Today

More graph theory.

Today

More graph theory.

Modular Arithmetic.

Today

More graph theory.

Modular Arithmetic.

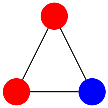
Inverses.

Graph Coloring.

Given $G=(V,E)$, a coloring of a G assigns colors to vertices V where for each edge the endpoints have different colors.

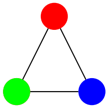
Graph Coloring.

Given $G = (V, E)$, a coloring of a G assigns colors to vertices V where for each edge the endpoints have different colors.



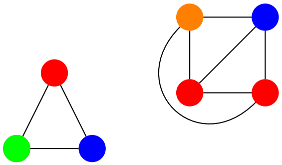
Graph Coloring.

Given $G = (V, E)$, a coloring of a G assigns colors to vertices V where for each edge the endpoints have different colors.



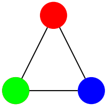
Graph Coloring.

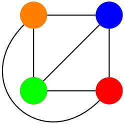
Given $G = (V, E)$, a coloring of a G assigns colors to vertices V where for each edge the endpoints have different colors.



Graph Coloring.

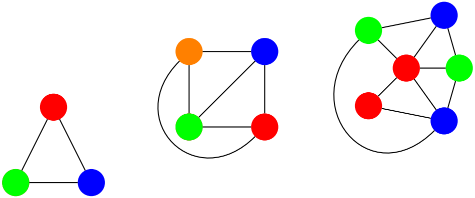
Given $G = (V, E)$, a coloring of a G assigns colors to vertices V where for each edge the endpoints have different colors.





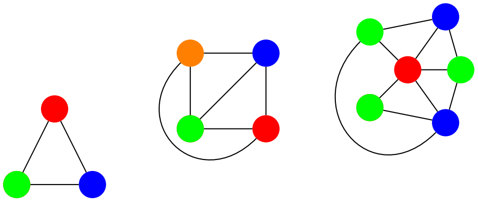
Graph Coloring.

Given $G = (V, E)$, a coloring of a G assigns colors to vertices V where for each edge the endpoints have different colors.



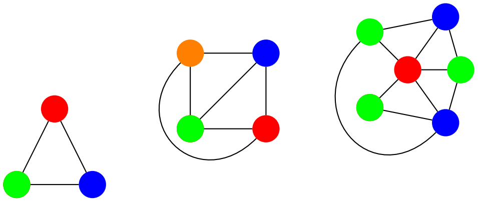
Graph Coloring.

Given $G = (V, E)$, a coloring of a G assigns colors to vertices V where for each edge the endpoints have different colors.



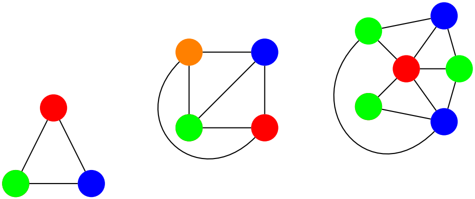
Graph Coloring.

Given $G = (V, E)$, a coloring of a G assigns colors to vertices V where for each edge the endpoints have different colors.



Graph Coloring.

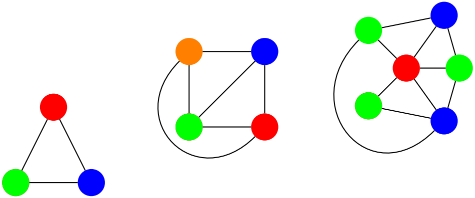
Given $G = (V, E)$, a coloring of a G assigns colors to vertices V where for each edge the endpoints have different colors.



Notice that the last one, has one three colors.

Graph Coloring.

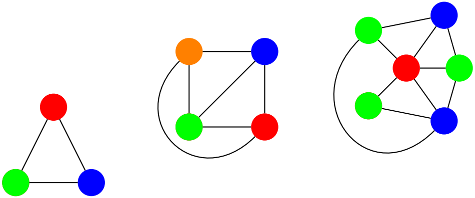
Given $G = (V, E)$, a coloring of a G assigns colors to vertices V where for each edge the endpoints have different colors.



Notice that the last one, has one three colors.
  Fewer colors than number of vertices.

Graph Coloring.

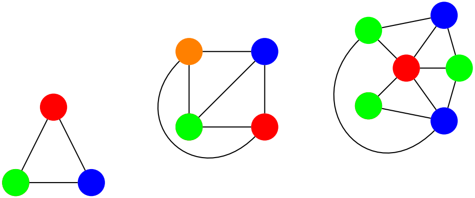
Given $G = (V, E)$, a coloring of a G assigns colors to vertices V where for each edge the endpoints have different colors.



Notice that the last one, has one three colors.
   Fewer colors than number of vertices.
   Fewer colors than max degree node.

Graph Coloring.

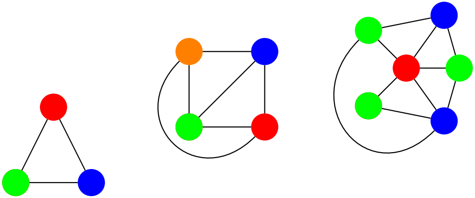
Given $G = (V, E)$, a coloring of a G assigns colors to vertices V where for each edge the endpoints have different colors.



Notice that the last one, has one three colors.
  Fewer colors than number of vertices.
  Fewer colors than max degree node.

Graph Coloring.

Given $G = (V, E)$, a coloring of a G assigns colors to vertices V where for each edge the endpoints have different colors.

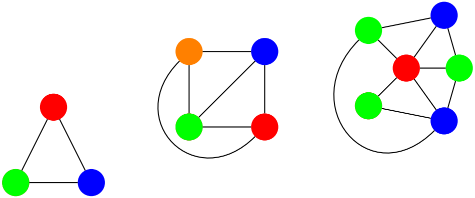


Notice that the last one, has one three colors.
  Fewer colors than number of vertices.
  Fewer colors than max degree node.

Interesting things to do.

Graph Coloring.

Given $G = (V, E)$, a coloring of a G assigns colors to vertices V where for each edge the endpoints have different colors.

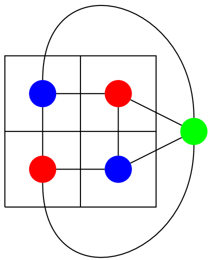


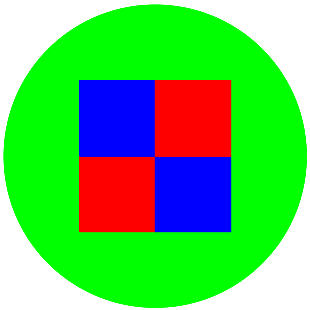
Notice that the last one, has one three colors.
  Fewer colors than number of vertices.
  Fewer colors than max degree node.

Interesting things to do. Algorithm!

Planar graphs and maps.

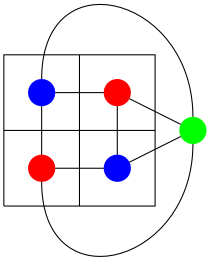
Planar graph coloring $\equiv$ map coloring.

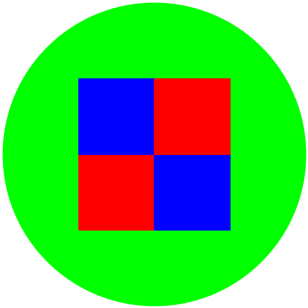




Planar graphs and maps.

Planar graph coloring $\equiv$ map coloring.





Four color theorem is about planar graphs!

Six color theorem.

Theorem: Every planar graph can be colored with six colors.

Six color theorem.

Theorem: Every planar graph can be colored with six colors.

Proof:

Six color theorem.

Theorem: Every planar graph can be colored with six colors.

Proof:
Recall: $e \leq 3v - 6$ for any planar graph where $v > 2$.

Six color theorem.

Theorem: Every planar graph can be colored with six colors.

Proof:
Recall: $e \leq 3v - 6$ for any planar graph where $v > 2$.
From Euler's Formula.

Six color theorem.

Theorem: Every planar graph can be colored with six colors.

Proof:
Recall: $e \leq 3v - 6$ for any planar graph where $v > 2$.
From Euler's Formula.

Total degree: $2e$

Six color theorem.

Theorem: Every planar graph can be colored with six colors.

Proof:
Recall: $e \leq 3v - 6$ for any planar graph where $v > 2$.
From Euler's Formula.

Total degree: $2e$
Average degree: $\leq \frac{2e}{v}$

Six color theorem.

Theorem: Every planar graph can be colored with six colors.

Proof:
Recall: $e \leq 3v - 6$ for any planar graph where $v > 2$.
From Euler's Formula.

Total degree: $2e$
Average degree: $\leq \frac{2e}{v} \leq \frac{2(3v-6)}{v}$

Six color theorem.

Theorem: Every planar graph can be colored with six colors.

Proof:
Recall: $e \leq 3v - 6$ for any planar graph where $v > 2$.
From Euler's Formula.

Total degree: $2e$
Average degree: $\leq \frac{2e}{v} \leq \frac{2(3v-6)}{v} \leq 6 - \frac{12}{v}$.

Six color theorem.

Theorem: Every planar graph can be colored with six colors.

Proof:
Recall: $e \leq 3v - 6$ for any planar graph where $v > 2$.
From Euler's Formula.

Total degree: $2e$
Average degree: $\leq \frac{2e}{v} \leq \frac{2(3v-6)}{v} \leq 6 - \frac{12}{v}$.

There exists a vertex with degree < 6

Six color theorem.

Theorem: Every planar graph can be colored with six colors.

Proof:
Recall: $e \leq 3v - 6$ for any planar graph where $v > 2$.
From Euler's Formula.

Total degree: $2e$
Average degree: $\leq \frac{2e}{v} \leq \frac{2(3v-6)}{v} \leq 6 - \frac{12}{v}$.

There exists a vertex with degree < 6 or at most 5.

Six color theorem.

Theorem: Every planar graph can be colored with six colors.

Proof:
Recall: $e \leq 3v - 6$ for any planar graph where $v > 2$.
From Euler's Formula.

Total degree: $2e$
Average degree: $\leq \frac{2e}{v} \leq \frac{2(3v-6)}{v} \leq 6 - \frac{12}{v}$.

There exists a vertex with degree < 6 or at most 5.

Remove vertex v of degree at most 5.

Six color theorem.

Theorem: Every planar graph can be colored with six colors.

Proof:
Recall: $e \leq 3v - 6$ for any planar graph where $v > 2$.
From Euler's Formula.

Total degree: $2e$
Average degree: $\leq \frac{2e}{v} \leq \frac{2(3v-6)}{v} \leq 6 - \frac{12}{v}$.

There exists a vertex with degree < 6 or at most 5.

Remove vertex v of degree at most 5.
Inductively color remaining graph.

Six color theorem.

Theorem: Every planar graph can be colored with six colors.

Proof:
Recall: $e \leq 3v - 6$ for any planar graph where $v > 2$.
From Euler's Formula.

Total degree: $2e$
Average degree: $\leq \frac{2e}{v} \leq \frac{2(3v-6)}{v} \leq 6 - \frac{12}{v}$.

There exists a vertex with degree < 6 or at most 5.

Remove vertex v of degree at most 5.
Inductively color remaining graph.
Color is available for v since only five neighbors...

Six color theorem.

Theorem: Every planar graph can be colored with six colors.

Proof:
Recall: $e \leq 3v - 6$ for any planar graph where $v > 2$.
From Euler's Formula.

Total degree: $2e$
Average degree: $\leq \frac{2e}{v} \leq \frac{2(3v-6)}{v} \leq 6 - \frac{12}{v}$.

There exists a vertex with degree < 6 or at most 5.

Remove vertex v of degree at most 5.
Inductively color remaining graph.
Color is available for v since only five neighbors...
and only five colors are used.

Six color theorem.

Theorem: Every planar graph can be colored with six colors.

Proof:
Recall: $e \leq 3v - 6$ for any planar graph where $v > 2$.
From Euler's Formula.

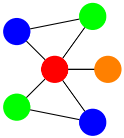
Total degree: $2e$
Average degree: $\leq \frac{2e}{v} \leq \frac{2(3v-6)}{v} \leq 6 - \frac{12}{v}$.

There exists a vertex with degree < 6 or at most 5.

Remove vertex v of degree at most 5.
Inductively color remaining graph.
Color is available for v since only five neighbors...
and only five colors are used. $\square$

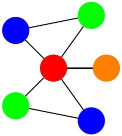
Five color theorem: prelimnary.

Preliminary Observation: Connected components of vertices with two colors in a legal coloring can switch colors.



Five color theorem: prelimnary.

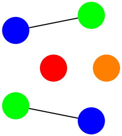
Preliminary Observation: Connected components of vertices with two colors in a legal coloring can switch colors.



Look at only green and blue.

Five color theorem: prelimnary.

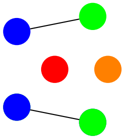
Preliminary Observation: Connected components of vertices with two colors in a legal coloring can switch colors.



Look at only green and blue.
Connected components.

Five color theorem: prelimnary.

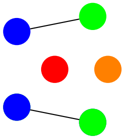
Preliminary Observation: Connected components of vertices with two colors in a legal coloring can switch colors.



Look at only green and blue.
Connected components.
Can switch in one component.

Five color theorem: prelimnary.

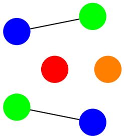
Preliminary Observation: Connected components of vertices with two colors in a legal coloring can switch colors.



Look at only green and blue.
Connected components.
Can switch in one component.

Five color theorem: prelimnary.

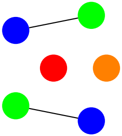
Preliminary Observation: Connected components of vertices with two colors in a legal coloring can switch colors.



Look at only green and blue.
Connected components.
Can switch in one component.

Five color theorem: prelimnary.

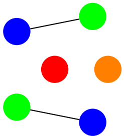
Preliminary Observation: Connected components of vertices with two colors in a legal coloring can switch colors.



Look at only green and blue.
Connected components.
Can switch in one component.
Or the other.

Five color theorem: prelimnary.

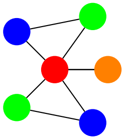
Preliminary Observation: Connected components of vertices with two colors in a legal coloring can switch colors.



Look at only green and blue.
Connected components.
Can switch in one component.
Or the other.

Five color theorem: prelimnary.

Preliminary Observation: Connected components of vertices with two colors in a legal coloring can switch colors.



Look at only green and blue.
Connected components.
Can switch in one component.
Or the other.

Five color theorem

Theorem: Every planar graph can be colored with five colors.

Five color theorem

Theorem: Every planar graph can be colored with five colors.

Preliminary Observation: Connected components of vertices with two colors in a legal coloring can switch colors.

Five color theorem

Theorem: Every planar graph can be colored with five colors.

Preliminary Observation: Connected components of vertices with two colors in a legal coloring can switch colors.

Proof:

Five color theorem

Theorem: Every planar graph can be colored with five colors.

Preliminary Observation: Connected components of vertices with two colors in a legal coloring can switch colors.

Proof: Again with the degree 5 vertex.

Five color theorem

Theorem: Every planar graph can be colored with five colors.

Preliminary Observation: Connected components of vertices with two colors in a legal coloring can switch colors.

Proof: Again with the degree 5 vertex. Again recurse.

Five color theorem

Theorem: Every planar graph can be colored with five colors.

Preliminary Observation: Connected components of vertices with two colors in a legal coloring can switch colors.

Proof: Again with the degree 5 vertex. Again recurse.

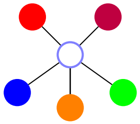
Five color theorem

Theorem: Every planar graph can be colored with five colors.

Preliminary Observation: Connected components of vertices with two colors in a legal coloring can switch colors.

Proof: Again with the degree 5 vertex. Again recurse.

Assume neighbors are colored all differently.



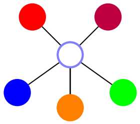
Five color theorem

Theorem: Every planar graph can be colored with five colors.

Preliminary Observation: Connected components of vertices with two colors in a legal coloring can switch colors.

Proof: Again with the degree 5 vertex. Again recurse.

Assume neighbors are colored all differently.
Otherwise done.

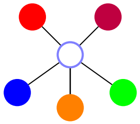


Five color theorem

Theorem: Every planar graph can be colored with five colors.

Preliminary Observation: Connected components of vertices with two colors in a legal coloring can switch colors.

Proof: Again with the degree 5 vertex. Again recurse.



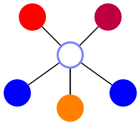
Assume neighbors are colored all differently.
Otherwise done.
Switch green to blue in component.

Five color theorem

Theorem: Every planar graph can be colored with five colors.

Preliminary Observation: Connected components of vertices with two colors in a legal coloring can switch colors.

Proof: Again with the degree 5 vertex. Again recurse.



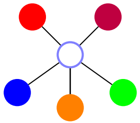
Assume neighbors are colored all differently.
Otherwise done.
Switch green to blue in component.
Done.

Five color theorem

Theorem: Every planar graph can be colored with five colors.

Preliminary Observation: Connected components of vertices with two colors in a legal coloring can switch colors.

Proof: Again with the degree 5 vertex. Again recurse.



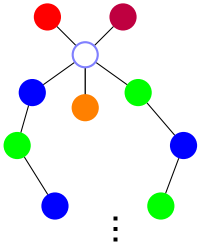
Assume neighbors are colored all differently.
Otherwise done.
Switch green to blue in component.
Done. Unless blue-green path to blue.

Five color theorem

Theorem: Every planar graph can be colored with five colors.

Preliminary Observation: Connected components of vertices with two colors in a legal coloring can switch colors.

Proof: Again with the degree 5 vertex. Again recurse.



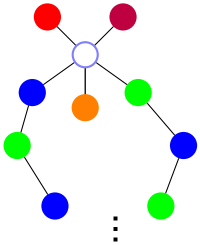
Assume neighbors are colored all differently.
Otherwise done.
Switch green to blue in component.
Done. Unless blue-green path to blue.

Five color theorem

Theorem: Every planar graph can be colored with five colors.

Preliminary Observation: Connected components of vertices with two colors in a legal coloring can switch colors.

Proof: Again with the degree 5 vertex. Again recurse.



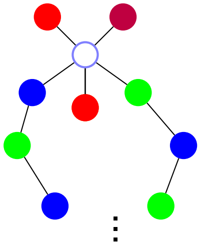
Assume neighbors are colored all differently.
Otherwise done.
Switch green to blue in component.
Done. Unless blue-green path to blue.
Switch orange to red in its component.

Five color theorem

Theorem: Every planar graph can be colored with five colors.

Preliminary Observation: Connected components of vertices with two colors in a legal coloring can switch colors.

Proof: Again with the degree 5 vertex. Again recurse.



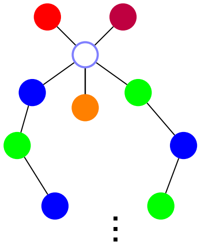
Assume neighbors are colored all differently.
Otherwise done.
Switch green to blue in component.
Done. Unless blue-green path to blue.
Switch orange to red in its component.
Done.

Five color theorem

Theorem: Every planar graph can be colored with five colors.

Preliminary Observation: Connected components of vertices with two colors in a legal coloring can switch colors.

Proof: Again with the degree 5 vertex. Again recurse.



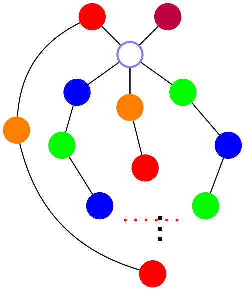
Assume neighbors are colored all differently.
Otherwise done.
Switch green to blue in component.
Done. Unless blue-green path to blue.
Switch orange to red in its component.
Done. Unless red-orange path to red.

Five color theorem

Theorem: Every planar graph can be colored with five colors.

Preliminary Observation: Connected components of vertices with two colors in a legal coloring can switch colors.

Proof: Again with the degree 5 vertex. Again recurse.



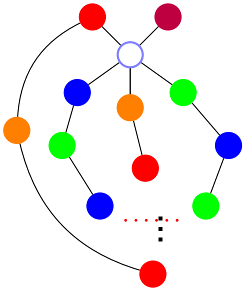
Assume neighbors are colored all differently.
Otherwise done.
Switch green to blue in component.
Done. Unless blue-green path to blue.
Switch orange to red in its component.
Done. Unless red-orange path to red.

Five color theorem

Theorem: Every planar graph can be colored with five colors.

Preliminary Observation: Connected components of vertices with two colors in a legal coloring can switch colors.

Proof: Again with the degree 5 vertex. Again recurse.



Assume neighbors are colored all differently.
Otherwise done.
Switch green to blue in component.
Done. Unless blue-green path to blue.
Switch orange to red in its component.
Done. Unless red-orange path to red.

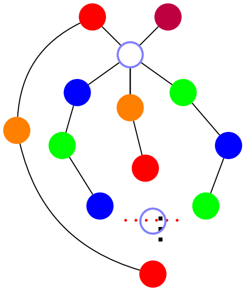
Planar.

Five color theorem

Theorem: Every planar graph can be colored with five colors.

Preliminary Observation: Connected components of vertices with two colors in a legal coloring can switch colors.

Proof: Again with the degree 5 vertex. Again recurse.



Assume neighbors are colored all differently.
Otherwise done.
Switch green to blue in component.
Done. Unless blue-green path to blue.
Switch orange to red in its component.
Done. Unless red-orange path to red.

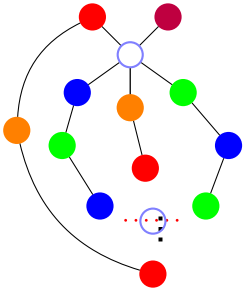
Planar. $\implies$ paths intersect at a vertex!

Five color theorem

Theorem: Every planar graph can be colored with five colors.

Preliminary Observation: Connected components of vertices with two colors in a legal coloring can switch colors.

Proof: Again with the degree 5 vertex. Again recurse.



Assume neighbors are colored all differently.
Otherwise done.
Switch green to blue in component.
Done. Unless blue-green path to blue.
Switch orange to red in its component.
Done. Unless red-orange path to red.

Planar. $\Longrightarrow$ paths intersect at a vertex!

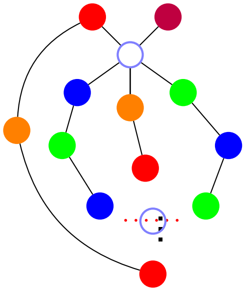
What color is it?

Five color theorem

Theorem: Every planar graph can be colored with five colors.

Preliminary Observation: Connected components of vertices with two colors in a legal coloring can switch colors.

Proof: Again with the degree 5 vertex. Again recurse.



Assume neighbors are colored all differently.
Otherwise done.
Switch green to blue in component.
Done. Unless blue-green path to blue.
Switch orange to red in its component.
Done. Unless red-orange path to red.

Planar. $\implies$ paths intersect at a vertex!

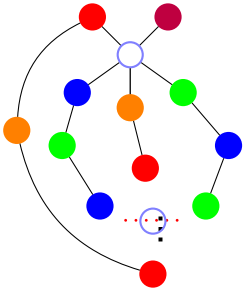
What color is it?

Five color theorem

Theorem: Every planar graph can be colored with five colors.

Preliminary Observation: Connected components of vertices with two colors in a legal coloring can switch colors.

Proof: Again with the degree 5 vertex. Again recurse.



Assume neighbors are colored all differently.
Otherwise done.
Switch green to blue in component.
Done. Unless blue-green path to blue.
Switch orange to red in its component.
Done. Unless red-orange path to red.

Planar. $\Longrightarrow$ paths intersect at a vertex!

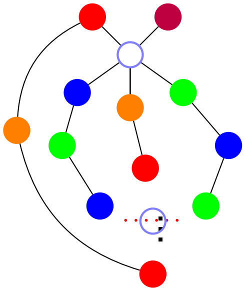
What color is it?
Must be blue or green to be on that path.

Five color theorem

Theorem: Every planar graph can be colored with five colors.

Preliminary Observation: Connected components of vertices with two colors in a legal coloring can switch colors.

Proof: Again with the degree 5 vertex. Again recurse.



Assume neighbors are colored all differently.
Otherwise done.
Switch green to blue in component.
Done. Unless blue-green path to blue.
Switch orange to red in its component.
Done. Unless red-orange path to red.

Planar. $\Longrightarrow$ paths intersect at a vertex!

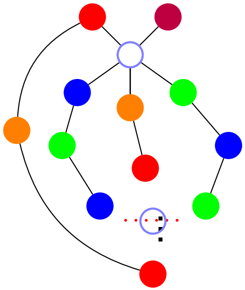
What color is it?
Must be blue or green to be on that path.
Must be red or orange to be on that path.

Five color theorem

Theorem: Every planar graph can be colored with five colors.

Preliminary Observation: Connected components of vertices with two colors in a legal coloring can switch colors.

Proof: Again with the degree 5 vertex. Again recurse.



Assume neighbors are colored all differently.
Otherwise done.
Switch green to blue in component.
Done. Unless blue-green path to blue.
Switch orange to red in its component.
Done. Unless red-orange path to red.

Planar. $\Longrightarrow$ paths intersect at a vertex!

What color is it?
Must be blue or green to be on that path.
Must be red or orange to be on that path.

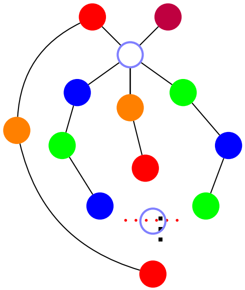
Contradiction.

Five color theorem

Theorem: Every planar graph can be colored with five colors.

Preliminary Observation: Connected components of vertices with two colors in a legal coloring can switch colors.

Proof: Again with the degree 5 vertex. Again recurse.



Assume neighbors are colored all differently.
  Otherwise done.
Switch green to blue in component.
  Done. Unless blue-green path to blue.
Switch orange to red in its component.
  Done. Unless red-orange path to red.

Planar. $\Longrightarrow$ paths intersect at a vertex!

What color is it?
  Must be blue or green to be on that path.
  Must be red or orange to be on that path.

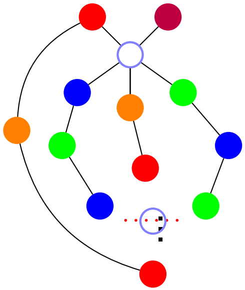
Contradiction. Can recolor one of the neighbors.
And recolor "center" vertex.

Five color theorem

Theorem: Every planar graph can be colored with five colors.

Preliminary Observation: Connected components of vertices with two colors in a legal coloring can switch colors.

Proof: Again with the degree 5 vertex. Again recurse.



Assume neighbors are colored all differently.
  Otherwise done.
Switch green to blue in component.
  Done. Unless blue-green path to blue.
Switch orange to red in its component.
  Done. Unless red-orange path to red.

Planar. $\Longrightarrow$ paths intersect at a vertex!

What color is it?
  Must be blue or green to be on that path.
  Must be red or orange to be on that path.

Contradiction. Can recolor one of the neighbors.
And recolor "center" vertex. □

Four Color Theorem

Four Color Theorem

Theorem: Any planar graph can be colored with four colors.

Four Color Theorem

Theorem: Any planar graph can be colored with four colors.

Proof:

Four Color Theorem

Theorem: Any planar graph can be colored with four colors.

Proof: Not Today!

Four Color Theorem

Theorem: Any planar graph can be colored with four colors.

Proof: Not Today!

Hypercubes.

Complete graphs, really connected!

Hypercubes.

Complete graphs, really connected! But lots of edges.

$|V|(|V|-1)/2$

Hypercubes.

Complete graphs, really connected! But lots of edges.

$|V|(|V|-1)/2$

Trees,

Hypercubes.

Complete graphs, really connected! But lots of edges.

$|V|(|V|-1)/2$

Trees, few edges. $(|V|-1)$

Hypercubes.

Complete graphs, really connected! But lots of edges.

$|V|(|V|-1)/2$

Trees, few edges. $(|V|-1)$

but just falls apart!

Hypercubes.

Complete graphs, really connected! But lots of edges.

$|V|(|V|-1)/2$

Trees, few edges. $(|V|-1)$

but just falls apart!

Hypercubes.

Complete graphs, really connected! But lots of edges.

$|V|(|V|-1)/2$

Trees, few edges. $(|V|-1)$

but just falls apart!

Hypercubes.

Hypercubes.

Complete graphs, really connected! But lots of edges.

$|V|(|V|-1)/2$

Trees, few edges. $(|V|-1)$

but just falls apart!

Hypercubes. Really connected.

Hypercubes.

Complete graphs, really connected! But lots of edges.

$|V|(|V|-1)/2$

Trees, few edges. $(|V|-1)$

but just falls apart!

Hypercubes. Really connected. $|V|\log|V|$ edges!

Hypercubes.

Complete graphs, really connected! But lots of edges.

$|V|(|V|-1)/2$

Trees, few edges. $(|V|-1)$

but just falls apart!

Hypercubes. Really connected. $|V|\log|V|$ edges!

Also represents bit-strings nicely.

Hypercubes.

Complete graphs, really connected! But lots of edges.
$|V|(|V|-1)/2$
Trees, few edges. $(|V|-1)$
but just falls apart!

Hypercubes. Really connected. $|V|\log|V|$ edges!
Also represents bit-strings nicely.

Hypercubes.

Complete graphs, really connected! But lots of edges.

$|V|(|V|-1)/2$

Trees, few edges. $(|V|-1)$

but just falls apart!

Hypercubes. Really connected. $|V|\log|V|$ edges!

Also represents bit-strings nicely.

$G=(V,E)$

Hypercubes.

Complete graphs, really connected! But lots of edges.

$|V|(|V|-1)/2$

Trees, few edges. $(|V|-1)$

but just falls apart!

Hypercubes. Really connected. $|V|\log|V|$ edges!

Also represents bit-strings nicely.

$G = (V, E)$

$|V| = \{0,1\}^n$,

Hypercubes.

Complete graphs, really connected! But lots of edges.

$|V|(|V|-1)/2$

Trees, few edges. $(|V|-1)$

but just falls apart!

Hypercubes. Really connected. $|V|\log|V|$ edges!

Also represents bit-strings nicely.

$G = (V, E)$

$|V| = \{0,1\}^n$,

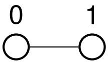
$|E| = \{(x,y)|x$ and y differ in one bit position.$\}$

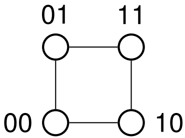
Hypercubes.

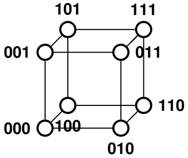
Complete graphs, really connected! But lots of edges.
$|V|(|V|-1)/2$
Trees, few edges. $(|V|-1)$
but just falls apart!

Hypercubes. Really connected. $|V|\log|V|$ edges!
Also represents bit-strings nicely.

$G = (V, E)$
$|V| = \{0,1\}^n$,
$|E| = \{(x,y) | x$ and y differ in one bit position.$\}$





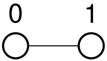


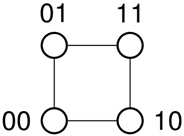
Hypercubes.

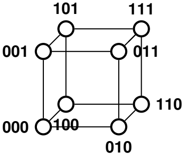
Complete graphs, really connected! But lots of edges.
$|V|(|V|-1)/2$
Trees, few edges. $(|V|-1)$
but just falls apart!

Hypercubes. Really connected. $|V|\log|V|$ edges!
Also represents bit-strings nicely.

$G=(V,E)$
$|V|=\{0,1\}^n$,
$|E|=\{(x,y)|x$ and y differ in one bit position.$\}$







2^n vertices.

Hypercubes.

Complete graphs, really connected! But lots of edges.

$|V|(|V|-1)/2$

Trees, few edges. $(|V|-1)$

but just falls apart!

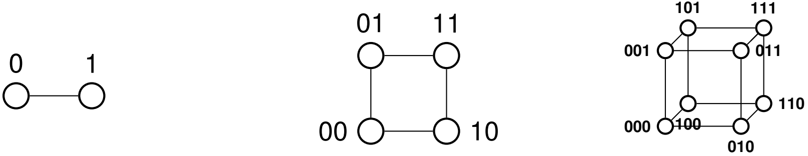
Hypercubes. Really connected. $|V|\log|V|$ edges!

Also represents bit-strings nicely.

$G=(V,E)$

$|V|=\{0,1\}^n$,

$|E|=\{(x,y)|x$ and y differ in one bit position.$\}$



2^n vertices. number of n-bit strings!

Hypercubes.

Complete graphs, really connected! But lots of edges.

$|V|(|V|-1)/2$

Trees, few edges. $(|V|-1)$

but just falls apart!

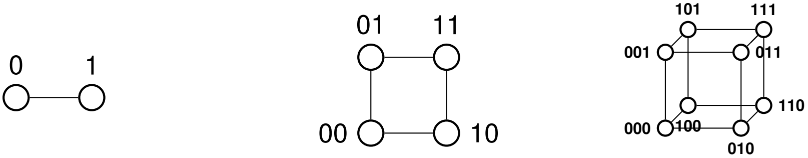
Hypercubes. Really connected. $|V|\log|V|$ edges!

Also represents bit-strings nicely.

$G=(V,E)$

$|V|=\{0,1\}^n$,

$|E|=\{(x,y)|x$ and y differ in one bit position.$\}$



2^n vertices. number of n-bit strings!

$n2^{n-1}$ edges.

Hypercubes.

Complete graphs, really connected! But lots of edges.

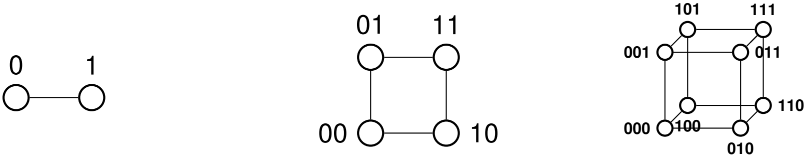
$|V|(|V|-1)/2$

Trees, few edges. $(|V|-1)$

but just falls apart!

Hypercubes. Really connected. $|V|\log|V|$ edges!
Also represents bit-strings nicely.

$G=(V,E)$
$|V|=\{0,1\}^n$,
$|E|=\{(x,y)|x$ and y differ in one bit position.$\}$



2^n vertices. number of n-bit strings!
$n2^{n-1}$ edges.

2^n vertices each of degree n

Hypercubes.

Complete graphs, really connected! But lots of edges.

$|V|(|V|-1)/2$

Trees, few edges. $(|V|-1)$

but just falls apart!

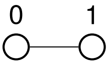
Hypercubes. Really connected. $|V|\log|V|$ edges!

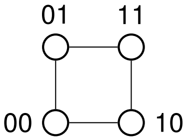
Also represents bit-strings nicely.

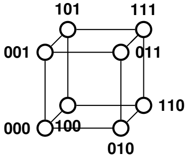
$G=(V,E)$

$|V|=\{0,1\}^n$,

$|E|=\{(x,y)|x$ and y differ in one bit position.$\}$







2^n vertices. number of n-bit strings!

$n2^{n-1}$ edges.

2^n vertices each of degree n

total degree is $n2^n$

Hypercubes.

Complete graphs, really connected! But lots of edges.

$|V|(|V|-1)/2$

Trees, few edges. $(|V|-1)$

but just falls apart!

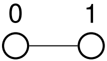
Hypercubes. Really connected. $|V|\log|V|$ edges!

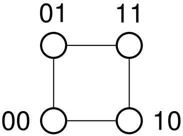
Also represents bit-strings nicely.

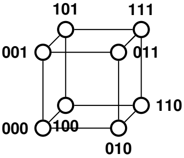
$G=(V,E)$

$|V|=\{0,1\}^n$,

$|E|=\{(x,y)|x$ and y differ in one bit position.$\}$







2^n vertices. number of n-bit strings!

$n2^{n-1}$ edges.

2^n vertices each of degree n

total degree is $n2^n$ and half as many edges!

Hypercubes.

Complete graphs, really connected! But lots of edges.

$|V|(|V|-1)/2$

Trees, few edges. $(|V|-1)$

but just falls apart!

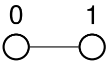
Hypercubes. Really connected. $|V|\log|V|$ edges!

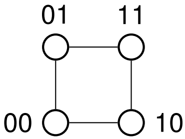
Also represents bit-strings nicely.

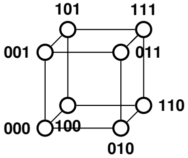
$G=(V,E)$

$|V|=\{0,1\}^n$,

$|E|=\{(x,y)|x$ and y differ in one bit position.$\}$







2^n vertices. number of n-bit strings!

$n2^{n-1}$ edges.

2^n vertices each of degree n

total degree is $n2^n$ and half as many edges!

Recursive Definition.

A 0-dimensional hypercube is a node labelled with the empty string of bits.

Recursive Definition.

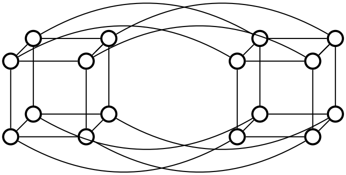
A 0-dimensional hypercube is a node labelled with the empty string of bits.

An n-dimensional hypercube consists of a 0-subcube (1-subcube) which is a $n-1$-dimensional hypercube with nodes labelled $0x$ ($1x$) with the additional edges $(0x, 1x)$.

Recursive Definition.

A 0-dimensional hypercube is a node labelled with the empty string of bits.

An n-dimensional hypercube consists of a 0-subcube (1-subcube) which is a $n-1$-dimensional hypercube with nodes labelled $0x$ ($1x$) with the additional edges $(0x, 1x)$.



Hypercube: Can’t cut me!

Hypercube: Can't cut me!

Thm: Any subset S of the hypercube where $|S| \le |V|/2$ has $\ge |S|$ edges connecting it to $V - S$;

Hypercube: Can't cut me!

Thm: Any subset S of the hypercube where $|S| \leq |V|/2$ has $\geq |S|$ edges connecting it to $V - S$; $|E \cap S \times (V - S)| \geq |S|$

Hypercube: Can't cut me!

Thm: Any subset S of the hypercube where $|S| \leq |V|/2$ has $\geq |S|$ edges connecting it to $V - S$; $|E \cap S \times (V - S)| \geq |S|$

Terminology:

Hypercube: Can't cut me!

Thm: Any subset S of the hypercube where $|S| \leq |V|/2$ has $\geq |S|$ edges connecting it to $V - S$; $|E \cap S \times (V - S)| \geq |S|$

Terminology:
$(S, V - S)$ is cut.

Hypercube: Can't cut me!

Thm: Any subset S of the hypercube where $|S| \leq |V|/2$ has $\geq |S|$ edges connecting it to $V - S$; $|E \cap S \times (V - S)| \geq |S|$

Terminology:
$(S, V - S)$ is cut.
$(E \cap S \times (V - S))$ - cut edges.

Hypercube: Can't cut me!

Thm: Any subset S of the hypercube where $|S| \leq |V|/2$ has $\geq |S|$ edges connecting it to $V - S$; $|E \cap S \times (V - S)| \geq |S|$

Terminology:
$(S, V - S)$ is cut.
$(E \cap S \times (V - S))$ - cut edges.

Hypercube: Can't cut me!

Thm: Any subset S of the hypercube where $|S| \leq |V|/2$ has $\geq |S|$ edges connecting it to $V - S$; $|E \cap S \times (V - S)| \geq |S|$

Terminology:
$(S, V - S)$ is cut.
$(E \cap S \times (V - S))$ - cut edges.

Restatement: for any cut in the hypercube, the number of cut edges is at least the size of the small side.

Proof of Large Cuts.

Thm: For any cut $(S, V - S)$ in the hypercube, the number of cut edges is at least the size of the small side.
Proof:

Proof of Large Cuts.

Thm: For any cut $(S, V - S)$ in the hypercube, the number of cut edges is at least the size of the small side.

Proof:

Base Case: $n = 1$

Proof of Large Cuts.

Thm: For any cut $(S, V-S)$ in the hypercube, the number of cut edges is at least the size of the small side.

Proof:

Base Case: $n = 1$ V= $\{0,1\}$.

Proof of Large Cuts.

Thm: For any cut $(S, V-S)$ in the hypercube, the number of cut edges is at least the size of the small side.
Proof:
Base Case: $n = 1$ V= $\{0,1\}$.
$S = \{0\}$ has one edge leaving.

Proof of Large Cuts.

Thm: For any cut $(S, V-S)$ in the hypercube, the number of cut edges is at least the size of the small side.
Proof:
Base Case: $n = 1$ V= $\{0,1\}$.
$S = \{0\}$ has one edge leaving. $|S| = \phi$ has 0.

Proof of Large Cuts.

Thm: For any cut $(S, V - S)$ in the hypercube, the number of cut edges is at least the size of the small side.
Proof:
Base Case: $n = 1$ V= $\{0,1\}$.
$S = \{0\}$ has one edge leaving. $|S| = \phi$ has 0.

Proof of Large Cuts.

Thm: For any cut $(S, V - S)$ in the hypercube, the number of cut edges is at least the size of the small side.

Proof:

Base Case: $n = 1$ V= $\{0,1\}$.

$S = \{0\}$ has one edge leaving. $|S| = \phi$ has 0.

Induction Step Idea

Thm: For any cut $(S, V - S)$ in the hypercube, the number of cut edges is at least the size of the small side.

Induction Step Idea

Thm: For any cut $(S, V - S)$ in the hypercube, the number of cut edges is at least the size of the small side.

Use recursive definition into two subcubes: $S = S_0 \cup S_1$.

Induction Step Idea

Thm: For any cut $(S, V - S)$ in the hypercube, the number of cut edges is at least the size of the small side.

Use recursive definition into two subcubes: $S = S_0 \cup S_1$.

Two cubes connected by edges.

Induction Step Idea

Thm: For any cut $(S, V - S)$ in the hypercube, the number of cut edges is at least the size of the small side.

Use recursive definition into two subcubes: $S = S_0 \cup S_1$.

Two cubes connected by edges.

Case 1: Count edges inside subcube inductively.

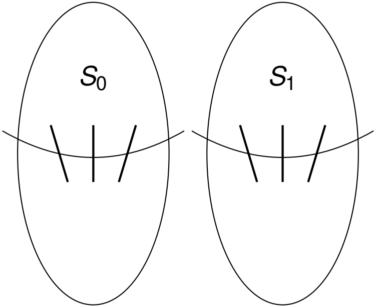
Induction Step Idea

Thm: For any cut $(S, V - S)$ in the hypercube, the number of cut edges is at least the size of the small side.

Use recursive definition into two subcubes: $S = S_0 \cup S_1$.

Two cubes connected by edges.

Case 1: Count edges inside subcube inductively.



Induction Step Idea

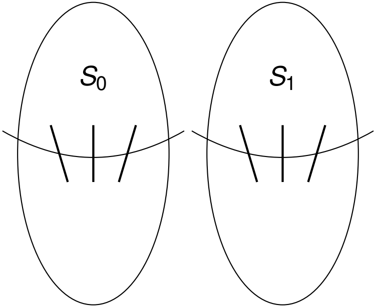
Thm: For any cut $(S, V - S)$ in the hypercube, the number of cut edges is at least the size of the small side.

Use recursive definition into two subcubes: $S = S_0 \cup S_1$.

Two cubes connected by edges.

Case 1: Count edges inside subcube inductively.

Case 2: Count inside and across.



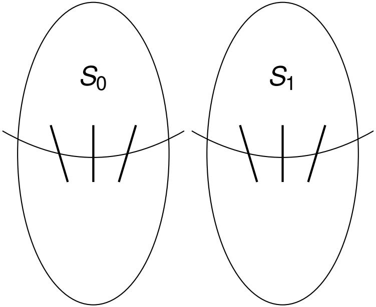
Induction Step Idea

Thm: For any cut $(S, V-S)$ in the hypercube, the number of cut edges is at least the size of the small side.

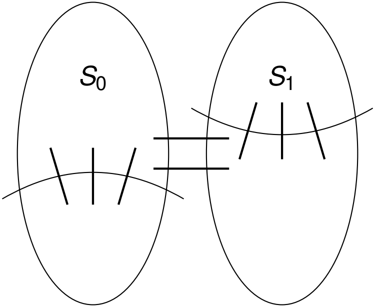
Use recursive definition into two subcubes: $S = S_0 \cup S_1$.

Two cubes connected by edges.

Case 1: Count edges inside subcube inductively.



Case 2: Count inside and across.



Induction Step :Optional Material

Thm: For any cut $(S, V - S)$ in the hypercube, the number of cut edges is at least the size of the small side, $|S|$.

Induction Step :Optional Material

Thm: For any cut $(S, V - S)$ in the hypercube, the number of cut edges is at least the size of the small side, $|S|$.

Proof: Induction Step.

Induction Step :Optional Material

Thm: For any cut $(S, V - S)$ in the hypercube, the number of cut edges is at least the size of the small side, $|S|$.

Proof: Induction Step.
Recursive definition:

Induction Step :Optional Material

Thm: For any cut $(S, V - S)$ in the hypercube, the number of cut edges is at least the size of the small side, $|S|$.

Proof: Induction Step.
Recursive definition:
$H_0 = (V_0, E_0)$,$H_1 = (V_1, E_1)$, edges E_x that connect them.

Induction Step :Optional Material

Thm: For any cut $(S, V - S)$ in the hypercube, the number of cut edges is at least the size of the small side, $|S|$.

Proof: Induction Step.
Recursive definition:
$H_0 = (V_0, E_0)$,$H_1 = (V_1, E_1)$, edges E_x that connect them.
$H = (V_0 \cup V_1, E_0 \cup E_1 \cup E_x)$

Induction Step :Optional Material

Thm: For any cut $(S, V-S)$ in the hypercube, the number of cut edges is at least the size of the small side, $|S|$.

Proof: Induction Step.
Recursive definition:

$H_0 = (V_0, E_0)$,$H_1 = (V_1, E_1)$, edges E_x that connect them.
$H = (V_0 \cup V_1, E_0 \cup E_1 \cup E_x)$
$S = S_0 \cup S_1$ where S_0 in first, and S_1 in other.

Induction Step :Optional Material

Thm: For any cut $(S, V - S)$ in the hypercube, the number of cut edges is at least the size of the small side, $|S|$.

Proof: Induction Step.
Recursive definition:
$H_0 = (V_0, E_0)$,$H_1 = (V_1, E_1)$, edges E_x that connect them.
$H = (V_0 \cup V_1, E_0 \cup E_1 \cup E_x)$
$S = S_0 \cup S_1$ where S_0 in first, and S_1 in other.

Case 1: $|S_0| \leq |V_0|/2, |S_1| \leq |V_1|/2$

Induction Step :Optional Material

Thm: For any cut $(S, V-S)$ in the hypercube, the number of cut edges is at least the size of the small side, $|S|$.

Proof: Induction Step.
Recursive definition:
$H_0 = (V_0, E_0)$,$H_1 = (V_1, E_1)$, edges E_x that connect them.
$H = (V_0 \cup V_1, E_0 \cup E_1 \cup E_x)$
$S = S_0 \cup S_1$ where S_0 in first, and S_1 in other.

Case 1: $|S_0| \leq |V_0|/2, |S_1| \leq |V_1|/2$
Both S_0 and S_1 are small sides.

Induction Step :Optional Material

Thm: For any cut $(S, V-S)$ in the hypercube, the number of cut edges is at least the size of the small side, $|S|$.

Proof: Induction Step.
Recursive definition:
$H_0 = (V_0, E_0)$,$H_1 = (V_1, E_1)$, edges E_x that connect them.
$H = (V_0 \cup V_1, E_0 \cup E_1 \cup E_x)$
$S = S_0 \cup S_1$ where S_0 in first, and S_1 in other.

Case 1: $|S_0| \leq |V_0|/2, |S_1| \leq |V_1|/2$
Both S_0 and S_1 are small sides. So by induction.

Induction Step :Optional Material

Thm: For any cut $(S, V-S)$ in the hypercube, the number of cut edges is at least the size of the small side, $|S|$.

Proof: Induction Step.
Recursive definition:
$H_0 = (V_0, E_0)$,$H_1 = (V_1, E_1)$, edges E_x that connect them.
$H = (V_0 \cup V_1, E_0 \cup E_1 \cup E_x)$
$S = S_0 \cup S_1$ where S_0 in first, and S_1 in other.

Case 1: $|S_0| \leq |V_0|/2, |S_1| \leq |V_1|/2$
Both S_0 and S_1 are small sides. So by induction.
Edges cut in $H_0 \geq |S_0|$.

Induction Step :Optional Material

Thm: For any cut $(S, V-S)$ in the hypercube, the number of cut edges is at least the size of the small side, $|S|$.

Proof: Induction Step.
Recursive definition:
$H_0 = (V_0, E_0)$,$H_1 = (V_1, E_1)$, edges E_x that connect them.
$H = (V_0 \cup V_1, E_0 \cup E_1 \cup E_x)$
$S = S_0 \cup S_1$ where S_0 in first, and S_1 in other.

Case 1: $|S_0| \leq |V_0|/2, |S_1| \leq |V_1|/2$
Both S_0 and S_1 are small sides. So by induction.
Edges cut in $H_0 \geq |S_0|$.
Edges cut in $H_1 \geq |S_1|$.

Induction Step :Optional Material

Thm: For any cut $(S, V-S)$ in the hypercube, the number of cut edges is at least the size of the small side, $|S|$.

Proof: Induction Step.
Recursive definition:
$H_0 = (V_0, E_0)$,$H_1 = (V_1, E_1)$, edges E_x that connect them.
$H = (V_0 \cup V_1, E_0 \cup E_1 \cup E_x)$
$S = S_0 \cup S_1$ where S_0 in first, and S_1 in other.

Case 1: $|S_0| \leq |V_0|/2, |S_1| \leq |V_1|/2$
Both S_0 and S_1 are small sides. So by induction.
Edges cut in $H_0 \geq |S_0|$.
Edges cut in $H_1 \geq |S_1|$.

Induction Step :Optional Material

Thm: For any cut $(S, V - S)$ in the hypercube, the number of cut edges is at least the size of the small side, $|S|$.

Proof: Induction Step.
Recursive definition:
$H_0 = (V_0, E_0)$,$H_1 = (V_1, E_1)$, edges E_x that connect them.
$H = (V_0 \cup V_1, E_0 \cup E_1 \cup E_x)$
$S = S_0 \cup S_1$ where S_0 in first, and S_1 in other.

Case 1: $|S_0| \leq |V_0|/2, |S_1| \leq |V_1|/2$
Both S_0 and S_1 are small sides. So by induction.
Edges cut in $H_0 \geq |S_0|$.
Edges cut in $H_1 \geq |S_1|$.

Total cut edges $\geq |S_0| + |S_1| = |S|$.

Induction Step :Optional Material

Thm: For any cut $(S, V-S)$ in the hypercube, the number of cut edges is at least the size of the small side, $|S|$.

Proof: Induction Step.
Recursive definition:
$H_0 = (V_0, E_0)$,$H_1 = (V_1, E_1)$, edges E_x that connect them.
$H = (V_0 \cup V_1, E_0 \cup E_1 \cup E_x)$
$S = S_0 \cup S_1$ where S_0 in first, and S_1 in other.

Case 1: $|S_0| \leq |V_0|/2, |S_1| \leq |V_1|/2$
Both S_0 and S_1 are small sides. So by induction.
Edges cut in $H_0 \geq |S_0|$.
Edges cut in $H_1 \geq |S_1|$.

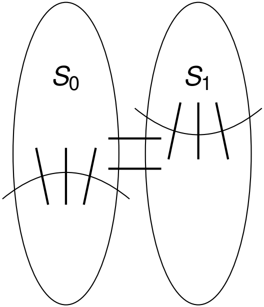
Total cut edges $\geq |S_0| + |S_1| = |S|$. $\square$

Induction Step. Case 2.

Thm: For any cut $(S, V-S)$ in the hypercube, the number of cut edges is at least the size of the small side, $|S|$.

Proof: Induction Step. Case 2.

$$|S_0| \geq |V_0|/2.$$



Induction Step. Case 2.

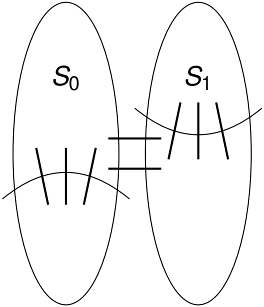
Thm: For any cut $(S, V - S)$ in the hypercube, the number of cut edges is at least the size of the small side, $|S|$.

Proof: Induction Step. Case 2.

$|S_0| \geq |V_0|/2$.

Recall Case 1: $|S_0|, |S_1| \leq |V|/2$

$|S_1| \leq |V_1|/2$ since $|S| \leq |V|/2$.



Induction Step. Case 2.

Thm: For any cut $(S, V - S)$ in the hypercube, the number of cut edges is at least the size of the small side, $|S|$.

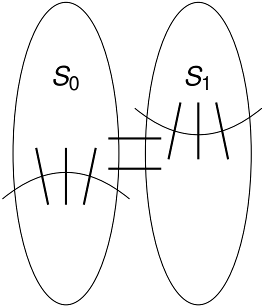
Proof: Induction Step. Case 2.

$|S_0| \geq |V_0|/2$.

Recall Case 1: $|S_0|, |S_1| \leq |V|/2$

$|S_1| \leq |V_1|/2$ since $|S| \leq |V|/2$.

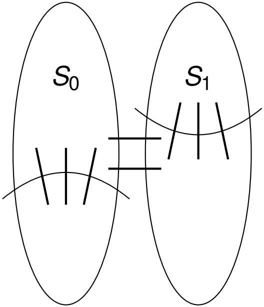
$\implies \geq |S_1|$ edges cut in E_1.



Induction Step. Case 2.

Thm: For any cut $(S, V - S)$ in the hypercube, the number of cut edges is at least the size of the small side, $|S|$.

Proof: Induction Step. Case 2.



$|S_0| \geq |V_0|/2$.

Recall Case 1: $|S_0|, |S_1| \leq |V|/2$

$|S_1| \leq |V_1|/2$ since $|S| \leq |V|/2$.

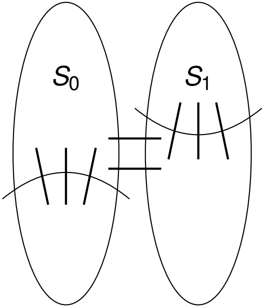
$\implies \geq |S_1|$ edges cut in E_1.

$|S_0| \geq |V_0|/2 \implies |V_0 - S| \leq |V_0|/2$

Induction Step. Case 2.

Thm: For any cut $(S, V-S)$ in the hypercube, the number of cut edges is at least the size of the small side, $|S|$.

Proof: Induction Step. Case 2.



$|S_0| \geq |V_0|/2$.

Recall Case 1: $|S_0|, |S_1| \leq |V|/2$

$|S_1| \leq |V_1|/2$ since $|S| \leq |V|/2$.

$\implies \geq |S_1|$ edges cut in E_1.

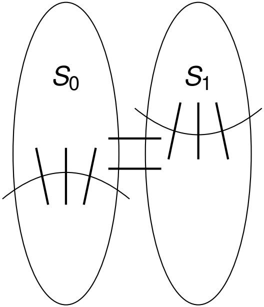
$|S_0| \geq |V_0|/2 \implies |V_0 - S| \leq |V_0|/2$

$\implies \geq |V_0| - |S_0|$ edges cut in E_0.

Induction Step. Case 2.

Thm: For any cut $(S, V - S)$ in the hypercube, the number of cut edges is at least the size of the small side, $|S|$.

Proof: Induction Step. Case 2.



$|S_0| \geq |V_0|/2$.

Recall Case 1: $|S_0|, |S_1| \leq |V|/2$

$|S_1| \leq |V_1|/2$ since $|S| \leq |V|/2$.

$\implies \geq |S_1|$ edges cut in E_1.

$|S_0| \geq |V_0|/2 \implies |V_0 - S| \leq |V_0|/2$

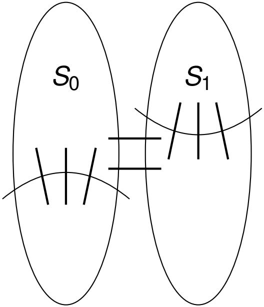
$\implies \geq |V_0| - |S_0|$ edges cut in E_0.

Edges in E_x connect corresponding nodes.

Induction Step. Case 2.

Thm: For any cut $(S, V-S)$ in the hypercube, the number of cut edges is at least the size of the small side, $|S|$.

Proof: Induction Step. Case 2.



$|S_0| \geq |V_0|/2$.

Recall Case 1: $|S_0|, |S_1| \leq |V|/2$

$|S_1| \leq |V_1|/2$ since $|S| \leq |V|/2$.

$\implies \geq |S_1|$ edges cut in E_1.

$|S_0| \geq |V_0|/2 \implies |V_0 - S| \leq |V_0|/2$

$\implies \geq |V_0| - |S_0|$ edges cut in E_0.

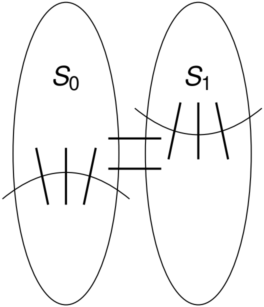
Edges in E_x connect corresponding nodes.

$\implies = |S_0| - |S_1|$ edges cut in E_x.

Induction Step. Case 2.

Thm: For any cut $(S, V-S)$ in the hypercube, the number of cut edges is at least the size of the small side, $|S|$.

Proof: Induction Step. Case 2.



$|S_0| \geq |V_0|/2$.

Recall Case 1: $|S_0|, |S_1| \leq |V|/2$

$|S_1| \leq |V_1|/2$ since $|S| \leq |V|/2$.

$\implies \geq |S_1|$ edges cut in E_1.

$|S_0| \geq |V_0|/2 \implies |V_0 - S| \leq |V_0|/2$

$\implies \geq |V_0| - |S_0|$ edges cut in E_0.

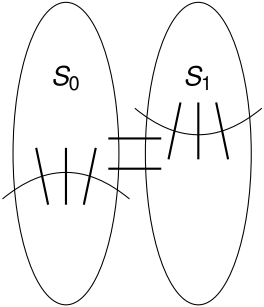
Edges in E_x connect corresponding nodes.

$\implies = |S_0| - |S_1|$ edges cut in E_x.

Induction Step. Case 2.

Thm: For any cut $(S, V-S)$ in the hypercube, the number of cut edges is at least the size of the small side, $|S|$.

Proof: Induction Step. Case 2.



$|S_0| \geq |V_0|/2$.

Recall Case 1: $|S_0|, |S_1| \leq |V|/2$

$|S_1| \leq |V_1|/2$ since $|S| \leq |V|/2$.

$\implies \geq |S_1|$ edges cut in E_1.

$|S_0| \geq |V_0|/2 \implies |V_0 - S| \leq |V_0|/2$

$\implies \geq |V_0| - |S_0|$ edges cut in E_0.

Edges in E_x connect corresponding nodes.

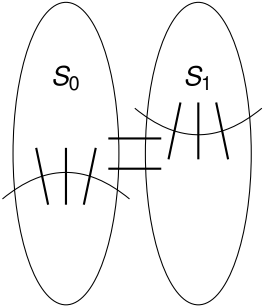
$\implies = |S_0| - |S_1|$ edges cut in E_x.

Total edges cut:

Induction Step. Case 2.

Thm: For any cut $(S, V - S)$ in the hypercube, the number of cut edges is at least the size of the small side, $|S|$.

Proof: Induction Step. Case 2.



$|S_0| \geq |V_0|/2$.

Recall Case 1: $|S_0|, |S_1| \leq |V|/2$

$|S_1| \leq |V_1|/2$ since $|S| \leq |V|/2$.

$\implies \geq |S_1|$ edges cut in E_1.

$|S_0| \geq |V_0|/2 \implies |V_0 - S| \leq |V_0|/2$

$\implies \geq |V_0| - |S_0|$ edges cut in E_0.

Edges in E_x connect corresponding nodes.

$\implies = |S_0| - |S_1|$ edges cut in E_x.

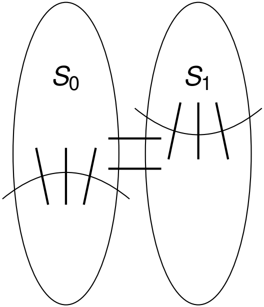
Total edges cut:

$\geq$

Induction Step. Case 2.

Thm: For any cut $(S, V-S)$ in the hypercube, the number of cut edges is at least the size of the small side, $|S|$.

Proof: Induction Step. Case 2.



$|S_0| \geq |V_0|/2$.

Recall Case 1: $|S_0|, |S_1| \leq |V|/2$

$|S_1| \leq |V_1|/2$ since $|S| \leq |V|/2$.

$\implies \geq |S_1|$ edges cut in E_1.

$|S_0| \geq |V_0|/2 \implies |V_0 - S| \leq |V_0|/2$

$\implies \geq |V_0| - |S_0|$ edges cut in E_0.

Edges in E_x connect corresponding nodes.

$\implies = |S_0| - |S_1|$ edges cut in E_x.

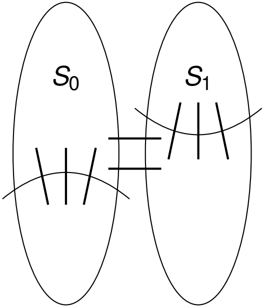
Total edges cut:

$\geq \ |S_1|$

Induction Step. Case 2.

Thm: For any cut $(S, V - S)$ in the hypercube, the number of cut edges is at least the size of the small side, $|S|$.

Proof: Induction Step. Case 2.



$|S_0| \geq |V_0|/2$.

Recall Case 1: $|S_0|, |S_1| \leq |V|/2$

$|S_1| \leq |V_1|/2$ since $|S| \leq |V|/2$.

$\implies \geq |S_1|$ edges cut in E_1.

$|S_0| \geq |V_0|/2 \implies |V_0 - S| \leq |V_0|/2$

$\implies \geq |V_0| - |S_0|$ edges cut in E_0.

Edges in E_x connect corresponding nodes.

$\implies = |S_0| - |S_1|$ edges cut in E_x.

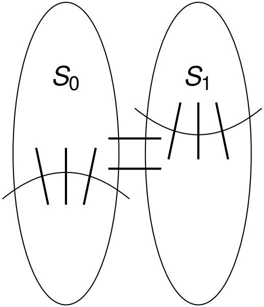
Total edges cut:

$\geq \ |S_1| + |V_0| - |S_0|$

Induction Step. Case 2.

Thm: For any cut $(S, V-S)$ in the hypercube, the number of cut edges is at least the size of the small side, $|S|$.

Proof: Induction Step. Case 2.



$|S_0| \geq |V_0|/2$.

Recall Case 1: $|S_0|, |S_1| \leq |V|/2$

$|S_1| \leq |V_1|/2$ since $|S| \leq |V|/2$.

$\implies \geq |S_1|$ edges cut in E_1.

$|S_0| \geq |V_0|/2 \implies |V_0 - S| \leq |V_0|/2$

$\implies \geq |V_0| - |S_0|$ edges cut in E_0.

Edges in E_x connect corresponding nodes.

$\implies = |S_0| - |S_1|$ edges cut in E_x.

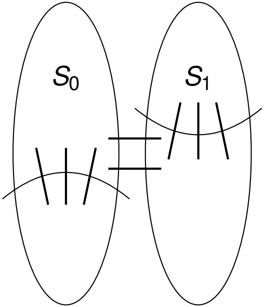
Total edges cut:

$\geq \ |S_1| + |V_0| - |S_0| + |S_0| - |S_1|$

Induction Step. Case 2.

Thm: For any cut $(S, V-S)$ in the hypercube, the number of cut edges is at least the size of the small side, $|S|$.

Proof: Induction Step. Case 2.



$|S_0| \geq |V_0|/2$.

Recall Case 1: $|S_0|, |S_1| \leq |V|/2$

$|S_1| \leq |V_1|/2$ since $|S| \leq |V|/2$.

$\implies \geq |S_1|$ edges cut in E_1.

$|S_0| \geq |V_0|/2 \implies |V_0 - S| \leq |V_0|/2$

$\implies \geq |V_0| - |S_0|$ edges cut in E_0.

Edges in E_x connect corresponding nodes.

$\implies = |S_0| - |S_1|$ edges cut in E_x.

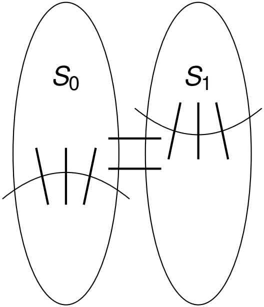
Total edges cut:

$\geq |S_1| + |V_0| - |S_0| + |S_0| - |S_1| = |V_0|$

Induction Step. Case 2.

Thm: For any cut $(S, V-S)$ in the hypercube, the number of cut edges is at least the size of the small side, $|S|$.

Proof: Induction Step. Case 2.



$|S_0| \geq |V_0|/2$.

Recall Case 1: $|S_0|, |S_1| \leq |V|/2$

$|S_1| \leq |V_1|/2$ since $|S| \leq |V|/2$.

$\implies \geq |S_1|$ edges cut in E_1.

$|S_0| \geq |V_0|/2 \implies |V_0 - S| \leq |V_0|/2$

$\implies \geq |V_0| - |S_0|$ edges cut in E_0.

Edges in E_x connect corresponding nodes.

$\implies = |S_0| - |S_1|$ edges cut in E_x.

Total edges cut:

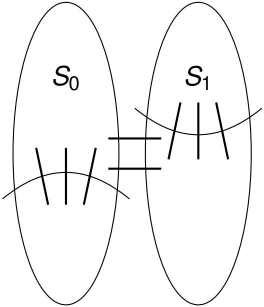
$\geq \ |S_1| + |V_0| - |S_0| + |S_0| - |S_1| = |V_0|$

$|V_0|$

Induction Step. Case 2.

Thm: For any cut $(S, V - S)$ in the hypercube, the number of cut edges is at least the size of the small side, $|S|$.

Proof: Induction Step. Case 2.



$|S_0| \geq |V_0|/2$.

Recall Case 1: $|S_0|, |S_1| \leq |V|/2$

$|S_1| \leq |V_1|/2$ since $|S| \leq |V|/2$.

$\implies \geq |S_1|$ edges cut in E_1.

$|S_0| \geq |V_0|/2 \implies |V_0 - S| \leq |V_0|/2$

$\implies \geq |V_0| - |S_0|$ edges cut in E_0.

Edges in E_x connect corresponding nodes.

$\implies = |S_0| - |S_1|$ edges cut in E_x.

Total edges cut:

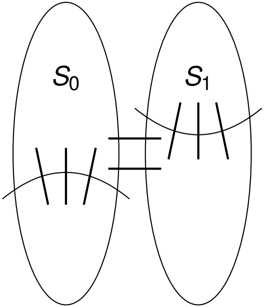
$\geq \ |S_1| + |V_0| - |S_0| + |S_0| - |S_1| = |V_0|$

$|V_0| = |V|/2 \geq |S|$.

Induction Step. Case 2.

Thm: For any cut $(S, V-S)$ in the hypercube, the number of cut edges is at least the size of the small side, $|S|$.

Proof: Induction Step. Case 2.



$|S_0| \geq |V_0|/2$.

Recall Case 1: $|S_0|, |S_1| \leq |V|/2$

$|S_1| \leq |V_1|/2$ since $|S| \leq |V|/2$.

$\implies \geq |S_1|$ edges cut in E_1.

$|S_0| \geq |V_0|/2 \implies |V_0 - S| \leq |V_0|/2$

$\implies \geq |V_0| - |S_0|$ edges cut in E_0.

Edges in E_x connect corresponding nodes.

$\implies = |S_0| - |S_1|$ edges cut in E_x.

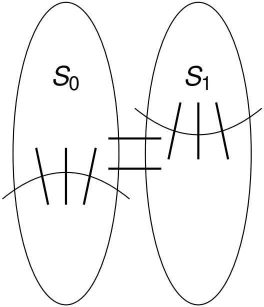
Total edges cut:

$\geq |S_1| + |V_0| - |S_0| + |S_0| - |S_1| = |V_0|$

$|V_0| = |V|/2 \geq |S|$. $\square$

Induction Step. Case 2.

Thm: For any cut $(S, V-S)$ in the hypercube, the number of cut edges is at least the size of the small side, $|S|$.
Proof: Induction Step. Case 2.



$|S_0| \geq |V_0|/2$.
Recall Case 1: $|S_0|, |S_1| \leq |V|/2$
$|S_1| \leq |V_1|/2$ since $|S| \leq |V|/2$.
$\implies \geq |S_1|$ edges cut in E_1.
$|S_0| \geq |V_0|/2 \implies |V_0 - S| \leq |V_0|/2$
$\implies \geq |V_0| - |S_0|$ edges cut in E_0.

Edges in E_x connect corresponding nodes.
$\implies = |S_0| - |S_1|$ edges cut in E_x.

Total edges cut:
$\geq \; |S_1| + |V_0| - |S_0| + |S_0| - |S_1| = |V_0|$
$|V_0| = |V|/2 \geq |S|$. $\square$
Also, case 3 where $|S_1| \geq |V|/2$ is symmetric.

Hypercubes and Boolean Functions.

The cuts in the hypercubes are exactly the transitions from 0 valued vertices to 1 valued vertices on boolean functions on $\{0,1\}^n$.

Hypercubes and Boolean Functions.

The cuts in the hypercubes are exactly the transitions from 0 valued vertices to 1 valued vertices on boolean functions on $\{0,1\}^n$.

Central area of study in computer science!

Hypercubes and Boolean Functions.

The cuts in the hypercubes are exactly the transitions from 0 valued vertices to 1 valued vertices on boolean functions on $\{0,1\}^n$.

Central area of study in computer science!

Yes/No Computer Programs $\equiv$ Boolean function on $\{0,1\}^n$

Hypercubes and Boolean Functions.

The cuts in the hypercubes are exactly the transitions from 0 valued vertices to 1 valued vertices on boolean functions on $\{0,1\}^n$.

Central area of study in computer science!

Yes/No Computer Programs $\equiv$ Boolean function on $\{0,1\}^n$

Hypercubes central in error correcting codes.

Hypercubes and Boolean Functions.

The cuts in the hypercubes are exactly the transitions from 0 valued vertices to 1 valued vertices on boolean functions on $\{0,1\}^n$.

Central area of study in computer science!

Yes/No Computer Programs $\equiv$ Boolean function on $\{0,1\}^n$

Hypercubes central in error correcting codes.

Central object of study.

And now for Modular Arithmetic.

1. Modular Arithmetic.

And now for Modular Arithmetic.

1. Modular Arithmetic.
   Clock Math!!!

And now for Modular Arithmetic.

1. Modular Arithmetic.
   Clock Math!!!
2. Inverses for Modular Arithmetic: Greatest Common Divisor.

And now for Modular Arithmetic.

1. Modular Arithmetic.
   Clock Math!!!
2. Inverses for Modular Arithmetic: Greatest Common Divisor.
   Division!!!

And now for Modular Arithmetic.

1. Modular Arithmetic.
   Clock Math!!!
2. Inverses for Modular Arithmetic: Greatest Common Divisor.
   Division!!!
3. Euclid's GCD Algorithm.

And now for Modular Arithmetic.

1. Modular Arithmetic.
   Clock Math!!!
2. Inverses for Modular Arithmetic: Greatest Common Divisor.
   Division!!!
3. Euclid's GCD Algorithm.
   A little tricky here!

Clock Math

If it is 1:00 now.

Clock Math

If it is 1:00 now.
What time is it in 2 hours?

Clock Math

If it is 1:00 now.
What time is it in 2 hours? 3:00!

Clock Math

If it is 1:00 now.
  What time is it in 2 hours? 3:00!
  What time is it in 5 hours?

Clock Math

If it is 1:00 now.
  What time is it in 2 hours? 3:00!
  What time is it in 5 hours? 6:00!

Clock Math

If it is 1:00 now.

What time is it in 2 hours? 3:00!

What time is it in 5 hours? 6:00!

What time is it in 15 hours?

Clock Math

If it is 1:00 now.

What time is it in 2 hours? 3:00!

What time is it in 5 hours? 6:00!

What time is it in 15 hours? 16:00!

Clock Math

If it is 1:00 now.

What time is it in 2 hours? 3:00!

What time is it in 5 hours? 6:00!

What time is it in 15 hours? 16:00!

Actually 4:00.

Clock Math

If it is 1:00 now.

What time is it in 2 hours? 3:00!

What time is it in 5 hours? 6:00!

What time is it in 15 hours? 16:00!

Actually 4:00.

16 is the “same as 4” with respect to a 12 hour clock system.

Clock Math

If it is 1:00 now.
  What time is it in 2 hours? 3:00!
  What time is it in 5 hours? 6:00!
  What time is it in 15 hours? 16:00!
    Actually 4:00.

16 is the “same as 4” with respect to a 12 hour clock system.
  Clock time equivalent up to to addition/subtraction of 12.

Clock Math

If it is 1:00 now.

What time is it in 2 hours? 3:00!

What time is it in 5 hours? 6:00!

What time is it in 15 hours? 16:00!

Actually 4:00.

16 is the “same as 4” with respect to a 12 hour clock system.

Clock time equivalent up to to addition/subtraction of 12.

Clock Math

If it is 1:00 now.
  What time is it in 2 hours? 3:00!
  What time is it in 5 hours? 6:00!
  What time is it in 15 hours? 16:00!
    Actually 4:00.

16 is the “same as 4” with respect to a 12 hour clock system.
  Clock time equivalent up to to addition/subtraction of 12.

What time is it in 100 hours?

Clock Math

If it is 1:00 now.
- What time is it in 2 hours? 3:00!
- What time is it in 5 hours? 6:00!
- What time is it in 15 hours? 16:00!
  - Actually 4:00.

16 is the “same as 4” with respect to a 12 hour clock system.
Clock time equivalent up to to addition/subtraction of 12.

What time is it in 100 hours? 101:00!

Clock Math

If it is 1:00 now.

- What time is it in 2 hours? 3:00!
- What time is it in 5 hours? 6:00!
- What time is it in 15 hours? 16:00!
  - Actually 4:00.

16 is the “same as 4” with respect to a 12 hour clock system.
Clock time equivalent up to to addition/subtraction of 12.

What time is it in 100 hours? 101:00! or 5:00.

Clock Math

If it is 1:00 now.
What time is it in 2 hours? 3:00!
What time is it in 5 hours? 6:00!
What time is it in 15 hours? 16:00!
Actually 4:00.

16 is the “same as 4” with respect to a 12 hour clock system.
Clock time equivalent up to to addition/subtraction of 12.

What time is it in 100 hours? 101:00! or 5:00.
$101 = 12 \times 8 + 5$.

Clock Math

If it is 1:00 now.

What time is it in 2 hours? 3:00!

What time is it in 5 hours? 6:00!

What time is it in 15 hours? 16:00!

Actually 4:00.

16 is the "same as 4" with respect to a 12 hour clock system.

Clock time equivalent up to to addition/subtraction of 12.

What time is it in 100 hours? 101:00! or 5:00.

$101 = 12 \times 8 + 5$.

5 is the same as 101 for a 12 hour clock system.

Clock Math

If it is 1:00 now.
What time is it in 2 hours? 3:00!
What time is it in 5 hours? 6:00!
What time is it in 15 hours? 16:00!
Actually 4:00.

16 is the "same as 4" with respect to a 12 hour clock system.
Clock time equivalent up to to addition/subtraction of 12.

What time is it in 100 hours? 101:00! or 5:00.
$101 = 12 \times 8 + 5$.
5 is the same as 101 for a 12 hour clock system.
Clock time equivalent up to addition of any integer multiple of 12.

Clock Math

If it is 1:00 now.

What time is it in 2 hours? 3:00!

What time is it in 5 hours? 6:00!

What time is it in 15 hours? 16:00!

Actually 4:00.

16 is the “same as 4” with respect to a 12 hour clock system.

Clock time equivalent up to to addition/subtraction of 12.

What time is it in 100 hours? 101:00! or 5:00.

$101 = 12 \times 8 + 5$.

5 is the same as 101 for a 12 hour clock system.

Clock time equivalent up to addition of any integer multiple of 12.

Clock Math

If it is 1:00 now.
What time is it in 2 hours? 3:00!
What time is it in 5 hours? 6:00!
What time is it in 15 hours? 16:00!
Actually 4:00.

16 is the "same as 4" with respect to a 12 hour clock system.
Clock time equivalent up to to addition/subtraction of 12.

What time is it in 100 hours? 101:00! or 5:00.
$101 = 12 \times 8 + 5$.
5 is the same as 101 for a 12 hour clock system.
Clock time equivalent up to addition of any integer multiple of 12.

Custom is only to use the representative in $\{12, 1, \ldots, 11\}$

Clock Math

If it is 1:00 now.
What time is it in 2 hours? 3:00!
What time is it in 5 hours? 6:00!
What time is it in 15 hours? 16:00!
Actually 4:00.

16 is the "same as 4" with respect to a 12 hour clock system.
Clock time equivalent up to to addition/subtraction of 12.

What time is it in 100 hours? 101:00! or 5:00.
$101 = 12 \times 8 + 5$.
5 is the same as 101 for a 12 hour clock system.
Clock time equivalent up to addition of any integer multiple of 12.

Custom is only to use the representative in $\{12, 1, \ldots, 11\}$
(Almost remainder, except for 12 and 0 are equivalent.)

Day of the week.

Today is Monday.

Day of the week.

Today is Monday.

What day is it a year from now?

Day of the week.

Today is Monday.

What day is it a year from now? on September 11, 2018?

Day of the week.

Today is Monday.

What day is it a year from now? on September 11, 2018?

Number days.

Day of the week.

Today is Monday.
- What day is it a year from now? on September 11, 2018?
  - Number days.
    - 0 for Sunday, 1 for Monday, . . . , 6 for Saturday.

Day of the week.

Today is Monday.

What day is it a year from now? on September 11, 2018?

Number days.

0 for Sunday, 1 for Monday, . . . , 6 for Saturday.

Day of the week.

Today is Monday.

- What day is it a year from now? on September 11, 2018?
  - Number days.
    - 0 for Sunday, 1 for Monday, . . . , 6 for Saturday.

Today: day 1.

Day of the week.

Today is Monday.

What day is it a year from now? on September 11, 2018?

Number days.

0 for Sunday, 1 for Monday, . . . , 6 for Saturday.

Today: day 1.

6 days from now.

Day of the week.

Today is Monday.

What day is it a year from now? on September 11, 2018?

Number days.

0 for Sunday, 1 for Monday, . . . , 6 for Saturday.

Today: day 1.

6 days from now. day 7

Day of the week.

Today is Monday.

What day is it a year from now? on September 11, 2018?

Number days.

0 for Sunday, 1 for Monday, . . . , 6 for Saturday.

Today: day 1.

6 days from now. day 7 or day 0

Day of the week.

Today is Monday.

What day is it a year from now? on September 11, 2018?

Number days.

0 for Sunday, 1 for Monday, . . . , 6 for Saturday.

Today: day 1.

6 days from now. day 7 or day 0 or Sunday.

Day of the week.

Today is Monday.

What day is it a year from now? on September 11, 2018?

Number days.

0 for Sunday, 1 for Monday, . . . , 6 for Saturday.

Today: day 1.

6 days from now. day 7 or day 0 or Sunday.

26 days from now.

Day of the week.

Today is Monday.

What day is it a year from now? on September 11, 2018?

Number days.

0 for Sunday, 1 for Monday, . . . , 6 for Saturday.

Today: day 1.

6 days from now. day 7 or day 0 or Sunday.

26 days from now. day 27

Day of the week.

Today is Monday.

What day is it a year from now? on September 11, 2018?

Number days.

0 for Sunday, 1 for Monday, . . . , 6 for Saturday.

Today: day 1.

6 days from now. day 7 or day 0 or Sunday.

26 days from now. day 27 or day 6.

Day of the week.

Today is Monday.

What day is it a year from now? on September 11, 2018?

Number days.

0 for Sunday, 1 for Monday, . . . , 6 for Saturday.

Today: day 1.

6 days from now. day 7 or day 0 or Sunday.

26 days from now. day 27 or day 6.

two days are equivalent up to addition/subtraction of multiple of 7.

Day of the week.

Today is Monday.
- What day is it a year from now? on September 11, 2018?
  - Number days.
    - 0 for Sunday, 1 for Monday, . . . , 6 for Saturday.

Today: day 1.
- 6 days from now. day 7 or day 0 or Sunday.
- 26 days from now. day 27 or day 6.
  - two days are equivalent up to addition/subtraction of multiple of 7.
  - 12 days from now

Day of the week.

Today is Monday.
- What day is it a year from now? on September 11, 2018?
  - Number days.
    - 0 for Sunday, 1 for Monday, ..., 6 for Saturday.

Today: day 1.
- 6 days from now. day 7 or day 0 or Sunday.
- 26 days from now. day 27 or day 6.
  - two days are equivalent up to addition/subtraction of multiple of 7.
  - 12 days from now is day 6

Day of the week.

Today is Monday.

What day is it a year from now? on September 11, 2018?

Number days.

0 for Sunday, 1 for Monday, . . . , 6 for Saturday.

Today: day 1.

6 days from now. day 7 or day 0 or Sunday.

26 days from now. day 27 or day 6.

two days are equivalent up to addition/subtraction of multiple of 7.

12 days from now is day 6 which is Saturday!

Day of the week.

Today is Monday.

What day is it a year from now? on September 11, 2018?

Number days.

0 for Sunday, 1 for Monday, . . . , 6 for Saturday.

Today: day 1.

6 days from now. day 7 or day 0 or Sunday.

26 days from now. day 27 or day 6.

two days are equivalent up to addition/subtraction of multiple of 7.

12 days from now is day 6 which is Saturday!

What day is it a year from now?

Day of the week.

Today is Monday.
  What day is it a year from now? on September 11, 2018?
    Number days.
      0 for Sunday, 1 for Monday, . . . , 6 for Saturday.

Today: day 1.
  6 days from now. day 7 or day 0 or Sunday.
  26 days from now. day 27 or day 6.
    two days are equivalent up to addition/subtraction of multiple of 7.
    12 days from now is day 6 which is Saturday!

What day is it a year from now?
  Next year is not a leap year.

Day of the week.

Today is Monday.
What day is it a year from now? on September 11, 2018?
Number days.
0 for Sunday, 1 for Monday, ..., 6 for Saturday.

Today: day 1.
6 days from now. day 7 or day 0 or Sunday.
26 days from now. day 27 or day 6.
two days are equivalent up to addition/subtraction of multiple of 7.
12 days from now is day 6 which is Saturday!

What day is it a year from now?
Next year is not a leap year. So 365 days from now.

Day of the week.

Today is Monday.
What day is it a year from now? on September 11, 2018?
Number days.
0 for Sunday, 1 for Monday, . . . , 6 for Saturday.

Today: day 1.
6 days from now. day 7 or day 0 or Sunday.
26 days from now. day 27 or day 6.
two days are equivalent up to addition/subtraction of multiple of 7.
12 days from now is day 6 which is Saturday!

What day is it a year from now?
Next year is not a leap year. So 365 days from now.
Day 1+365 or day 366.

Day of the week.

Today is Monday.
What day is it a year from now? on September 11, 2018?
Number days.
0 for Sunday, 1 for Monday, ..., 6 for Saturday.

Today: day 1.
6 days from now. day 7 or day 0 or Sunday.
26 days from now. day 27 or day 6.
two days are equivalent up to addition/subtraction of multiple of 7.
12 days from now is day 6 which is Saturday!

What day is it a year from now?
Next year is not a leap year. So 365 days from now.
Day 1+365 or day 366.
Smallest representation:

Day of the week.

Today is Monday.
What day is it a year from now? on September 11, 2018?
Number days.
0 for Sunday, 1 for Monday, . . . , 6 for Saturday.

Today: day 1.
6 days from now. day 7 or day 0 or Sunday.
26 days from now. day 27 or day 6.
two days are equivalent up to addition/subtraction of multiple of 7.
12 days from now is day 6 which is Saturday!

What day is it a year from now?
Next year is not a leap year. So 365 days from now.
Day 1+365 or day 366.
Smallest representation:
subtract 7 until smaller than 7.

Day of the week.

Today is Monday.
What day is it a year from now? on September 11, 2018?
Number days.
0 for Sunday, 1 for Monday, . . . , 6 for Saturday.

Today: day 1.
6 days from now. day 7 or day 0 or Sunday.
26 days from now. day 27 or day 6.
two days are equivalent up to addition/subtraction of multiple of 7.
12 days from now is day 6 which is Saturday!

What day is it a year from now?
Next year is not a leap year. So 365 days from now.
Day 1+365 or day 366.
Smallest representation:
subtract 7 until smaller than 7.
divide and get remainder.

Day of the week.

Today is Monday.
- What day is it a year from now? on September 11, 2018?
  - Number days.
    - 0 for Sunday, 1 for Monday, . . . , 6 for Saturday.

Today: day 1.
- 6 days from now. day 7 or day 0 or Sunday.
- 26 days from now. day 27 or day 6.
  - two days are equivalent up to addition/subtraction of multiple of 7.
  - 12 days from now is day 6 which is Saturday!

What day is it a year from now?
- Next year is not a leap year. So 365 days from now.
- Day 1+365 or day 366.

Smallest representation:
- subtract 7 until smaller than 7.
- divide and get remainder.
- 366/6

Day of the week.

Today is Monday.
What day is it a year from now? on September 11, 2018?
Number days.
0 for Sunday, 1 for Monday, . . . , 6 for Saturday.

Today: day 1.
6 days from now. day 7 or day 0 or Sunday.
26 days from now. day 27 or day 6.
two days are equivalent up to addition/subtraction of multiple of 7.
12 days from now is day 6 which is Saturday!

What day is it a year from now?
Next year is not a leap year. So 365 days from now.
Day 1+365 or day 366.
Smallest representation:
subtract 7 until smaller than 7.
divide and get remainder.
366/6 leaves quotient of 52 and remainder 2.

Day of the week.

Today is Monday.
  What day is it a year from now? on September 11, 2018?
    Number days.
      0 for Sunday, 1 for Monday, . . . , 6 for Saturday.

Today: day 1.
  6 days from now. day 7 or day 0 or Sunday.
  26 days from now. day 27 or day 6.
    two days are equivalent up to addition/subtraction of multiple of 7.
    12 days from now is day 6 which is Saturday!

What day is it a year from now?
  Next year is not a leap year. So 365 days from now.
  Day 1+365 or day 366.
Smallest representation:
  subtract 7 until smaller than 7.
  divide and get remainder.
  366/6 leaves quotient of 52 and remainder 2.
    or September 11, 2018 is a Tuesday.

Day of the week.

Today is Monday.
  What day is it a year from now? on September 11, 2018?
    Number days.
      0 for Sunday, 1 for Monday, . . . , 6 for Saturday.

Today: day 1.
  6 days from now. day 7 or day 0 or Sunday.
  26 days from now. day 27 or day 6.
    two days are equivalent up to addition/subtraction of multiple of 7.
    12 days from now is day 6 which is Saturday!

What day is it a year from now?
  Next year is not a leap year. So 365 days from now.
  Day 1+365 or day 366.
Smallest representation:
  subtract 7 until smaller than 7.
  divide and get remainder.
  366/6 leaves quotient of 52 and remainder 2.
    or September 11, 2018 is a Tuesday.

Years and years...

80 years from now?

Years and years...

80 years from now? 20 leap years.

Years and years...

80 years from now? 20 leap years. 366×20 days

Years and years...

80 years from now? 20 leap years. 366×20 days
60 regular years.

Years and years...

80 years from now? 20 leap years. 366×20 days
60 regular years. 365×60 days

Years and years...

80 years from now?   20 leap years. 366×20 days
  60 regular years. 365×60 days
Today is day 1.

Years and years...

80 years from now? 20 leap years. 366×20 days
60 regular years. 365×60 days
Today is day 1.
It is day $1 + 366 \times 20 + 365 \times 60$.

Years and years...

80 years from now? 20 leap years. 366×20 days
60 regular years. 365×60 days
Today is day 1.
It is day $1 + 366 \times 20 + 365 \times 60$. Equivalent to?

Years and years...

80 years from now? 20 leap years. 366×20 days
60 regular years. 365×60 days
Today is day 1.
It is day $1 + 366 \times 20 + 365 \times 60$. Equivalent to?

Hmm.

Years and years...

80 years from now? 20 leap years. 366×20 days
60 regular years. 365×60 days
Today is day 1.
It is day $1 + 366 \times 20 + 365 \times 60$. Equivalent to?

Hmm.
What is remainder of 366 when dividing by 7?

Years and years...

80 years from now? 20 leap years. 366×20 days
60 regular years. 365×60 days
Today is day 1.
It is day $1 + 366 \times 20 + 365 \times 60$. Equivalent to?

Hmm.
What is remainder of 366 when dividing by 7? $52 \times 7 + 2$.

Years and years...

80 years from now?   20 leap years. 366×20 days
  60 regular years. 365×60 days
Today is day 1.
It is day $1 + 366 \times 20 + 365 \times 60$. Equivalent to?

Hmm.
  What is remainder of 366 when dividing by 7? $52 \times 7 + 2$.
  What is remainder of 365 when dividing by 7?

Years and years...

80 years from now? 20 leap years. 366×20 days
60 regular years. 365×60 days
Today is day 1.
It is day $1 + 366 \times 20 + 365 \times 60$. Equivalent to?

Hmm.
What is remainder of 366 when dividing by 7? $52 \times 7 + 2$.
What is remainder of 365 when dividing by 7? 1

Years and years...

80 years from now? 20 leap years. 366×20 days
60 regular years. 365×60 days
Today is day 1.
It is day $1 + 366 \times 20 + 365 \times 60$. Equivalent to?

Hmm.
What is remainder of 366 when dividing by 7? $52 \times 7 + 2$.
What is remainder of 365 when dividing by 7? 1

Years and years...

80 years from now? 20 leap years. 366×20 days
60 regular years. 365×60 days
Today is day 1.
It is day $1 + 366 \times 20 + 365 \times 60$. Equivalent to?

Hmm.
What is remainder of 366 when dividing by 7? $52 \times 7 + 2$.
What is remainder of 365 when dividing by 7? 1
Today is day 1.

Years and years...

80 years from now? 20 leap years. 366×20 days
60 regular years. 365×60 days
Today is day 1.
It is day $1 + 366 \times 20 + 365 \times 60$. Equivalent to?

Hmm.
What is remainder of 366 when dividing by 7? $52 \times 7 + 2$.
What is remainder of 365 when dividing by 7? 1
Today is day 1.
Get Day: $1 + 2 \times 20 + 1 \times 60$

Years and years...

80 years from now? 20 leap years. 366×20 days
60 regular years. 365×60 days
Today is day 1.
It is day $1 + 366 \times 20 + 365 \times 60$. Equivalent to?

Hmm.
What is remainder of 366 when dividing by 7? $52 \times 7 + 2$.
What is remainder of 365 when dividing by 7? 1
Today is day 1.
Get Day: $1 + 2 \times 20 + 1 \times 60 = 101$

Years and years...

80 years from now? 20 leap years. 366×20 days
60 regular years. 365×60 days
Today is day 1.
It is day $1 + 366 \times 20 + 365 \times 60$. Equivalent to?

Hmm.
What is remainder of 366 when dividing by 7? $52 \times 7 + 2$.
What is remainder of 365 when dividing by 7? 1
Today is day 1.
Get Day: $1 + 2 \times 20 + 1 \times 60 = 101$
Remainder when dividing by 7?

Years and years...

80 years from now? 20 leap years. 366×20 days

60 regular years. 365×60 days

Today is day 1.

It is day $1 + 366 \times 20 + 365 \times 60$. Equivalent to?

Hmm.

What is remainder of 366 when dividing by 7? $52 \times 7 + 2$.

What is remainder of 365 when dividing by 7? 1

Today is day 1.

Get Day: $1 + 2 \times 20 + 1 \times 60 = 101$

Remainder when dividing by 7? $102 = 14 \times 7$

Years and years...

80 years from now? 20 leap years. 366×20 days
60 regular years. 365×60 days
Today is day 1.
It is day $1 + 366 \times 20 + 365 \times 60$. Equivalent to?

Hmm.
What is remainder of 366 when dividing by 7? $52 \times 7 + 2$.
What is remainder of 365 when dividing by 7? 1
Today is day 1.
Get Day: $1 + 2 \times 20 + 1 \times 60 = 101$
Remainder when dividing by 7? $102 = 14 \times 7 + 3$.

Years and years...

80 years from now? 20 leap years. 366×20 days
60 regular years. 365×60 days
Today is day 1.
It is day $1 + 366 \times 20 + 365 \times 60$. Equivalent to?

Hmm.
What is remainder of 366 when dividing by 7? $52 \times 7 + 2$.
What is remainder of 365 when dividing by 7? 1
Today is day 1.
Get Day: $1 + 2 \times 20 + 1 \times 60 = 101$
Remainder when dividing by 7? $102 = 14 \times 7 + 3$.
Or September 11, 2097 is Wednesday!

Years and years...

80 years from now? 20 leap years. 366×20 days
60 regular years. 365×60 days
Today is day 1.
It is day $1 + 366 \times 20 + 365 \times 60$. Equivalent to?

Hmm.
What is remainder of 366 when dividing by 7? $52 \times 7 + 2$.
What is remainder of 365 when dividing by 7? 1
Today is day 1.
Get Day: $1 + 2 \times 20 + 1 \times 60 = 101$
Remainder when dividing by 7? $102 = 14 \times 7 + 3$.
Or September 11, 2097 is Wednesday!

Further Simplify Calculation:

Years and years...

80 years from now? 20 leap years. 366×20 days
60 regular years. 365×60 days
Today is day 1.
It is day $1 + 366 \times 20 + 365 \times 60$. Equivalent to?

Hmm.
What is remainder of 366 when dividing by 7? $52 \times 7 + 2$.
What is remainder of 365 when dividing by 7? 1
Today is day 1.
Get Day: $1 + 2 \times 20 + 1 \times 60 = 101$
Remainder when dividing by 7? $102 = 14 \times 7 + 3$.
Or September 11, 2097 is Wednesday!

Further Simplify Calculation:
20 has remainder 6 when divided by 7.

Years and years...

80 years from now? 20 leap years. 366×20 days
60 regular years. 365×60 days
Today is day 1.
It is day $1 + 366 \times 20 + 365 \times 60$. Equivalent to?

Hmm.
What is remainder of 366 when dividing by 7? $52 \times 7 + 2$.
What is remainder of 365 when dividing by 7? 1
Today is day 1.
Get Day: $1 + 2 \times 20 + 1 \times 60 = 101$
Remainder when dividing by 7? $102 = 14 \times 7 + 3$.
Or September 11, 2097 is Wednesday!

Further Simplify Calculation:
20 has remainder 6 when divided by 7.
60 has remainder 4 when divided by 7.

Years and years...

80 years from now? 20 leap years. 366×20 days
60 regular years. 365×60 days
Today is day 1.
It is day $1 + 366 \times 20 + 365 \times 60$. Equivalent to?

Hmm.
What is remainder of 366 when dividing by 7? $52 \times 7 + 2$.
What is remainder of 365 when dividing by 7? 1
Today is day 1.
Get Day: $1 + 2 \times 20 + 1 \times 60 = 101$
Remainder when dividing by 7? $102 = 14 \times 7 + 3$.
Or September 11, 2097 is Wednesday!

Further Simplify Calculation:
20 has remainder 6 when divided by 7.
60 has remainder 4 when divided by 7.
Get Day: $1 + 2 \times 6 + 1 \times 4 = 17$.

Years and years...

80 years from now? 20 leap years. 366×20 days
60 regular years. 365×60 days
Today is day 1.
It is day $1 + 366 \times 20 + 365 \times 60$. Equivalent to?

Hmm.
What is remainder of 366 when dividing by 7? $52 \times 7 + 2$.
What is remainder of 365 when dividing by 7? 1
Today is day 1.
Get Day: $1 + 2 \times 20 + 1 \times 60 = 101$
Remainder when dividing by 7? $102 = 14 \times 7 + 3$.
Or September 11, 2097 is Wednesday!

Further Simplify Calculation:
20 has remainder 6 when divided by 7.
60 has remainder 4 when divided by 7.
Get Day: $1 + 2 \times 6 + 1 \times 4 = 17$.
Or Day 4.

Years and years...

80 years from now? 20 leap years. 366×20 days
60 regular years. 365×60 days
Today is day 1.
It is day $1 + 366 \times 20 + 365 \times 60$. Equivalent to?

Hmm.
What is remainder of 366 when dividing by 7? $52 \times 7 + 2$.
What is remainder of 365 when dividing by 7? 1
Today is day 1.
Get Day: $1 + 2 \times 20 + 1 \times 60 = 101$
Remainder when dividing by 7? $102 = 14 \times 7 + 3$.
Or September 11, 2097 is Wednesday!

Further Simplify Calculation:
20 has remainder 6 when divided by 7.
60 has remainder 4 when divided by 7.
Get Day: $1 + 2 \times 6 + 1 \times 4 = 17$.
Or Day 4. September 11, 2097 is Wednesday.

Years and years...

80 years from now? 20 leap years. 366×20 days
60 regular years. 365×60 days
Today is day 1.
It is day $1 + 366 \times 20 + 365 \times 60$. Equivalent to?

Hmm.
What is remainder of 366 when dividing by 7? $52 \times 7 + 2$.
What is remainder of 365 when dividing by 7? 1
Today is day 1.
Get Day: $1 + 2 \times 20 + 1 \times 60 = 101$
Remainder when dividing by 7? $102 = 14 \times 7 + 3$.
Or September 11, 2097 is Wednesday!

Further Simplify Calculation:
20 has remainder 6 when divided by 7.
60 has remainder 4 when divided by 7.
Get Day: $1 + 2 \times 6 + 1 \times 4 = 17$.
Or Day 4. September 11, 2097 is Wednesday.

“Reduce” at any time in calculation!

Modular Arithmetic: formalism.

For $x, y \in \mathbb{N}$, x **is congruent to** y **modulo** m or "$x \equiv y \pmod{m}$" if and only if $(x - y)$ is divisible by m.

Modular Arithmetic: formalism.

For $x, y \in \mathbb{N}$, x **is congruent to** y **modulo** m or "$x \equiv y \pmod{m}$"
if and only if $(x - y)$ is divisible by m.
...or x and y have the same remainder w.r.t. m.

Modular Arithmetic: formalism.

For $x, y \in \mathbb{N}$, x **is congruent to** y **modulo** m or "$x \equiv y \pmod{m}$"
if and only if $(x - y)$ is divisible by m.
...or x and y have the same remainder w.r.t. m.
...or $x = y + km$ for some integer k.

Modular Arithmetic: formalism.

For $x, y \in \mathbb{N}$, x **is congruent to** y **modulo** m or "$x \equiv y \pmod{m}$" if and only if $(x - y)$ is divisible by m.
...or x and y have the same remainder w.r.t. m.
...or $x = y + km$ for some integer k.

Modular Arithmetic: formalism.

For $x, y \in \mathbb{N}$, x **is congruent to** y **modulo** m or "$x \equiv y \pmod{m}$" if and only if $(x - y)$ is divisible by m.
...or x and y have the same remainder w.r.t. m.
...or $x = y + km$ for some integer k.

Mod 7 equivalence classes:

Modular Arithmetic: formalism.

For $x, y \in \mathbb{N}$, x **is congruent to** y **modulo** m or "$x \equiv y \pmod{m}$"
if and only if $(x - y)$ is divisible by m.
...or x and y have the same remainder w.r.t. m.
...or $x = y + km$ for some integer k.

Mod 7 equivalence classes:
$\{\ldots, -7, 0, 7, 14, \ldots\}$

Modular Arithmetic: formalism.

For $x, y \in \mathbb{N}$, x **is congruent to** y **modulo** m or "$x \equiv y \pmod{m}$" if and only if $(x - y)$ is divisible by m.
...or x and y have the same remainder w.r.t. m.
...or $x = y + km$ for some integer k.

Mod 7 equivalence classes:
$\{\ldots, -7, 0, 7, 14, \ldots\}$ $\{\ldots, -6, 1, 8, 15, \ldots\}$

Modular Arithmetic: formalism.

For $x, y \in \mathbb{N}$, x **is congruent to** y **modulo** m or "$x \equiv y \pmod{m}$"
if and only if $(x - y)$ is divisible by m.
...or x and y have the same remainder w.r.t. m.
...or $x = y + km$ for some integer k.

Mod 7 equivalence classes:
$\{\ldots, -7, 0, 7, 14, \ldots\}$ $\{\ldots, -6, 1, 8, 15, \ldots\}$ ...

Modular Arithmetic: formalism.

For $x, y \in \mathbb{N}$, x **is congruent to** y **modulo** m or "$x \equiv y \pmod{m}$" if and only if $(x - y)$ is divisible by m.
...or x and y have the same remainder w.r.t. m.
...or $x = y + km$ for some integer k.

Mod 7 equivalence classes:
$\{\ldots, -7, 0, 7, 14, \ldots\}$ $\{\ldots, -6, 1, 8, 15, \ldots\}$ ...

Useful Fact: Addition, subtraction, multiplication can be done with any equivalent x and y.

Modular Arithmetic: formalism.

For $x, y \in \mathbb{N}$, x **is congruent to** y **modulo** m or "$x \equiv y \pmod{m}$" if and only if $(x - y)$ is divisible by m.
...or x and y have the same remainder w.r.t. m.
...or $x = y + km$ for some integer k.

Mod 7 equivalence classes:
$\{\ldots, -7, 0, 7, 14, \ldots\}$ $\{\ldots, -6, 1, 8, 15, \ldots\}$ ...

Useful Fact: Addition, subtraction, multiplication can be done with any equivalent x and y.

or " $a \equiv c \pmod{m}$ and $b \equiv d \pmod{m}$

Modular Arithmetic: formalism.

For $x, y \in \mathbb{N}$, x **is congruent to** y **modulo** m or "$x \equiv y \pmod{m}$" if and only if $(x - y)$ is divisible by m.
...or x and y have the same remainder w.r.t. m.
...or $x = y + km$ for some integer k.

Mod 7 equivalence classes:
$\{\ldots, -7, 0, 7, 14, \ldots\}$ $\{\ldots, -6, 1, 8, 15, \ldots\}$ ...

Useful Fact: Addition, subtraction, multiplication can be done with any equivalent x and y.

or " $a \equiv c \pmod{m}$ and $b \equiv d \pmod{m}$
$\implies a + b \equiv c + d \pmod{m}$ and $a \cdot b = c \cdot d \pmod{m}$"

Modular Arithmetic: formalism.

For $x, y \in \mathbb{N}$, x **is congruent to** y **modulo** m or "$x \equiv y \pmod{m}$"
if and only if $(x - y)$ is divisible by m.
...or x and y have the same remainder w.r.t. m.
...or $x = y + km$ for some integer k.

Mod 7 equivalence classes:
$\{\ldots, -7, 0, 7, 14, \ldots\}$ $\{\ldots, -6, 1, 8, 15, \ldots\}$ ...

Useful Fact: Addition, subtraction, multiplication can be done with any equivalent x and y.

or " $a \equiv c \pmod{m}$ and $b \equiv d \pmod{m}$
$\implies a + b \equiv c + d \pmod{m}$ and $a \cdot b = c \cdot d \pmod{m}$"

Proof: If $a \equiv c \pmod{m}$, then $a = c + km$ for some integer k.

Modular Arithmetic: formalism.

For $x, y \in \mathbb{N}$, x **is congruent to** y **modulo** m or "$x \equiv y \pmod{m}$"
if and only if $(x - y)$ is divisible by m.
...or x and y have the same remainder w.r.t. m.
...or $x = y + km$ for some integer k.

Mod 7 equivalence classes:
$\{\ldots, -7, 0, 7, 14, \ldots\}$ $\{\ldots, -6, 1, 8, 15, \ldots\}$ ...

Useful Fact: Addition, subtraction, multiplication can be done with any equivalent x and y.

or " $a \equiv c \pmod{m}$ and $b \equiv d \pmod{m}$
$\implies a + b \equiv c + d \pmod{m}$ and $a \cdot b = c \cdot d \pmod{m}$"

Proof: If $a \equiv c \pmod{m}$, then $a = c + km$ for some integer k.
If $b \equiv d \pmod{m}$, then $b = d + jm$ for some integer j.

Modular Arithmetic: formalism.

For $x, y \in \mathbb{N}$, x **is congruent to** y **modulo** m or "$x \equiv y \pmod{m}$"
if and only if $(x - y)$ is divisible by m.
...or x and y have the same remainder w.r.t. m.
...or $x = y + km$ for some integer k.

Mod 7 equivalence classes:
$\{\ldots, -7, 0, 7, 14, \ldots\}$ $\{\ldots, -6, 1, 8, 15, \ldots\}$ ...

Useful Fact: Addition, subtraction, multiplication can be done with any equivalent x and y.

or " $a \equiv c \pmod{m}$ and $b \equiv d \pmod{m}$
$\implies a + b \equiv c + d \pmod{m}$ and $a \cdot b = c \cdot d \pmod{m}$"

Proof: If $a \equiv c \pmod{m}$, then $a = c + km$ for some integer k.
If $b \equiv d \pmod{m}$, then $b = d + jm$ for some integer j.
Therefore,

Modular Arithmetic: formalism.

For $x, y \in \mathbb{N}$, x **is congruent to** y **modulo** m or "$x \equiv y \pmod{m}$"
if and only if $(x - y)$ is divisible by m.
...or x and y have the same remainder w.r.t. m.
...or $x = y + km$ for some integer k.

Mod 7 equivalence classes:
$\{\ldots, -7, 0, 7, 14, \ldots\}$ $\{\ldots, -6, 1, 8, 15, \ldots\}$ ...

Useful Fact: Addition, subtraction, multiplication can be done with any equivalent x and y.

or " $a \equiv c \pmod{m}$ and $b \equiv d \pmod{m}$
$\implies a + b \equiv c + d \pmod{m}$ and $a \cdot b = c \cdot d \pmod{m}$"

Proof: If $a \equiv c \pmod{m}$, then $a = c + km$ for some integer k.
If $b \equiv d \pmod{m}$, then $b = d + jm$ for some integer j.
Therefore, $a + b = c + d + (k + j)m$

Modular Arithmetic: formalism.

For $x, y \in \mathbb{N}$, x **is congruent to** y **modulo** m or "$x \equiv y \pmod{m}$" if and only if $(x - y)$ is divisible by m.
...or x and y have the same remainder w.r.t. m.
...or $x = y + km$ for some integer k.

Mod 7 equivalence classes:
$\{\ldots, -7, 0, 7, 14, \ldots\}$ $\{\ldots, -6, 1, 8, 15, \ldots\}$ ...

Useful Fact: Addition, subtraction, multiplication can be done with any equivalent x and y.

or " $a \equiv c \pmod{m}$ and $b \equiv d \pmod{m}$
$\implies a + b \equiv c + d \pmod{m}$ and $a \cdot b = c \cdot d \pmod{m}$"

Proof: If $a \equiv c \pmod{m}$, then $a = c + km$ for some integer k.
If $b \equiv d \pmod{m}$, then $b = d + jm$ for some integer j.
Therefore, $a + b = c + d + (k + j)m$ and since $k + j$ is integer.

Modular Arithmetic: formalism.

For $x, y \in \mathbb{N}$, x **is congruent to** y **modulo** m or "$x \equiv y \pmod{m}$" if and only if $(x-y)$ is divisible by m.
...or x and y have the same remainder w.r.t. m.
...or $x = y + km$ for some integer k.

Mod 7 equivalence classes:
$\{\ldots, -7, 0, 7, 14, \ldots\}$ $\{\ldots, -6, 1, 8, 15, \ldots\}$ ...

Useful Fact: Addition, subtraction, multiplication can be done with any equivalent x and y.

or " $a \equiv c \pmod{m}$ and $b \equiv d \pmod{m}$
$\implies a + b \equiv c + d \pmod{m}$ and $a \cdot b = c \cdot d \pmod{m}$"

Proof: If $a \equiv c \pmod{m}$, then $a = c + km$ for some integer k.
If $b \equiv d \pmod{m}$, then $b = d + jm$ for some integer j.
Therefore, $a + b = c + d + (k + j)m$ and since $k + j$ is integer.
$\implies a + b \equiv c + d \pmod{m}$.

Modular Arithmetic: formalism.

For $x, y \in \mathbb{N}$, x **is congruent to** y **modulo** m or "$x \equiv y \pmod{m}$"
if and only if $(x - y)$ is divisible by m.
...or x and y have the same remainder w.r.t. m.
...or $x = y + km$ for some integer k.

Mod 7 equivalence classes:
$\{\ldots, -7, 0, 7, 14, \ldots\}$ $\{\ldots, -6, 1, 8, 15, \ldots\}$ ...

Useful Fact: Addition, subtraction, multiplication can be done with any equivalent x and y.

or " $a \equiv c \pmod{m}$ and $b \equiv d \pmod{m}$
$\implies a + b \equiv c + d \pmod{m}$ and $a \cdot b = c \cdot d \pmod{m}$"

Proof: If $a \equiv c \pmod{m}$, then $a = c + km$ for some integer k.
If $b \equiv d \pmod{m}$, then $b = d + jm$ for some integer j.
Therefore, $a + b = c + d + (k + j)m$ and since $k + j$ is integer.
$\implies a + b \equiv c + d \pmod{m}$. $\square$

Modular Arithmetic: formalism.

For $x, y \in \mathbb{N}$, x **is congruent to** y **modulo** m or "$x \equiv y \pmod{m}$"
if and only if $(x - y)$ is divisible by m.
...or x and y have the same remainder w.r.t. m.
...or $x = y + km$ for some integer k.

Mod 7 equivalence classes:
$\{\ldots, -7, 0, 7, 14, \ldots\}$ $\{\ldots, -6, 1, 8, 15, \ldots\}$ ...

Useful Fact: Addition, subtraction, multiplication can be done with any equivalent x and y.

or " $a \equiv c \pmod{m}$ and $b \equiv d \pmod{m}$
$\implies a + b \equiv c + d \pmod{m}$ and $a \cdot b = c \cdot d \pmod{m}$"

Proof: If $a \equiv c \pmod{m}$, then $a = c + km$ for some integer k.
If $b \equiv d \pmod{m}$, then $b = d + jm$ for some integer j.
Therefore, $a + b = c + d + (k + j)m$ and since $k + j$ is integer.
$\implies a + b \equiv c + d \pmod{m}$. $\square$

Can calculate with representative in $\{0, \ldots, m - 1\}$.

Notation

$x \pmod{m}$ or $\mod(x, m)$

Notation

$x \pmod{m}$ or $\mod(x, m)$
- remainder of x divided by m in $\{0, \ldots, m-1\}$.

Notation

$x \pmod{m}$ or $\mod(x, m)$
- remainder of x divided by m in $\{0, \ldots, m-1\}$.

Notation

$x \pmod{m}$ or $\mod(x, m)$
- remainder of x divided by m in $\{0, \ldots, m-1\}$.

$\mod(x, m) = x - \lfloor \frac{x}{m} \rfloor m$

Notation

$x \pmod{m}$ or $\mod(x, m)$
- remainder of x divided by m in $\{0, \ldots, m-1\}$.

$\mod(x, m) = x - \lfloor \frac{x}{m} \rfloor m$

$\lfloor \frac{x}{m} \rfloor$ is quotient.

Notation

$x \pmod m$ or $\mod(x,m)$

- remainder of x divided by m in $\{0,\ldots,m-1\}$.

$\mod(x,m) = x - \lfloor \frac{x}{m} \rfloor m$

$\lfloor \frac{x}{m} \rfloor$ is quotient.

$\mod(29,12) = 29 - (\lfloor \frac{29}{12} \rfloor) \times 12$

Notation

$x \pmod{m}$ or $\mod(x, m)$
- remainder of x divided by m in $\{0, \ldots, m-1\}$.

$\mod(x, m) = x - \lfloor \frac{x}{m} \rfloor m$

$\lfloor \frac{x}{m} \rfloor$ is quotient.

$\mod(29, 12) = 29 - (\lfloor \frac{29}{12} \rfloor) \times 12 = 29 - (2) \times 12$

Notation

$x \pmod{m}$ or $\mod(x, m)$
- remainder of x divided by m in $\{0, \ldots, m-1\}$.

$\mod(x, m) = x - \lfloor \frac{x}{m} \rfloor m$

$\lfloor \frac{x}{m} \rfloor$ is quotient.

$\mod(29, 12) = 29 - (\lfloor \frac{29}{12} \rfloor) \times 12 = 29 - (2) \times 12 = 4$

Notation

$x \pmod m$ or $\mod(x, m)$

- remainder of x divided by m in $\{0, \ldots, m-1\}$.

$\mod(x, m) = x - \lfloor \frac{x}{m} \rfloor m$

$\lfloor \frac{x}{m} \rfloor$ is quotient.

$\mod(29, 12) = 29 - (\lfloor \frac{29}{12} \rfloor) \times 12 = 29 - (2) \times 12 = \cancel{4} = 5$

Notation

$x \pmod{m}$ or $\mod(x,m)$

- remainder of x divided by m in $\{0,\ldots,m-1\}$.

$\mod(x,m) = x - \lfloor \frac{x}{m} \rfloor m$

$\lfloor \frac{x}{m} \rfloor$ is quotient.

$\mod(29,12) = 29 - (\lfloor \frac{29}{12} \rfloor) \times 12 = 29 - (2) \times 12 = \cancel{4} = 5$

Work in this system.

Notation

$x \pmod{m}$ or $\mod(x, m)$
- remainder of x divided by m in $\{0, \ldots, m-1\}$.

$\mod(x, m) = x - \lfloor \frac{x}{m} \rfloor m$

$\lfloor \frac{x}{m} \rfloor$ is quotient.

$\mod(29, 12) = 29 - (\lfloor \frac{29}{12} \rfloor) \times 12 = 29 - (2) \times 12 = \cancel{4} = 5$

Work in this system.
$a \equiv b \pmod{m}$.

Notation

$x \pmod{m}$ or $\mod(x, m)$
- remainder of x divided by m in $\{0, \ldots, m-1\}$.

$\mod(x,m) = x - \lfloor \frac{x}{m} \rfloor m$

$\lfloor \frac{x}{m} \rfloor$ is quotient.

$\mod(29,12) = 29 - (\lfloor \frac{29}{12} \rfloor) \times 12 = 29 - (2) \times 12 = \cancel{4} = 5$

Work in this system.

$a \equiv b \pmod{m}$.

Says two integers a and b are equivalent modulo m.

Notation

$x \pmod{m}$ or $\mod(x, m)$

- remainder of x divided by m in $\{0, \ldots, m-1\}$.

$\mod(x, m) = x - \lfloor \frac{x}{m} \rfloor m$

$\lfloor \frac{x}{m} \rfloor$ is quotient.

$\mod(29, 12) = 29 - (\lfloor \frac{29}{12} \rfloor) \times 12 = 29 - (2) \times 12 = \cancel{4} = 5$

Work in this system.

$a \equiv b \pmod{m}$.

Says two integers a and b are equivalent modulo m.

Modulus is m

Notation

$x \pmod{m}$ or $\mod(x, m)$
- remainder of x divided by m in $\{0, \ldots, m-1\}$.

$\mod(x, m) = x - \lfloor \frac{x}{m} \rfloor m$

$\lfloor \frac{x}{m} \rfloor$ is quotient.

$\mod(29, 12) = 29 - (\lfloor \frac{29}{12} \rfloor) \times 12 = 29 - (2) \times 12 = \cancel{4} = 5$

Work in this system.
$a \equiv b \pmod{m}$.
Says two integers a and b are equivalent modulo m.

Modulus is m

$6 \equiv$

Notation

$x \pmod{m}$ or $\mod(x, m)$

- remainder of x divided by m in $\{0, \ldots, m-1\}$.

$\mod(x, m) = x - \lfloor \frac{x}{m} \rfloor m$

$\lfloor \frac{x}{m} \rfloor$ is quotient.

$\mod(29, 12) = 29 - (\lfloor \frac{29}{12} \rfloor) \times 12 = 29 - (2) \times 12 = \cancel{4} = 5$

Work in this system.

$a \equiv b \pmod{m}$.

Says two integers a and b are equivalent modulo m.

Modulus is m

$6 \equiv 3 + 3$

Notation

$x \pmod{m}$ or $\mod(x, m)$
- remainder of x divided by m in $\{0, \ldots, m-1\}$.

$\mod(x, m) = x - \lfloor \frac{x}{m} \rfloor m$

$\lfloor \frac{x}{m} \rfloor$ is quotient.

$\mod(29, 12) = 29 - (\lfloor \frac{29}{12} \rfloor) \times 12 = 29 - (2) \times 12 = \cancel{4} = 5$

Work in this system.

$a \equiv b \pmod{m}$.

Says two integers a and b are equivalent modulo m.

Modulus is m

$6 \equiv 3 + 3 \equiv 3 + 10$

Notation

$x \pmod{m}$ or $\mod(x, m)$
- remainder of x divided by m in $\{0, \ldots, m-1\}$.

$\mod(x, m) = x - \lfloor \frac{x}{m} \rfloor m$

$\lfloor \frac{x}{m} \rfloor$ is quotient.

$\mod(29, 12) = 29 - (\lfloor \frac{29}{12} \rfloor) \times 12 = 29 - (2) \times 12 = \cancel{4} = 5$

Work in this system.
$a \equiv b \pmod{m}$.
Says two integers a and b are equivalent modulo m.

Modulus is m

$6 \equiv 3 + 3 \equiv 3 + 10 \pmod{7}$.

Notation

$x \pmod{m}$ or $\mod(x, m)$
- remainder of x divided by m in $\{0, \ldots, m-1\}$.

$\mod(x, m) = x - \lfloor \frac{x}{m} \rfloor m$

$\lfloor \frac{x}{m} \rfloor$ is quotient.

$\mod(29, 12) = 29 - (\lfloor \frac{29}{12} \rfloor) \times 12 = 29 - (2) \times 12 = \cancel{4} = 5$

Work in this system.
$a \equiv b \pmod{m}$.
Says two integers a and b are equivalent modulo m.

Modulus is m

$6 \equiv 3 + 3 \equiv 3 + 10 \pmod{7}$.

$6 =$

Notation

$x \pmod{m}$ or $\mod(x,m)$
- remainder of x divided by m in $\{0,\ldots,m-1\}$.

$\mod(x,m) = x - \lfloor \frac{x}{m} \rfloor m$

$\lfloor \frac{x}{m} \rfloor$ is quotient.

$\mod(29,12) = 29 - (\lfloor \frac{29}{12} \rfloor) \times 12 = 29 - (2) \times 12 = \cancel{4} = 5$

Work in this system.
$a \equiv b \pmod{m}$.
Says two integers a and b are equivalent modulo m.

Modulus is m

$6 \equiv 3+3 \equiv 3+10 \pmod{7}$.

$6 = 3+3$

Notation

$x \pmod{m}$ or $\mod(x, m)$
- remainder of x divided by m in $\{0, \ldots, m-1\}$.

$\mod(x, m) = x - \lfloor \frac{x}{m} \rfloor m$

$\lfloor \frac{x}{m} \rfloor$ is quotient.

$\mod(29, 12) = 29 - (\lfloor \frac{29}{12} \rfloor) \times 12 = 29 - (2) \times 12 = \cancel{4} = 5$

Work in this system.
$a \equiv b \pmod{m}$.
Says two integers a and b are equivalent modulo m.

Modulus is m

$6 \equiv 3 + 3 \equiv 3 + 10 \pmod{7}$.

$6 = 3 + 3 = 3 + 10$

Notation

$x \pmod{m}$ or $\mod(x, m)$
- remainder of x divided by m in $\{0, \dots, m-1\}$.

$\mod(x, m) = x - \lfloor \frac{x}{m} \rfloor m$

$\lfloor \frac{x}{m} \rfloor$ is quotient.

$\mod(29, 12) = 29 - (\lfloor \frac{29}{12} \rfloor) \times 12 = 29 - (2) \times 12 = \cancel{4} = 5$

Work in this system.

$a \equiv b \pmod{m}$.

Says two integers a and b are equivalent modulo m.

Modulus is m

$6 \equiv 3 + 3 \equiv 3 + 10 \pmod{7}$.

$6 = 3 + 3 = 3 + 10 \pmod{7}$.

Notation

$x \pmod{m}$ or $\mod(x, m)$
- remainder of x divided by m in $\{0, \ldots, m-1\}$.

$\mod(x, m) = x - \lfloor \frac{x}{m} \rfloor m$

$\lfloor \frac{x}{m} \rfloor$ is quotient.

$\mod(29, 12) = 29 - (\lfloor \frac{29}{12} \rfloor) \times 12 = 29 - (2) \times 12 = \cancel{4} = 5$

Work in this system.

$a \equiv b \pmod{m}$.

Says two integers a and b are equivalent modulo m.

Modulus is m

$6 \equiv 3 + 3 \equiv 3 + 10 \pmod{7}$.

$6 = 3 + 3 = 3 + 10 \pmod{7}$.

Generally, not $6 \pmod{7} = 13 \pmod{7}$.

Notation

$x \pmod{m}$ or $\mod(x,m)$
- remainder of x divided by m in $\{0,\ldots,m-1\}$.

$\mod(x,m) = x - \lfloor \frac{x}{m} \rfloor m$

$\lfloor \frac{x}{m} \rfloor$ is quotient.

$\mod(29,12) = 29 - (\lfloor \frac{29}{12} \rfloor) \times 12 = 29 - (2) \times 12 = \cancel{4} = 5$

Work in this system.
$a \equiv b \pmod{m}$.
Says two integers a and b are equivalent modulo m.

Modulus is m

$6 \equiv 3+3 \equiv 3+10 \pmod{7}$.

$6 = 3+3 = 3+10 \pmod{7}$.

Generally, not $6 \pmod{7} = 13 \pmod{7}$.
But ok, if you really want.

Inverses and Factors.

Division: multiply by multiplicative inverse.

$$2x = 3 \implies (\frac{1}{2}) \cdot 2x = (\frac{1}{2}) \cdot 3 \implies x = \frac{3}{2}.$$

Inverses and Factors.

Division: multiply by multiplicative inverse.

$$2x = 3 \implies (\frac{1}{2}) \cdot 2x = (\frac{1}{2}) \cdot 3 \implies x = \frac{3}{2}.$$

Multiplicative inverse of x is y where $xy = 1$;

Inverses and Factors.

Division: multiply by multiplicative inverse.

$$2x = 3 \implies (\frac{1}{2}) \cdot 2x = (\frac{1}{2}) \cdot 3 \implies x = \frac{3}{2}.$$

Multiplicative inverse of x is y where $xy = 1$;
1 **is multiplicative identity element.**

Inverses and Factors.

Division: multiply by multiplicative inverse.

$$2x = 3 \implies (\frac{1}{2}) \cdot 2x = (\frac{1}{2}) \cdot 3 \implies x = \frac{3}{2}.$$

Multiplicative inverse of x is y where $xy = 1$;
1 **is multiplicative identity element.**

In modular arithmetic, 1 is the multiplicative identity element.

Inverses and Factors.

Division: multiply by multiplicative inverse.

$$2x = 3 \implies (\frac{1}{2}) \cdot 2x = (\frac{1}{2}) \cdot 3 \implies x = \frac{3}{2}.$$

Multiplicative inverse of x is y where $xy = 1$;
1 **is multiplicative identity element.**

In modular arithmetic, 1 is the multiplicative identity element.

Multiplicative inverse of x **mod** m is y with $xy = 1 \pmod{m}$.

Inverses and Factors.

Division: multiply by multiplicative inverse.

$$2x = 3 \implies (\frac{1}{2}) \cdot 2x = (\frac{1}{2}) \cdot 3 \implies x = \frac{3}{2}.$$

Multiplicative inverse of x is y where $xy = 1$;
1 **is multiplicative identity element.**

In modular arithmetic, 1 is the multiplicative identity element.

Multiplicative inverse of x **mod** m is y with $xy = 1 \pmod{m}$.

For 4 modulo 7 inverse is 2: $\quad 2 \cdot 4 \equiv 8 \equiv 1 \pmod{7}$.

Inverses and Factors.

Division: multiply by multiplicative inverse.

$$2x = 3 \implies (\frac{1}{2}) \cdot 2x = (\frac{1}{2}) \cdot 3 \implies x = \frac{3}{2}.$$

Multiplicative inverse of x is y where $xy = 1$;
1 **is multiplicative identity element.**

In modular arithmetic, 1 is the multiplicative identity element.

Multiplicative inverse of x **mod** m is y with $xy = 1 \pmod{m}$.

For 4 modulo 7 inverse is 2: $\quad 2 \cdot 4 \equiv 8 \equiv 1 \pmod{7}$.

Can solve $4x = 5 \pmod{7}$.

Inverses and Factors.

Division: multiply by multiplicative inverse.

$$2x = 3 \implies (\frac{1}{2}) \cdot 2x = (\frac{1}{2}) \cdot 3 \implies x = \frac{3}{2}.$$

Multiplicative inverse of x is y where $xy = 1$;
1 **is multiplicative identity element.**

In modular arithmetic, 1 is the multiplicative identity element.

Multiplicative inverse of x **mod** m is y with $xy = 1 \pmod{m}$.

For 4 modulo 7 inverse is 2: $\quad 2 \cdot 4 \equiv 8 \equiv 1 \pmod{7}$.

Can solve $4x = 5 \pmod{7}$.
$2 \cdot 4x = 2 \cdot 5 \pmod{7}$

Inverses and Factors.

Division: multiply by multiplicative inverse.

$$2x = 3 \implies (\frac{1}{2}) \cdot 2x = (\frac{1}{2}) \cdot 3 \implies x = \frac{3}{2}.$$

Multiplicative inverse of x is y where $xy = 1$;
1 **is multiplicative identity element.**

In modular arithmetic, 1 is the multiplicative identity element.

Multiplicative inverse of x **mod** m is y with $xy = 1 \pmod{m}$.

For 4 modulo 7 inverse is 2: $\quad 2 \cdot 4 \equiv 8 \equiv 1 \pmod{7}$.

Can solve $4x = 5 \pmod{7}$.
$2 \cdot 4x = 2 \cdot 5 \pmod{7}$
$8x = 10 \pmod{7}$

Inverses and Factors.

Division: multiply by multiplicative inverse.

$$2x = 3 \implies (\frac{1}{2}) \cdot 2x = (\frac{1}{2}) \cdot 3 \implies x = \frac{3}{2}.$$

Multiplicative inverse of x is y where $xy = 1$;
1 **is multiplicative identity element.**

In modular arithmetic, 1 is the multiplicative identity element.

Multiplicative inverse of x **mod** m is y with $xy = 1 \pmod{m}$.

For 4 modulo 7 inverse is 2: $2 \cdot 4 \equiv 8 \equiv 1 \pmod{7}$.

Can solve $4x = 5 \pmod{7}$.
$2 \cdot 4x = 2 \cdot 5 \pmod{7}$
$8x = 10 \pmod{7}$
$x = 3 \pmod{7}$

Inverses and Factors.

Division: multiply by multiplicative inverse.

$$2x = 3 \implies (\frac{1}{2}) \cdot 2x = (\frac{1}{2}) \cdot 3 \implies x = \frac{3}{2}.$$

Multiplicative inverse of x is y where $xy = 1$;
1 **is multiplicative identity element.**

In modular arithmetic, 1 is the multiplicative identity element.

Multiplicative inverse of x **mod** m is y with $xy = 1 \pmod{m}$.

For 4 modulo 7 inverse is 2: $2 \cdot 4 \equiv 8 \equiv 1 \pmod{7}$.

Can solve $4x = 5 \pmod{7}$.
$2 \cdot 4x = 2 \cdot 5 \pmod{7}$
$8x = 10 \pmod{7}$
$x = 3 \pmod{7}$
Check!

Inverses and Factors.

Division: multiply by multiplicative inverse.

$$2x = 3 \implies (\frac{1}{2}) \cdot 2x = (\frac{1}{2}) \cdot 3 \implies x = \frac{3}{2}.$$

Multiplicative inverse of x is y where $xy = 1$;
1 **is multiplicative identity element.**

In modular arithmetic, 1 is the multiplicative identity element.

Multiplicative inverse of x **mod** m is y with $xy = 1 \pmod{m}$.

For 4 modulo 7 inverse is 2: $2 \cdot 4 \equiv 8 \equiv 1 \pmod{7}$.

Can solve $4x = 5 \pmod{7}$.
$2 \cdot 4x = 2 \cdot 5 \pmod{7}$
$8x = 10 \pmod{7}$
$x = 3 \pmod{7}$
Check! $4(3) = 12 = 5 \pmod{7}$.

Inverses and Factors.

Division: multiply by multiplicative inverse.

$$2x = 3 \implies (\frac{1}{2}) \cdot 2x = (\frac{1}{2}) \cdot 3 \implies x = \frac{3}{2}.$$

Multiplicative inverse of x is y where $xy = 1$;
1 **is multiplicative identity element.**

In modular arithmetic, 1 is the multiplicative identity element.

Multiplicative inverse of x **mod** m is y with $xy = 1 \pmod{m}$.

For 4 modulo 7 inverse is 2: $2 \cdot 4 \equiv 8 \equiv 1 \pmod{7}$.

Can solve $4x = 5 \pmod{7}$.
$x = 3 \pmod{7}$ ::: Check! $4(3) = 12 = 5 \pmod{7}$.

Inverses and Factors.

Division: multiply by multiplicative inverse.

$$2x = 3 \implies (\frac{1}{2}) \cdot 2x = (\frac{1}{2}) \cdot 3 \implies x = \frac{3}{2}.$$

Multiplicative inverse of x is y where $xy = 1$;
1 **is multiplicative identity element.**

In modular arithmetic, 1 is the multiplicative identity element.

Multiplicative inverse of x **mod** m is y with $xy = 1 \pmod{m}$.

For 4 modulo 7 inverse is 2: $\quad 2 \cdot 4 \equiv 8 \equiv 1 \pmod{7}$.

Can solve $4x = 5 \pmod{7}$.
$x = 3 \pmod{7}$ ::: Check! $4(3) = 12 = 5 \pmod{7}$.

For 8 modulo 12: no multiplicative inverse!

Inverses and Factors.

Division: multiply by multiplicative inverse.

$$2x = 3 \implies (\frac{1}{2}) \cdot 2x = (\frac{1}{2}) \cdot 3 \implies x = \frac{3}{2}.$$

Multiplicative inverse of x is y where $xy = 1$;
1 **is multiplicative identity element.**

In modular arithmetic, 1 is the multiplicative identity element.

Multiplicative inverse of x **mod** m is y with $xy = 1 \pmod{m}$.

For 4 modulo 7 inverse is 2: $\quad 2 \cdot 4 \equiv 8 \equiv 1 \pmod{7}$.

Can solve $4x = 5 \pmod{7}$.
$x = 3 \pmod{7}$ ::: Check! $4(3) = 12 = 5 \pmod{7}$.

For 8 modulo 12: no multiplicative inverse!

"Common factor of 4"

Inverses and Factors.

Division: multiply by multiplicative inverse.

$$2x = 3 \implies (\frac{1}{2}) \cdot 2x = (\frac{1}{2}) \cdot 3 \implies x = \frac{3}{2}.$$

Multiplicative inverse of x is y where $xy = 1$;
1 **is multiplicative identity element.**

In modular arithmetic, 1 is the multiplicative identity element.

Multiplicative inverse of x **mod** m is y with $xy = 1 \pmod{m}$.

For 4 modulo 7 inverse is 2: $\quad 2 \cdot 4 \equiv 8 \equiv 1 \pmod{7}$.

Can solve $4x = 5 \pmod{7}$.
$x = 3 \pmod{7}$ ::: Check! $4(3) = 12 = 5 \pmod{7}$.

For 8 modulo 12: no multiplicative inverse!

"Common factor of 4" $\implies$
$8k - 12\ell$ is a multiple of four for any ℓ and k $\implies$

Inverses and Factors.

Division: multiply by multiplicative inverse.

$$2x = 3 \implies (\frac{1}{2}) \cdot 2x = (\frac{1}{2}) \cdot 3 \implies x = \frac{3}{2}.$$

Multiplicative inverse of x is y where $xy = 1$;
1 **is multiplicative identity element.**

In modular arithmetic, 1 is the multiplicative identity element.

Multiplicative inverse of x **mod** m is y with $xy = 1 \pmod{m}$.

For 4 modulo 7 inverse is 2: $2 \cdot 4 \equiv 8 \equiv 1 \pmod{7}$.

Can solve $4x = 5 \pmod{7}$.
$x = 3 \pmod{7}$ ::: Check! $4(3) = 12 = 5 \pmod{7}$.

For 8 modulo 12: no multiplicative inverse!

"Common factor of 4" $\implies$
$8k - 12\ell$ is a multiple of four for any ℓ and $k \implies$
$8k \not\equiv 1 \pmod{12}$ for any k.

Greatest Common Divisor and Inverses.

Thm:
If greatest common divisor of x and m, $\gcd(x, m)$, is 1, then x has a multiplicative inverse modulo m.

Greatest Common Divisor and Inverses.

Thm:
If greatest common divisor of x and m, $\gcd(x,m)$, is 1, then x has a multiplicative inverse modulo m.

Proof $\Longrightarrow$ **:** The set $S = \{0x, 1x, \ldots, (m-1)x\}$ contains $y \equiv 1 \pmod{m}$ if all distinct modulo m.

Greatest Common Divisor and Inverses.

Thm:
If greatest common divisor of x and m, $\gcd(x,m)$, is 1, then x has a multiplicative inverse modulo m.

Proof $\Longrightarrow$: The set $S = \{0x, 1x, \ldots, (m-1)x\}$ contains $y \equiv 1 \pmod m$ if all distinct modulo m.

Pigenhole principle: Each of m numbers in S correspond to different one of m equivalence classes modulo m.

Greatest Common Divisor and Inverses.

Thm:
If greatest common divisor of x and m, $\gcd(x,m)$, is 1, then x has a multiplicative inverse modulo m.

Proof $\implies$: The set $S = \{0x, 1x, \ldots, (m-1)x\}$ contains $y \equiv 1 \pmod{m}$ if all distinct modulo m.

Pigenhole principle: Each of m numbers in S correspond to different one of m equivalence classes modulo m.
$\implies$ One must correspond to 1 modulo m.

Greatest Common Divisor and Inverses.

Thm:
If greatest common divisor of x and m, $\gcd(x,m)$, is 1, then x has a multiplicative inverse modulo m.

Proof $\implies$: The set $S = \{0x, 1x, \ldots, (m-1)x\}$ contains $y \equiv 1 \pmod m$ if all distinct modulo m.

Pigenhole principle: Each of m numbers in S correspond to different one of m equivalence classes modulo m.
$\implies$ One must correspond to 1 modulo m.

If not distinct, then $\exists a, b \in \{0, \ldots, m-1\}$, $a \neq b$,

Greatest Common Divisor and Inverses.

Thm:
If greatest common divisor of x and m, $\gcd(x,m)$, is 1, then x has a multiplicative inverse modulo m.

Proof $\implies$: The set $S = \{0x, 1x, \ldots, (m-1)x\}$ contains $y \equiv 1 \mod m$ if all distinct modulo m.

Pigenhole principle: Each of m numbers in S correspond to different one of m equivalence classes modulo m.
$\implies$ One must correspond to 1 modulo m.

If not distinct, then $\exists a, b \in \{0, \ldots, m-1\}$, $a \neq b$, where
$(ax \equiv bx \pmod{m}) \implies (a-b)x \equiv 0 \pmod{m}$

Greatest Common Divisor and Inverses.

Thm:
If greatest common divisor of x and m, $\gcd(x,m)$, is 1, then x has a multiplicative inverse modulo m.

Proof $\implies$: The set $S = \{0x, 1x, \ldots, (m-1)x\}$ contains $y \equiv 1 \mod m$ if all distinct modulo m.

Pigenhole principle: Each of m numbers in S correspond to different one of m equivalence classes modulo m.
$\implies$ One must correspond to 1 modulo m.

If not distinct, then $\exists a, b \in \{0, \ldots, m-1\}$, $a \neq b$, where
$(ax \equiv bx \pmod{m}) \implies (a-b)x \equiv 0 \pmod{m}$
Or $(a-b)x = km$ for some integer k.

Greatest Common Divisor and Inverses.

Thm:
If greatest common divisor of x and m, $\gcd(x, m)$, is 1, then x has a multiplicative inverse modulo m.

Proof $\implies$ **:** The set $S = \{0x, 1x, \ldots, (m-1)x\}$ contains $y \equiv 1 \mod m$ if all distinct modulo m.

Pigenhole principle: Each of m numbers in S correspond to different one of m equivalence classes modulo m.
$\implies$ One must correspond to 1 modulo m.

If not distinct, then $\exists a, b \in \{0, \ldots, m-1\}$, $a \neq b$, where
$(ax \equiv bx \pmod{m}) \implies (a-b)x \equiv 0 \pmod{m}$
Or $(a-b)x = km$ for some integer k.

$gcd(x, m) = 1$

Greatest Common Divisor and Inverses.

Thm:
If greatest common divisor of x and m, gcd(x,m), is 1, then x has a multiplicative inverse modulo m.

Proof $\implies$ **:** The set $S = \{0x, 1x, \ldots, (m-1)x\}$ contains $y \equiv 1 \mod m$ if all distinct modulo m.

Pigenhole principle: Each of m numbers in S correspond to different one of m equivalence classes modulo m.
$\implies$ One must correspond to 1 modulo m.

If not distinct, then $\exists a, b \in \{0, \ldots, m-1\}$, $a \neq b$, where
$(ax \equiv bx \pmod{m}) \implies (a-b)x \equiv 0 \pmod{m}$
Or $(a-b)x = km$ for some integer k.

$gcd(x,m) = 1$
$\implies$ Prime factorization of m and x do not contain common primes.

Greatest Common Divisor and Inverses.

Thm:
If greatest common divisor of x and m, gcd(x,m), is 1, then x has a multiplicative inverse modulo m.

Proof $\implies$: The set $S = \{0x, 1x, \ldots, (m-1)x\}$ contains $y \equiv 1 \mod m$ if all distinct modulo m.

Pigenhole principle: Each of m numbers in S correspond to different one of m equivalence classes modulo m.
$\implies$ One must correspond to 1 modulo m.

If not distinct, then $\exists a, b \in \{0, \ldots, m-1\}$, $a \neq b$, where
$(ax \equiv bx \pmod{m}) \implies (a-b)x \equiv 0 \pmod{m}$
Or $(a-b)x = km$ for some integer k.

$gcd(x,m) = 1$
$\implies$ Prime factorization of m and x do not contain common primes.
$\implies$ $(a-b)$ factorization contains all primes in m's factorization.

Greatest Common Divisor and Inverses.

Thm:
If greatest common divisor of x and m, gcd(x,m), is 1, then x has a multiplicative inverse modulo m.

Proof $\implies$: The set $S = \{0x, 1x, \ldots, (m-1)x\}$ contains $y \equiv 1 \mod m$ if all distinct modulo m.

Pigenhole principle: Each of m numbers in S correspond to different one of m equivalence classes modulo m.
$\implies$ One must correspond to 1 modulo m.

If not distinct, then $\exists a, b \in \{0, \ldots, m-1\}$, $a \neq b$, where
$(ax \equiv bx \pmod{m}) \implies (a-b)x \equiv 0 \pmod{m}$
Or $(a-b)x = km$ for some integer k.

$gcd(x,m) = 1$
$\implies$ Prime factorization of m and x do not contain common primes.
$\implies$ $(a-b)$ factorization contains all primes in m's factorization.
So $(a-b)$ has to be multiple of m.

Greatest Common Divisor and Inverses.

Thm:
If greatest common divisor of x and m, gcd(x,m), is 1, then x has a multiplicative inverse modulo m.

Proof $\Longrightarrow$: The set $S = \{0x, 1x, \ldots, (m-1)x\}$ contains $y \equiv 1 \mod m$ if all distinct modulo m.

Pigenhole principle: Each of m numbers in S correspond to different one of m equivalence classes modulo m.
$\Longrightarrow$ One must correspond to 1 modulo m.

If not distinct, then $\exists a, b \in \{0, \ldots, m-1\}$, $a \neq b$, where
$(ax \equiv bx \pmod{m}) \Longrightarrow (a-b)x \equiv 0 \pmod{m}$
Or $(a-b)x = km$ for some integer k.

$gcd(x,m) = 1$
$\Longrightarrow$ Prime factorization of m and x do not contain common primes.
$\Longrightarrow$ $(a-b)$ factorization contains all primes in m's factorization.
So $(a-b)$ has to be multiple of m.
$\Longrightarrow$ $(a-b) \geq m$.

Greatest Common Divisor and Inverses.

Thm:
If greatest common divisor of x and m, gcd(x,m), is 1, then x has a multiplicative inverse modulo m.

Proof $\implies$: The set $S = \{0x, 1x, \ldots, (m-1)x\}$ contains $y \equiv 1 \mod m$ if all distinct modulo m.

Pigenhole principle: Each of m numbers in S correspond to different one of m equivalence classes modulo m.
$\implies$ One must correspond to 1 modulo m.

If not distinct, then $\exists a, b \in \{0, \ldots, m-1\}$, $a \neq b$, where
$(ax \equiv bx \pmod{m}) \implies (a-b)x \equiv 0 \pmod{m}$
Or $(a-b)x = km$ for some integer k.

$gcd(x,m) = 1$
$\implies$ Prime factorization of m and x do not contain common primes.
$\implies$ $(a-b)$ factorization contains all primes in m's factorization.
So $(a-b)$ has to be multiple of m.
$\implies (a-b) \geq m$. But $a, b \in \{0, ...m-1\}$.

Greatest Common Divisor and Inverses.

Thm:
If greatest common divisor of x and m, gcd(x,m), is 1, then x has a multiplicative inverse modulo m.

Proof $\implies$: The set $S = \{0x, 1x, \ldots, (m-1)x\}$ contains $y \equiv 1 \mod m$ if all distinct modulo m.

Pigenhole principle: Each of m numbers in S correspond to different one of m equivalence classes modulo m.
$\implies$ One must correspond to 1 modulo m.

If not distinct, then $\exists a, b \in \{0, \ldots, m-1\}$, $a \neq b$, where
$(ax \equiv bx \pmod{m}) \implies (a-b)x \equiv 0 \pmod{m}$
Or $(a-b)x = km$ for some integer k.

$gcd(x,m) = 1$
$\implies$ Prime factorization of m and x do not contain common primes.
$\implies$ $(a-b)$ factorization contains all primes in m's factorization.
So $(a-b)$ has to be multiple of m.
$\implies$ $(a-b) \geq m$. But $a, b \in \{0, ...m-1\}$. Contradiction.

Greatest Common Divisor and Inverses.

Thm:
If greatest common divisor of x and m, gcd(x,m), is 1, then x has a multiplicative inverse modulo m.

Proof $\implies$: The set $S = \{0x, 1x, \ldots, (m-1)x\}$ contains $y \equiv 1 \mod m$ if all distinct modulo m.

Pigenhole principle: Each of m numbers in S correspond to different one of m equivalence classes modulo m.
$\implies$ One must correspond to 1 modulo m.

If not distinct, then $\exists a, b \in \{0, \ldots, m-1\}$, $a \neq b$, where
$(ax \equiv bx \pmod{m}) \implies (a-b)x \equiv 0 \pmod{m}$
Or $(a-b)x = km$ for some integer k.

$gcd(x,m) = 1$
$\implies$ Prime factorization of m and x do not contain common primes.
$\implies$ $(a-b)$ factorization contains all primes in m's factorization.
So $(a-b)$ has to be multiple of m.
$\implies$ $(a-b) \geq m$. But $a, b \in \{0, ...m-1\}$. Contradiction. $\square$

Summary

Planar Coloring.

Summary

Planar Coloring.
  Induction.

Summary

Planar Coloring.

- Induction.
- Recoloring again.

Summary

Planar Coloring.
- Induction.
- Recoloring again.

Hypercubes.

Summary

Planar Coloring.
- Induction.
- Recoloring again.

Hypercubes.

Modular Arithmetic.

Summary

Planar Coloring.
- Induction.
- Recoloring again.

Hypercubes.

Modular Arithmetic.
- Another form of arithmetic.

Summary

Planar Coloring.
- Induction.
- Recoloring again.

Hypercubes.

Modular Arithmetic.
- Another form of arithmetic.
- Multiplicative inverses.

Summary

Planar Coloring.
  Induction.
  Recoloring again.

Hypercubes.

Modular Arithmetic.
  Another form of arithmetic.
  Multiplicative inverses.

Have a good week!