Engaging Activities & Ideas for Teaching Discrete Math

André Mathurin
Bellarmine College Preparatory (San Jose, CA)

Looking for ways to engage students in authentic mathematics regardless of their algebraic competence? Come see how graph theory, number theory, and cryptography can provide realistic, understandable opportunities for students to engage in rich mathematics regardless of their algebra ability.

Contact & Resource Information

amathurin@bcp.org

http://www.tinyurl.com/amathurin-NCTM2012

⓿ WARM-UP ACVITITY

BIG IDEAS: Identifying Patterns, Making Connections, Algorithms

The letters in the phrase "What is Discrete Math" have been scrambled and placed in groups of three.

Scramble #1:	H T A	T E M	E R C	D I S	S I T	W H A
Scramble #2:	W E T	H R E	A C M	T S A	I I T	S D H
Scramble #3:	S T E	D M A	I T T	H A W	R E I	S C H
Scramble #4:	A H W	T M E	I A T	S T E	D H R	I S C

One of the scrambles was generated by randomly selecting the message letters from a hat while the other three scrambles were generated using an algorithm based on a basic geometrical concept.

Identify which is the random selection scramble and explain how/why you arrived at your decision.

⓿ WARM-UP ACVITITY

BIG IDEAS: Identifying Patterns, Making Connections, Algorithms

The letters in the phrase "What is Discrete Math" have been scrambled and placed in groups of three.

Scramble #1:	H T A	T E M	E R C	D I S	S I T	W H A
Scramble #2:	W E T	H R E	A C M	T S A	I I T	S D H
Scramble #3:	S T E	D M A	I T T	H A W	R E I	S C H
Scramble #4:	A H W	T M E	I A T	S T E	D H R	I S C

One of the scrambles was generated by randomly selecting the message letters from a hat while the other three scrambles were generated using an algorithm based on a basic geometrical concept.

Identify which is the random selection scramble and explain how/why you arrived at your decision.

Does this help?

#1	#2	#3	#4
H T A	W E T	S T E	A H W
T E M	H R E	D M A	T M E
E R C	A C M	I T T	I A T
D I S	T S A	H A W	S T E
S I T	I I T	R E I	D H R
W H A	S D H	S C H	I S C

⓿ WARM-UP ACVITITY

BIG IDEAS: Identifying Patterns, Making Connections, Algorithms

The letters in the phrase "What is Discrete Math" have been scrambled and placed in groups of three.

Scramble #1:	H T A	T E M	E R C	D I S	S I T	W H A
Scramble #2:	W E T	H R E	A C M	T S A	I I T	S D H
Scramble #3:	S T E	D M A	I T T	H A W	R E I	S C H
Scramble #4:	A H W	T M E	I A T	S T E	D H R	I S C

One of the scrambles was generated by randomly selecting the message letters from a hat while the other three scrambles were generated using an algorithm based on a basic geometrical concept.

Some Connections/Ideas for Extensions

- How would using other shapes affect the scrambling algorithm? (Geometry)
- How many total possible ways are there for scrambling the letters in the phrase? (Combinatorics)
- What are some modifications could you make to the scrambling algorithm? (Cryptography)

Preliminaries

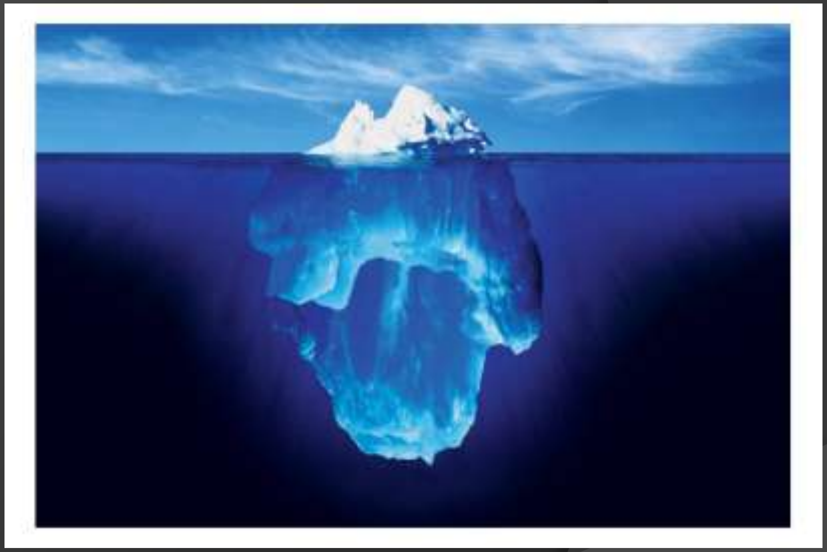
- Goals
- Format
- Background/Context

Preliminaries

- Goals
  - ✓ *Spark Interest in Exploring More*
  - ✓ *Highlight "Big-Ticket" Mathematical Ideas*
  - ✓ *Provide Ideas for Links & Extensions*
- Format
- Background/Context

Preliminaries

- Goals
  - ✓ *Spark Interest in Exploring More*
  - ✓ *Highlight "Big-Ticket" Mathematical Ideas*
  - ✓ *Provide Ideas for Links & Extensions*
- Format
- Background/Context



Preliminaries

- Goals
- Format
  - ✓ *Graph Theory, Number Theory, Cryptography*
  - ✓ *Quick Introductory Activity*
  - ✓ *More In-Depth Investigation Activity*
  - ✓ *Discuss Variations for Implementation*
- Background/Context

Preliminaries

- ✷ Goals
- ✷ Format
- ✷ Background/Context
  - ✓ *Evolution & Relevance*
  - ✓ *Unknown & Undervalued*
  - ✓ *Meaningful & Timely*

NATIONAL COUNCIL OF TEACHERS OF MATHEMATICS

MATHEMATICAL ASSOCIATION OF AMERICA

Calculus

A Joint Position Statement of the Mathematical Association of America and the National Council of Teachers of Mathematics

Question: How should secondary schools and colleges envision calculus as the course that sits astride the transition from secondary to postsecondary mathematics for most students heading into mathematically intensive careers?

MAA/NCTM Position

Although calculus can play an important role in secondary school, the ultimate goal of the K–12 mathematics curriculum should not be to get students into and through a course in calculus by twelfth grade but to have established the mathematical foundation that will enable students to pursue whatever course of study interests them when they get to college. The college curriculum should offer students an experience that is new and engaging, broadening their understanding of the world of mathematics while strengthening their mastery of tools that they will need if they choose to pursue a mathematically intensive discipline.

❶ QUICK START ➢➢ ANIMAL SURVIVAL

BIG IDEAS: Visual Representations, Equivalence, Appearance vs. Structure

source of this activity: http://www.colorado.edu/education/DMP

The zoo keeper of a major zoo wants to redo the zoo in such a way that the animals live together in their natural habitat. Unfortunately, it is not possible to put all the animals together in one location because some are predators of others. The X marks in the chart at right show a predator-prey relationship, so those pair of animals cannot be safely placed in the same location.

	A	B	C	D	E	F	G	H
A		X			X			
B	X			X			X	
C								X
D		X				X		
E	X							
F				X				
G		X						
H			X					

Create a graph that represents the relationships indicated in the chart.

❶ QUICK START ≫ ANIMAL SURVIVAL

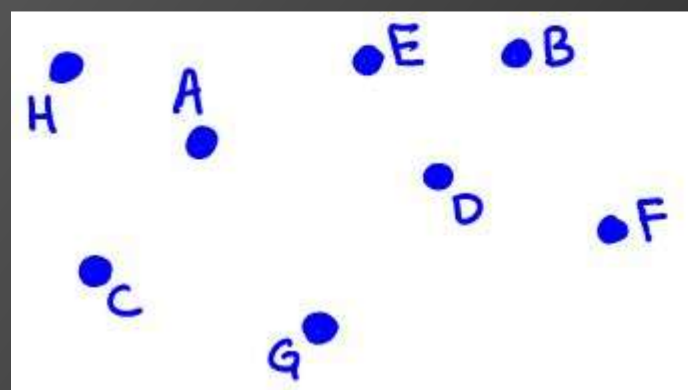
BIG IDEAS: Visual Representations, Equivalence, Appearance vs. Structure

source of this activity: http://www.colorado.edu/education/DMP

The zoo keeper of a major zoo wants to redo the zoo in such a way that the animals live together in their natural habitat. Unfortunately, it is not possible to put all the animals together in one location because some are predators of others. The X marks in the chart at right show a predator-prey relationship, so those pair of animals cannot be safely placed in the same location.

	A	B	C	D	E	F	G	H
A		X			X			
B	X			X			X	
C								X
D		X				X		
E	X							
F				X				
G		X						
H			X					

Create a graph that represents the relationships indicated in the chart.



❶ QUICK START ➤➤ ANIMAL SURVIVAL

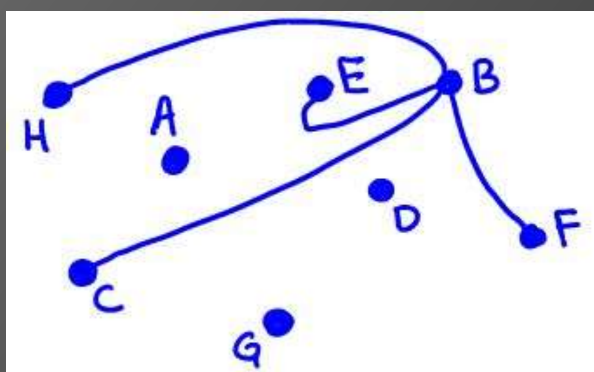
BIG IDEAS: Visual Representations, Equivalence, Appearance vs. Structure

source of this activity: http://www.colorado.edu/education/DMP

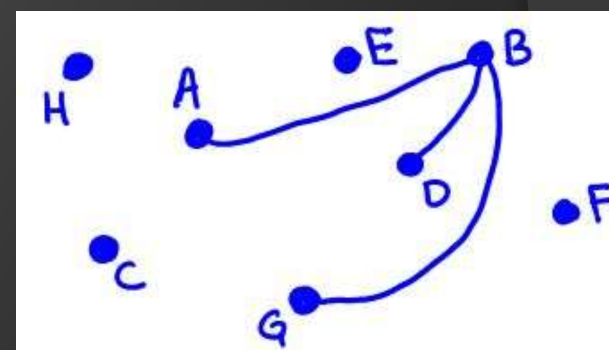
The zoo keeper of a major zoo wants to redo the zoo in such a way that the animals live together in their natural habitat. Unfortunately, it is not possible to put all the animals together in one location because some are predators of others. The X marks in the chart at right show a predator-prey relationship, so those pair of animals cannot be safely placed in the same location.

Create a graph that represents the relationships indicated in the chart.

	A	B	C	D	E	F	G	H
A		X			X			
B	X			X			X	
C								X
D		X				X		
E	X							
F				X				
G		X						
H			X					



What's the Difference?



❶ QUICK START ≻≻ ANIMAL SURVIVAL

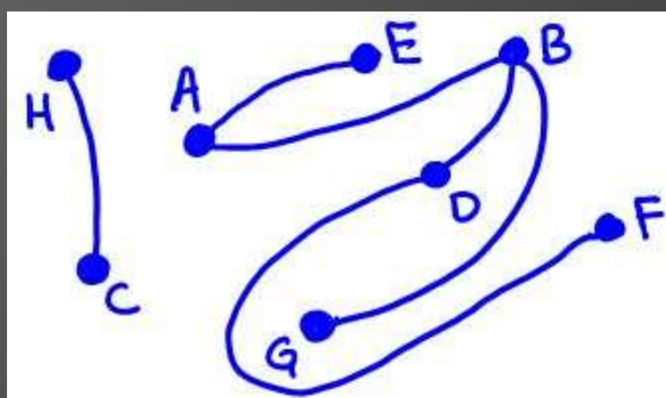
BIG IDEAS: Visual Representations, Equivalence, Appearance vs. Structure

source of this activity: http://www.colorado.edu/education/DMP

The zoo keeper of a major zoo wants to redo the zoo in such a way that the animals live together in their natural habitat. Unfortunately, it is not possible to put all the animals together in one location because some are predators of others. The X marks in the chart at right show a predator-prey relationship, so those pair of animals cannot be safely placed in the same location.

	A	B	C	D	E	F	G	H
A		X			X			
B	X			X			X	
C								X
D		X				X		
E	X							
F				X				
G		X						
H			X					

Create a graph that represents the relationships indicated in the chart.



Is Your Graph the Same as My Graph?

❶ QUICK START ➢➢ ANIMAL SURVIVAL

BIG IDEAS: Visual Representations, Equivalence, Appearance vs. Structure

source of this activity: http://www.colorado.edu/education/DMP

The zoo keeper of a major zoo wants to redo the zoo in such a way that the animals live together in their natural habitat. Unfortunately, it is not possible to put all the animals together in one location because some are predators of others. The X marks in the chart at right show a predator-prey relationship, so those pair of animals cannot be safely placed in the same location.

Create a graph that represents the relationships indicated in the chart.

	A	B	C	D	E	F	G	H
A		X			X			
B	X			X			X	
C								X
D		X				X		
E	X							
F				X				
G		X						
H			X					

Some Connections/Ideas for Extensions

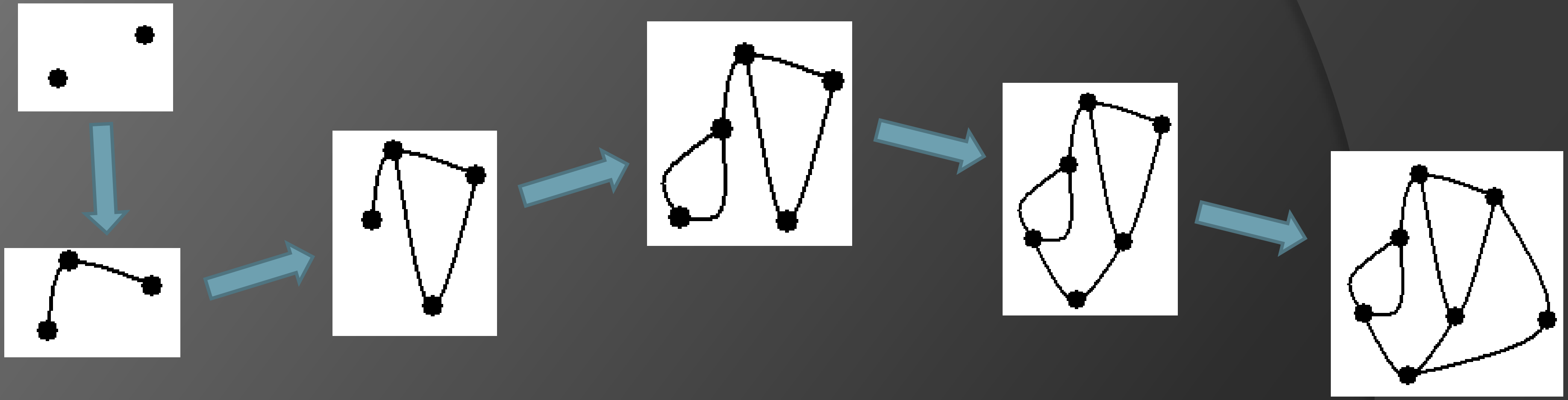
- What is the minimum number of locations required to safely house all of the animals? (4-Color Problem)
- If the graph represented a computer network, what are the most crucial edges? (Connectivity)
- If you needed to deliver items to 6 different classrooms, what would be the most efficient route? (Flow)

❷ # ACTIVITY: SPROUTS

BIG IDEAS: Quantifiable Differences, Data Collection & Analysis, Pattern Recognition

The Game of Sprouts was invented in 1967 by Princeton mathematician John H. Conway and by Michael S. Paterson, when both were at the University of Cambridge in the UK.

Start of Game



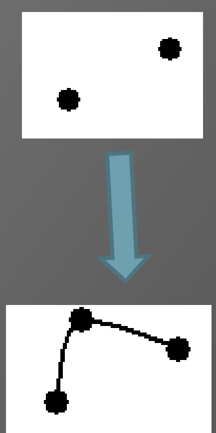
End of Game

❷ ACTIVITY: SPROUTS

BIG IDEAS: Quantifiable Differences, Data Collection & Analysis, Pattern Recognition

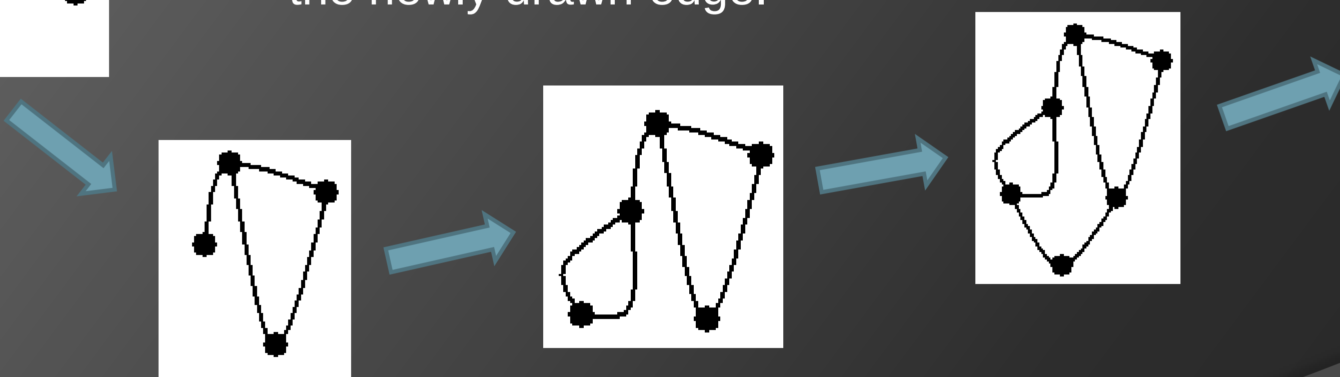
The Game of Sprouts was invented in 1967 by Princeton mathematician John H. Conway and by Michael S. Paterson, when both were at the University of Cambridge in the UK.

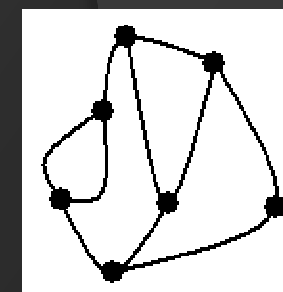
Start of Game



Rules for Playing Sprouts

1. The winner is the player who makes the last move.
2. No vertex have more than 3 edges.
3. A move starts by drawing an edge such that:
    - the edge starts and ends at a vertex
    - the edge does not cross an existing edge
4. The move ends by placing a new vertex along the newly drawn edge.





End of Game

❷ **ACTIVITY: SPROUTS**

BIG IDEAS: Quantifiable Differences, Data Collection & Analysis, Pattern Recognition

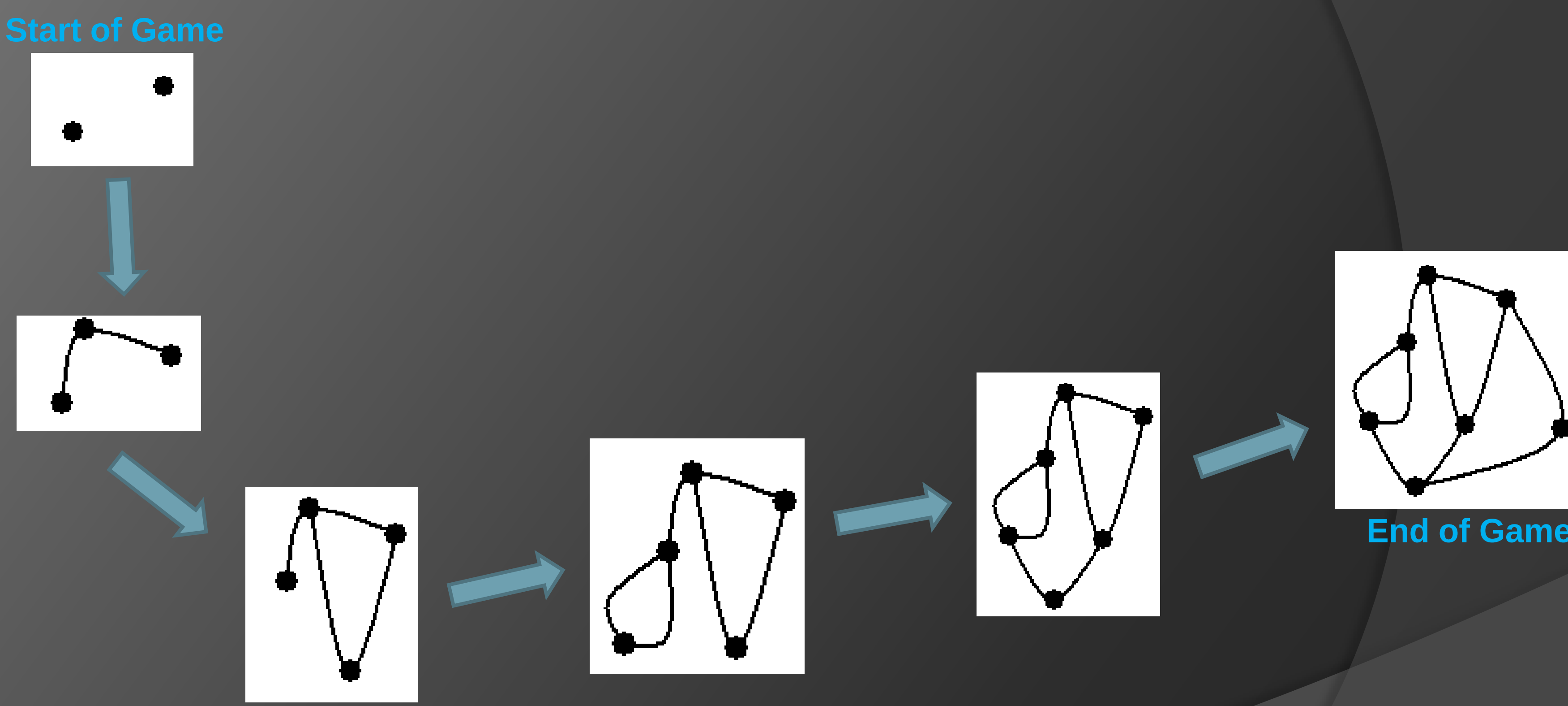
The Game of Sprouts was invented in 1967 by Princeton mathematician John H. Conway and by Michael S. Paterson, when both were at the University of Cambridge in the UK.

Determine the maximum number of moves possible in a Sprouts game that begins with 42 vertices.
(without actually playing a game with that many vertices)

❷ ACTIVITY: SPROUTS

BIG IDEAS: Quantifiable Differences, Data Collection & Analysis, Pattern Recognition

The Game of Sprouts was invented in 1967 by Princeton mathematician John H. Conway and by Michael S. Paterson, when both were at the University of Cambridge in the UK.

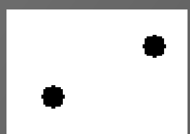


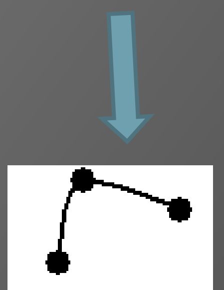
❷ ACTIVITY: SPROUTS

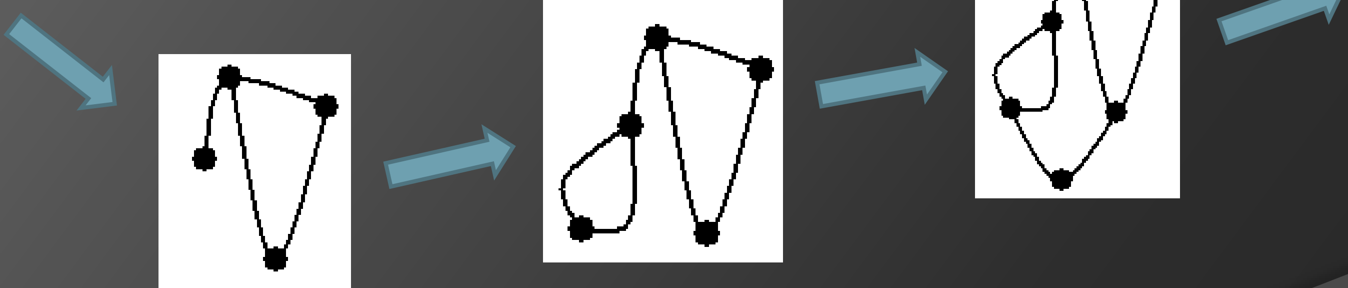
BIG IDEAS: Quantifiable Differences, Data Collection & Analysis, Pattern Recognition

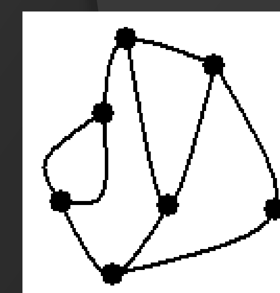
The Game of Sprouts was invented in 1967 by Princeton mathematician John H. Conway and by Michael S. Paterson, when both were at the University of Cambridge in the UK.

Start of Game









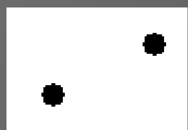
End of Game

❷ # ACTIVITY: SPROUTS

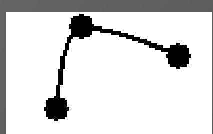
BIG IDEAS: Quantifiable Differences, Data Collection & Analysis, Pattern Recognition

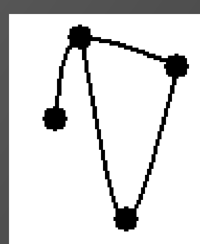
The Game of Sprouts was invented in 1967 by Princeton mathematician John H. Conway and by Michael S. Paterson, when both were at the University of Cambridge in the UK.

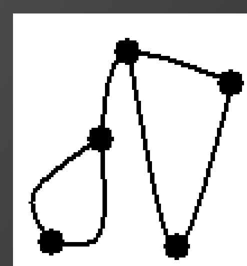
Start of Game

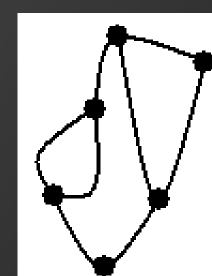


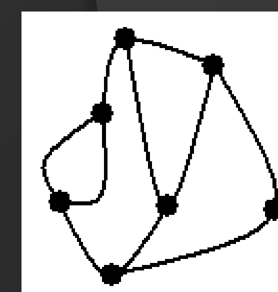
Move Number	Number of Vertices	The Degree of Each Vertex (separate each using a comma)	Sum of all Degrees	Number of Edges
0	2	0, 0	0	0
1	3	1, 1, 2	4	2











End of Game

❷ ACTIVITY: SPROUTS

BIG IDEAS: Quantifiable Differences, Data Collection & Analysis, Pattern Recognition

The Game of Sprouts was invented in 1967 by Princeton mathematician John H. Conway and by Michael S. Paterson, when both were at the University of Cambridge in the UK.

Move Number	Number of Vertices	The Degree of Each Vertex (separate each using a comma)	Sum of all Degrees	Number of Edges
0	2	0, 0	0	0
1	3	1, 1, 2	4	2
2	4	1, 2, 2, 3	8	4
3	5	2, 2, 2, 3, 3	12	6
4	6	2, 2, 3, 3, 3, 3	16	8
5	7	2, 3, 3, 3, 3, 3, 3	20	10

❷ ACTIVITY: SPROUTS

BIG IDEAS: Quantifiable Differences, Data Collection & Analysis, Pattern Recognition

The Game of Sprouts was invented in 1967 by Princeton mathematician John H. Conway and by Michael S. Paterson, when both were at the University of Cambridge in the UK.

Some Connections/Ideas for Extensions

- What would happen to the game if you changed some of the rules?
- How could you figure out if there is a winning strategy?
- How are Sprouts games connected to 3-dimenional nets and Euler?

❸ QUICK START ⮚⮚ DECEPTIVE CALCULATOR

BIG IDEAS: Divisibility Rules, Number System, Limits of Technology

Below is a screen capture from a division calculation done using a TI-84 calculator.

```
5374867391/3
           1791622464
```

Discuss at least two ways that you can show that the calculator is providing false information.

❸ QUICK START >> DECEPTIVE CALCULATOR

BIG IDEAS: Divisibility Rules, Number System, Limits of Technology

Below is a screen capture from a division calculation done using a TI-84 calculator.

```
5374867391/3
      1791622464
```

Discuss at least two ways that you can show that the calculator is providing false information.

$$\begin{array}{r} 1{,}791{,}622{,}464 \\ \times \qquad\qquad\qquad 3 \\ \hline \ldots 392 \end{array}$$

Forwards Argument

❸ QUICK START ➢➢ DECEPTIVE CALCULATOR

BIG IDEAS: Divisibility Rules, Number System, Limits of Technology

Below is a screen capture from a division calculation done using a TI-84 calculator.

```
5374867391/3
      1791622464
```

Discuss at least two ways that you can show that the calculator is providing false information.

Subtle Argument

$$5+3+7+4+8+6+7+3+9+1=43$$

43 is not divisible by 3

❸ QUICK START ⮚⮚ DECEPTIVE CALCULATOR

BIG IDEAS: Divisibility Rules, Number System, Limits of Technology

Below is a screen capture from a division calculation done using a TI-84 calculator.

```
5374867391/3
        1791622464
```

Discuss at least two ways that you can show that the calculator is providing false information.

$$\begin{aligned} 472 &= 400+70+2 \\ &= 4(100)+7(10)+2(1) \\ &= 4(99+1)+7(9+1)+2(1) \\ &= 4(99)+4(1)+7(9)+4(1)+2(1) \\ &= 4(99)+7(9)+4(1)+7(1)+2(1) \end{aligned}$$

$$5+3+7+4+8+6+7+3+9+1=43$$

43 is not divisible by 3

❸ QUICK START ➢➢ DECEPTIVE CALCULATOR

BIG IDEAS: Divisibility Rules, Number System, Limits of Technology

Below is a screen capture from a division calculation done using a TI-84 calculator.

```
5374867391/3
      1791622464
```

Discuss at least two ways that you can show that the calculator is providing false information.

<u>Some Connections/Ideas for Extensions</u>

- What is "casting out nines" and why was it important before computing devices?
- Is there a divisibility rule for multiples of 7?
- What are some algorithms for determining if a number is prime or composite?

❹ ACTIVITY: UNLUCKY 13

BIG IDEAS: Organizing Patterns, Modular Arithmetic, Taming the Infinite, Proof

What is the maximum number of times Friday the 13th that can occur within a single January to December calendar year? Show/Explain your method.

❹ ACTIVITY: UNLUCKY 13

BIG IDEAS: Organizing Patterns, Modular Arithmetic, Taming the Infinite, Proof

What is the maximum number of times Friday the 13th that can occur within a single January to December calendar year? Show/Explain your method.

Mon	Tue	Wed	Thu	Fri	Sat	Sun
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
1	2	3	4	5	6	7
8	9	10	11	12	13	14

❹ **ACTIVITY: UNLUCKY 13**

BIG IDEAS: Organizing Patterns, Modular Arithmetic, Taming the Infinite, Proof

What is the maximum number of times Friday the 13th that can occur within a single January to December calendar year? Show/Explain your method.

Mon	Tue	Wed	Thu	Fri	Sat	Sun
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
1	2	3	4	5	6	7
8	9	10	11	12	13	14

Mon	Tue	Wed	Thu	Fri	Sat	Sun
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31
32	33	34	35	36	37	38
39	40	41	42	43	44	45
46	47	48	49	50	51	52
53	54	55	56	57	58	59
60	61	62	63	64	65	66
67	68	69	70	71	72	73

❹ ACTIVITY: UNLUCKY 13

BIG IDEAS: Organizing Patterns, Modular Arithmetic, Taming the Infinite, Proof

What is the maximum number of times Friday the 13th that can occur within a single January to December calendar year? Show/Explain your method.

Mon	Tue	Wed	Thu	Fri	Sat	Sun
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
⋮	⋮	⋮	⋮	⋮	⋮	⋮
			42	43	44	
⋮	⋮	⋮	⋮	⋮	⋮	⋮
			70	71	72	
⋮	⋮	⋮	⋮	⋮	⋮	⋮
			98	99	100	101
102	103					
⋮	⋮	⋮	⋮	⋮	⋮	⋮

The 13th of	Corresponding Day of Year
JAN	13
FEB	31 + 13 = 44
MAR	28 + 44 = 72
APR	31 + 72 = 103
MAY	⋮
JUN	⋮
JUL	⋮
AUG	⋮
SEP	
OCT	
NOV	

❹ **ACTIVITY: UNLUCKY 13**

BIG IDEAS: Organizing Patterns, Modular Arithmetic, Taming the Infinite, Proof

What is the maximum number of times Friday the 13th that can occur within a single January to December calendar year? Show/Explain your method.

The 13th of	Corresponding Day of Year	Partitions Based on 7	Modular Form	Same Day of the week as
JAN	13	$13 = 1(7) + 6$	$13 \equiv 6 \pmod{7}$	6th
FEB	31 + 13 = 44	$44 = 6(7) + 2$	$44 \equiv 2 \pmod{7}$	2nd
MAR	28 + 44 = 72	$72 = 10(7) + 2$	$72 \equiv 2 \pmod{7}$	2nd
APR	31 + 72 = 103	$103 = 14(7) + 5$	$103 \equiv 5 \pmod{7}$	5th
MAY	⋮	⋮	⋮	⋮

❹ ACTIVITY: UNLUCKY 13

BIG IDEAS: Organizing Patterns, Modular Arithmetic, Taming the Infinite, Proof

What is the maximum number of times Friday the 13th that can occur within a single January to December calendar year? Show/Explain your method.

The 13th of	Corresponding Day of Year	Partitions Based on 7	Modular Form	Same Day of the week as
JAN	13	$13 = 1(7) + 6$	$13 \equiv 6 \pmod 7$	6th
FEB	31 + 13 = 44	$44 = 6(7) + 2$	$44 \equiv 2 \pmod 7$	2nd
MAR	28 + 44 = 72	$72 = 10(7) + 2$	$72 \equiv 2 \pmod 7$	2nd
APR	31 + 72 = 103	$103 = 14(7) + 5$	$103 \equiv 5 \pmod 7$	5th
MAY	⋮	⋮	⋮	⋮

How can this chart help answer the original question?

❹ ACTIVITY: UNLUCKY 13

BIG IDEAS: Organizing Patterns, Modular Arithmetic, Taming the Infinite, Proof

What is the maximum number of times Friday the 13th that can occur within a single January to December calendar year? Show/Explain your method.

The 13th of	Corresponding Day of Year	Partitions Based on 7	Modular Form	Same Day of the week as
JAN	13	$13 = 1(7) + 6$	$13 \equiv 6 \pmod 7$	6th
FEB	31 + 13 = 44	$44 = 6(7) + 2$	$44 \equiv 2 \pmod 7$	2nd
MAR	28 + 44 = 72	$72 = 10(7) + 2$	$72 \equiv 2 \pmod 7$	2nd
APR	31 + 72 = 103	$103 = 14(7) + 5$	$103 \equiv 5 \pmod 7$	5th
MAY	⋮	⋮	⋮	⋮

Is there a better way to answer the original question?

❹ ACTIVITY: UNLUCKY 13

BIG IDEAS: Organizing Patterns, Modular Arithmetic, Taming the Infinite, Proof

What is the maximum number of times Friday the 13th that can occur within a single January to December calendar year? Show/Explain your method.

The 13th of	Corresponding Day of Year	Partitions Based on 7	Modular Form	Same Day of the week as
JAN	13	$13 = 1(7) + 6$	$13 \equiv 6 \pmod{7}$	6th
FEB	31 + 13 = 44	$44 = 6(7) + 2$	$44 \equiv 2 \pmod{7}$	2nd
MAR	28 + 44 = 72	$72 = 10(7) + 2$	$72 \equiv 2 \pmod{7}$	2nd
APR	31 + 72 = 103	$103 = 14(7) + 5$	$103 \equiv 5 \pmod{7}$	5th
MAY	⋮	⋮	⋮	⋮

Doh! What about Leap Years??

❹ ACTIVITY: UNLUCKY 13

BIG IDEAS: Organizing Patterns, Modular Arithmetic, Taming the Infinite, Proof

What is the maximum number of times Friday the 13th that can occur within a single January to December calendar year? Show/Explain your method.

Some Connections/Ideas for Extensions

- How can you tell if a book ISBN number is valid or not?
- What is Goldbach's Conjecture and how is it related to partitions?
- How do you deal with negative numbers in a modular system?

❺ ACTIVITY: BYPASSING THE CHARTS

BIG IDEAS: Modular Arithmetic, Functions, Combinatorics, Going Backwards is Usually Harder

Here are two different schemes for replacing plaintext with ciphertext (i.e. encrypting a message)

Random Scramble:	Y	X	D	N	K	T	…	…	…
	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕
Plaintext:	A	B	C	D	E	F	…	…	…
	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕
Modular Scramble:	E	J	O	T	Y	D	…	…	…

❺ ACTIVITY: BYPASSING THE CHARTS

BIG IDEAS: Modular Arithmetic, Functions, Combinatorics, Going Backwards is Usually Harder

Here are two different schemes for replacing plaintext with ciphertext (i.e. encrypting a message)

Random Scramble:	Y	X	D	N	K	T	…	…	…
	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕
Plaintext:	A	B	C	D	E	F	…	…	…
	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕
Modular Scramble:	E	J	O	T	Y	D	…	…	…

Based on the information given, write the word "SECRET" using the Random Scramble ciphertext .

❺ ACTIVITY: BYPASSING THE CHARTS

BIG IDEAS: Modular Arithmetic, Functions, Combinatorics, Going Backwards is Usually Harder

Random Scramble:	Y	X	D	N	K	T	B	I	Z	F	U	J	A	C	O	W	H	S	V	Q	G	P	L	R	M	E
	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕
Plaintext:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Based on the information given, write the word "SECRET" using the Random Scramble ciphertext .

❺ ACTIVITY: BYPASSING THE CHARTS

BIG IDEAS: Modular Arithmetic, Functions, Combinatorics, Going Backwards is Usually Harder

Here are two different schemes for replacing plaintext with ciphertext (i.e. encrypting a message)

Random Scramble:	Y	X	D	N	K	T	…	…	…
	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕
Plaintext:	A	B	C	D	E	F	…	…	…
	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕
Modular Scramble:	E	J	O	T	Y	D	…	…	…

Based on the information given, write the word "SECRET" using the Modular Scramble ciphertext.

$$H \Rightarrow 8 \Rightarrow \underbrace{5 \cdot 8 = 40}_{multiplicative\ step} \Rightarrow \underbrace{40 \equiv 14 \pmod{26}}_{equivalence\ step} \Rightarrow 14 \Rightarrow N$$

❺ ACTIVITY: BYPASSING THE CHARTS

BIG IDEAS: Modular Arithmetic, Functions, Combinatorics, Going Backwards is Usually Harder

Here are two different schemes for replacing plaintext with ciphertext (i.e. encrypting a message)

Random Scramble:	Y	X	D	N	K	T	…	…	…
	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕
Plaintext:	A	B	C	D	E	F	…	…	…
	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕
Modular Scramble:	E	J	O	T	Y	D	…	…	…

W	S	Z	A	K
B	L	S	M	Y

We've received a secret word that has been encrypted using each of the schemes.

You're job is to decode this secret word.

❺ ACTIVITY: BYPASSING THE CHARTS

BIG IDEAS: Modular Arithmetic, Functions, Combinatorics, Going Backwards is Usually Harder

$$\mathrm{L} \Rightarrow 12 \Rightarrow \underbrace{12 \div 5 = 2.4}_{division\ step} \Rightarrow \underbrace{2.4 \equiv eek!\ (\bmod 26)}_{equivalence\ step} \Rightarrow ?? \Rightarrow ??$$

W	S	Z	A	K
B	L	S	M	Y

We've received a secret word that has been encrypted using each of the schemes.

You're job is to decode this secret word.

❺ ACTIVITY: BYPASSING THE CHARTS

BIG IDEAS: Modular Arithmetic, Functions, Combinatorics, Going Backwards is Usually Harder

$$5 \cdot ? \equiv 12 \pmod{26}$$

W	S	Z	A	K
B	L	S	M	Y

We've received a secret word that has been encrypted using each of the schemes.

You're job is to decode this secret word.

❺ ACTIVITY: BYPASSING THE CHARTS

BIG IDEAS: Modular Arithmetic, Functions, Combinatorics, Going Backwards is Usually Harder

1	2	3	4	5	...	11	12	13	...	25	26
27	28	29	30	31	...	37	38	39	...	51	52
53	54	55	56	57	...	63	64	65	...	77	78
79	80	81	82	83	...	89	90	91	...	103	104
105	106	107	108	109	...	115	116	117	...	129	130

W	S	Z	A	K
B	L	S	M	Y

We've received a secret word that has been encrypted using each of the schemes.

You're job is to decode this secret word.

❺ ACTIVITY: BYPASSING THE CHARTS

BIG IDEAS: Modular Arithmetic, Functions, Combinatorics, Going Backwards is Usually Harder

$$5 \cdot ? \equiv 12 \pmod{26}$$
$$\underbrace{21 \cdot 5}_{inverse} \cdot ? \equiv 21 \cdot 12 \pmod{26}$$
$$1 \cdot ? \equiv 252 \pmod{26}$$
$$? \equiv 18 \pmod{26}$$

W	S	Z	A	K
B	L	S	M	Y

We've received a secret word that has been encrypted using each of the schemes.

You're job is to decode this secret word.

❺ ACTIVITY: BYPASSING THE CHARTS

BIG IDEAS: Modular Arithmetic, Functions, Combinatorics, Going Backwards is Usually Harder

$$L \Rightarrow 12 \Rightarrow \underbrace{21 \cdot 12 = 252}_{\text{multiplicative step}} \Rightarrow \underbrace{252 \equiv 18 \pmod{26}}_{\text{equivalence step}} \Rightarrow 18 \Rightarrow R$$

$$\begin{aligned} 5 \cdot ? &\equiv 12 \pmod{26} \\ \underbrace{21 \cdot 5}_{\text{inverse}} \cdot ? &\equiv 21 \cdot 12 \pmod{26} \\ 1 \cdot ? &\equiv 252 \pmod{26} \\ ? &\equiv 18 \pmod{26} \end{aligned}$$

W	S	Z	A	K
B	L	S	M	Y

We've received a secret word that has been encrypted using each of the schemes.

You're job is to decode this secret word.

❺ ACTIVITY: BYPASSING THE CHARTS

BIG IDEAS: Modular Arithmetic, Functions, Combinatorics, Going Backwards is Usually Harder

Random Scramble:	W	S	Z	A	K
	⇕	⇕	⇕	⇕	⇕
Plaintext:	?	?	?	?	?
	⇕	⇕	⇕	⇕	⇕
Modular Scramble:	B	L	S	M	Y

Based on the information given, what is the SECRET word?

❺ ACTIVITY: BYPASSING THE CHARTS

BIG IDEAS: Modular Arithmetic, Functions, Combinatorics, Going Backwards is Usually Harder

$$5^{11} = 48{,}828{,}125 \equiv 21 \pmod{26}$$

$$5^{11} \bullet 5 = 5^{12} = 244{,}140{,}625 \equiv 1 \pmod{26}$$

W	S	Z	A	K
B	L	S	M	Y

We've received a secret word that has been encrypted using each of the schemes.

You're job is to decode this secret word.

❺ ACTIVITY: BYPASSING THE CHARTS

BIG IDEAS: Modular Arithmetic, Functions, Combinatorics, Going Backwards is Usually Harder

$$L \Rightarrow 12 \Rightarrow \underbrace{5^{11} \cdot 12 = 585,937,500}_{\textit{multiplicative step}} \Rightarrow$$

$$\underbrace{585,937,500 \equiv 18 \pmod{26}}_{\textit{equivalence step}} \Rightarrow 18 \Rightarrow R$$

$$5^{11} = 48,828,125 \equiv 21 \pmod{26}$$

$$5^{11} \bullet 5 = 5^{12} = 244,140,625 \equiv 1 \pmod{26}$$

W	S	Z	A	K
B	L	S	M	Y

We've received a secret word that has been encrypted using each of the schemes.

You're job is to decode this secret word.

❺ **ACTIVITY: BYPASSING THE CHARTS**

BIG IDEAS: Modular Arithmetic, Functions, Combinatorics, Going Backwards is Usually Harder

<u>Some Connections/Ideas for Extensions</u>

- What are some ways to increase the number of modular scrambles?
- How can you use matrix algebra in conjunction with modular arithmetic to encipher/decipher?
- Create your own cipher system!