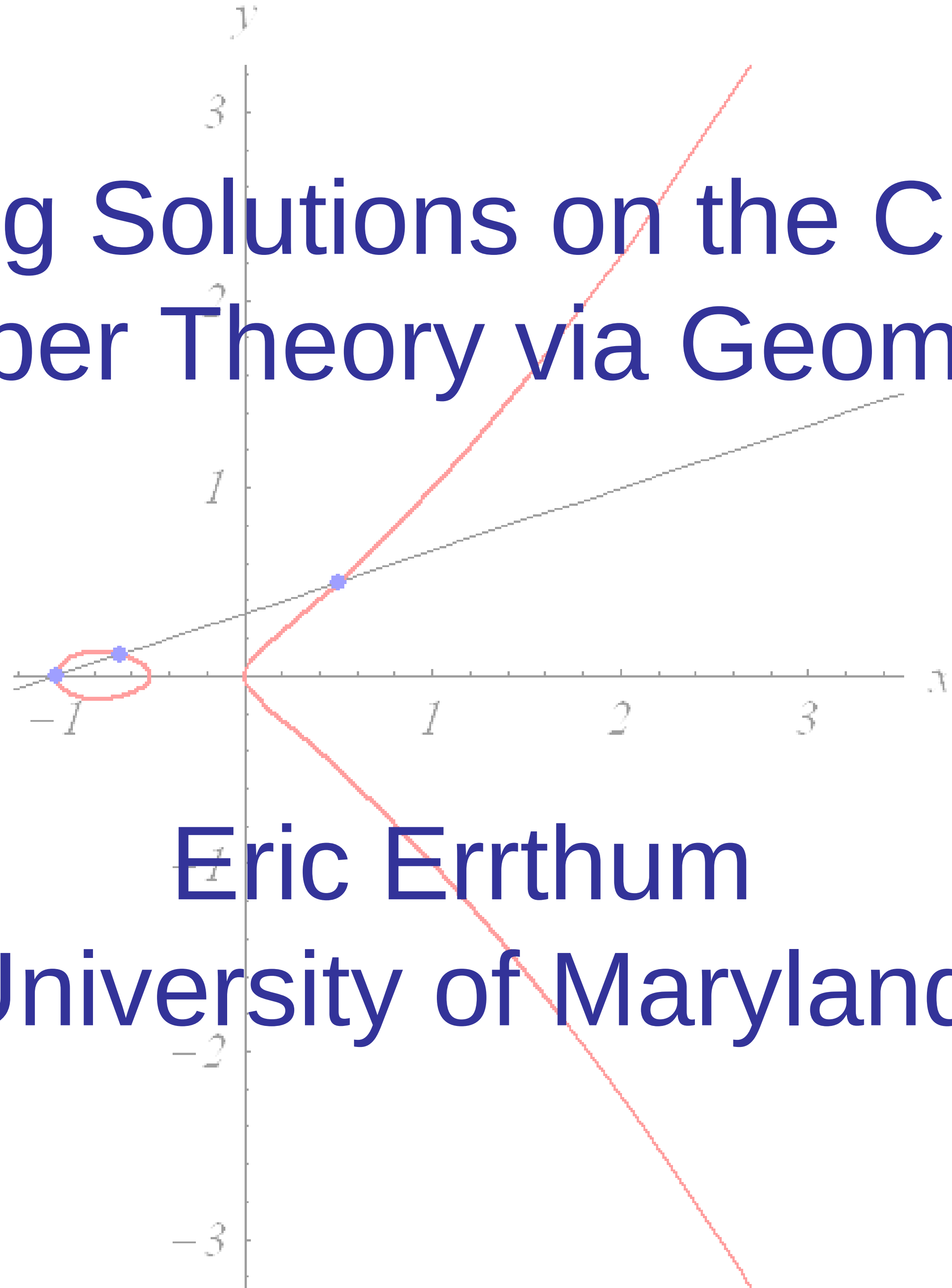
Finding Solutions on the Curve: Number Theory via Geometry



Eric Errthum
University of Maryland

What is Number Theory?

What is Number Theory?

- Classically, interested in problems involving only whole numbers.

What is Number Theory?

- Classically, interested in problems involving only whole numbers.
- Prime numbers play major roles.

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, …

What is Number Theory?

- Classically, interested in problems involving only whole numbers.
- Prime numbers play major roles.

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, …

- One of the oldest areas of mathematics.

What is Number Theory?

- Classically, interested in problems involving only whole numbers.
- Prime numbers play major roles.

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, …

- One of the oldest areas of mathematics.

Gauss: “Mathematics is the queen of sciences and number theory is the queen of mathematics.”

The Most Famous Number Theory Problem

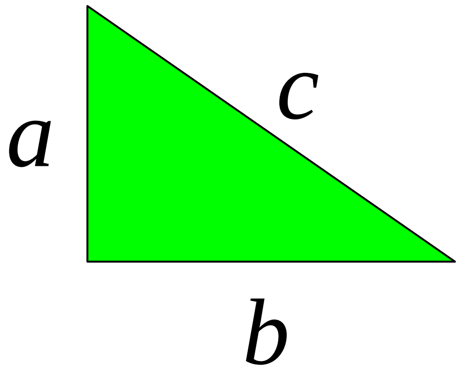
- Recall Pythagorean Triples satisfy:

$$a^2 + b^2 = c^2$$

The Most Famous Number Theory Problem

- Recall Pythagorean Triples satisfy:

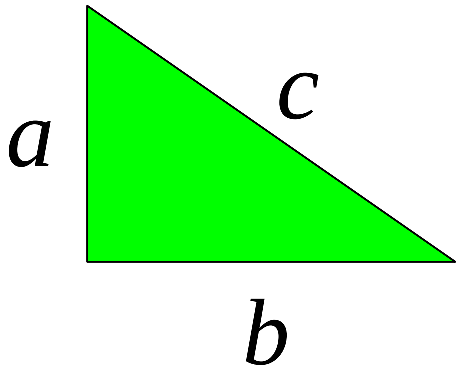
$$a^2 + b^2 = c^2$$



The Most Famous Number Theory Problem

- Recall Pythagorean Triples satisfy:

$$a^2 + b^2 = c^2$$



$$3^2 + 4^2 = 5^2$$

$$5^2 + 12^2 = 13^2$$

$$8^2 + 15^2 = 17^2$$

$$9^2 + 40^2 = 41^2$$

$$12^2 + 35^2 = 37^2$$

$$\vdots$$

The Most Famous Number Theory Problem

- Recall Pythagorean Triples satisfy:

$$a^2 + b^2 = c^2$$

- Question: Are there positive integers satisfying

$$a^n + b^n = c^n$$

for $n \geq 3$? (Fermat, 1637).

The Most Famous Number Theory Problem

- Recall Pythagorean Triples satisfy:

$$a^2 + b^2 = c^2$$

- Question: Are there positive integers satisfying

$$a^n + b^n = c^n$$

for $n \geq 3$? (Fermat, 1637).

- Answer: No. (Wiles, 1994).

The Most Famous Number Theory Problem

- Recall Pythagorean Triples satisfy:

$$a^2 + b^2 = c^2$$

- Question: Are there positive integers satisfying

$$a^n + b^n = c^n$$

  for $n \geq 3$? (Fermat, 1637).

- Answer: No. (Wiles, 1994).
- A lot of math developed along the way.

Modern Number Theory

- Modern number theory comes in a variety of flavors: Algebraic, Analytic, Combinatorial, Geometric.

Modern Number Theory

- Modern number theory comes in a variety of flavors: Algebraic, Analytic, Combinatorial, Geometric.
- Wiles's proof used all of these together.
- It's a really complicated proof.

Modern Number Theory

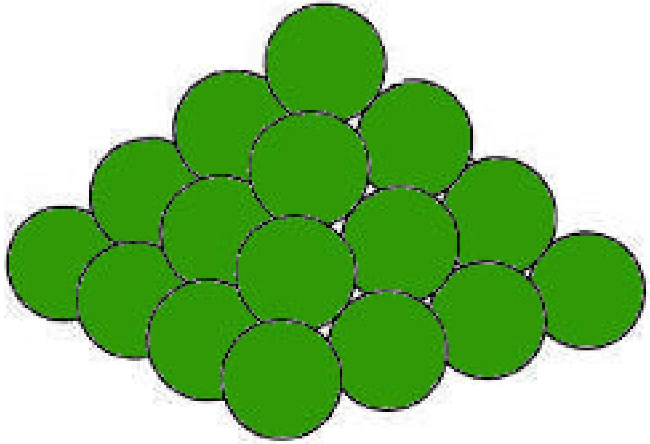
- Modern number theory comes in a variety of flavors: Algebraic, Analytic, Combinatorial, Geometric.
- Wiles's proof used all of these together.
- It's a really complicated proof.
- A crucial step involved a property of Elliptic Curves, fundamental objects in geometric number theory.

The Cannonball Problem

- Legend has it…

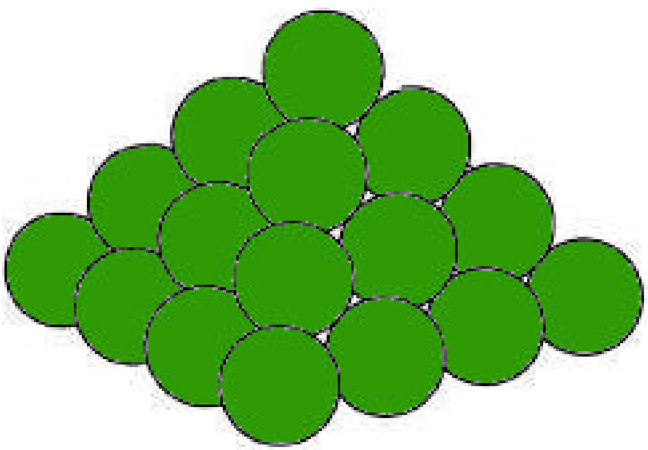
The Cannonball Problem

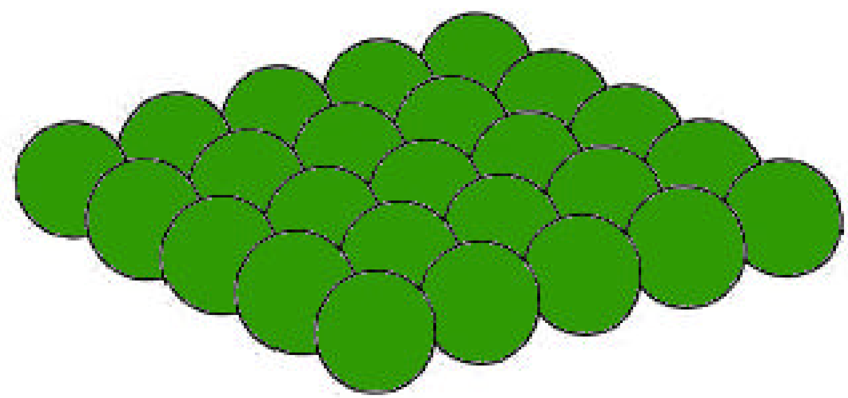
- Legend has it…
- Two ways to arrange cannonballs:
- In a pyramid:



The Cannonball Problem

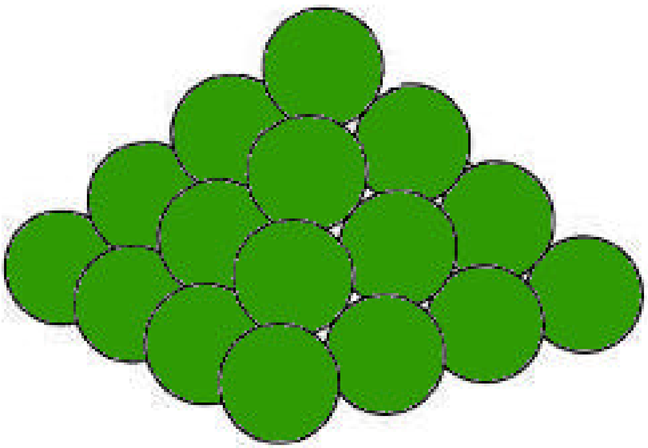
- Legend has it…
- Two ways to arrange cannonballs:
- In a pyramid: In a square:



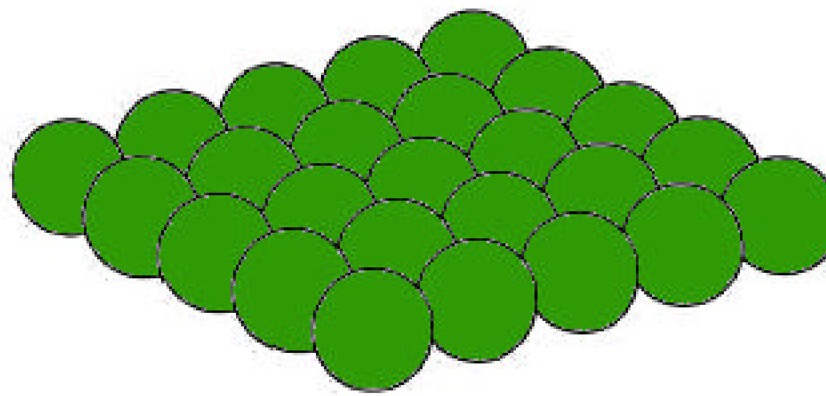


The Cannonball Problem

- Legend has it…
- Two ways to arrange cannonballs:
- In a pyramid: In a square:



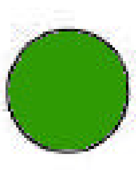
$\stackrel{?}{=}$



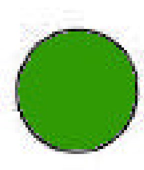
- Question: Is there a number of cannonballs which can be arranged in both ways?

The Cannonball Problem

- Legend has it…
- Two ways to arrange cannonballs:
- In a pyramid: In a square:



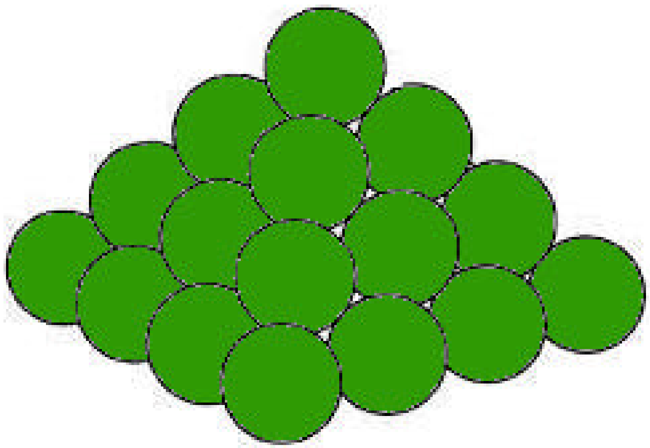
=



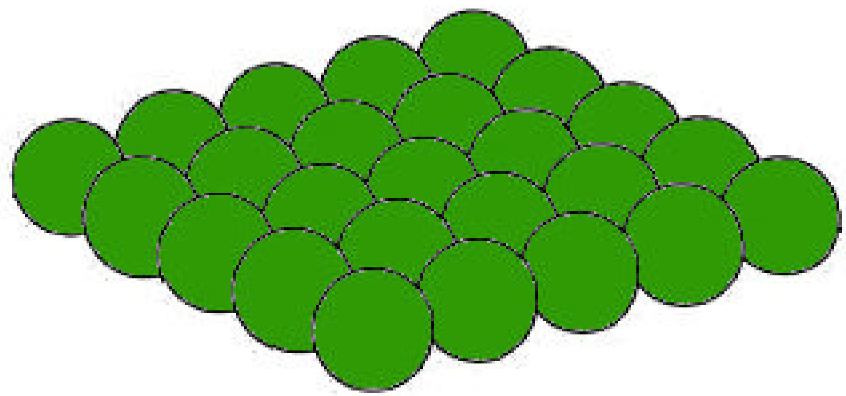
- Question: Is there a number of cannonballs which can be arranged in both ways?
- One cannonball can.

The Cannonball Problem

- Legend has it…
- Two ways to arrange cannonballs:
- In a pyramid: In a square:



$$\stackrel{?}{=}$$



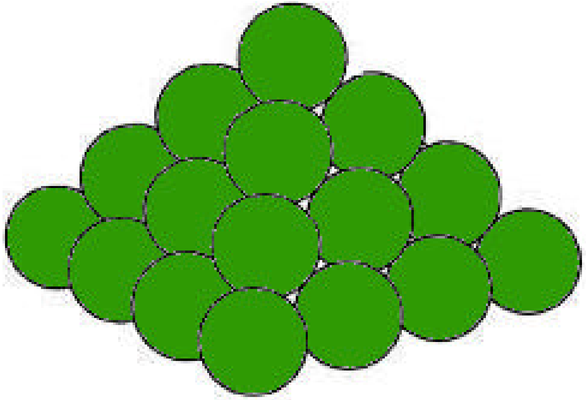
- Question: Is there a number of cannonballs which can be arranged in both ways?
- One cannonball can. Other solutions?

Convert to Math

- Formula for number of cannonballs in a pyramid of x levels:

Convert to Math

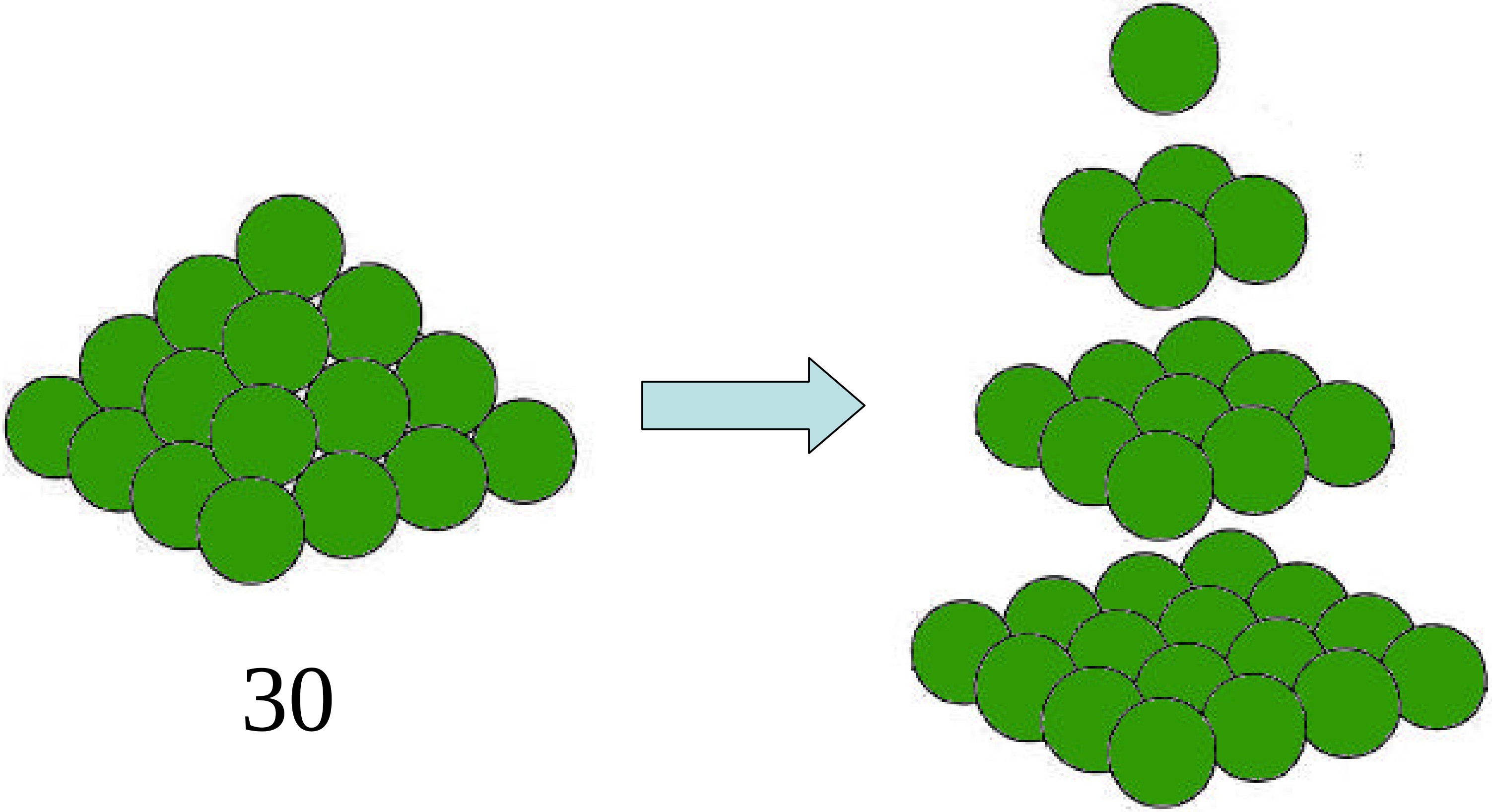
- Formula for number of cannonballs in a pyramid of x levels:



30

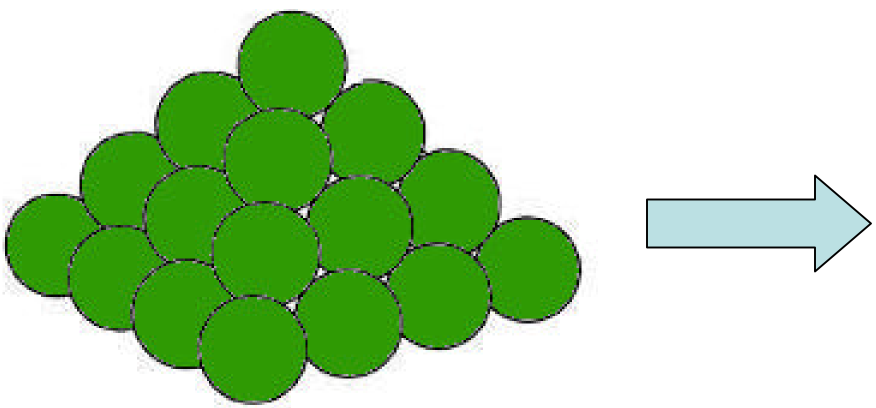
Convert to Math

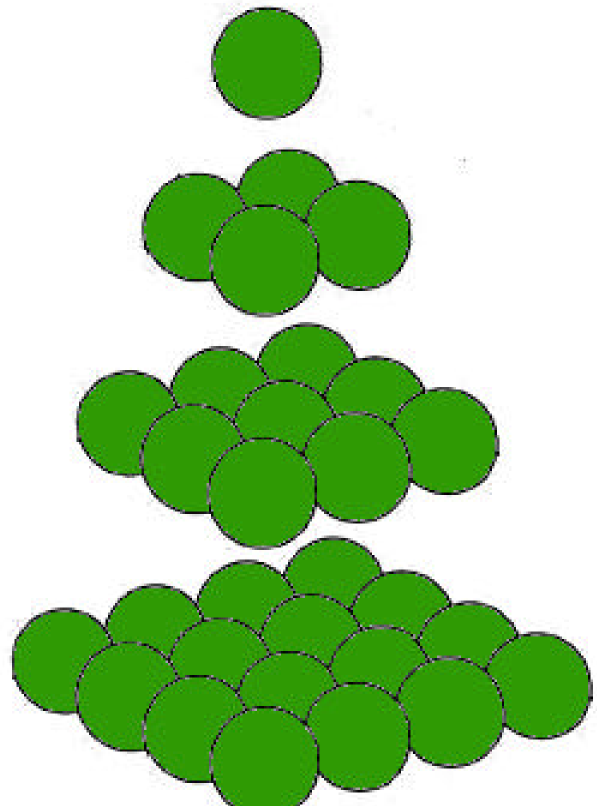
- Formula for number of cannonballs in a pyramid of x levels:



Convert to Math

- Formula for number of cannonballs in a pyramid of x levels:



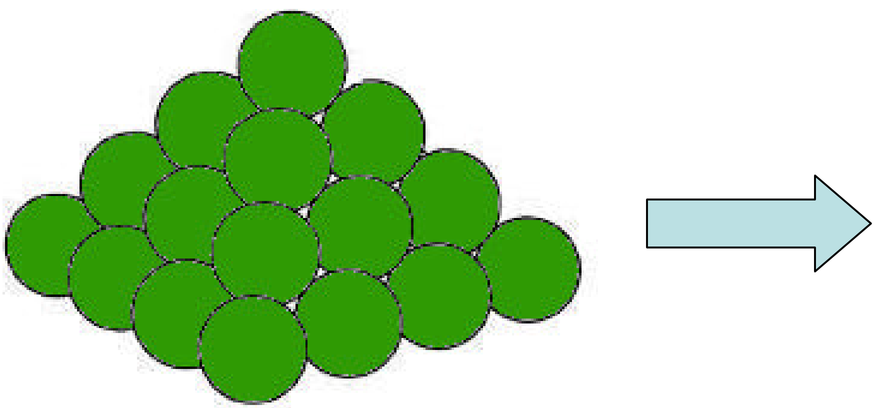


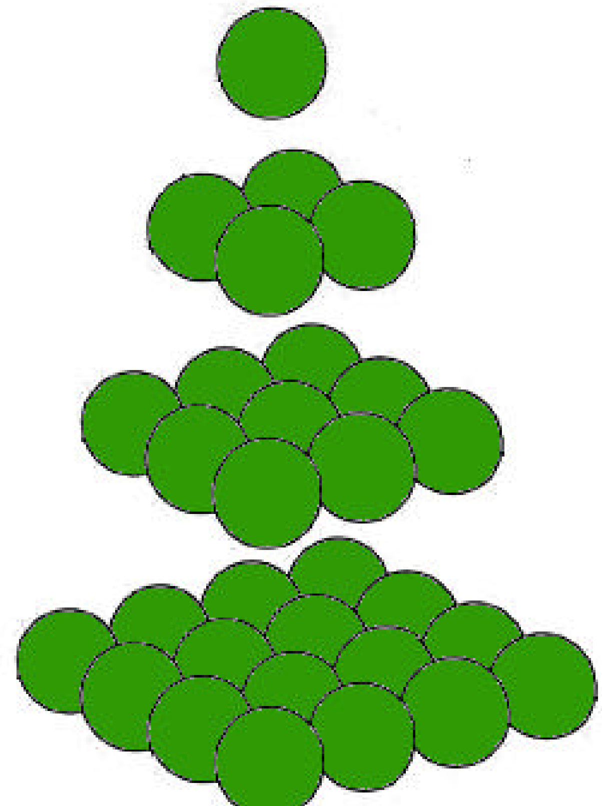
$$30 = 1^2 + 2^2 + 3^2 + 4^2$$

Convert to Math

- Formula for number of cannonballs in a pyramid of x levels:

$$1^2 + 2^2 + 3^2 + \ldots + x^2$$





$$30 = 1^2 + 2^2 + 3^2 + 4^2$$

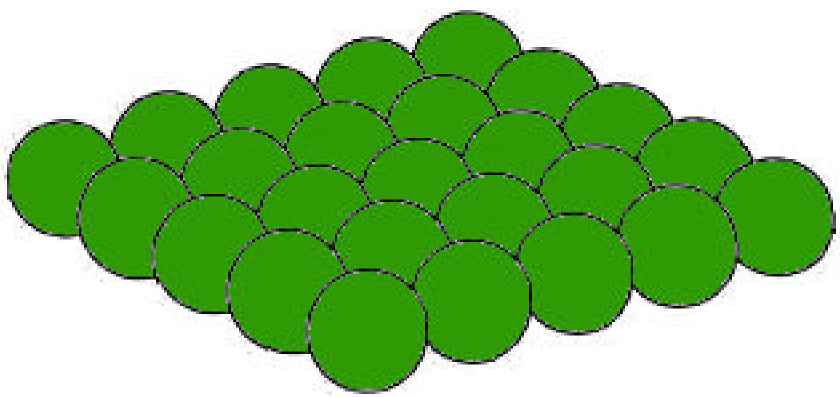
Convert to Math

- Formula for number of cannonballs in a pyramid of x levels:

$$1^2 + 2^2 + 3^2 + \ldots + x^2$$

- Formula for a square with y cannonballs on one side:

$$y^2$$



Convert to Math

- Formula for number of cannonballs in a pyramid of x levels:

$$1^2 + 2^2 + 3^2 + \ldots + x^2$$

- Formula for a square with y cannonballs on one side:

$$y^2$$

- Want two integers x and y so that:

$$y^2 = 1^2 + 2^2 + 3^2 + \ldots + x^2$$

Sum of Squares

- Better formula for $1^2 + 2^2 + 3^2 + \ldots + x^2$

Sum of Squares

- Better formula for $1^2 + 2^2 + 3^2 + \ldots + x^2$

$$1^2 = 1$$

$$1^2 + 2^2 = 5$$

$$1^2 + 2^2 + 3^2 = 14$$

$$1^2 + 2^2 + 3^2 + 4^2 = 30$$

$$\vdots$$

Sum of Squares

- Better formula for $1^2+2^2+3^2+\ldots+x^2$

$$1^2=1$$

$$1^2+2^2=5$$

$$1^2+2^2+3^2=14$$

$$1^2+2^2+3^2+4^2=30$$

$$\vdots$$

$$1^2+2^2+\ldots+x^2=\frac{x(x+1)(2x+1)}{6}$$

Sum of Squares

- Better formula for $1^2 + 2^2 + 3^2 + \ldots + x^2$

$$1^2 = 1 = \frac{1(2)(3)}{6} = \frac{6}{6}$$

$$1^2 + 2^2 = 5 = \frac{2(3)(5)}{6} = \frac{30}{6}$$

$$1^2 + 2^2 + 3^2 = 14 = \frac{3(4)(7)}{6} = \frac{84}{6}$$

$$1^2 + 2^2 + 3^2 + 4^2 = 30 = \frac{4(5)(9)}{6} = \frac{180}{6}$$

$$\vdots$$

$$1^2 + 2^2 + \ldots + x^2 = \frac{x(x+1)(2x+1)}{6}$$

Question Restated

- Want two integers x and y so that:

$$y^2 = 1^2 + 2^2 + \ldots + x^2$$

$$y^2 = \frac{x(x+1)(2x+1)}{6}$$

$$y^2 = \tfrac{1}{3}x^3 + \tfrac{1}{2}x^2 + \tfrac{1}{6}x$$

Question Restated

- Want two integers x and y so that:

$$y^2 = 1^2 + 2^2 + \ldots + x^2$$

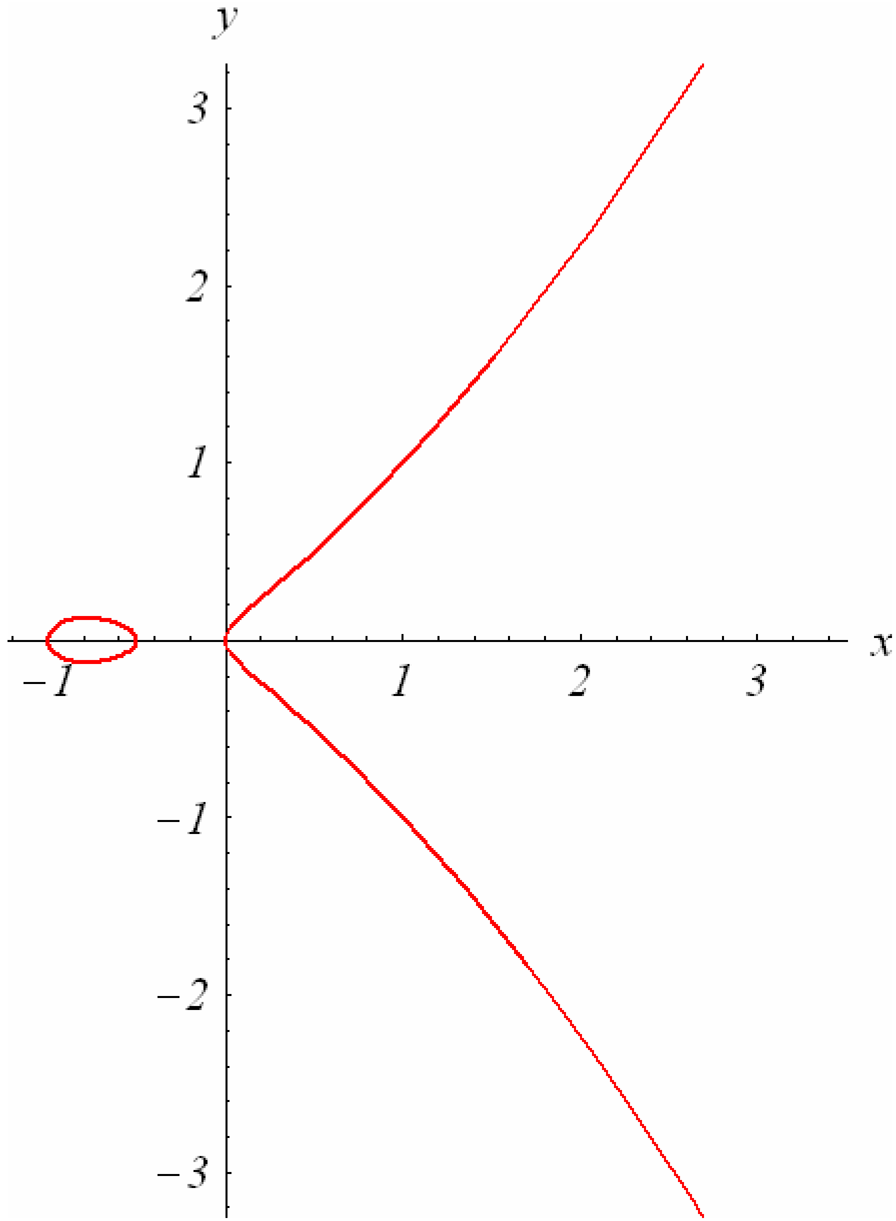
$$y^2 = \frac{x(x+1)(2x+1)}{6}$$

$$y^2 = \tfrac{1}{3}x^3 + \tfrac{1}{2}x^2 + \tfrac{1}{6}x$$

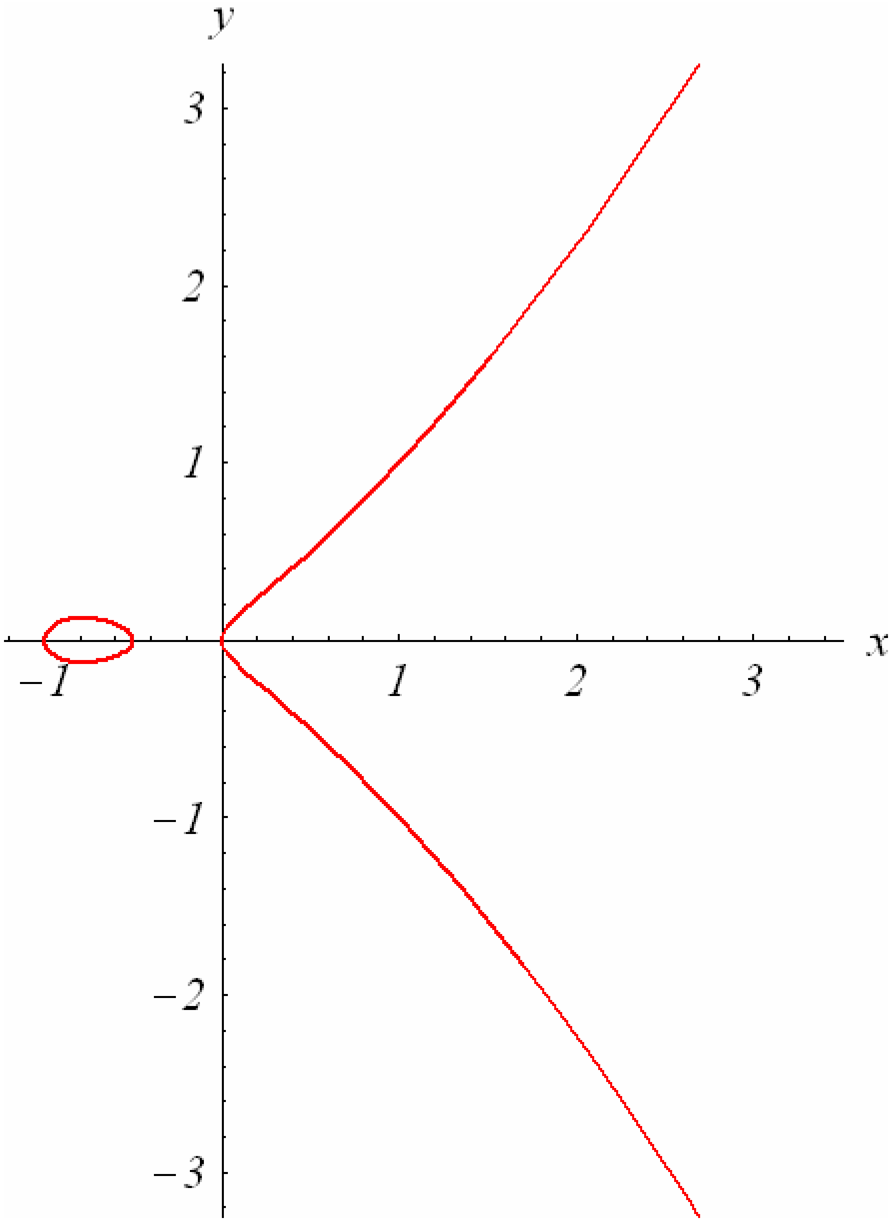
- Plan: consider the *curve*

$$y^2 = \tfrac{1}{3}x^3 + \tfrac{1}{2}x^2 + \tfrac{1}{6}x$$

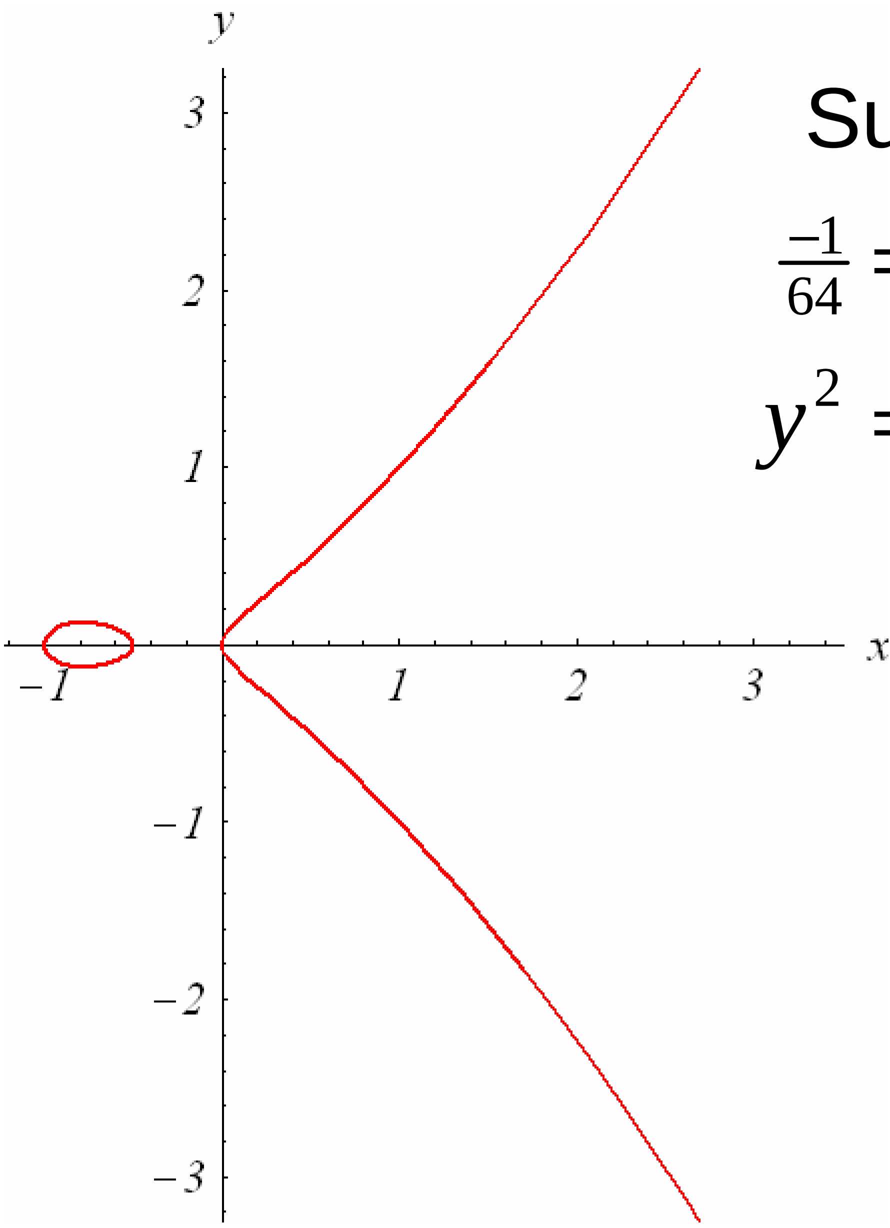
The Curve $y^2 = \frac{1}{3}x^3 + \frac{1}{2}x^2 + \frac{1}{6}x$



The Curve $y^2 = \frac{1}{3}x^3 + \frac{1}{2}x^2 + \frac{1}{6}x$



The Curve $y^2 = \frac{1}{3}x^3 + \frac{1}{2}x^2 + \frac{1}{6}x$

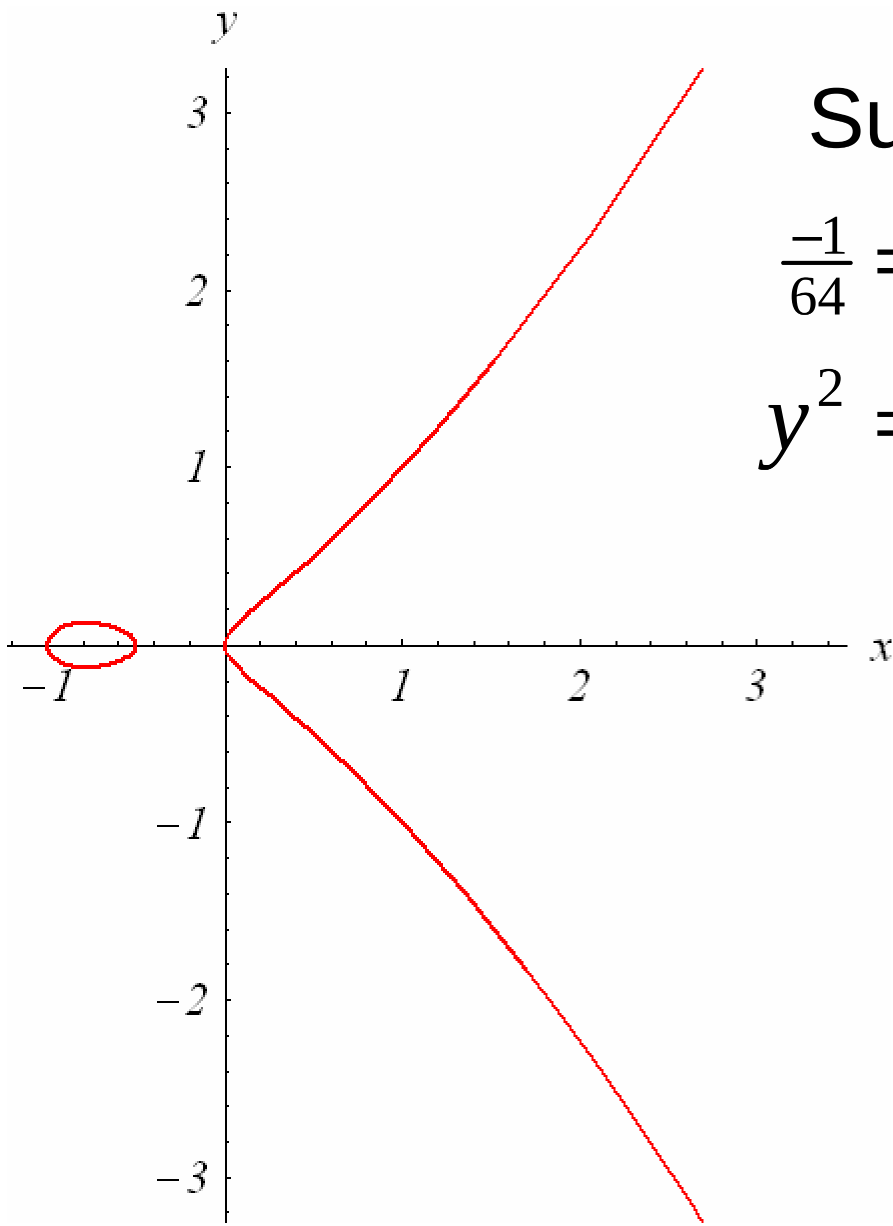


Suppose: $x = \frac{-1}{4}$

$$\frac{-1}{64} = \frac{1}{3}\left(\frac{-1}{4}\right)^3 + \frac{1}{2}\left(\frac{-1}{4}\right)^2 + \frac{1}{6}\left(\frac{-1}{4}\right)$$

$y^2 = \frac{-1}{64}$ No Solution.

The Curve $y^2 = \frac{1}{3}x^3 + \frac{1}{2}x^2 + \frac{1}{6}x$



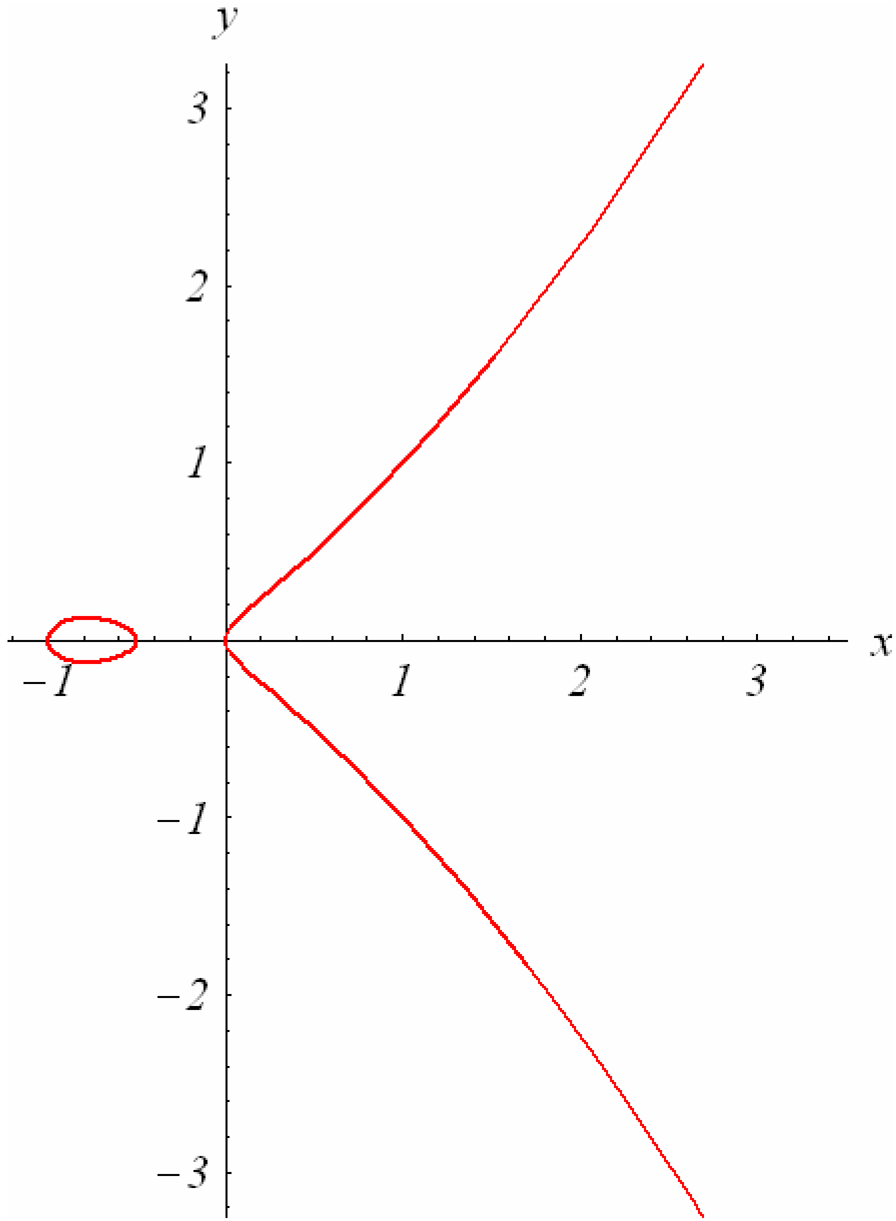
Suppose: $x = \frac{-1}{4}$

$$\frac{-1}{64} = \frac{1}{3}\left(\frac{-1}{4}\right)^3 + \frac{1}{2}\left(\frac{-1}{4}\right)^2 + \frac{1}{6}\left(\frac{-1}{4}\right)$$

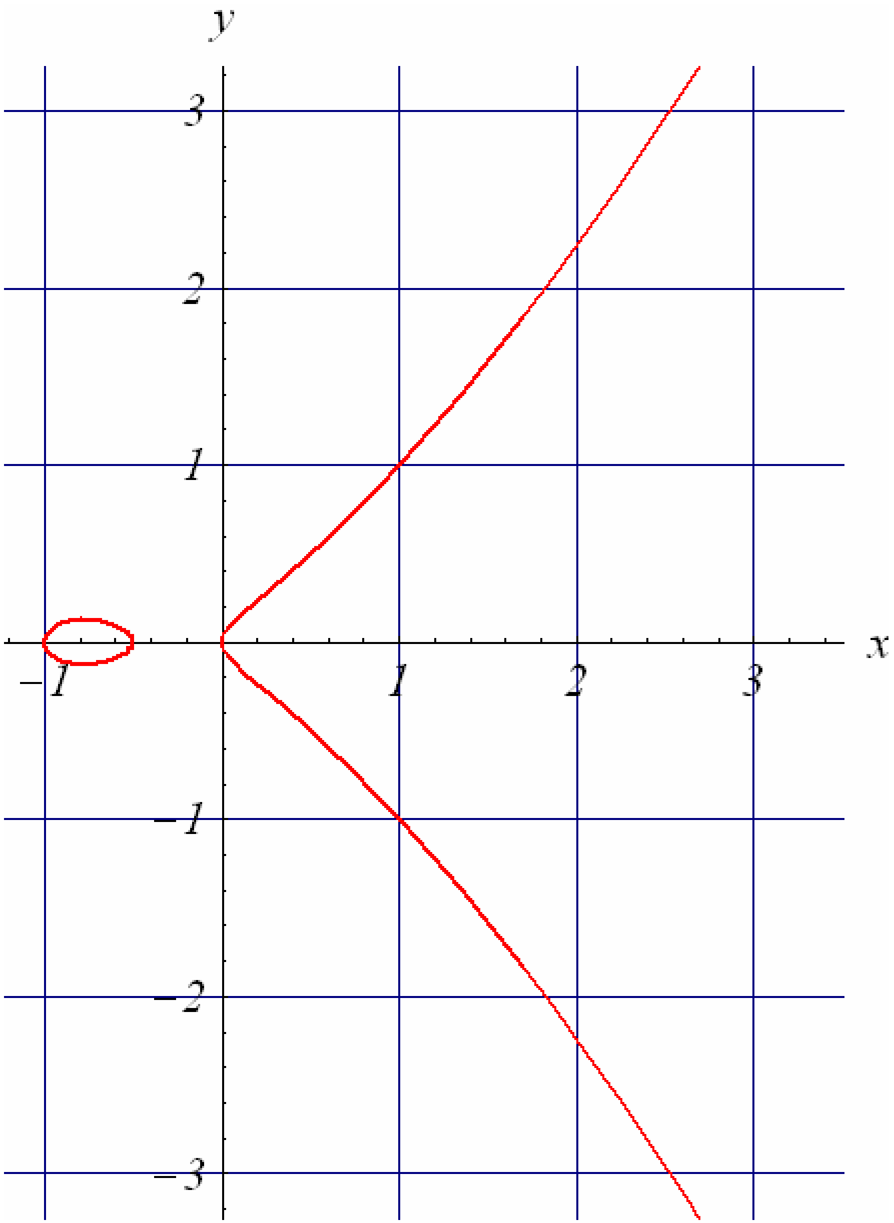
$y^2 = \frac{-1}{64}$ No Solution.

Symmetry about the x-axis.

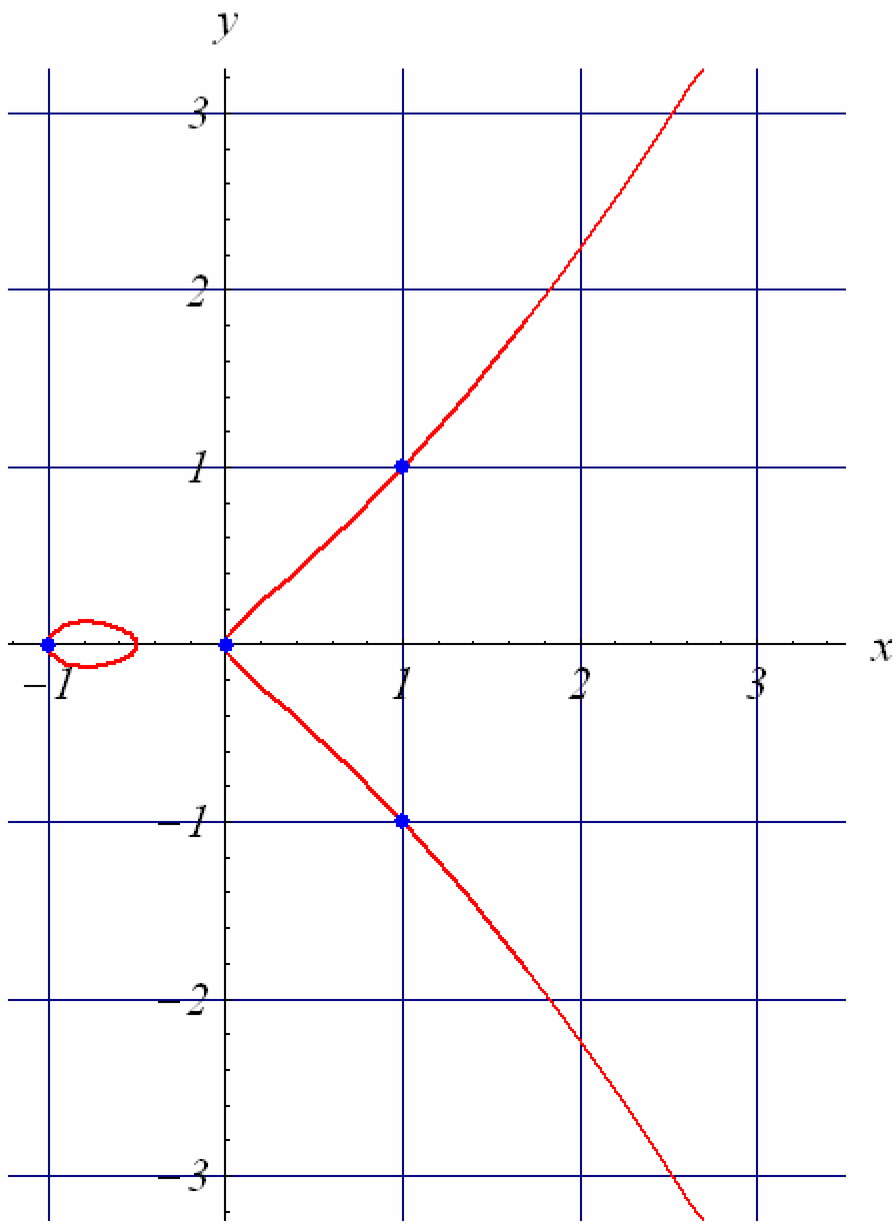
The Curve $y^2 = \frac{1}{3}x^3 + \frac{1}{2}x^2 + \frac{1}{6}x$



The Curve $y^2 = \frac{1}{3}x^3 + \frac{1}{2}x^2 + \frac{1}{6}x$



The Curve $y^2 = \frac{1}{3}x^3 + \frac{1}{2}x^2 + \frac{1}{6}x$

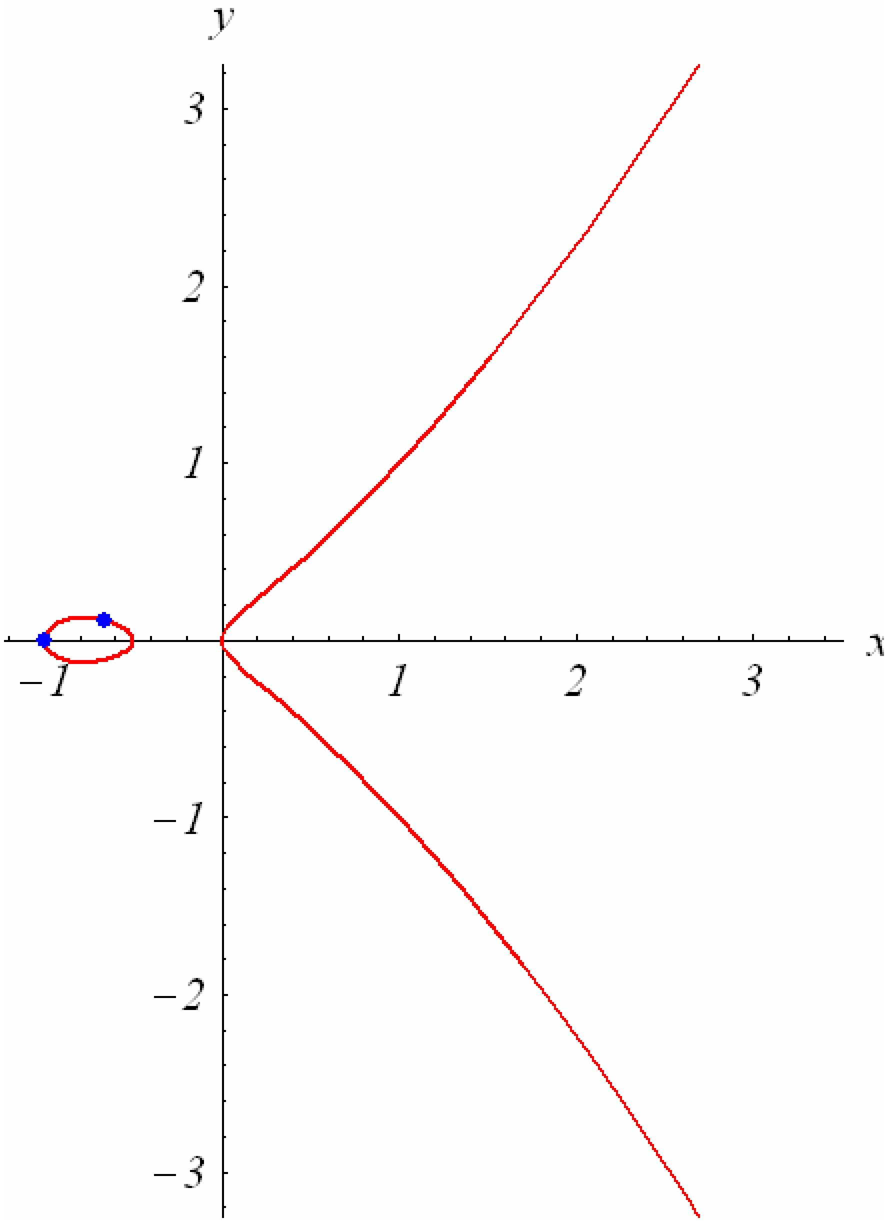


The Curve $y^2 = \frac{1}{3}x^3 + \frac{1}{2}x^2 + \frac{1}{6}x$

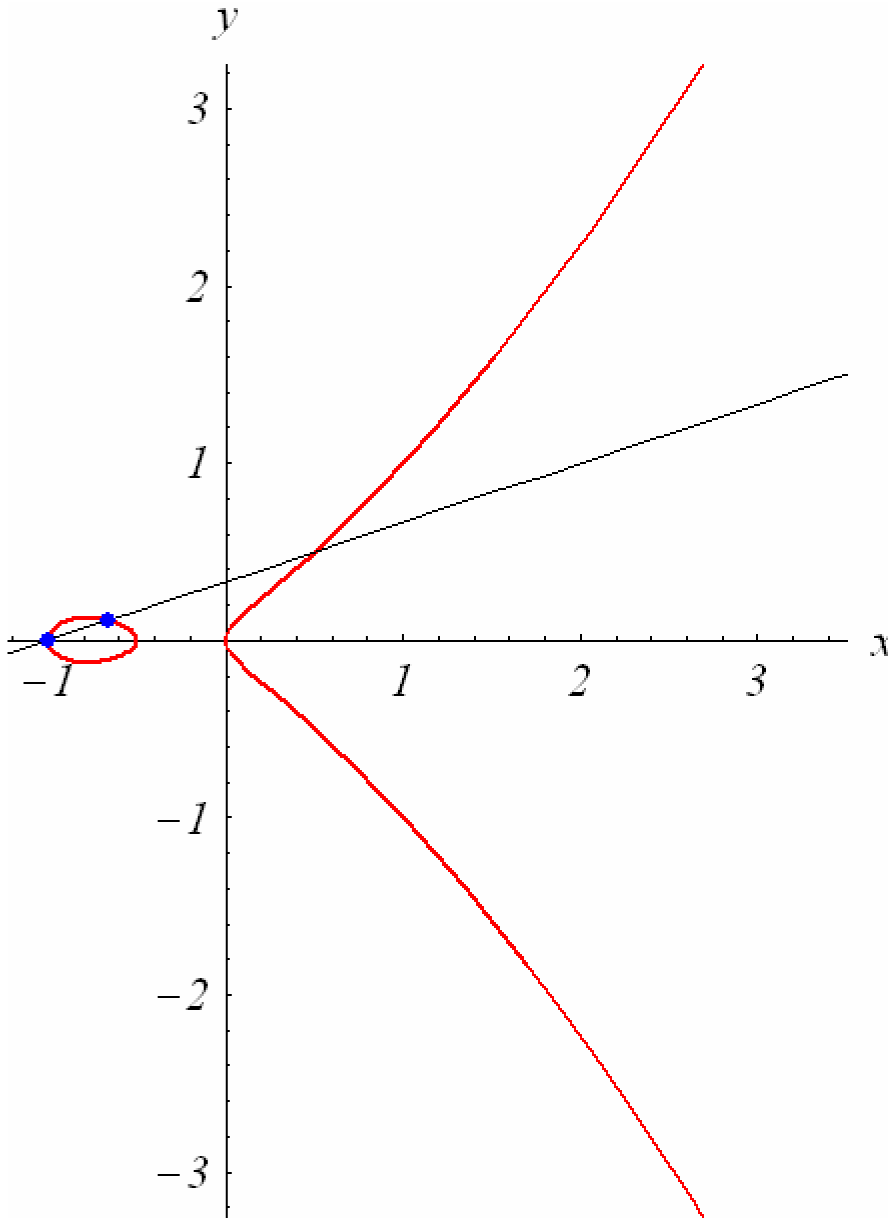
Properties of the Curve:

1. A line through any two points on the curve hits the curve in a third point.

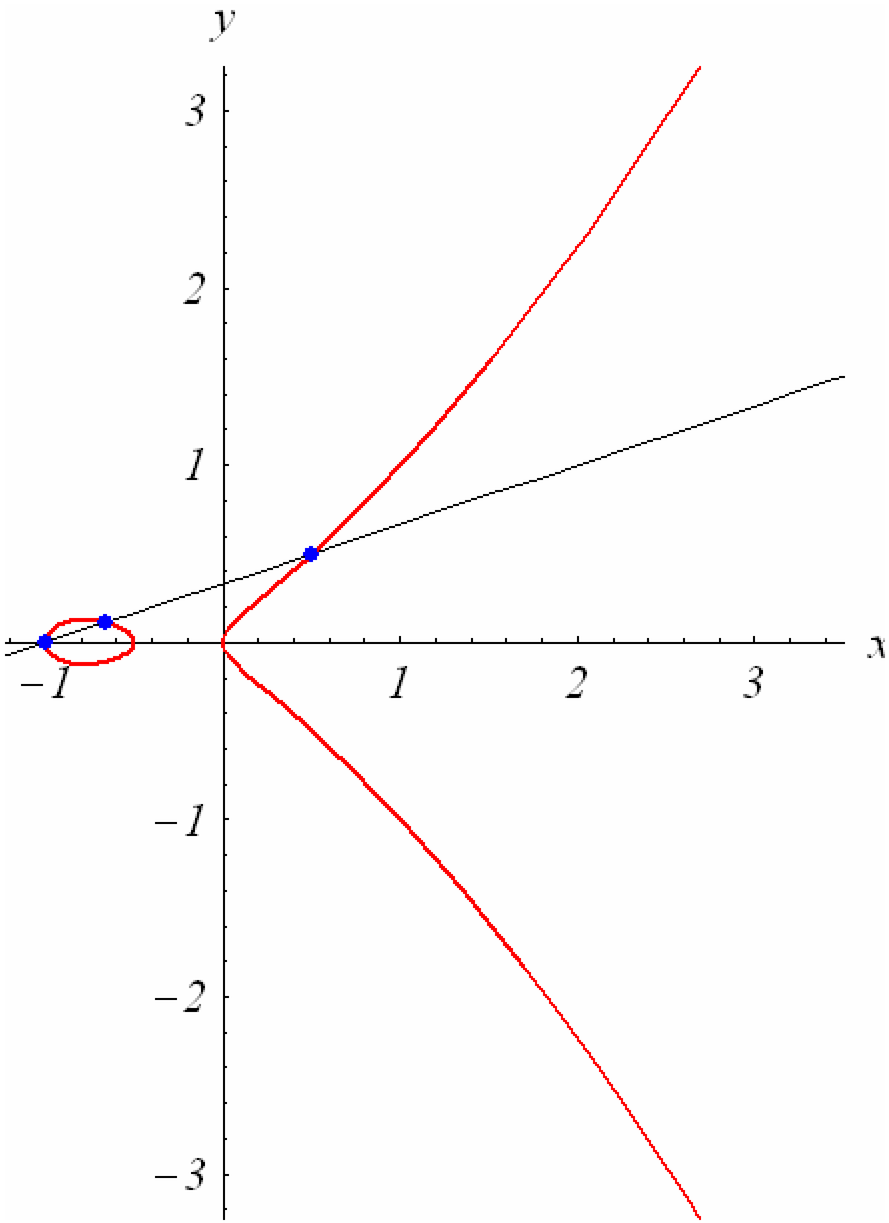
The Curve $y^2 = \frac{1}{3}x^3 + \frac{1}{2}x^2 + \frac{1}{6}x$



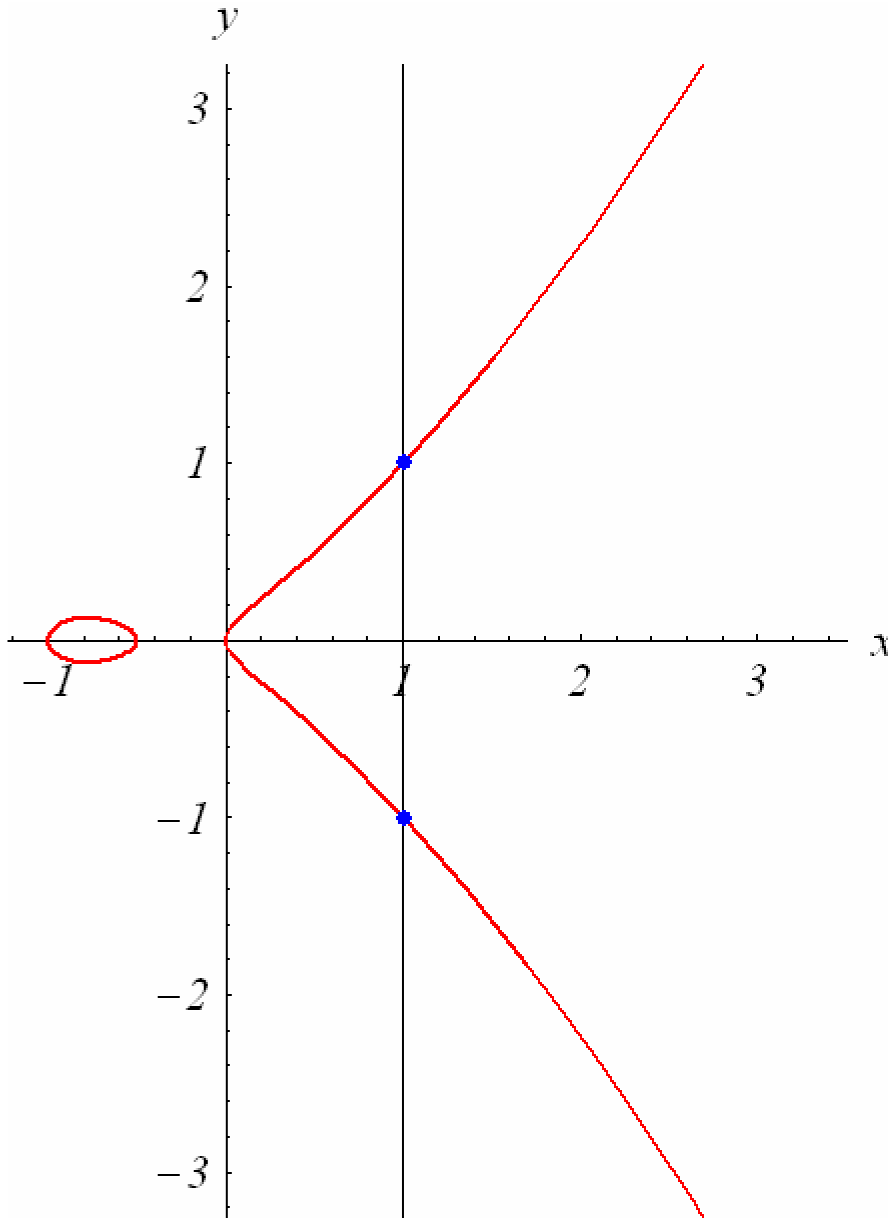
The Curve $y^2 = \frac{1}{3}x^3 + \frac{1}{2}x^2 + \frac{1}{6}x$



The Curve $y^2 = \frac{1}{3}x^3 + \frac{1}{2}x^2 + \frac{1}{6}x$



The Curve $y^2 = \frac{1}{3}x^3 + \frac{1}{2}x^2 + \frac{1}{6}x$



The Curve $y^2 = \frac{1}{3}x^3 + \frac{1}{2}x^2 + \frac{1}{6}x$

Properties of the Curve:

1. A line through any two points on the curve hits the curve in a third point *or is vertical*.

The Curve $y^2 = \frac{1}{3}x^3 + \frac{1}{2}x^2 + \frac{1}{6}x$

Properties of the Curve:

1. A line through any two points on the curve hits the curve in a third point or is vertical.
2. If the first two points have rational coordinates, so will the third.

The Curve $y^2 = \frac{1}{3}x^3 + \frac{1}{2}x^2 + \frac{1}{6}x$

Properties of the Curve:

1. A line through any two points on the curve hits the curve in a third point or is vertical.
2. If the first two points have rational coordinates, so will the third.
   Note: Two points with integral coordinates do *not* always give a third point with integral coordinates.

The Curve $y^2 = \frac{1}{3}x^3 + \frac{1}{2}x^2 + \frac{1}{6}x$

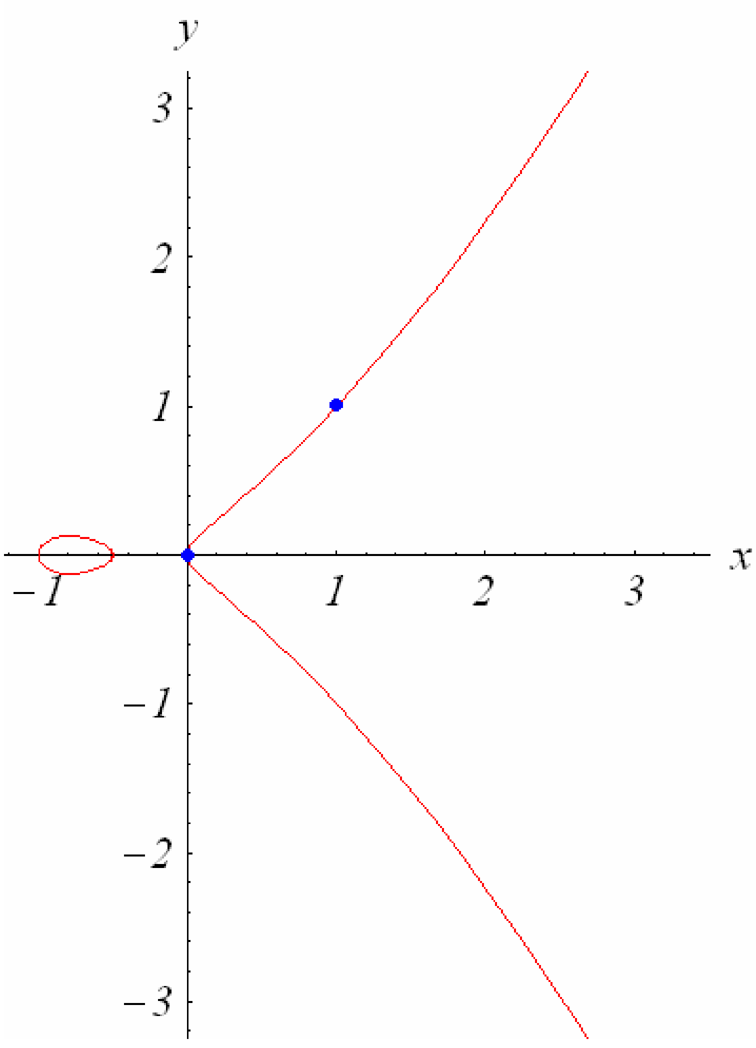
<u>Properties of the Curve:</u>

1. A line through any two points on the curve hits the curve in a third point or is vertical.
2. If the first two points have rational coordinates, so will the third.
   Note: Two points with integral coordinates do <u>*not*</u> always give a third point with integral coordinates.

- Method: Use these properties to find more rational points on the curve. Hopefully we'll find an integral point.

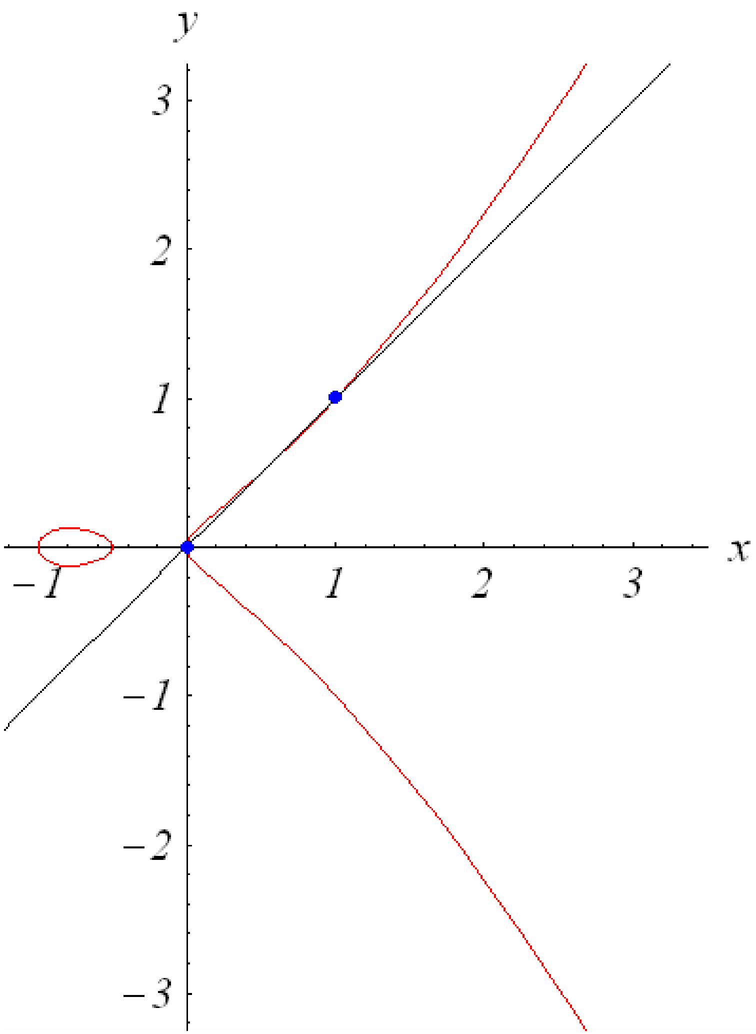
Finding New Points

- Consider the line through (0,0) and (1,1).



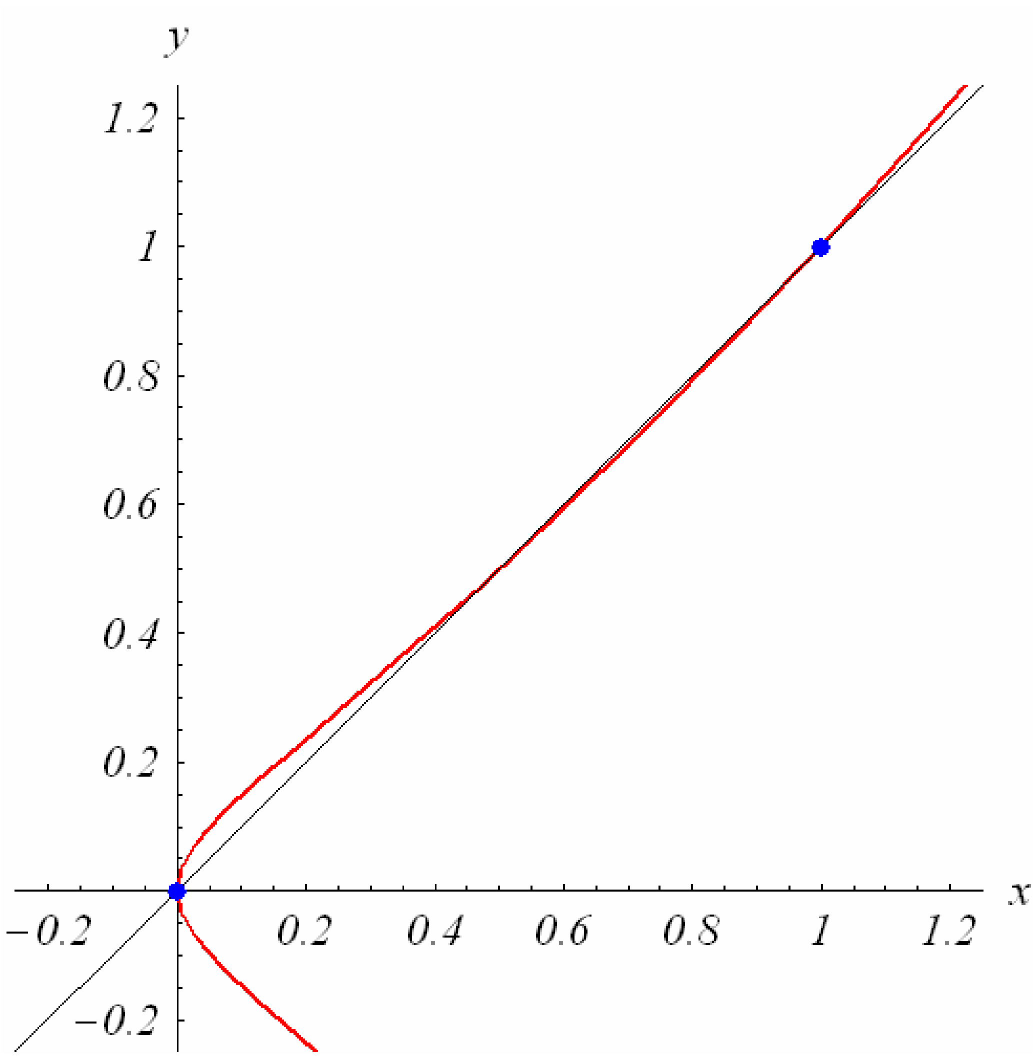
Finding New Points

- Consider the line through (0,0) and (1,1).



Finding New Points

- Consider the line through (0,0) and (1,1).



Finding New Points

- Consider the line through (0,0) and (1,1).

$$y = x$$

Finding New Points

- Consider the line through (0,0) and (1,1).

$$y = x$$

- Curve is:

$$y^2 = \tfrac{1}{3}x^3 + \tfrac{1}{2}x^2 + \tfrac{1}{6}x$$

Finding New Points

- Consider the line through (0,0) and (1,1).

$$y = x$$

- Curve is:

$$y^2 = \tfrac{1}{3}x^3 + \tfrac{1}{2}x^2 + \tfrac{1}{6}x$$

- Put them together:

$$x^2 = \tfrac{1}{3}x^3 + \tfrac{1}{2}x^2 + \tfrac{1}{6}x$$

$$\Rightarrow 0 = \tfrac{1}{3}x^3 - \tfrac{1}{2}x^2 + \tfrac{1}{6}x$$

Finding New Points

- Need to solve:

$$0 = \tfrac{1}{3}x^3 - \tfrac{1}{2}x^2 + \tfrac{1}{6}x$$

Finding New Points

- Need to solve:

$$0 = \tfrac{1}{3}x^3 - \tfrac{1}{2}x^2 + \tfrac{1}{6}x$$

- We already know two solutions, 0 and 1:

$$\tfrac{1}{3}x^3 - \tfrac{1}{2}x^2 + \tfrac{1}{6}x = x(x-1)(x-?)$$

so it's easy to find the third.

Finding New Points

- Need to solve:

$$0 = \tfrac{1}{3}x^3 - \tfrac{1}{2}x^2 + \tfrac{1}{6}x$$

- We already know two solutions, 0 and 1:

$$\tfrac{1}{3}x^3 - \tfrac{1}{2}x^2 + \tfrac{1}{6}x = x(x-1)\left(x-\tfrac{1}{2}\right)$$

so it's easy to find the third.

Finding New Points

- Need to solve:

$$0 = \tfrac{1}{3}x^3 - \tfrac{1}{2}x^2 + \tfrac{1}{6}x$$

- We already know two solutions, 0 and 1:

$$\tfrac{1}{3}x^3 - \tfrac{1}{2}x^2 + \tfrac{1}{6}x = x(x-1)\left(x - \tfrac{1}{2}\right)$$

so it's easy to find the third.

- We get a new point: $\left(\tfrac{1}{2}, \tfrac{1}{2}\right)$.

Finding New Points

- Need to solve:

$$0 = \tfrac{1}{3}x^3 - \tfrac{1}{2}x^2 + \tfrac{1}{6}x$$

- We already know two solutions, 0 and 1:

$$\tfrac{1}{3}x^3 - \tfrac{1}{2}x^2 + \tfrac{1}{6}x = x(x-1)\left(x-\tfrac{1}{2}\right)$$

so it's easy to find the third.

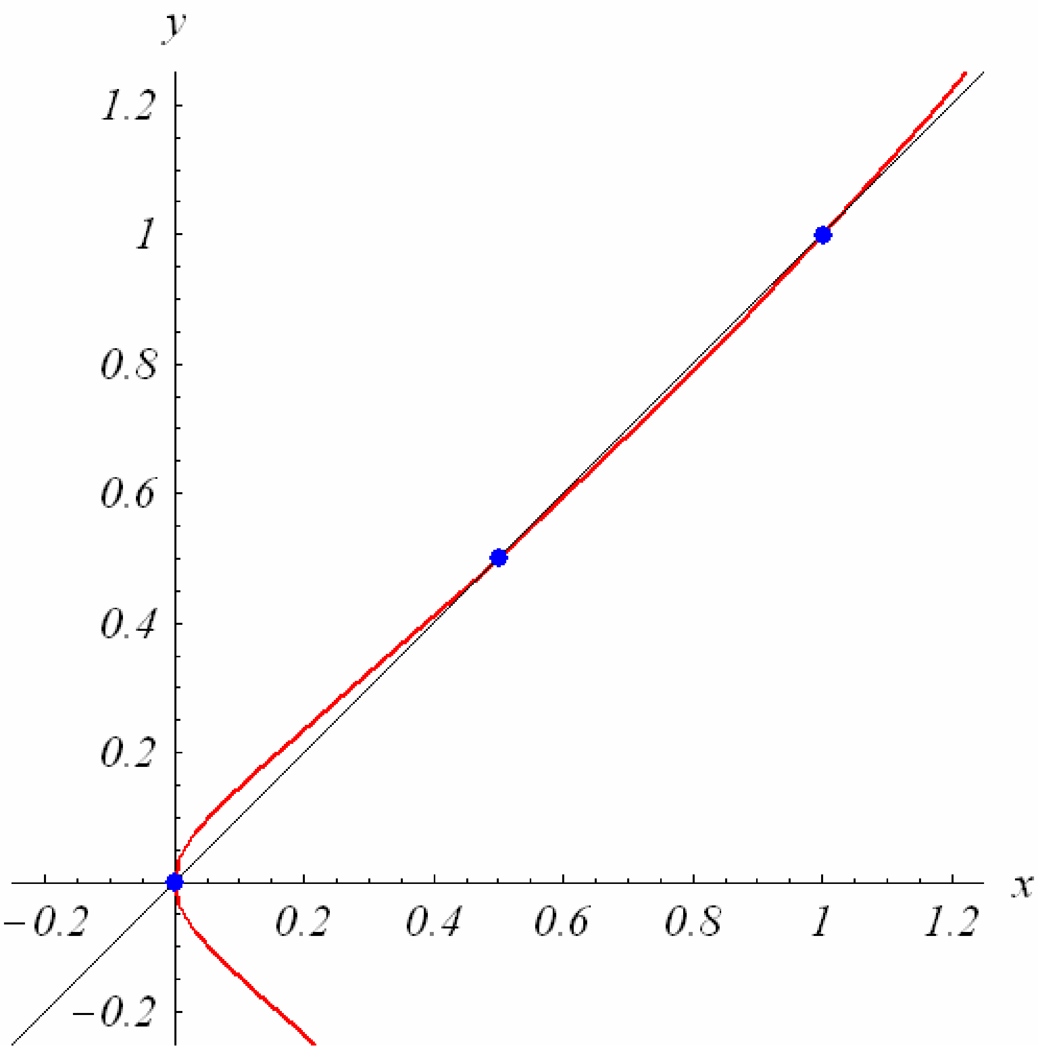
- We get a new point: $\left(\tfrac{1}{2}, \tfrac{1}{2}\right)$.

$$y^2 = \left(\tfrac{1}{2}\right)^2 = \tfrac{1}{4}$$

$$\tfrac{1}{3}x^3 + \tfrac{1}{2}x^2 + \tfrac{1}{6}x = \tfrac{1}{3}\left(\tfrac{1}{2}\right)^3 + \tfrac{1}{2}\left(\tfrac{1}{2}\right)^2 + \tfrac{1}{6}\left(\tfrac{1}{2}\right) = \tfrac{1}{4}$$

Finding New Points

- The new point on the line and curve: $\left(\frac{1}{2}, \frac{1}{2}\right)$



Finding New Points

- Need to solve:

$$0 = \tfrac{1}{3}x^3 - \tfrac{1}{2}x^2 + \tfrac{1}{6}x$$

- We already know two solutions, 0 and 1:

$$\tfrac{1}{3}x^3 - \tfrac{1}{2}x^2 + \tfrac{1}{6}x = x(x-1)\left(x-\tfrac{1}{2}\right)$$

so it's easy to find the third.

- We get a new point: $\left(\tfrac{1}{2}, \tfrac{1}{2}\right)$.
- It's not integral.

Try Again…

	(-1,0)	(0,0)	(1,-1)	(1,1)
(-1,0)				
(0,0)				
(1,-1)				
(1,1)				

Try Again…

	(-1,0)	(0,0)	(1,-1)	(1,1)
(-1,0)				
(0,0)				$\left(\frac{1}{2}, \frac{1}{2}\right)$
(1,-1)				
(1,1)		$\left(\frac{1}{2}, \frac{1}{2}\right)$		

The point found in our example.

Try Again…

	(-1,0)	(0,0)	(1,-1)	(1,1)
(-1,0)				
(0,0)			$\left(\tfrac{1}{2},-\tfrac{1}{2}\right)$	$\left(\tfrac{1}{2},\tfrac{1}{2}\right)$
(1,-1)		$\left(\tfrac{1}{2},-\tfrac{1}{2}\right)$		
(1,1)		$\left(\tfrac{1}{2},\tfrac{1}{2}\right)$		

Because of the symmetry about the x-axis.

Try Again…

	(-1,0)	(0,0)	(1,-1)	(1,1)
(-1,0)	?			
(0,0)		?	$\left(\frac{1}{2}, -\frac{1}{2}\right)$	$\left(\frac{1}{2}, \frac{1}{2}\right)$
(1,-1)		$\left(\frac{1}{2}, -\frac{1}{2}\right)$	?	
(1,1)		$\left(\frac{1}{2}, \frac{1}{2}\right)$		?

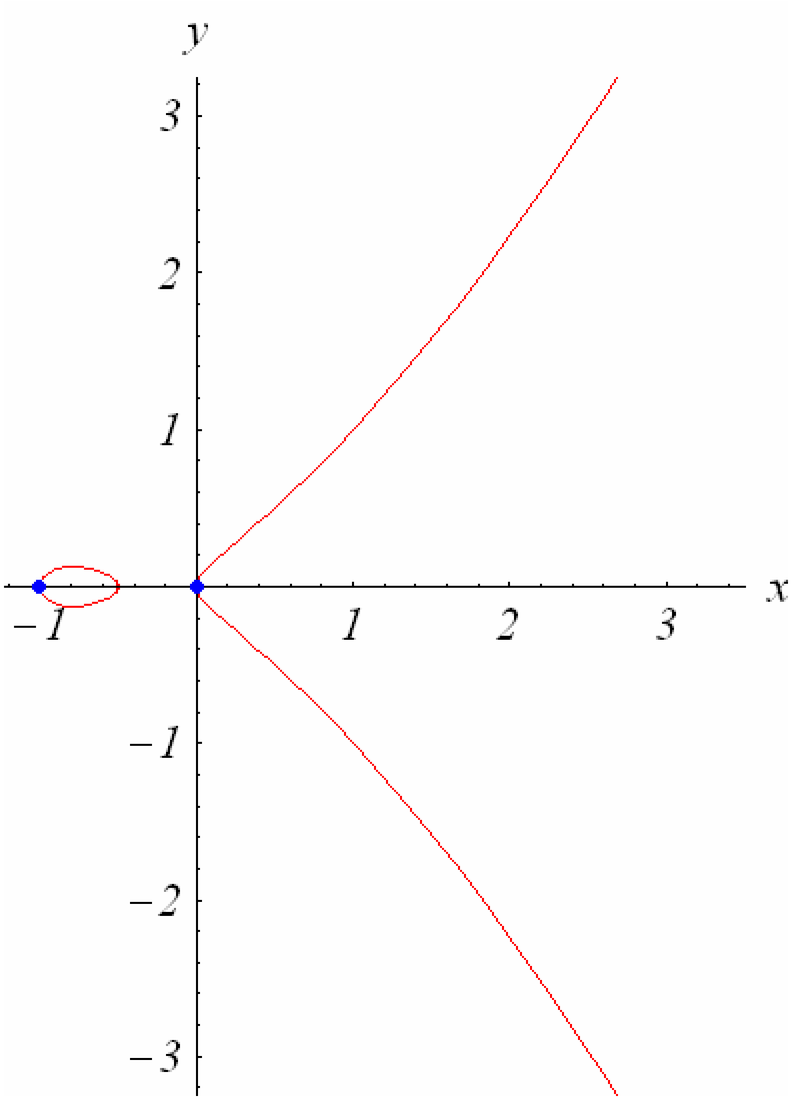
Try Again...

	(-1,0)	(0,0)	(1,-1)	(1,1)
(-1,0)	?			
(0,0)		?	$\left(\frac{1}{2}, -\frac{1}{2}\right)$	$\left(\frac{1}{2}, \frac{1}{2}\right)$
(1,-1)		$\left(\frac{1}{2}, -\frac{1}{2}\right)$	?	vertical
(1,1)		$\left(\frac{1}{2}, \frac{1}{2}\right)$	vertical	?

Try Again...

	(-1,0)	(0,0)	(1,-1)	(1,1)
(-1,0)	?			
(0,0)		?	$\left(\frac{1}{2}, -\frac{1}{2}\right)$	$\left(\frac{1}{2}, \frac{1}{2}\right)$
(1,-1)		$\left(\frac{1}{2}, -\frac{1}{2}\right)$	?	vertical
(1,1)		$\left(\frac{1}{2}, \frac{1}{2}\right)$	vertical	?

Try Again…



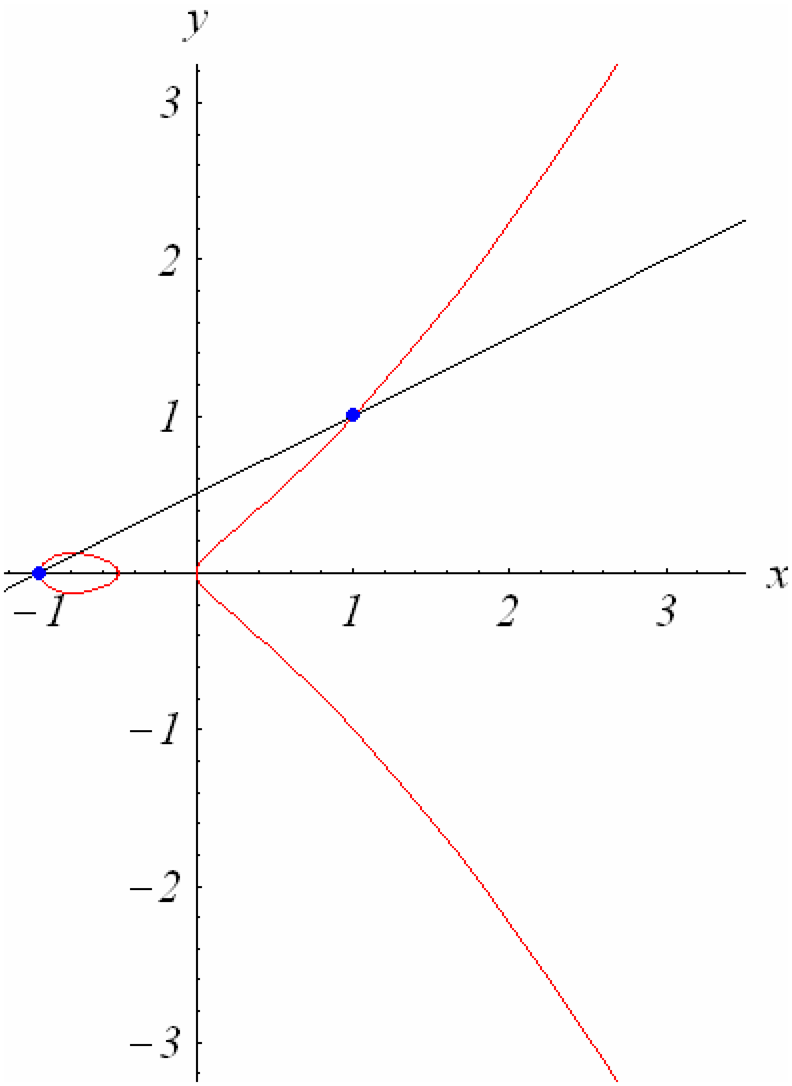
Try Again…

	(-1,0)	(0,0)	(1,-1)	(1,1)
(-1,0)	?	$\left(-\tfrac{1}{2},0\right)$		
(0,0)	$\left(-\tfrac{1}{2},0\right)$	?	$\left(\tfrac{1}{2},-\tfrac{1}{2}\right)$	$\left(\tfrac{1}{2},\tfrac{1}{2}\right)$
(1,-1)		$\left(\tfrac{1}{2},-\tfrac{1}{2}\right)$	?	vertical
(1,1)		$\left(\tfrac{1}{2},\tfrac{1}{2}\right)$	vertical	?

Try Again…

	(-1,0)	(0,0)	(1,-1)	(1,1)
(-1,0)	?	$\left(-\frac{1}{2},0\right)$		
(0,0)	$\left(-\frac{1}{2},0\right)$	?	$\left(\frac{1}{2},-\frac{1}{2}\right)$	$\left(\frac{1}{2},\frac{1}{2}\right)$
(1,-1)		$\left(\frac{1}{2},-\frac{1}{2}\right)$	?	vertical
(1,1)		$\left(\frac{1}{2},\frac{1}{2}\right)$	vertical	?

Try Again…



Try Again…

	(-1,0)	(0,0)	(1,-1)	(1,1)
(-1,0)	?	$\left(-\frac{1}{2},0\right)$		$\left(-\frac{3}{4},\frac{1}{8}\right)$
(0,0)	$\left(-\frac{1}{2},0\right)$	?	$\left(\frac{1}{2},-\frac{1}{2}\right)$	$\left(\frac{1}{2},\frac{1}{2}\right)$
(1,-1)		$\left(\frac{1}{2},-\frac{1}{2}\right)$	?	vertical
(1,1)	$\left(-\frac{3}{4},\frac{1}{8}\right)$	$\left(\frac{1}{2},\frac{1}{2}\right)$	vertical	?

Try Again…

	(-1,0)	(0,0)	(1,-1)	(1,1)
(-1,0)	?	$\left(-\frac{1}{2},0\right)$	$\left(-\frac{3}{4},-\frac{1}{8}\right)$	$\left(-\frac{3}{4},\frac{1}{8}\right)$
(0,0)	$\left(-\frac{1}{2},0\right)$	?	$\left(\frac{1}{2},-\frac{1}{2}\right)$	$\left(\frac{1}{2},\frac{1}{2}\right)$
(1,-1)	$\left(-\frac{3}{4},-\frac{1}{8}\right)$	$\left(\frac{1}{2},-\frac{1}{2}\right)$	?	vertical
(1,1)	$\left(-\frac{3}{4},\frac{1}{8}\right)$	$\left(\frac{1}{2},\frac{1}{2}\right)$	vertical	?

Because of the symmetry about the x-axis.

Try Again…

	(-1,0)	(0,0)	(1,-1)	(1,1)
(-1,0)	?	$\left(-\tfrac{1}{2},0\right)$	$\left(-\frac{3}{4},-\frac{1}{8}\right)$	$\left(-\frac{3}{4},\frac{1}{8}\right)$
(0,0)	$\left(-\tfrac{1}{2},0\right)$	?	$\left(\tfrac{1}{2},-\tfrac{1}{2}\right)$	$\left(\tfrac{1}{2},\tfrac{1}{2}\right)$
(1,-1)	$\left(-\frac{3}{4},-\frac{1}{8}\right)$	$\left(\tfrac{1}{2},-\tfrac{1}{2}\right)$	?	vertical
(1,1)	$\left(-\frac{3}{4},\frac{1}{8}\right)$	$\left(\tfrac{1}{2},\tfrac{1}{2}\right)$	vertical	?

No new integral points.

Try Again…

	(-1,0)	(0,0)	(1,-1)	(1,1)
(-1,0)	?	$\left(-\tfrac{1}{2},0\right)$	$\left(-\frac{3}{4},-\frac{1}{8}\right)$	$\left(-\frac{3}{4},\frac{1}{8}\right)$
(0,0)	$\left(-\tfrac{1}{2},0\right)$	?	$\left(\tfrac{1}{2},-\tfrac{1}{2}\right)$	$\left(\tfrac{1}{2},\tfrac{1}{2}\right)$
(1,-1)	$\left(-\frac{3}{4},-\frac{1}{8}\right)$	$\left(\tfrac{1}{2},-\tfrac{1}{2}\right)$	?	vertical
(1,1)	$\left(-\frac{3}{4},\frac{1}{8}\right)$	$\left(\tfrac{1}{2},\tfrac{1}{2}\right)$	vertical	?

Something old, something new…

…and Again!

- Take the line through $\left(\frac{1}{2}, -\frac{1}{2}\right)$ and (1,1).

$$y = 3x - 2$$

…and Again!

- Take the line through $\left(\tfrac{1}{2}, -\tfrac{1}{2}\right)$ and (1,1).

$$y = 3x - 2$$

- Put this into the curve:

$$(3x-2)^2 = \tfrac{1}{3}x^3 + \tfrac{1}{2}x^2 + \tfrac{1}{6}x$$

$$0 = \tfrac{1}{3}x^3 - \tfrac{17}{2}x^2 + \tfrac{73}{6}x - 4$$

…and Again!

- Take the line through $\left(\tfrac{1}{2}, -\tfrac{1}{2}\right)$ and (1,1).

$$y = 3x - 2$$

- Put this into the curve:

$$(3x-2)^2 = \tfrac{1}{3}x^3 + \tfrac{1}{2}x^2 + \tfrac{1}{6}x$$

$$0 = \tfrac{1}{3}x^3 - \tfrac{17}{2}x^2 + \tfrac{73}{6}x - 4$$

$$0 = \left(x - \tfrac{1}{2}\right)\left(x-1\right)\left(x-?\right)$$

…and Again!

- Take the line through $\left(\tfrac{1}{2}, -\tfrac{1}{2}\right)$ and (1,1).

$$y = 3x - 2$$

- Put this into the curve:

$$(3x-2)^2 = \tfrac{1}{3}x^3 + \tfrac{1}{2}x^2 + \tfrac{1}{6}x$$

$$0 = \tfrac{1}{3}x^3 - \tfrac{17}{2}x^2 + \tfrac{73}{6}x - 4$$

$$0 = \left(x - \tfrac{1}{2}\right)\left(x - 1\right)\left(x - 24\right)$$

…and Again!

- Take the line through $\left(\tfrac{1}{2},-\tfrac{1}{2}\right)$ and (1,1).

$$y = 3x - 2$$

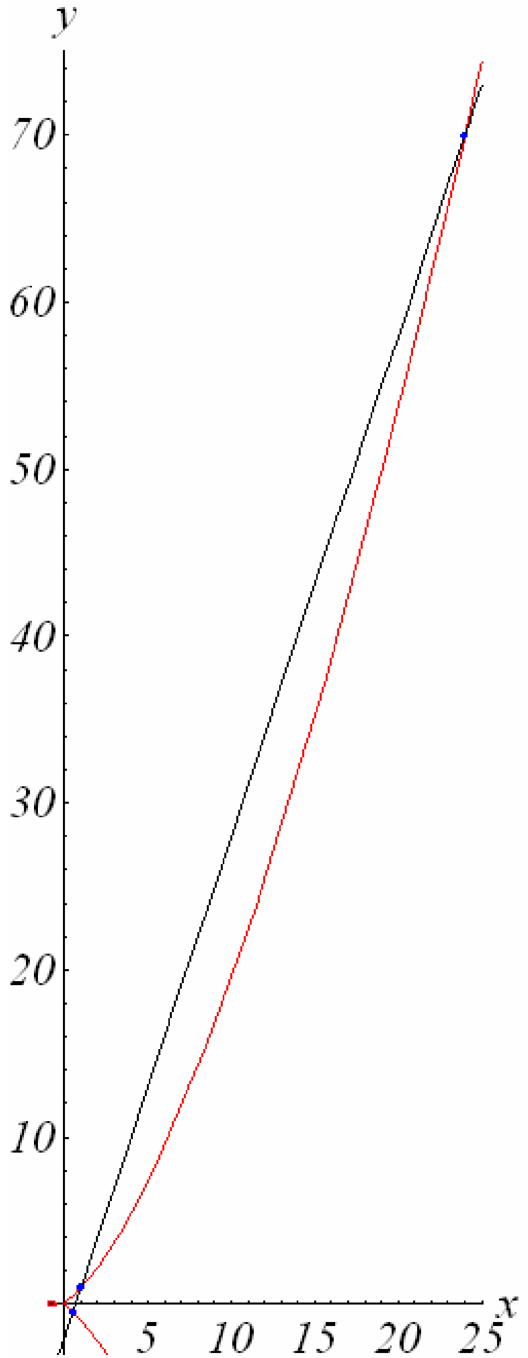
- Put this into the curve:

$$(3x-2)^2 = \tfrac{1}{3}x^3 + \tfrac{1}{2}x^2 + \tfrac{1}{6}x$$

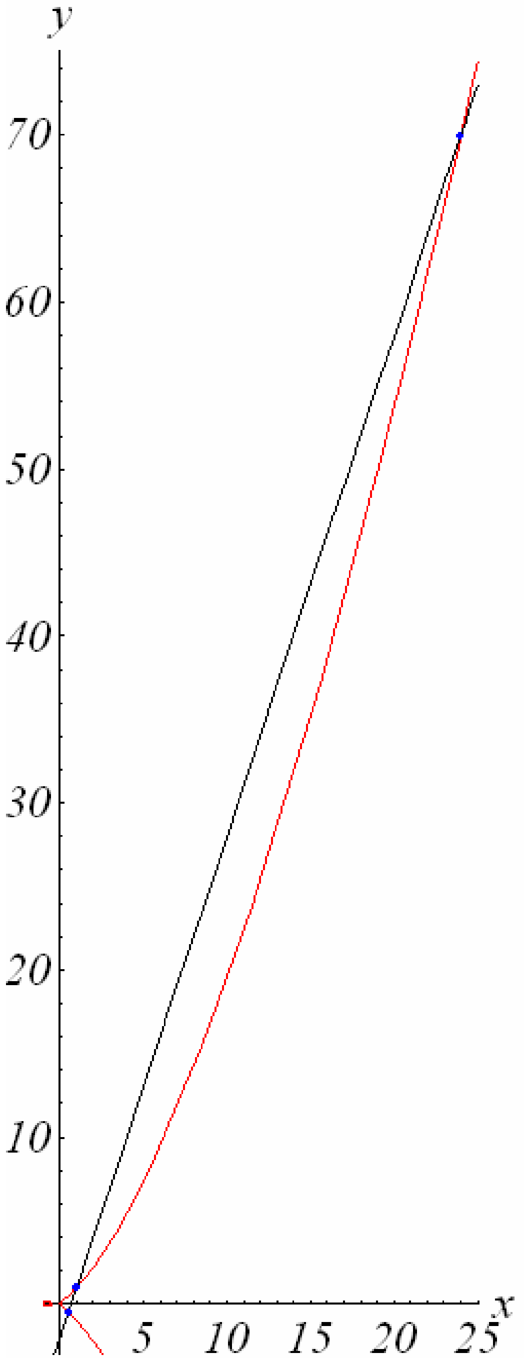
$$0 = \tfrac{1}{3}x^3 - \tfrac{17}{2}x^2 + \tfrac{73}{6}x - 4$$

$$0 = \left(x - \tfrac{1}{2}\right)\left(x-1\right)\left(x-24\right)$$

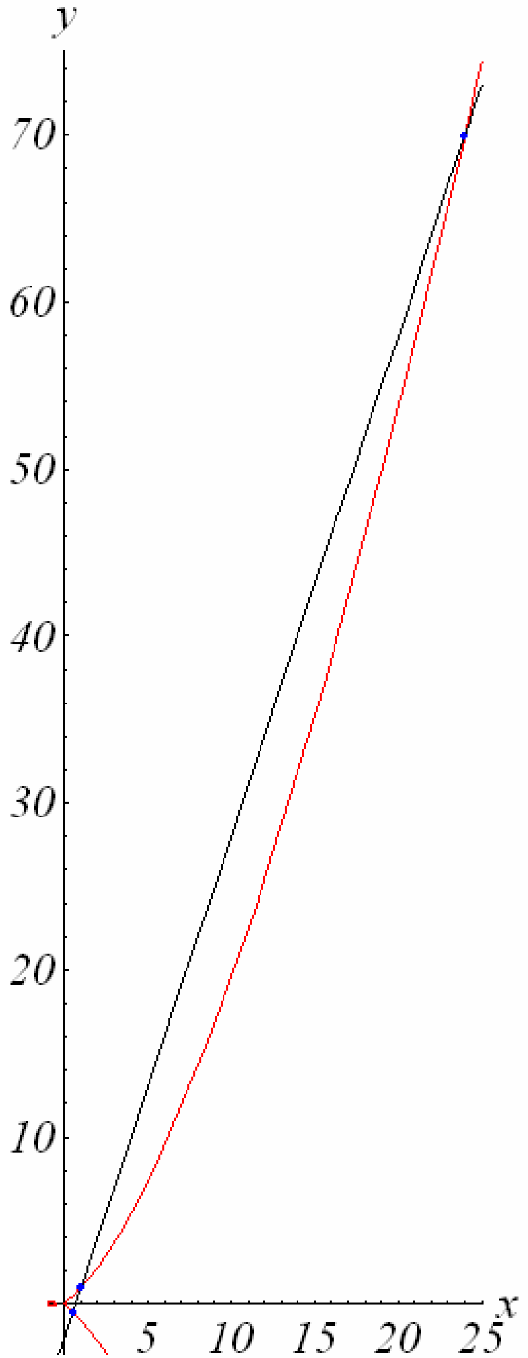
- This gives the point (24,70).


y
70
60
50
40
30
20
10
x
5
10
15
20
25

Cannonballs Solution



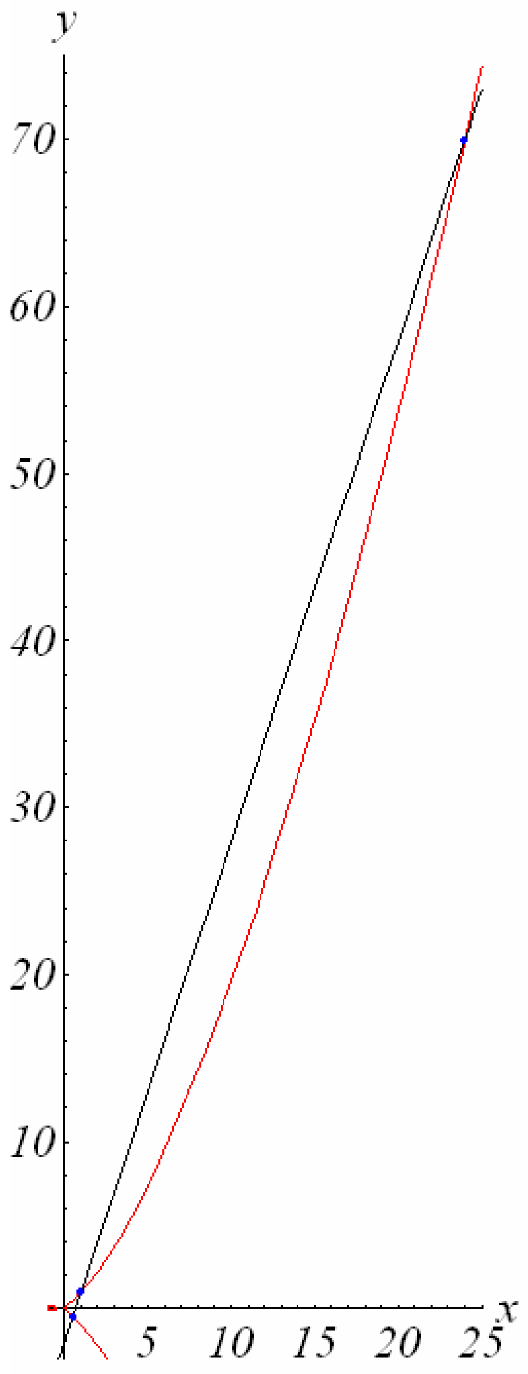
$$70^2 = 1^2 + 2^2 + \ldots + 24^2$$



Cannonballs Solution

$$70^2 = 1^2 + 2^2 + \ldots + 24^2$$

- A 70x70 square of cannonballs contains 4900 cannonballs.
- A pyramid of height 24 also contains 4900 cannonballs.

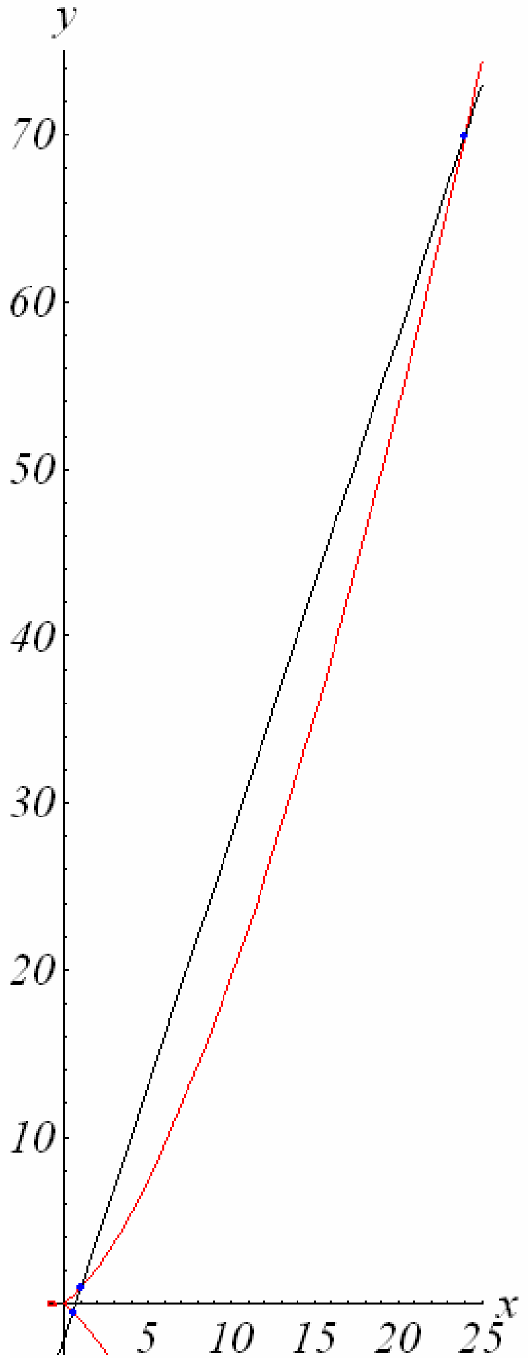


Cannonballs Solution

$$70^2 = 1^2 + 2^2 + \ldots + 24^2$$

- A 70x70 square of cannonballs contains 4900 cannonballs.
- A pyramid of height 24 also contains 4900 cannonballs.

Are there any more solutions?



Cannonballs Solution

$$70^2 = 1^2 + 2^2 + \ldots + 24^2$$

- A 70x70 square of cannonballs contains 4900 cannonballs.
- A pyramid of height 24 also contains 4900 cannonballs.

Are there any more solutions?

Watson (1918): No.

Beyond Cannonballs

- The curve

$$y^2 = \tfrac{1}{3}x^3 + \tfrac{1}{2}x^2 + \tfrac{1}{6}x$$

is an example of an Elliptic Curve.

Beyond Cannonballs

- The curve

$$y^2 = \tfrac{1}{3}x^3 + \tfrac{1}{2}x^2 + \tfrac{1}{6}x$$

  is an example of an Elliptic Curve.

- Elliptic curves are special because you can “add” two points to get a third.

Beyond Cannonballs

- The curve

$$y^2 = \tfrac{1}{3}x^3 + \tfrac{1}{2}x^2 + \tfrac{1}{6}x$$

is an example of an Elliptic Curve.

- Elliptic curves are special because you can “add” two points to get a third.
  - When adding a point to itself, use the tangent line.

Beyond Cannonballs

- The curve

$$y^2 = \tfrac{1}{3}x^3 + \tfrac{1}{2}x^2 + \tfrac{1}{6}x$$

  is an example of an Elliptic Curve.

- Elliptic curves are special because you can “add” two points to get a third.

  – When adding a point to itself, use the tangent line.

  – Need to include one more special point, ¥, that lies at the top and bottom of every vertical line.

Addition Table

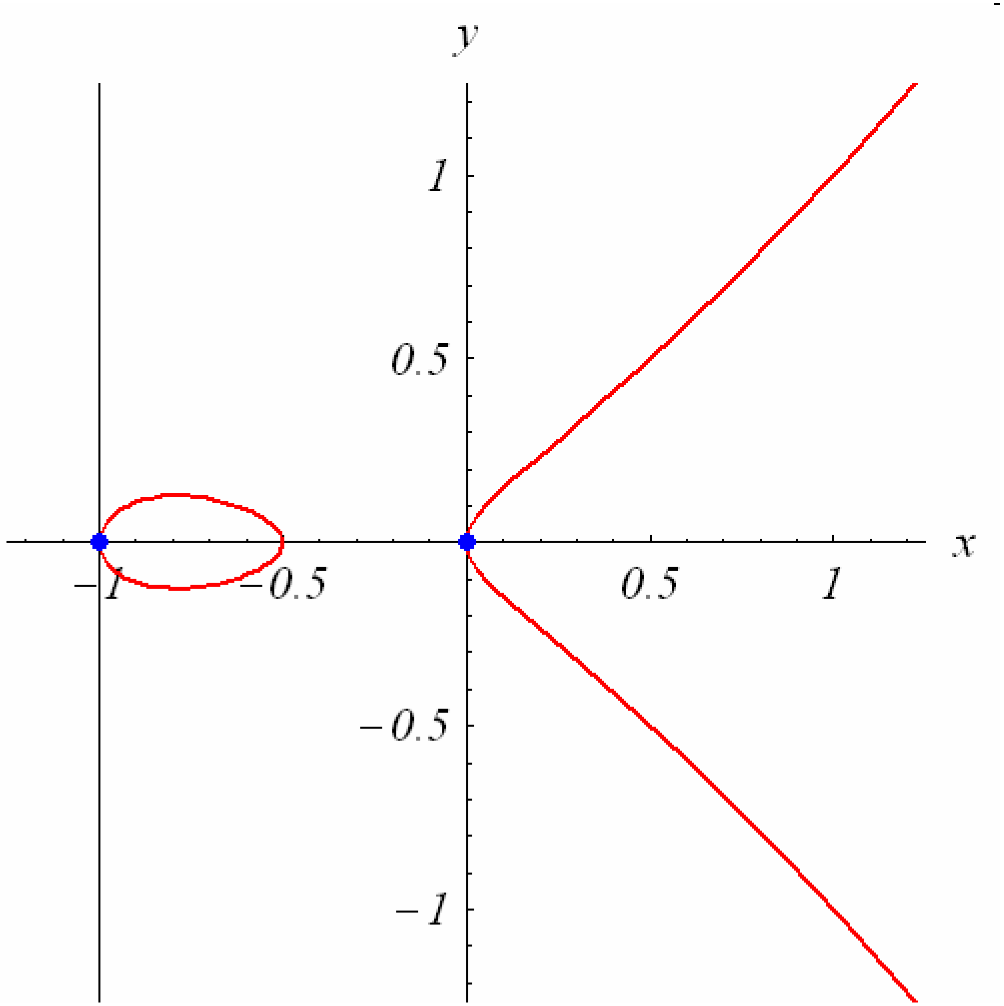
	(-1,0)	(0,0)	(1,-1)	(1,1)
(-1,0)	?	$\left(-\frac{1}{2},0\right)$	$\left(-\frac{3}{4},-\frac{1}{8}\right)$	$\left(-\frac{3}{4},\frac{1}{8}\right)$
(0,0)	$\left(-\frac{1}{2},0\right)$	?	$\left(\frac{1}{2},-\frac{1}{2}\right)$	$\left(\frac{1}{2},\frac{1}{2}\right)$
(1,-1)	$\left(-\frac{3}{4},-\frac{1}{8}\right)$	$\left(\frac{1}{2},-\frac{1}{2}\right)$	?	vertical
(1,1)	$\left(-\frac{3}{4},\frac{1}{8}\right)$	$\left(\frac{1}{2},\frac{1}{2}\right)$	vertical	?

Addition Table

	(-1,0)	(0,0)	(1,-1)	(1,1)
(-1,0)	?	$\left(-\tfrac{1}{2},0\right)$	$\left(-\frac{3}{4},-\frac{1}{8}\right)$	$\left(-\frac{3}{4},\frac{1}{8}\right)$
(0,0)	$\left(-\tfrac{1}{2},0\right)$	?	$\left(\tfrac{1}{2},-\tfrac{1}{2}\right)$	$\left(\tfrac{1}{2},\tfrac{1}{2}\right)$
(1,-1)	$\left(-\frac{3}{4},-\frac{1}{8}\right)$	$\left(\tfrac{1}{2},-\tfrac{1}{2}\right)$	?	¥
(1,1)	$\left(-\frac{3}{4},\frac{1}{8}\right)$	$\left(\tfrac{1}{2},\tfrac{1}{2}\right)$	¥	?

Vertical lines include the point ¥

Tangent Lines Through (-1,0) and (0,0)

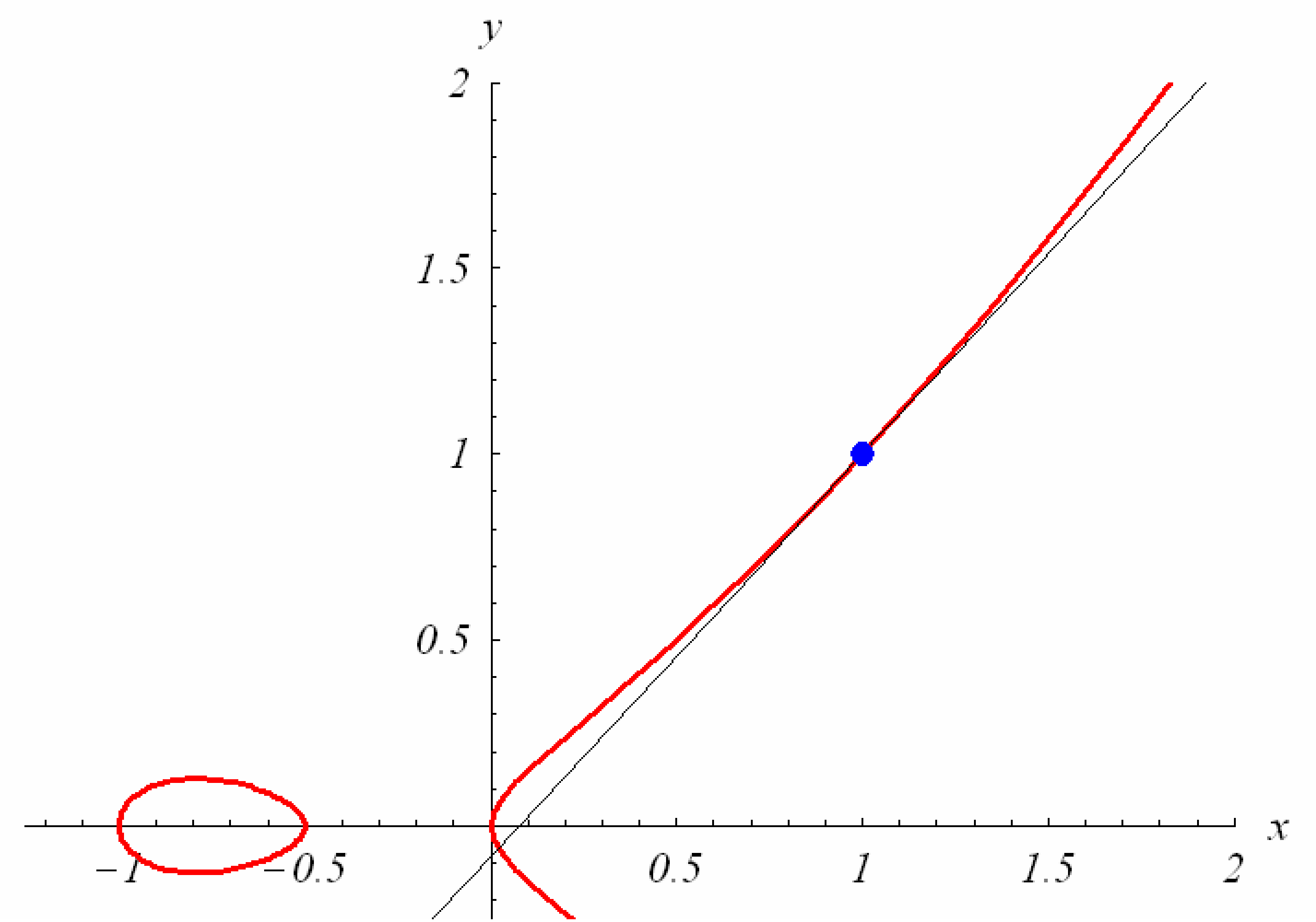


Addition Table

	(-1,0)	(0,0)	(1,-1)	(1,1)
(-1,0)	¥	$\left(-\tfrac{1}{2}, 0\right)$	$\left(-\frac{3}{4}, -\frac{1}{8}\right)$	$\left(-\frac{3}{4}, \frac{1}{8}\right)$
(0,0)	$\left(-\tfrac{1}{2}, 0\right)$	¥	$\left(\tfrac{1}{2}, -\tfrac{1}{2}\right)$	$\left(\tfrac{1}{2}, \tfrac{1}{2}\right)$
(1,-1)	$\left(-\frac{3}{4}, -\frac{1}{8}\right)$	$\left(\tfrac{1}{2}, -\tfrac{1}{2}\right)$	?	¥
(1,1)	$\left(-\frac{3}{4}, \frac{1}{8}\right)$	$\left(\tfrac{1}{2}, \tfrac{1}{2}\right)$	¥	?

Vertical lines include the point ¥

Tangent Line Through (1,1)



Addition Table

	(-1,0)	(0,0)	(1,-1)	(1,1)
(-1,0)	¥	$\left(-\tfrac{1}{2},0\right)$	$\left(-\frac{3}{4},-\frac{1}{8}\right)$	$\left(-\frac{3}{4},\frac{1}{8}\right)$
(0,0)	$\left(-\tfrac{1}{2},0\right)$	¥	$\left(\tfrac{1}{2},-\tfrac{1}{2}\right)$	$\left(\tfrac{1}{2},\tfrac{1}{2}\right)$
(1,-1)	$\left(-\frac{3}{4},-\frac{1}{8}\right)$	$\left(\tfrac{1}{2},-\tfrac{1}{2}\right)$	?	¥
(1,1)	$\left(-\frac{3}{4},\frac{1}{8}\right)$	$\left(\tfrac{1}{2},\tfrac{1}{2}\right)$	¥	$\left(\frac{1}{48},\frac{-35}{576}\right)$

Addition Table

	(-1,0)	(0,0)	(1,-1)	(1,1)
(-1,0)	¥	$\left(-\frac{1}{2},0\right)$	$\left(-\frac{3}{4},-\frac{1}{8}\right)$	$\left(-\frac{3}{4},\frac{1}{8}\right)$
(0,0)	$\left(-\frac{1}{2},0\right)$	¥	$\left(\frac{1}{2},-\frac{1}{2}\right)$	$\left(\frac{1}{2},\frac{1}{2}\right)$
(1,-1)	$\left(-\frac{3}{4},-\frac{1}{8}\right)$	$\left(\frac{1}{2},-\frac{1}{2}\right)$	$\left(\frac{1}{48},\frac{35}{576}\right)$	¥
(1,1)	$\left(-\frac{3}{4},\frac{1}{8}\right)$	$\left(\frac{1}{2},\frac{1}{2}\right)$	¥	$\left(\frac{1}{48},\frac{-35}{576}\right)$

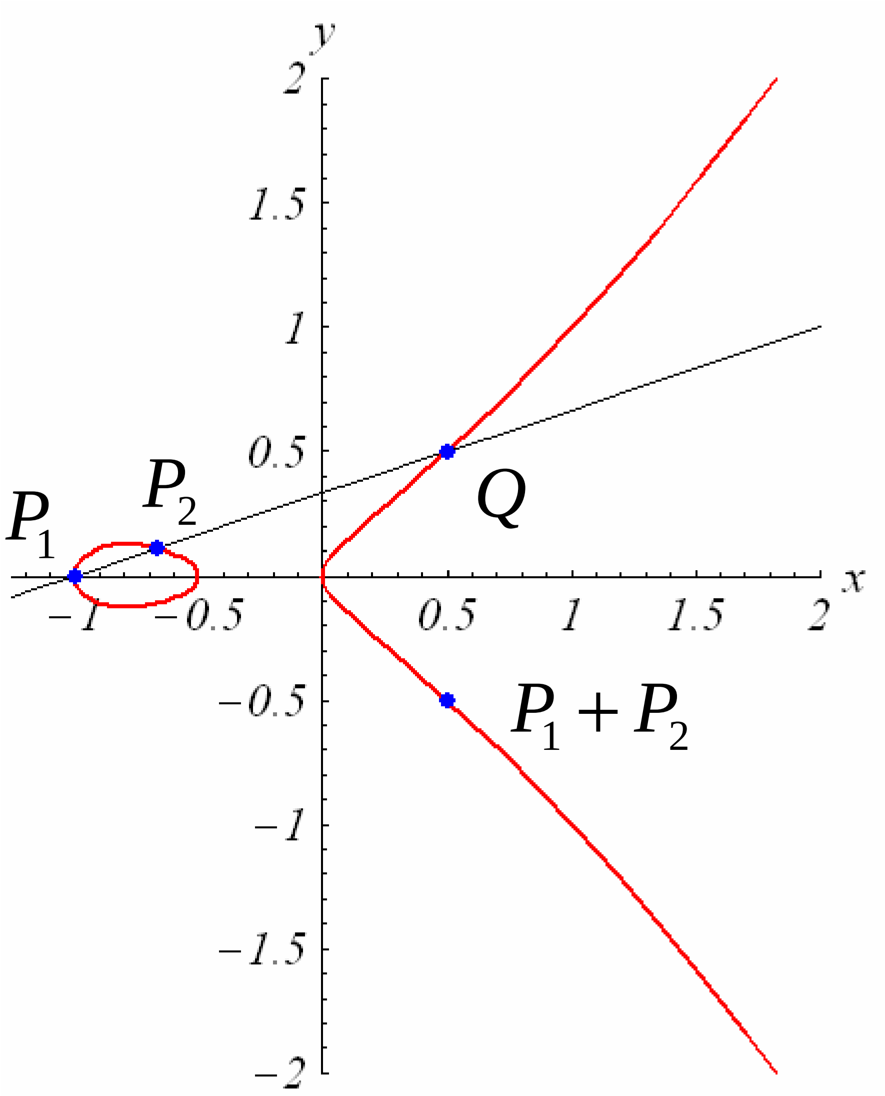
Because of the symmetry about the x-axis.

Addition Table

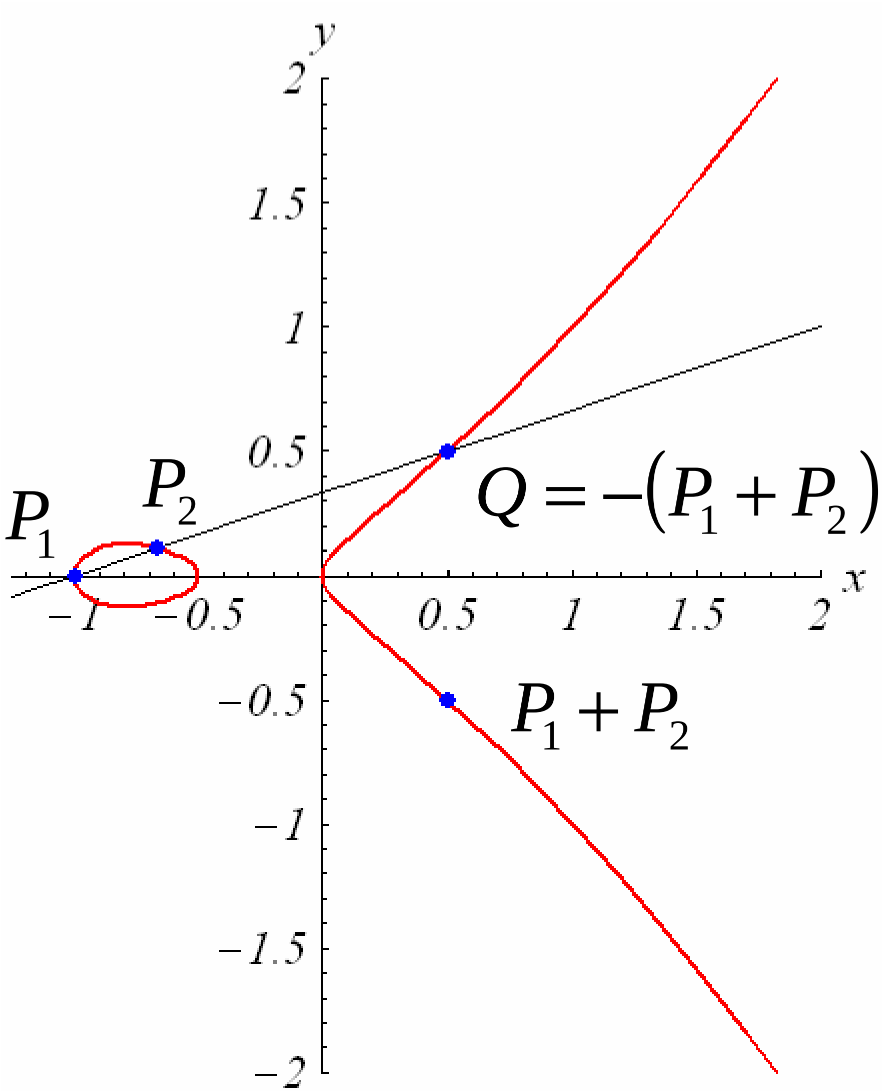
	(-1,0)	(0,0)	(1,-1)	(1,1)
(-1,0)	¥	$\left(-\,{}^{1}\!/_{2},0\right)$	$\left(-\frac{3}{4},-\frac{1}{8}\right)$	$\left(-\frac{3}{4},\frac{1}{8}\right)$
(0,0)	$\left(-\,{}^{1}\!/_{2},0\right)$	¥	$\left({}^{1}\!/_{2},-\,{}^{1}\!/_{2}\right)$	$\left({}^{1}\!/_{2},{}^{1}\!/_{2}\right)$
(1,-1)	$\left(-\frac{3}{4},-\frac{1}{8}\right)$	$\left({}^{1}\!/_{2},-\,{}^{1}\!/_{2}\right)$	$\left(\frac{1}{48},\frac{35}{576}\right)$	¥
(1,1)	$\left(-\frac{3}{4},\frac{1}{8}\right)$	$\left({}^{1}\!/_{2},{}^{1}\!/_{2}\right)$	¥	$\left(\frac{1}{48},\frac{-35}{576}\right)$

Adding Points the Right Way

Adding Points the Right Way



Adding Points the Right Way



Addition Table

+	(-1,0)	(0,0)	(1,-1)	(1,1)
(-1,0)	¥	$\left(-\tfrac{1}{2},0\right)$	$\left(-\frac{3}{4},\frac{1}{8}\right)$	$\left(-\frac{3}{4},-\frac{1}{8}\right)$
(0,0)	$\left(-\tfrac{1}{2},0\right)$	¥	$\left(\tfrac{1}{2},\tfrac{1}{2}\right)$	$\left(\tfrac{1}{2},-\tfrac{1}{2}\right)$
(1,-1)	$\left(-\frac{3}{4},\frac{1}{8}\right)$	$\left(\tfrac{1}{2},\tfrac{1}{2}\right)$	$\left(\frac{1}{48},\frac{-35}{576}\right)$	¥
(1,1)	$\left(-\frac{3}{4},-\frac{1}{8}\right)$	$\left(\tfrac{1}{2},-\tfrac{1}{2}\right)$	¥	$\left(\frac{1}{48},\frac{35}{576}\right)$

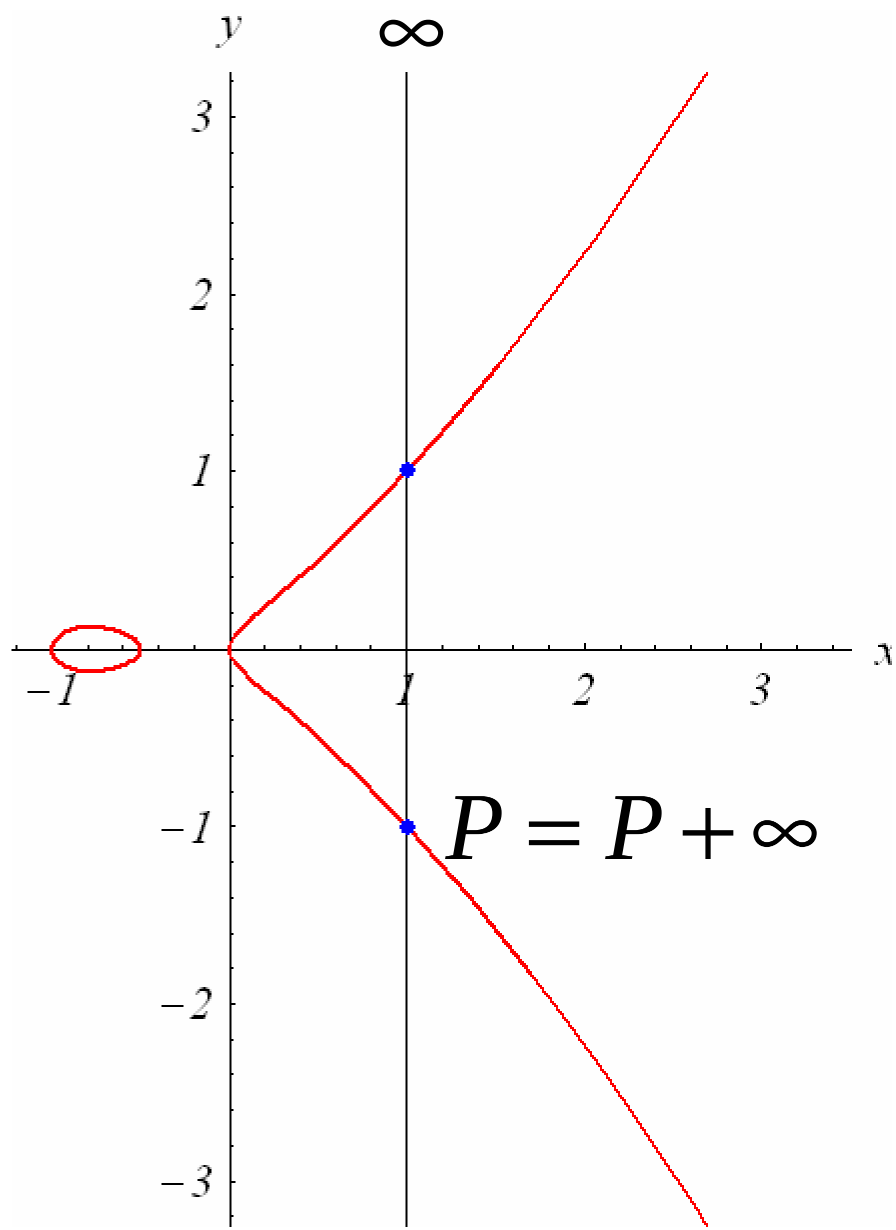
Reverses the sign on the y-coordinate.

Why Do We Add Points This Way?

- By defining addition of points using the reflected point, addition of points behaves like addition of numbers.

Why Do We Add Points This Way?

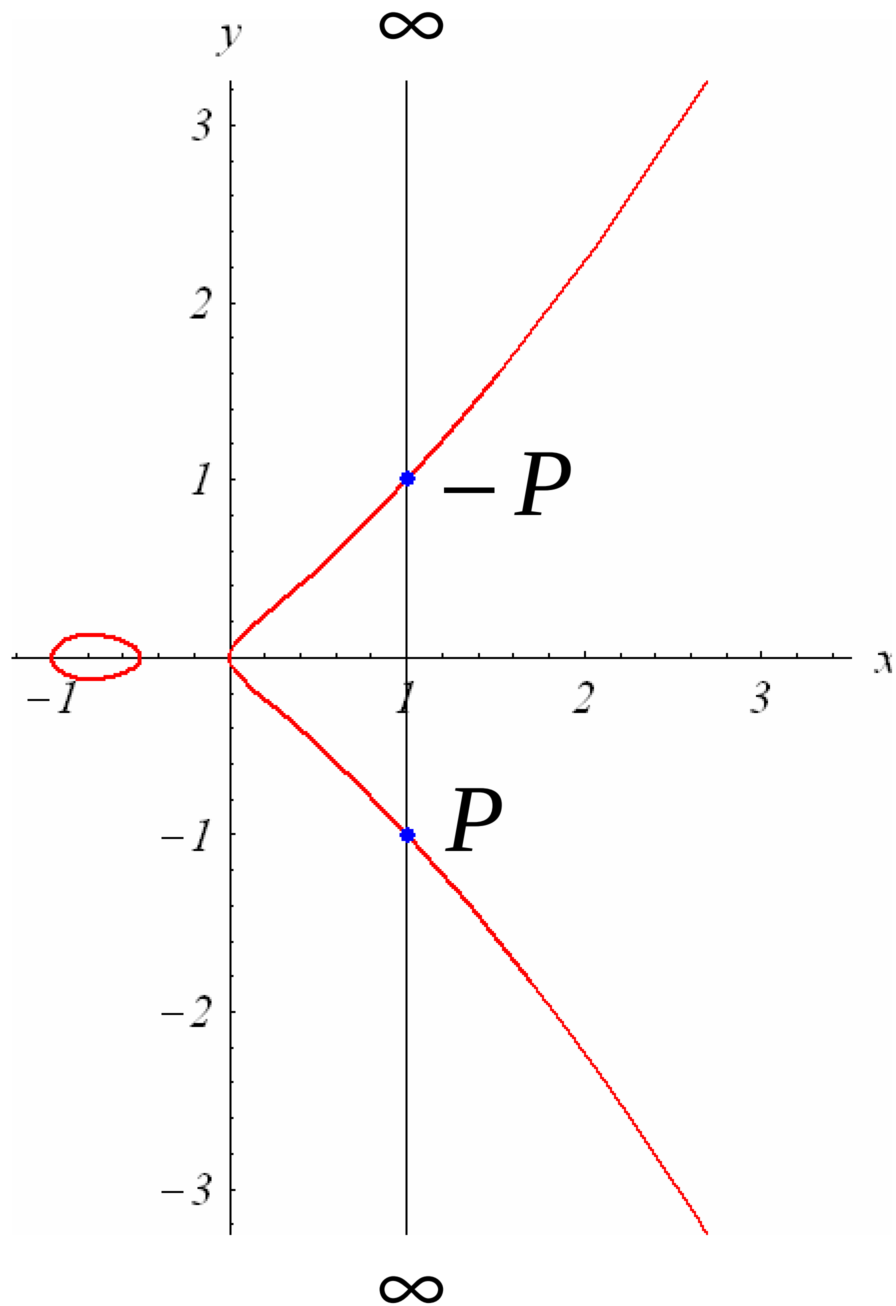
- By defining addition of points using the reflected point, addition of points behaves like addition of numbers.
- Identity: $P + \infty = P$



y
∞
3
2
1
−1
−2
−3
x
−1
1
2
3
$P = P + \infty$

Why Do We Add Points This Way?

- By defining addition of points using the reflected point, addition of points behaves like addition of numbers.
- Identity: $P + \infty = P$
- Inverses: $P + \left(-P\right) = \infty$



∞
y
3
2
1
$-P$
x
-1
1
2
3
P
-1
-2
-3
∞

Why Do We Add Points This Way?

- By defining addition of points using the reflected point, addition of points behaves like addition of numbers.
- Identity: $$P + \infty = P$$
- Inverses: $$P + (-P) = \infty$$
- Associativity: $$(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$$

Why Do We Add Points This Way?

- By defining addition of points using the reflected point, addition of points behaves like addition of numbers.
- Identity: $P + \infty = P$
- Inverses: $P + \left(-P\right) = \infty$
- Associativity: $\left(P_1 + P_2\right) + P_3 = P_1 + \left(P_2 + P_3\right)$
- Commutivity: $P_1 + P_2 = P_2 + P_1$

Why Do We Add Points This Way?

- By defining addition of points using the reflected point, addition of points behaves like addition of numbers.
- Identity: $P + \infty = P$
- Inverses: $P + (-P) = \infty$
- Associativity: $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$
- Commutivity: $P_1 + P_2 = P_2 + P_1$
- The rational points form an abelian group.

Real World Applications

Real World Applications

- Cryptography

Real World Applications

- Cryptography
- Define

$$nP = \underbrace{P + P + \ldots + P}_{n \text{ times}}$$

Real World Applications

- Cryptography
- Define

$$nP = \underbrace{P + P + \ldots + P}_{n \text{ times}}$$

Recall: Adding points means drawing lines and solving for intersections.

Addition Table

+	(-1,0)	(0,0)	(1,-1)	(1,1)
(-1,0)	¥	$\left(-\tfrac{1}{2},0\right)$	$\left(-\frac{3}{4},\frac{1}{8}\right)$	$\left(-\frac{3}{4},-\frac{1}{8}\right)$
(0,0)	$\left(-\tfrac{1}{2},0\right)$	¥	$\left(\tfrac{1}{2},\tfrac{1}{2}\right)$	$\left(\tfrac{1}{2},-\tfrac{1}{2}\right)$
(1,-1)	$\left(-\frac{3}{4},\frac{1}{8}\right)$	$\left(\tfrac{1}{2},\tfrac{1}{2}\right)$	$\left(\frac{1}{48},\frac{-35}{576}\right)$	¥
(1,1)	$\left(-\frac{3}{4},-\frac{1}{8}\right)$	$\left(\tfrac{1}{2},-\tfrac{1}{2}\right)$	¥	$\left(\frac{1}{48},\frac{35}{576}\right)$

For example: $2\left(1,-1\right)=\left(\frac{1}{48},\frac{-35}{576}\right)$.

Real World Applications

- Cryptography
- Define

$$nP = \underbrace{P + P + \ldots + P}_{n \text{ times}}$$

Recall: Adding points means drawing lines and solving for intersections.

Real World Applications

- Cryptography
- Define

$$nP = \underbrace{P + P + \ldots + P}_{n \text{ times}}$$

Recall: Adding points means drawing lines and solving for intersections.

- To find $3(1,-1)$, use the line through $\left(\frac{1}{48}, \frac{-35}{576}\right)$ and $(1,-1)$, determine the new intersection with the curve and reflect.

Real World Applications

- Really Hard Problem:

  Given two points on the curve P and Q, find an integer n such that

$$Q = nP$$

Real World Applications

- Really Hard Problem:

  Given two points on the curve P and Q, find an integer n such that

$$Q = nP$$

- Example: $\left(\frac{1324801}{235200}, \frac{1726556399}{197568000}\right) = n(1,-1)$.

Real World Applications

- Really Hard Problem:

  Given two points on the curve P and Q, find an integer n such that

$$Q = nP$$

- Example: $\left(\frac{1324801}{235200}, \frac{1726556399}{197568000}\right) = n(1,-1)$.
- If n is really large (~200 digits), this is computationally infeasible to solve.

Real World Applications

- Really Hard Problem:

  Given two points on the curve P and Q, find an integer n such that

$$Q = nP$$

- Example: $\left(\frac{1324801}{235200}, \frac{1726556399}{197568000}\right) = n(1,-1)$.
- If n is really large (~200 digits), this is computationally infeasible to solve.
- If I know n and P, it is easy to compute Q.

Real World Applications

- Really Hard Problem:
  Given two points on the curve P and Q, find an integer n such that

$$Q = nP$$

- Example: $\left(\frac{1324801}{235200}, \frac{1726556399}{197568000}\right) = 4(1, -1)$.
- If n is really large (~200 digits), this is computationally infeasible to solve.
- If I know n and P, it is easy to compute Q.

Diffie-Hellman Key Exchange

Diffie-Hellman Key Exchange

- Alice and Bob want to establish a secret key.

Alice	Public	Bob

Diffie-Hellman Key Exchange

- Alice and Bob want to establish a secret key.

Alice	Public	Bob
	Curve equation	
	Point P	

Diffie-Hellman Key Exchange

- Alice and Bob want to establish a secret key.

Alice	Public	Bob
Secret number a	Curve equation Point P	Secret number b

Diffie-Hellman Key Exchange

- Alice and Bob want to establish a secret key.

Alice	Public	Bob
Secret number a	Curve equation Point P	Secret number b
Sends aP	$\xrightarrow{aP}$	
	$\xleftarrow{bP}$	Sends bP

Diffie-Hellman Key Exchange

- Alice and Bob want to establish a secret key.

Alice	Public	Bob
Secret number a	Curve equation Point P	Secret number b
Sends aP	$aP \longrightarrow$	Gets aP
Gets bP	$\longleftarrow bP$	Sends bP

Diffie-Hellman Key Exchange

- Alice and Bob want to establish a secret key.

Alice	Public	Bob
Secret number a	Curve equation Point P	Secret number b
Sends aP	aP	Gets aP
Gets bP	bP	Sends bP
Computes: $a(bP) = (ab)P$		Computes: $b(aP) = (ba)P$

Diffie-Hellman Key Exchange

- Alice and Bob want to establish a secret key.

Alice	Public	Bob
Secret number a	Curve equation Point P	Secret number b
Sends aP	aP	Gets aP
Gets bP	bP	Sends bP
Computes: $a(bP) = (ab)P$		Computes: $b(aP) = (ba)P$ $= (ab)P$

Diffie-Hellman Key Exchange

- Alice and Bob want to establish a secret key.

Alice	Public	Bob
Secret number a	Curve equation	Secret number b
	Point P	
Sends aP	aP	Gets aP
Gets bP	bP	Sends bP
Computes:		Computes:
$a(bP) = (ab)P$	?	$b(aP) = (ba)P$
		$= (ab)P$

Thank you.

Questions?