

# Disc 2b

Andy

UC Berkeley

June 26, 2018

# Mini Lecture: Euler's Formula

- 1  $v = \text{vertex}$ ,  $e = \text{edges}$ ,  $f = \text{faces}$ .

# Mini Lecture: Euler's Formula

- ①  $v = \text{vertex}, e = \text{edges}, f = \text{faces}.$
- ②  $v + f = 2 + e$

# Mini Lecture: Euler's Formula

- 1  $v$  = vertex,  $e$  = edges,  $f$  = faces.
- 2  $v + f = 2 + e$
- 3 Proof?

# Mini Lecture: Euler's Formula

- 1  $v$  = vertex,  $e$  = edges,  $f$  = faces.
- 2  $v + f = 2 + e$
- 3 Proof?
- 4 Base case. Some sort of tree.

# Mini Lecture: Euler's Formula

- 1  $v$  = vertex,  $e$  = edges,  $f$  = faces.
- 2  $v + f = 2 + e$
- 3 Proof?
- 4 Base case. Some sort of tree.
- 5 How many faces? edges? (assume  $v$  vertices)

# Mini Lecture: Euler's Formula

- 1  $v$  = vertex,  $e$  = edges,  $f$  = faces.
- 2  $v + f = 2 + e$
- 3 Proof?
- 4 Base case. Some sort of tree.
- 5 How many faces? edges? (assume  $v$  vertices)
- 6 2 faces,  $v - 1$  edges,  $v$  vertices

# Mini Lecture: Euler's Formula

- ①  $v$  = vertex,  $e$  = edges,  $f$  = faces.
- ②  $v + f = 2 + e$
- ③ Proof?
- ④ Base case. Some sort of tree.
- ⑤ How many faces? edges? (assume  $v$  vertices)
- ⑥ 2 faces,  $v - 1$  edges,  $v$  vertices
- ⑦  $v + 1 = 2 + v - 1$ . Base case is correct!



# Mini Lecture: Euler's Formula

- ①  $v$  = vertex,  $e$  = edges,  $f$  = faces.
- ②  $v + f = 2 + e$
- ③ Proof?
- ④ Base case. Some sort of tree.
- ⑤ How many faces? edges? (assume  $v$  vertices)
- ⑥ 2 faces,  $v - 1$  edges,  $v$  vertices
- ⑦  $v + 1 = 2 + v - 1$ . Base case is correct!
- ⑧ Assume some non-tree graph.

# Mini Lecture: Euler's Formula

- 1  $v$  = vertex,  $e$  = edges,  $f$  = faces.
- 2  $v + f = 2 + e$
- 3 Proof?
- 4 Base case. Some sort of tree.
- 5 How many faces? edges? (assume  $v$  vertices)
- 6 2 faces,  $v - 1$  edges,  $v$  vertices
- 7  $v + 1 = 2 + v - 1$ . Base case is correct!
- 8 Assume some non-tree graph.
- 9 Recursively remove edges until we have a tree and  $v + f = 2 + e$  holds

# Mini Lecture: Euler's Formula

- 1  $v$  = vertex,  $e$  = edges,  $f$  = faces.
- 2  $v + f = 2 + e$
- 3 Proof?
- 4 Base case. Some sort of tree.
- 5 How many faces? edges? (assume  $v$  vertices)
- 6 2 faces,  $v - 1$  edges,  $v$  vertices
- 7  $v + 1 = 2 + v - 1$ . Base case is correct!
- 8 Assume some non-tree graph.
- 9 Recursively remove edges until we have a tree and  $v + f = 2 + e$  holds
- 10 Add an edge back in. How much will  $v$ ,  $f$ ,  $e$  increment by?

# Mini Lecture: Euler's Formula

- ①  $v$  = vertex,  $e$  = edges,  $f$  = faces.
- ②  $v + f = 2 + e$
- ③ Proof?
- ④ Base case. Some sort of tree.
- ⑤ How many faces? edges? (assume  $v$  vertices)
- ⑥ 2 faces,  $v - 1$  edges,  $v$  vertices
- ⑦  $v + 1 = 2 + v - 1$ . Base case is correct!
- ⑧ Assume some non-tree graph.
- ⑨ Recursively remove edges until we have a tree and  $v + f = 2 + e$  holds
- ⑩ Add an edge back in. How much will  $v$ ,  $f$ ,  $e$  increment by?
- ⑪  $+0$  vertices,  $+1$  face,  $+1$  edge.

# Mini Lecture: Euler's Formula

- 1  $v = \text{vertex}$ ,  $e = \text{edges}$ ,  $f = \text{faces}$ .
- 2  $v + f = 2 + e$
- 3 Proof?
- 4 Base case. Some sort of tree.
- 5 How many faces? edges? (assume  $v$  vertices)
- 6 2 faces,  $v - 1$  edges,  $v$  vertices
- 7  $v + 1 = 2 + v - 1$ . Base case is correct!
- 8 Assume some non-tree graph.
- 9 Recursively remove edges until we have a tree and  $v + f = 2 + e$  holds
- 10 Add an edge back in. How much will  $v$ ,  $f$ ,  $e$  increment by?
- 11  $+0$  vertices,  $+1$  face,  $+1$  edge.
- 12 Euler's formula holds under induction!

# Mini Lecture: Euler's Formula p2

- 1 Side, face, edge.

# Mini Lecture: Euler's Formula p2

- ① Side, face, edge.
- ②  $Sides = 2e$ .

## Mini Lecture: Euler's Formula p2

- 1 Side, face, edge.
- 2 Sides= $2e$ .
- 3 How minimum number of sides for a face?



## Mini Lecture: Euler's Formula p2

- 1 Side, face, edge.
- 2 Sides=2e.
- 3 How minimum number of sides for a face?
- 4  $3f \leq 2e$

## Mini Lecture: Euler's Formula p2

- 1 Side, face, edge.
- 2 Sides=2e.
- 3 How minimum number of sides for a face?
- 4  $3f \leq 2e$
- 5  $v + f = 2 + e$ , or  $3v + 3f = 6 + 3e$

## Mini Lecture: Euler's Formula p2

- ① Side, face, edge.
- ②  $Sides = 2e$ .
- ③ How minimum number of sides for a face?
- ④  $3f \leq 2e$
- ⑤  $v + f = 2 + e$ , or  $3v + 3f = 6 + 3e$
- ⑥  $3v + 2e \geq 6 + 3e$ .

## Mini Lecture: Euler's Formula p2

- ① Side, face, edge.
- ② Sides=2e.
- ③ How minimum number of sides for a face?
- ④  $3f \leq 2e$
- ⑤  $v + f = 2 + e$ , or  $3v + 3f = 6 + 3e$
- ⑥  $3v + 2e \geq 6 + 3e$ .
- ⑦  $e \leq 3v - 6$

## Mini Lecture: Euler's Formula p2

- ① Side, face, edge.
- ② Sides=2e.
- ③ How minimum number of sides for a face?
- ④  $3f \leq 2e$
- ⑤  $v + f = 2 + e$ , or  $3v + 3f = 6 + 3e$
- ⑥  $3v + 2e \geq 6 + 3e$ .
- ⑦  $e \leq 3v - 6$
- ⑧ Sanity check  $K_5$ . 5 vertices, 10 edges.  $10 \leq 9$ . Not planar.

## Mini Lecture: Euler's Formula p2

- 1 Side, face, edge.
- 2 Sides=2e.
- 3 How minimum number of sides for a face?
- 4  $3f \leq 2e$
- 5  $v + f = 2 + e$ , or  $3v + 3f = 6 + 3e$
- 6  $3v + 2e \geq 6 + 3e$ .
- 7  $e \leq 3v - 6$
- 8 Sanity check  $K_5$ . 5 vertices, 10 edges.  $10 \leq 9$ . Not planar.
- 9 Sanity check  $K_{3,3}$  has 9 edges, 6 vertices  $9 \leq 12$  is true?

## Mini Lecture: Euler's Formula p2

- ① Side, face, edge.
- ②  $Sides = 2e$ .
- ③ How minimum number of sides for a face?
- ④  $3f \leq 2e$
- ⑤  $v + f = 2 + e$ , or  $3v + 3f = 6 + 3e$
- ⑥  $3v + 2e \geq 6 + 3e$ .
- ⑦  $e \leq 3v - 6$
- ⑧ Sanity check  $K_5$ . 5 vertices, 10 edges.  $10 \leq 9$ . Not planar.
- ⑨ Sanity check  $K_{3,3}$  has 9 edges, 6 vertices  $9 \leq 12$  is true?
- ⑩ If your graph is planar,  $e \leq 3v - 6$  is true. If graph violates  $e \leq 3v - 6$ , graph is not planar. If you do not violate  $e \leq 3v - 6$ , graph is not necessarily planar.

## Mini Lecture: Euler's Formula p2

- ① Side, face, edge.
- ②  $Sides = 2e$ .
- ③ How minimum number of sides for a face?
- ④  $3f \leq 2e$
- ⑤  $v + f = 2 + e$ , or  $3v + 3f = 6 + 3e$
- ⑥  $3v + 2e \geq 6 + 3e$ .
- ⑦  $e \leq 3v - 6$
- ⑧ Sanity check  $K_5$ . 5 vertices, 10 edges.  $10 \leq 9$ . Not planar.
- ⑨ Sanity check  $K_{3,3}$  has 9 edges, 6 vertices  $9 \leq 12$  is true?
- ⑩ If your graph is planar,  $e \leq 3v - 6$  is true. If graph violates  $e \leq 3v - 6$ , graph is not planar. If you do not violate  $e \leq 3v - 6$ , graph is not necessarily planar.
- ⑪ Planar graphs tend to be sparse (number of edges grows proportionally to number of vertices).



# Mini Lecture: Euler's Formula p3

- 1 Side, face, edge.

# Mini Lecture: Euler's Formula p3

- 1 Side, face, edge.
- 2  $Sides=2e$ .

## Mini Lecture: Euler's Formula p3

- 1 Side, face, edge.
- 2  $Sides = 2e$ .
- 3 How minimum number of sides for a face for a bipartite graph?

# Mini Lecture: Euler's Formula p3

- ① Side, face, edge.
- ② Sides=2e.
- ③ How minimum number of sides for a face for a bipartite graph?
- ④  $4f \leq 2e$

## Mini Lecture: Euler's Formula p3

- ① Side, face, edge.
- ②  $Sides = 2e$ .
- ③ How minimum number of sides for a face for a bipartite graph?
- ④  $4f \leq 2e$
- ⑤  $v + f = 2 + e$ , or  $4v + 4f = 8 + 4e$

## Mini Lecture: Euler's Formula p3

- 1 Side, face, edge.
- 2 Sides=2e.
- 3 How minimum number of sides for a face for a bipartite graph?
- 4  $4f \leq 2e$
- 5  $v + f = 2 + e$ , or  $4v + 4f = 8 + 4e$
- 6  $4v + 2e \geq 8 + 4e$ .

## Mini Lecture: Euler's Formula p3

- ① Side, face, edge.
- ②  $\text{Sides} = 2e$ .
- ③ How minimum number of sides for a face for a bipartite graph?
- ④  $4f \leq 2e$
- ⑤  $v + f = 2 + e$ , or  $4v + 4f = 8 + 4e$
- ⑥  $4v + 2e \geq 8 + 4e$ .
- ⑦  $e \leq 2v - 4$

## Mini Lecture: Euler's Formula p3

- ① Side, face, edge.
- ②  $\text{Sides} = 2e$ .
- ③ How minimum number of sides for a face for a bipartite graph?
- ④  $4f \leq 2e$
- ⑤  $v + f = 2 + e$ , or  $4v + 4f = 8 + 4e$
- ⑥  $4v + 2e \geq 8 + 4e$ .
- ⑦  $e \leq 2v - 4$
- ⑧  $K_{3,3}$  has 9 edges, 6 vertices.  $9 \leq 8$  is false!



# Mini Lecture: bipartite fix

- 1 Side, face, edge.

# Mini Lecture: bipartite fix

- 1 Side, face, edge.
- 2 Sides= $2e$ .

# Mini Lecture: bipartite fix

- 1 Side, face, edge.
- 2 Sides= $2e$ .
- 3 How minimum number of sides for a face for a bipartite graph?

# Mini Lecture: bipartite fix

- 1 Side, face, edge.
- 2 Sides= $2e$ .
- 3 How minimum number of sides for a face for a bipartite graph?
- 4  $4f \leq 2e$

# Mini Lecture: bipartite fix

- 1 Side, face, edge.
- 2 Sides=2e.
- 3 How minimum number of sides for a face for a bipartite graph?
- 4  $4f \leq 2e$
- 5  $v + f = 2 + e$ , or  $4v + 4f = 8 + 4e$

## Mini Lecture: bipartite fix

- 1 Side, face, edge.
- 2 Sides=2e.
- 3 How minimum number of sides for a face for a bipartite graph?
- 4  $4f \leq 2e$
- 5  $v + f = 2 + e$ , or  $4v + 4f = 8 + 4e$
- 6  $4v + 2e \geq 8 + 4e$ .

## Mini Lecture: bipartite fix

- ① Side, face, edge.
- ②  $\text{Sides} = 2e$ .
- ③ How minimum number of sides for a face for a bipartite graph?
- ④  $4f \leq 2e$
- ⑤  $v + f = 2 + e$ , or  $4v + 4f = 8 + 4e$
- ⑥  $4v + 2e \geq 8 + 4e$ .
- ⑦  $e \leq 2v - 4$

## Mini Lecture: bipartite fix

- ① Side, face, edge.
- ② Sides=2e.
- ③ How minimum number of sides for a face for a bipartite graph?
- ④  $4f \leq 2e$
- ⑤  $v + f = 2 + e$ , or  $4v + 4f = 8 + 4e$
- ⑥  $4v + 2e \geq 8 + 4e$ .
- ⑦  $e \leq 2v - 4$
- ⑧  $K_{3,3}$  has 9 edges, 6 vertices.  $9 \leq 8$  is false!



# Mini Lecture: Slides 17, 18 lecture 5

- 1 Side, face, edge.

## Mini Lecture: Slides 17, 18 lecture 5

- 1 Side, face, edge.
- 2 Sides= $2e$ .

## Mini Lecture: Slides 17, 18 lecture 5

- ① Side, face, edge.
- ②  $Sides = 2e$ .
- ③ How minimum number of sides for a face for a bipartite graph?

## Mini Lecture: Slides 17, 18 lecture 5

- ① Side, face, edge.
- ② Sides=2e.
- ③ How minimum number of sides for a face for a bipartite graph?
- ④  $4f \leq 2e$

## Mini Lecture: Slides 17, 18 lecture 5

- ① Side, face, edge.
- ②  $\text{Sides} = 2e$ .
- ③ How minimum number of sides for a face for a bipartite graph?
- ④  $4f \leq 2e$
- ⑤  $v + f = 2 + e$ , or  $4v + 4f = 8 + 4e$

## Mini Lecture: Slides 17, 18 lecture 5

- ① Side, face, edge.
- ② Sides=2e.
- ③ How minimum number of sides for a face for a bipartite graph?
- ④  $4f \leq 2e$
- ⑤  $v + f = 2 + e$ , or  $4v + 4f = 8 + 4e$
- ⑥  $4v + 2e \geq 8 + 4e$ .

## Mini Lecture: Slides 17, 18 lecture 5

- ① Side, face, edge.
- ② Sides=2e.
- ③ How minimum number of sides for a face for a bipartite graph?
- ④  $4f \leq 2e$
- ⑤  $v + f = 2 + e$ , or  $4v + 4f = 8 + 4e$
- ⑥  $4v + 2e \geq 8 + 4e$ .
- ⑦  $e \leq 2v - 4$

## Mini Lecture: Slides 17, 18 lecture 5

- ① Side, face, edge.
- ②  $\text{Sides} = 2e$ .
- ③ How minimum number of sides for a face for a bipartite graph?
- ④  $4f \leq 2e$
- ⑤  $v + f = 2 + e$ , or  $4v + 4f = 8 + 4e$
- ⑥  $4v + 2e \geq 8 + 4e$ .
- ⑦  $e \leq 2v - 4$
- ⑧  $K_{3,3}$  has 9 edges, 6 vertices.  $9 \leq 8$  is false!



# Modular Spaces

- 1 In modulo  $N$ , simplest form ranges from  $0, \dots, N - 1$

# Modular Spaces

- 1 In modulo  $N$ , simplest form ranges from  $0, \dots, N - 1$
- 2  $x \equiv 0 \bmod N$ . What is significant about  $x$ ?

# Modular Spaces

- ① In modulo  $N$ , simplest form ranges from  $0, \dots, N - 1$
- ②  $x \equiv 0 \bmod N$ . What is significant about  $x$ ?
- ③ Everything except division works like in regular math

# Modular Inverses

- 1 We want to find  $a^{-1} \bmod N$

# Modular Inverses

- 1 We want to find  $a^{-1} \bmod N$
- 2 First verify that  $\gcd(a, N) = 1$

# Modular Inverses

- 1 We want to find  $a^{-1} \bmod N$
- 2 First verify that  $\gcd(a, N) = 1$
- 3 Then use extended gcd algorithm.

# Modular Inverses

- 1 We want to find  $a^{-1} \bmod N$
- 2 First verify that  $\gcd(a, N) = 1$
- 3 Then use extended gcd algorithm.
- 4  $1 = k * a + j * N$

# Modular Inverses

- 1 We want to find  $a^{-1} \bmod N$
- 2 First verify that  $\gcd(a, N) = 1$
- 3 Then use extended gcd algorithm.
- 4  $1 = k * a + j * N$
- 5 From here, which variable is the modular inverse of  $a$ ?



# Problem 1c

## Problem

Prove that any graph with maximum degree  $d$  can be edge coloured with  $2d - 1$  colours.

- 1 **Base case:** Max degree 1. We need 1 colour. ✓

# Problem 1c

## Problem

Prove that any graph with maximum degree  $d$  can be edge coloured with  $2d - 1$  colours.

- 1 **Base case:** Max degree 1. We need 1 colour. ✓
- 2 **Inductive Hypo:** Assume a max degree  $k - 1$  graph is colourable with  $2k - 3$  colors, for some  $k - 1$ .

# Problem 1c

## Problem

Prove that any graph with maximum degree  $d$  can be edge coloured with  $2d - 1$  colours.

- ① **Base case:** Max degree 1. We need 1 colour. ✓
- ② **Inductive Hypo:** Assume a max degree  $k - 1$  graph is colourable with  $2k - 3$  colors, for some  $k - 1$ .
- ③ **Inductive Step:** We need to try colouring a max degree  $k$ .

# Problem 1c

## Problem

Prove that any graph with maximum degree  $d$  can be edge coloured with  $2d - 1$  colours.

- 1 **Base case:** Max degree 1. We need 1 colour. ✓
- 2 **Inductive Hypo:** Assume a max degree  $k - 1$  graph is colourable with  $2k - 3$  colors, for some  $k - 1$ .
- 3 **Inductive Step:** We need to try colouring a max degree  $k$ .
- 4 Take the largest degree node, and remove an edge. Graph is now colourable in  $2k - 3$

# Problem 1c

## Problem

Prove that any graph with maximum degree  $d$  can be edge coloured with  $2d - 1$  colours.

- 1 **Base case:** Max degree 1. We need 1 colour. ✓
- 2 **Inductive Hypo:** Assume a max degree  $k - 1$  graph is colourable with  $2k - 3$  colors, for some  $k - 1$ .
- 3 **Inductive Step:** We need to try colouring a max degree  $k$ .
- 4 Take the largest degree node, and remove an edge. Graph is now colourable in  $2k - 3$
- 5 Max degree node is currently  $2(k - 1)$  degree. That means  $2k - 2$  colours are being used by this node.

# Problem 1c

## Problem

Prove that any graph with maximum degree  $d$  can be edge coloured with  $2d - 1$  colours.

- 1 **Base case:** Max degree 1. We need 1 colour. ✓
- 2 **Inductive Hypo:** Assume a max degree  $k - 1$  graph is colourable with  $2k - 3$  colors, for some  $k - 1$ .
- 3 **Inductive Step:** We need to try colouring a max degree  $k$ .
- 4 Take the largest degree node, and remove an edge. Graph is now colourable in  $2k - 3$
- 5 Max degree node is currently  $2(k - 1)$  degree. That means  $2k - 2$  colours are being used by this node.
- 6 Add the removed edge back in, and give it the  $2k - 1$ st color (new color).

# Problem 1c

## Problem

Prove that any graph with maximum degree  $d$  can be edge coloured with  $2d - 1$  colours.

- 1 **Base case:** Max degree 1. We need 1 colour. ✓
- 2 **Inductive Hypo:** Assume a max degree  $k - 1$  graph is colourable with  $2k - 3$  colors, for some  $k - 1$ .
- 3 **Inductive Step:** We need to try colouring a max degree  $k$ .
- 4 Take the largest degree node, and remove an edge. Graph is now colourable in  $2k - 3$
- 5 Max degree node is currently  $2(k - 1)$  degree. That means  $2k - 2$  colours are being used by this node.
- 6 Add the removed edge back in, and give it the  $2k - 1$ st color (new color).
- 7 No conflicts!

# Problem 1d

## Problem

Prove that any tree with maximum degree  $d$  can be edge coloured with  $d$  colours.

- 1 **Base case:** Max degree 0. We need 0 colours. ✓



# Problem 1d

## Problem

Prove that any tree with maximum degree  $d$  can be edge coloured with  $d$  colours.

- 1 **Base case:** Max degree 0. We need 0 colours. ✓
- 2 **Inductive Hypo:** Assume a max degree  $k$  graph is colourable with  $k$  colors, for some  $k$ .

# Problem 1d

## Problem

Prove that any tree with maximum degree  $d$  can be edge coloured with  $d$  colours.

- 1 **Base case:** Max degree 0. We need 0 colours. ✓
- 2 **Inductive Hypo:** Assume a max degree  $k$  graph is colourable with  $k$  colors, for some  $k$ .
- 3 **Inductive Step:** We need to try colouring a max degree  $k + 1$ .

# Problem 1d

## Problem

Prove that any tree with maximum degree  $d$  can be edge coloured with  $d$  colours.

- 1 **Base case:** Max degree 0. We need 0 colours. ✓
- 2 **Inductive Hypo:** Assume a max degree  $k$  graph is colourable with  $k$  colors, for some  $k$ .
- 3 **Inductive Step:** We need to try colouring a max degree  $k + 1$ .
- 4 Remove leaves until the maximum degree is  $k$ . Graph is now colourable in  $k$

# Problem 1d

## Problem

Prove that any tree with maximum degree  $d$  can be edge coloured with  $d$  colours.

- 1 **Base case:** Max degree 0. We need 0 colours. ✓
- 2 **Inductive Hypo:** Assume a max degree  $k$  graph is colourable with  $k$  colors, for some  $k$ .
- 3 **Inductive Step:** We need to try colouring a max degree  $k + 1$ .
- 4 Remove leaves until the maximum degree is  $k$ . Graph is now colourable in  $k$
- 5 The node the leaf was connected to currently has  $k - 1$  degree, which means there is a free color.

# Problem 1d

## Problem

Prove that any tree with maximum degree  $d$  can be edge coloured with  $d$  colours.

- 1 **Base case:** Max degree 0. We need 0 colours. ✓
- 2 **Inductive Hypo:** Assume a max degree  $k$  graph is colourable with  $k$  colors, for some  $k$ .
- 3 **Inductive Step:** We need to try colouring a max degree  $k + 1$ .
- 4 Remove leaves until the maximum degree is  $k$ . Graph is now colourable in  $k$
- 5 The node the leaf was connected to currently has  $k - 1$  degree, which means there is a free color.
- 6 Add the removed leaf back in, and give it the  $k$ th color (new color).

# Problem 1d

## Problem

Prove that any tree with maximum degree  $d$  can be edge coloured with  $d$  colours.

- 1 **Base case:** Max degree 0. We need 0 colours. ✓
- 2 **Inductive Hypo:** Assume a max degree  $k$  graph is colourable with  $k$  colors, for some  $k$ .
- 3 **Inductive Step:** We need to try colouring a max degree  $k + 1$ .
- 4 Remove leaves until the maximum degree is  $k$ . Graph is now colourable in  $k$
- 5 The node the leaf was connected to currently has  $k - 1$  degree, which means there is a free color.
- 6 Add the removed leaf back in, and give it the  $k$ th color (new color).
- 7 No conflicts!

## Problem 2

- 1 You need to prove both directions!

# Problem 3a

## Problem

$$9x \equiv 1 \pmod{11}$$

- 1 We need  $9^{-1} \pmod{11}$



# Problem 3a

## Problem

$$9x \equiv 1 \pmod{11}$$

- 1 We need  $9^{-1} \pmod{11}$
- 2 First verify  $\gcd(9, 11) = 1$ .

# Problem 3a

## Problem

$$9x \equiv 1 \pmod{11}$$

- 1 We need  $9^{-1} \pmod{11}$
- 2 First verify  $\gcd(9, 11) = 1$ .
- 3  $\gcd(11, 9)$

# Problem 3a

## Problem

$$9x \equiv 1 \pmod{11}$$

- ① We need  $9^{-1} \pmod{11}$
- ② First verify  $\gcd(9, 11) = 1$ .
- ③  $\gcd(11, 9)$
- ④  $\gcd(9, 2)$

# Problem 3a

## Problem

$$9x \equiv 1 \pmod{11}$$

- 1 We need  $9^{-1} \pmod{11}$
- 2 First verify  $\gcd(9, 11) = 1$ .
- 3  $\gcd(11, 9)$
- 4  $\gcd(9, 2)$
- 5  $\gcd(2, 1)$

# Problem 3a

## Problem

$$9x \equiv 1 \pmod{11}$$

- ① We need  $9^{-1} \pmod{11}$
- ② First verify  $\gcd(9, 11) = 1$ .
- ③  $\gcd(11, 9)$
- ④  $\gcd(9, 2)$
- ⑤  $\gcd(2, 1)$
- ⑥  $\gcd(1, 0)$

# Problem 3a

## Problem

$$9x \equiv 1 \pmod{11}$$

- ① We need  $9^{-1} \pmod{11}$
- ② First verify  $\gcd(9, 11) = 1$ .
- ③  $\gcd(11, 9)$
- ④  $\gcd(9, 2)$
- ⑤  $\gcd(2, 1)$
- ⑥  $\gcd(1, 0)$
- ⑦  $\gcd(a, b) = k$  means  
 $k = m * a + n * b$ .

## Problem 3a

### Problem

$$9x \equiv 1 \pmod{11}$$

- ① We need  $9^{-1} \pmod{11}$
  - ② First verify  $\gcd(9, 11) = 1$ .
  - ③  $\gcd(11, 9)$
  - ④  $\gcd(9, 2)$
  - ⑤  $\gcd(2, 1)$
  - ⑥  $\gcd(1, 0)$
  - ⑦  $\gcd(a, b) = k$  means  
 $k = m * a + n * b$ .
- ⑦  $= kmeansk = m * a + n * b$ .  
This is e-gcd!

# Problem 3a

## Problem

$$9x \equiv 1 \pmod{11}$$

- ① We need  $9^{-1} \pmod{11}$
- ② First verify  $\gcd(9, 11) = 1$ .
- ③  $\gcd(11, 9)$
- ④  $\gcd(9, 2)$
- ⑤  $\gcd(2, 1)$
- ⑥  $\gcd(1, 0)$   $= 1 = 1 * 1 + 0 * 0$
- ⑦  $\gcd(a, b) = k$  means  
 $k = m * a + n * b$ .



# Problem 3a

## Problem

$$9x \equiv 1 \pmod{11}$$

- ① We need  $9^{-1} \pmod{11}$
- ② First verify  $\gcd(9, 11) = 1$ .
- ③  $\gcd(11, 9)$
- ④  $\gcd(9, 2)$
- ⑤  $\gcd(2, 1)$
- ⑥  $\gcd(1, 0)$
- ⑦  $\gcd(a, b) = k$  means  
 $k = m * a + n * b$ .

$$\textcircled{5} = 1 = 0 * 2 + 1 * 1$$

# Problem 3a

## Problem

$$9x \equiv 1 \pmod{11}$$

- ① We need  $9^{-1} \pmod{11}$
- ② First verify  $\gcd(9, 11) = 1$ .
- ③  $\gcd(11, 9)$
- ④  $\gcd(9, 2)$  ④  $= 1 = 1 * 9 + (-4) * 2$
- ⑤  $\gcd(2, 1)$
- ⑥  $\gcd(1, 0)$
- ⑦  $\gcd(a, b) = k$  means  
 $k = m * a + n * b$ .

# Problem 3a

## Problem

$$9x \equiv 1 \pmod{11}$$

- ① We need  $9^{-1} \pmod{11}$
  - ② First verify  $\gcd(9, 11) = 1$ .
  - ③  $\gcd(11, 9)$
  - ④  $\gcd(9, 2)$
  - ⑤  $\gcd(2, 1)$
  - ⑥  $\gcd(1, 0)$
  - ⑦  $\gcd(a, b) = k$  means  
 $k = m * a + n * b$ .
- ③  $= 1 = (-4) * 11 + 5 * 9$

# Problem 3a

## Problem

$$9x \equiv 1 \pmod{11}$$

- ① We need  $9^{-1} \pmod{11}$
- ② First verify  $\gcd(9, 11) = 1$ .
- ③  $\gcd(11, 9)$
- ④  $\gcd(9, 2)$
- ⑤  $\gcd(2, 1)$
- ⑥  $\gcd(1, 0)$
- ⑦  $\gcd(a, b) = k$  means  
 $k = m * a + n * b$ .
- ⑧ First verify  $\gcd(9, 11) = 1$ .

# Problem 3a

## Problem

$$9x \equiv 1 \pmod{11}$$

- ① We need  $9^{-1} \pmod{11}$
- ② First verify  $\gcd(9, 11) = 1$ .
- ③  $\gcd(11, 9)$
- ④  $\gcd(9, 2)$
- ⑤  $\gcd(2, 1)$
- ⑥  $\gcd(1, 0)$
- ⑦  $\gcd(a, b) = k$  means  
 $k = m * a + n * b$ .

- ① We need  $9^{-1} \pmod{11}$