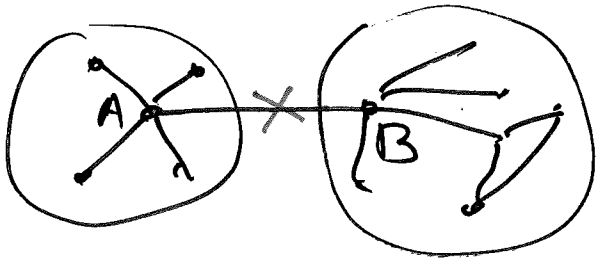
(Note: If we prove this, then we know
that can still get from any city C
to any other city D.
(If the path from C to D did not contain
the closed road, it would remain.
If it contained the closed road,
then still go from C to A)



Let us prove
that we can
still get from
A to B.

By contradiction: Suppose we could NOT get from A to B.

This would mean that after the road got closed, A and B ended up in different connected components of our graph.



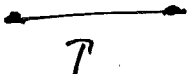
Then the connected component of A has:
one vertex of degree 9 (if it is A)
every other vertex still has degree 10.
So this connected component has only one vertex of odd degree. Contradiction!

Graphs and induction

Theorem: every connected graph G with at least 2 vertices has at least two vertices x_1, x_2 such that you can throw them away (with their edges) and the graph remains connected.

Proof: using strong induction.
(on the number of vertices)
(means: our statement $P(n)$ will be about all graphs with n vertices)

1. base case: $n=2$



↑ the only connected graph with 2 vertices.

Can take both away.
Get empty graph - connected.

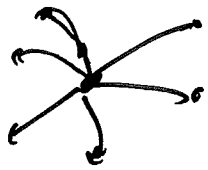
(might do $n=3$ ...)

Induction step: Suppose we have a graph with $n+1$ vertices.

Assume we know the statement for any graph with $\boxed{\leq n}$ vertices

↑ strong induction.

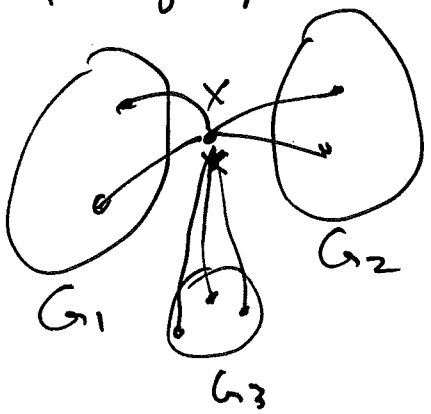
Take any vertex $x \in V_k$. erase x and all its edges.



2 cases: 1) Maybe the graph remains connected.

Then you have a graph with n vertices, it is connected, by induction assumption can remove one vertex so that it remains connected. Remove it, all is good.

2) The graph is no longer connected.



So we got at least two connected components.

$G_1, G_2, \ldots$ maybe more

We need: at least one of them has ≥ 2 vertices

Consider G_1, suppose at least 2 vertices

It is a connected graph with $\leq n$ vertices

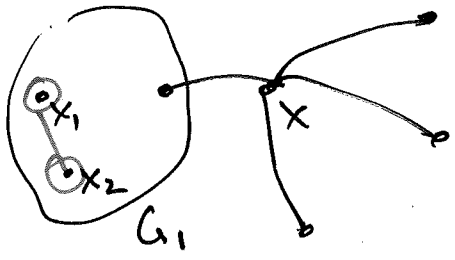
Use strong induction assumption:

exist x_1, x_2 in G_1 so that we can remove them, and G_1 remains connected.

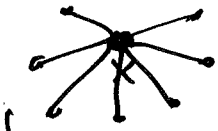
Then we could have removed x_1, x_2 and put x back!

Because we put x back, the graph becomes connected again.

and since removing x_1, x_2 did not destroy connectedness of G_1, removing them from G also leaves the graph connected.



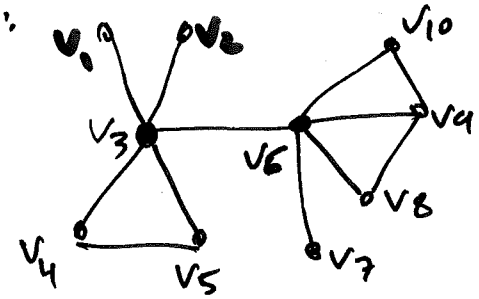
What if there was no component with ≥ 2 vertices? This means, the graph was:



then could remove any except x.

What did this mean?

example:

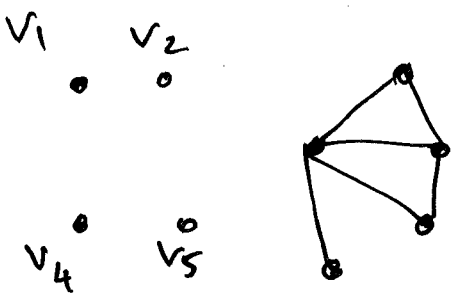


Which vertices can be removed so that the graph remains connected?

$v_1, v_2, v_4, v_5, v_7, v_8, v_9, v_{10}$ could be removed!

v_6, v_3 cannot be removed!

If remove v_3, get:



5 connected components!

Congruences:

- reduces questions about divisibility to a few cases.

Key theorem: $a \equiv b \mod m$
$c \equiv d \mod m$

then $a+c \equiv b+d \mod m$
$ac \equiv bd \mod m$.

Main point: Let $m = 9$.
Then any number is congruent to one of: $0, 1, 2, 3, 4, 5, 6, 7, 8 \mod 9$.
So many questions reduce to considering 9 cases.

Example: Prove that a^2 can only be congruent to $0, 1$ or $4 \mod 5$.

Proof: cases.
1) $a \equiv 0 \mod 5$ then $a^2 \equiv 0^2 \mod 5$
2) $a \equiv 1 \mod 5$, then $a^2 \equiv 1^2 = 1 \mod 5$
3) $a \equiv 2 \mod 5$
4) $a \equiv 3 \mod 5$ then $a^2 \equiv 4 \mod 5$
5) $a \equiv 4 \mod 5$ $a^2 \equiv 3^2 = 9 \equiv 4 \mod 5$
$4 \equiv -1 \mod 5$,
so $a^2 \equiv (-1)^2 = 1 \mod 5$.

---

one more Example: Prove that $a^2 + b^2 = c^2 - 1$ does not have integer solutions with c even.

How to solve: Try mod 3:

a^2 is 0 or 1 mod 3 (cannot be 2)

b^2 is 0 or 1 mod 3

a^2+b^2 is 0 or 1 or 2 mod 3.

all the possibilites. (Nothing is impossible!)

Mod 3 is NOT working!

Try mod 4: a^2 can be only 0 or 1 mod 4

(check!) ← 4 cases: $a \equiv 0,1,2,3 \bmod 4$, square all, see only get 0 or 1!

Then a^2+b^2 can only be $0, 1=0+1$ or $2=1+1$ mod 4.

We note that $a^2+b^2 \equiv 3 \bmod 4$ is impossible!

What about c^2-1? If c is even,

then $c^2 \equiv 0 \bmod 4$

Then $c^2-1 \equiv -1 \equiv 3 \bmod 4$

So we see that $a^2+b^2 = c^2-1$ is NOT possible!

(a^2+b^2: never $\equiv 3 \bmod 4$; c^2-1: always $\equiv 3 \bmod 4$ when c is even.)

This was scratch work.
Now write it nicely using proof by contradiction.

Proof: Suppose we had $a^2+b^2 = c^2-1$ with $a,b,c \in \mathbb{Z}$ and c even.

Then since c is even, $c^2 - 1 \equiv -1 \equiv 3 \bmod 4$

But $a^2 \equiv 0$ or $1 \bmod 4$ (Lemma)

$b^2 \equiv 0$ or $1 \bmod 4$

So $a^2 + b^2$ can only be congruent to 0, 1 or 2 mod 4,

so $a^2 + b^2 = c^2 - 1$ is a contradiction.

Problem: Any number written with 3^n same digits is divisible by 3^n.

$\underbrace{\overline{aa\ldots a}}_{3^n}$ digit a repeated 3^n times.

Example $\underbrace{888}_{3}$ is divisible by 3

Next one: $\underbrace{888888888}_{9}$ is divisible by 9.

Use induction base $n=1$: $\overline{aaa} = 100a + 10a + a$

$= a(100+10+1) = a \cdot 111$

$3 \mid 111$, so $3 \mid \overline{aaa}$.

Induction step: assume $\underbrace{\overline{aa\ldots a}}_{3^n}$ is divisible by 3^n.

Need to prove: $\underbrace{\overline{aa\ldots a}}_{3^{n+1}}$ is divisible by 3^{n+1}.

Proof: $\underbrace{\overline{a\ldots|\ldots a}}_{3^n}\underbrace{}_{3^n}\underbrace{}_{3^n} = \underbrace{\overline{aa\ldots a}}_{3^n} \cdot 10^{2 \cdot 3^n}$

$+ \underbrace{\overline{aa\ldots a}}_{3^n} \cdot 10^{3^n}$

$= \overline{aaa|000\ldots0}$

$+ \overline{aaa000}$

$+ \overline{aaa}$

$+ \underbrace{\overline{aaa\ldots a}}_{3^n} =$

$$= \underbrace{aa\ldots a}_{3^n}\left(10^{2\cdot 3^n} + 10^{3^n} + 1\right)$$

$$\Big\Vert$$

$$\underbrace{10\ldots0}_{3^n-1?}\,1\,\underbrace{0\ldots0}_{3^n-1?}\,1$$

☺ (doesn't matter how many 0's)

← is divisible by 3 (because the sum of its digits is 3).

We got: $3^n \cdot 3 \cdot k$, let it equal $3k$

which is divisible by 3^{n+1}.

Problem (induction)

Let $S = \{2^i : i \in \mathbb{N} \cup \{0\}\} = \{1, 2, 4, 8, 16, \ldots\}$ (2^0; powers of 2).

Prove that for any $n \in \mathbb{N}$, there exists a subset S_n of S such that

$$\sum_{a \in S_n} a = n.$$

In words: any number $n \in \mathbb{N}$ can be written as a sum of powers of 2 (without repetition)

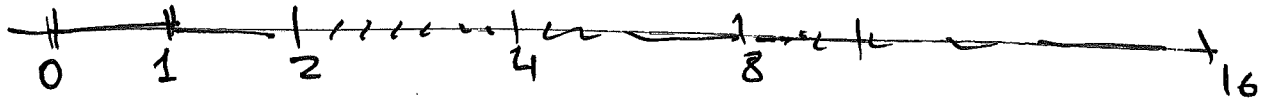
Same problem: You have coins of ~~denomination~~ 1c, 2c, 4c, 8c, 16c, ... (one of each)

Prove that you can pay any amount n (cents) using these coins.

Prove by induction: Not going from n to $n+1$.

Instead, Prove this:

any number n between 2^m and 2^{m+1} can be represented.



Assume know it for all $n \leq 2^m$.

Need to prove: for all $n \leq 2^{m+1}$.

So what we need to prove is:

can represent any n which satisfies

$$2^m < n \leq 2^{m+1}.$$

We have: $n = 2^m + (n - 2^m)$

$(n - 2^m)$ is between 1 and 2^m so by induction assumption we can represent it as sum of powers less than m.