Don't Stop Believin'

There Is a Group Law on the Cubic

Josh Mollner

MathFest, 2008

At The End of This Talk, You Should Know:

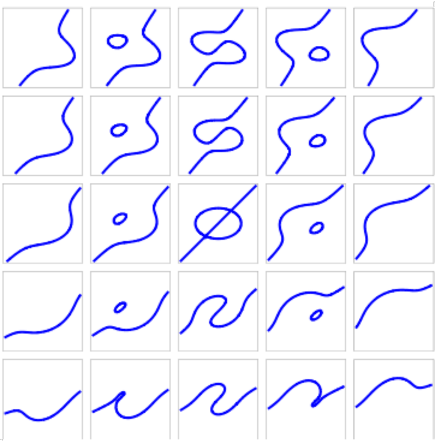
- The set of points on a non-singular, irreducible cubic plane curve can be formed into an abelian group.

Cubic Plane Curves.

A cubic plane curve is the set of solutions in $\mathbb{R}^2$ to an equation of the form:

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0$$

Examples of Cubics.



Special Types of Cubics.

- Irreducible Cubic: A cubic whose equation cannot be factored.
- Non-Singular Cubic:
  - A cubic is singular at a point (a, b) if:

$$\frac{\partial P}{\partial x}(a, b) = 0 \text{ and } \frac{\partial P}{\partial y}(a, b) = 0.$$

  - A cubic is non-singular if it has no points of singularity.

Special Types of Cubics.

- Irreducible Cubic: A cubic whose equation cannot be factored.
- Non-Singular Cubic:
  - A cubic is singular at a point (a, b) if:

$$\frac{\partial P}{\partial x}(a, b) = 0 \text{ and } \frac{\partial P}{\partial y}(a, b) = 0.$$

  - A cubic is non-singular if it has no points of singularity.

Definition of an Abelian Group.

An abelian group is a set of elements, G, together with an operation, $+$, such that the following properties hold:

1. There is an *identity* element.
2. Each element has an *inverse*.
3. Addition is *associative*.
4. Addition is *commutative*.

Definition of an Abelian Group.

An abelian group is a set of elements, G, together with an operation, $+$, such that the following properties hold:

1. There is an *identity* element.
2. Each element has an *inverse*.
3. Addition is *associative*.
4. Addition is *commutative*.

Definition of an Abelian Group.

An abelian group is a set of elements, G, together with an operation, $+$, such that the following properties hold:

1. There is an *identity* element.
2. Each element has an *inverse*.
3. Addition is *associative*.
4. Addition is *commutative*.

Definition of an Abelian Group.

An abelian group is a set of elements, G, together with an operation, $+$, such that the following properties hold:

1. There is an *identity* element.
2. Each element has an *inverse*.
3. Addition is *associative*.
4. Addition is *commutative*.

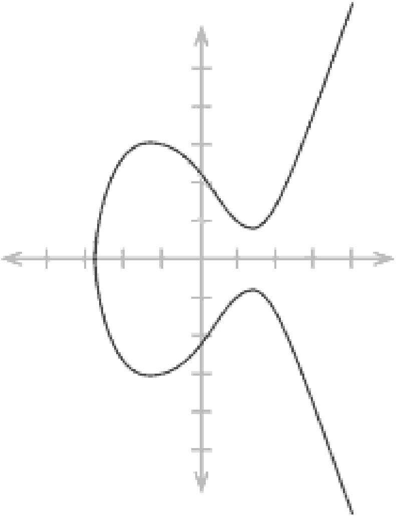
Definition of an Abelian Group.

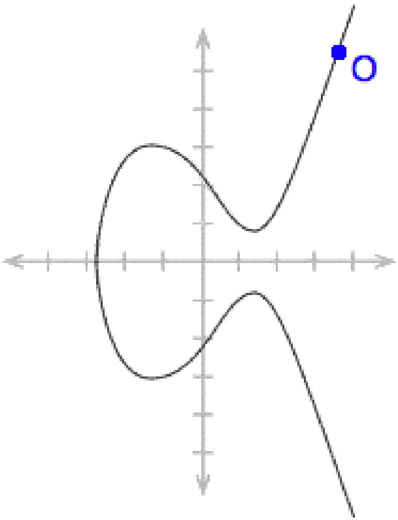
An abelian group is a set of elements, G, together with an operation, $+$, such that the following properties hold:

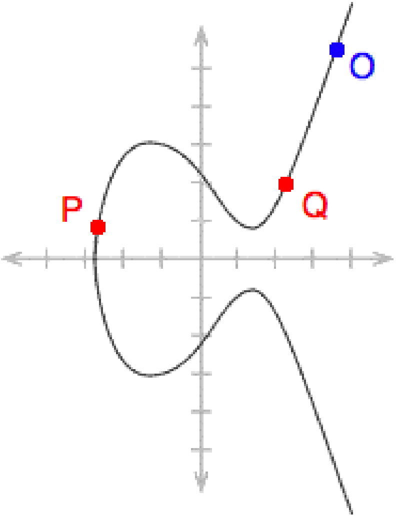
1. There is an *identity* element.
2. Each element has an *inverse*.
3. Addition is *associative*.
4. Addition is *commutative*.

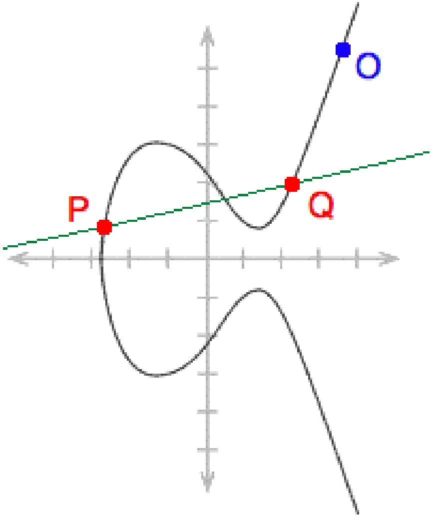
At The End of This Talk, You Should Know:

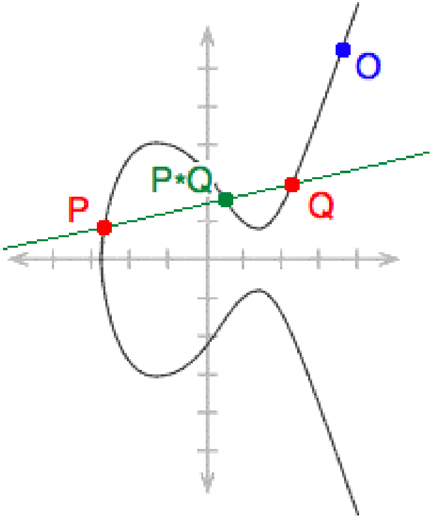
- We will show that the set of points of C, where C is a non-singular, irreducible cubic, is an abelian group.

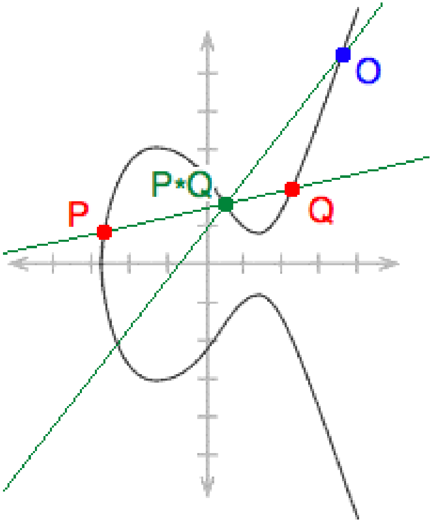


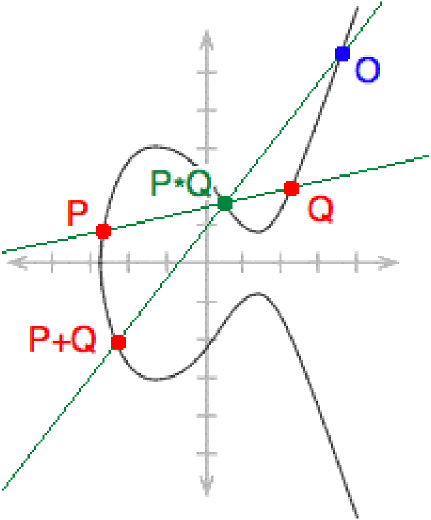

O


O
P
Q


P
Q
O


O
P∗Q
P
Q


O
P*Q
P
Q


O
P*Q
P
Q
P+Q

Is Addition of Points is Well-Defined?

- We might worry that addition of points is not well-defined.
  - What if the line between P and Q does not intersect C at a third point?
  - What if the line between P and Q intersects C at two additional points?
- Don't Stop Believin'

Is Addition of Points is Well-Defined?

- We might worry that addition of points is not well-defined.
  - What if the line between P and Q does not intersect C at a third point?
  - What if the line between P and Q intersects C at two additional points?
- Don't Stop Believin'

Is Addition of Points is Well-Defined?

- We might worry that addition of points is not well-defined.
  - What if the line between P and Q does not intersect C at a third point?
  - What if the line between P and Q intersects C at two additional points?
- Don't Stop Believin'

Is Addition of Points is Well-Defined?

- We might worry that addition of points is not well-defined.
  - What if the line between P and Q does not intersect C at a third point?
  - What if the line between P and Q intersects C at two additional points?
- Don't Stop Believin'

Yes! Addition of Points is Well-Defined.

Theorem

Let l be a line that intersects an irreducible cubic C at least twice, counting multiplicities. Then l intersects C exactly three times, counting multiplicities.

- A line tangent to C at a point P intersects C twice at P.
- A line tangent to C at an inflection point P intersects C three times at P.

Yes! Addition of Points is Well-Defined.

Theorem

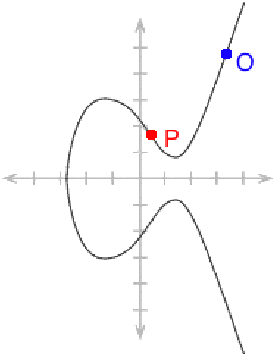
Let l be a line that intersects an irreducible cubic C at least twice, counting multiplicities. Then l intersects C exactly three times, counting multiplicities.

- A line tangent to C at a point P intersects C twice at P.
- A line tangent to C at an inflection point P intersects C three times at P.

There Is An Identity.

There exists an O on C such that $P + O = P$ for all P on C.

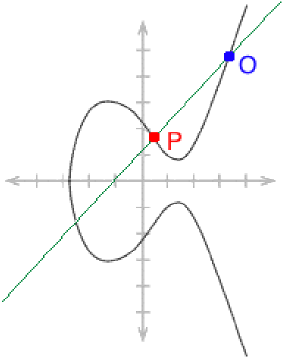
We will show that O is the identity. We must show that $P + O = P$ for all P.



There Is An Identity.

There exists an O on C such that $P + O = P$ for all P on C.

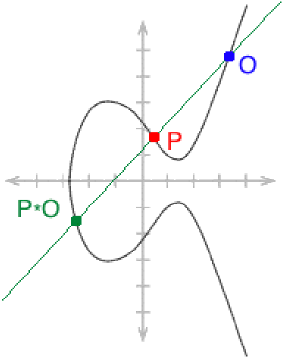
We will show that O is the identity. We must show that $P + O = P$ for all P.



There Is An Identity.

There exists an O on C such that $P + O = P$ for all P on C.

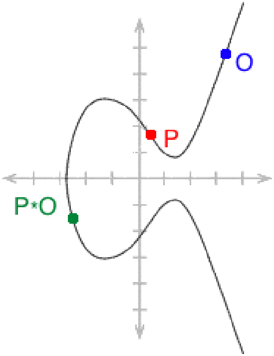
We will show that O is the identity. We must show that $P + O = P$ for all P.



There Is An Identity.

There exists an O on C such that $P + O = P$ for all P on C.

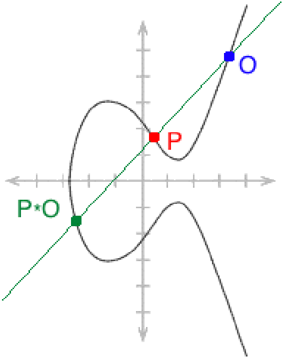
We will show that O is the identity. We must show that $P + O = P$ for all P.



There Is An Identity.

There exists an O on C such that $P + O = P$ for all P on C.

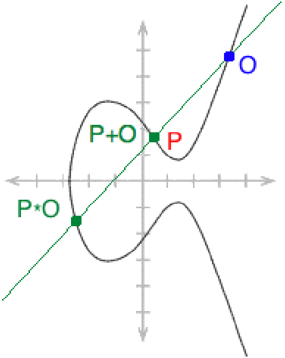
We will show that O is the identity. We must show that $P + O = P$ for all P.



There Is An Identity.

There exists an O on C such that $P + O = P$ for all P on C.

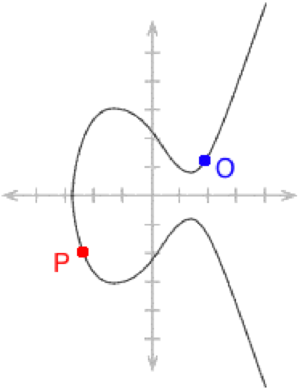
We will show that O is the identity. We must show that $P + O = P$ for all P.



Inverses Exist.

For every P on C, there is a $-P$ on C such that $P + (-P) = O$.

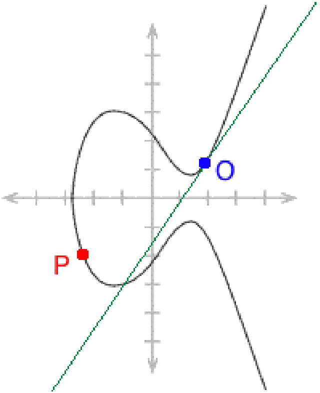
Given a point P on C, we construct $-P$ in the following manner:



Inverses Exist.

For every P on C, there is a $-P$ on C such that $P + (-P) = O$.

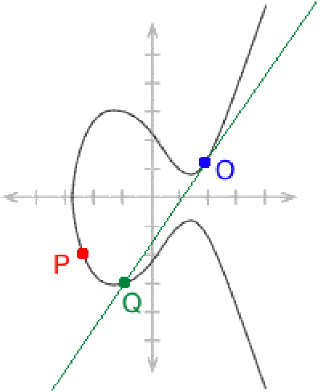
Given a point P on C, we construct $-P$ in the following manner:



Inverses Exist.

For every P on C, there is a $-P$ on C such that $P + (-P) = O$.

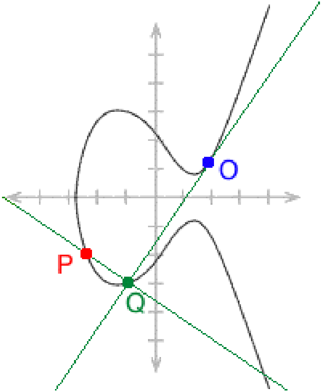
Given a point P on C, we construct $-P$ in the following manner:



Inverses Exist.

For every P on C, there is a $-P$ on C such that $P + (-P) = O$.

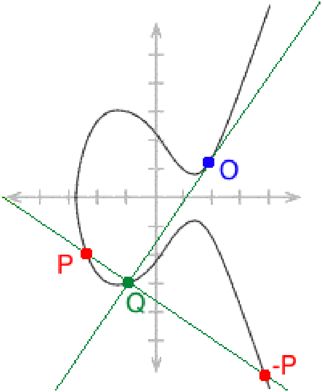
Given a point P on C, we construct $-P$ in the following manner:



Inverses Exist.

For every P on C, there is a $-P$ on C such that $P + (-P) = O$.

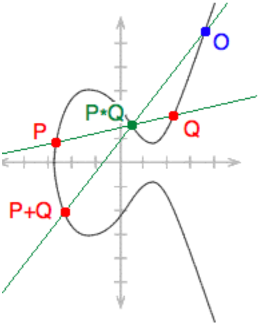
Given a point P on C, we construct $-P$ in the following manner:

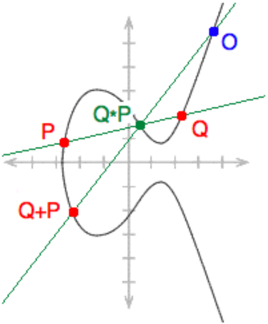


Addition is Commutative.

For every P and Q on C, $P + Q = Q + P$.

We must show that $P + Q = Q + P$. But this is clear, since the line between P and Q is the same as the line between Q and P.

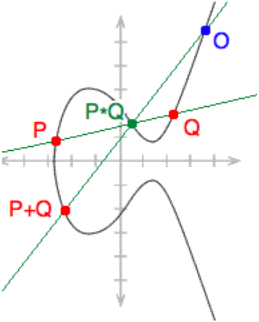


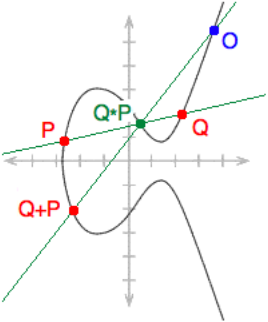


Addition is Commutative.

For every P and Q on C, $P + Q = Q + P$.

We must show that $P + Q = Q + P$. But this is clear, since the line between P and Q is the same as the line between Q and P.

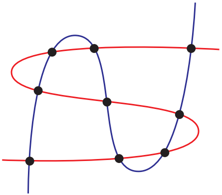




Associativity.
The Cayley-Bacharach Theorem.

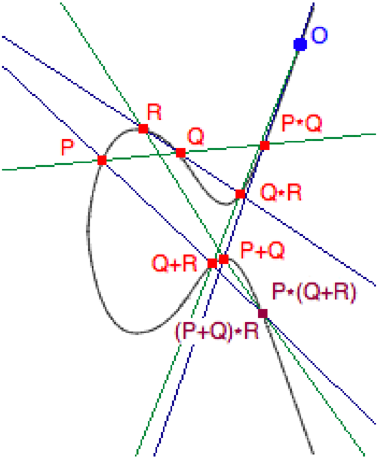
Theorem

Let C_1 and C_2 be two cubic curves which intersect in exactly nine points. Suppose C is a third cubic curve which passes through eight of these nine points. Then C also passes through the ninth point.



Associativity.

For all P, Q, and R on C, $(P+Q)+R = P+(Q+R)$.



The Set of Rational Points Is a Group Too.

- We have shown that the set of points on an irreducible, non-singular cubic is an abelian group.
- It is also true that the set of rational points on a rational, irreducible, non-singular cubic with at least one rational point is an abelian group.
  - A rational cubic is one whose equation can be written in the form

    $$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0$$

    Where $a, b, c, d, e, f, g, h, i$, and j are rational numbers.

The Set of Rational Points Is a Group Too.

- We have shown that the set of points on an irreducible, non-singular cubic is an abelian group.
- It is also true that the set of rational points on a rational, irreducible, non-singular cubic with at least one rational point is an abelian group.
  - A rational cubic is one whose equation can be written in the form

    $$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0$$

    Where $a, b, c, d, e, f, g, h, i$, and j are rational numbers.

The Set of Rational Points Is a Group Too.

- We have shown that the set of points on an irreducible, non-singular cubic is an abelian group.
- It is also true that the set of rational points on a rational, irreducible, non-singular cubic with at least one rational point is an abelian group.
  - A rational cubic is one whose equation can be written in the form

    $$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0$$

    Where $a, b, c, d, e, f, g, h, i$, and j are rational numbers.

Mordell's Theorem.

- Mordell's Theorem: The set of rational points on a rational, irreducible, non-singular cubic with at least one rational point is a finitely-generated abelian group.
- There is a set of rational points, $P_1, ..., P_n$, such that if Q is a rational point on C, we can write:

$$Q = \sum_{i=1}^{n} n_i P_i.$$

Mordell's Theorem.

- Mordell's Theorem: The set of rational points on a rational, irreducible, non-singular cubic with at least one rational point is a finitely-generated abelian group.
- There is a set of rational points, $P_1, ..., P_n$, such that if Q is a rational point on C, we can write:

$$Q = \sum_{i=1}^{n} n_i P_i.$$

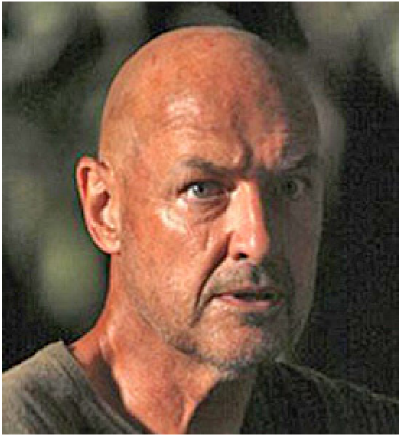
Mordell's Theorem Is Useful In The Real World.

- Here is a real-world example of how Mordell's Theorem is useful:
- Let's say you are LOST on an island ...

Mordell's Theorem Is Useful In The Real World.

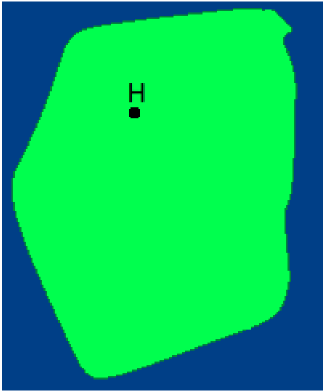
- Here is a real-world example of how Mordell's Theorem is useful:
- Let's say you are LOST on an island ...

Mordell's Theorem Is Useful In The Real World.



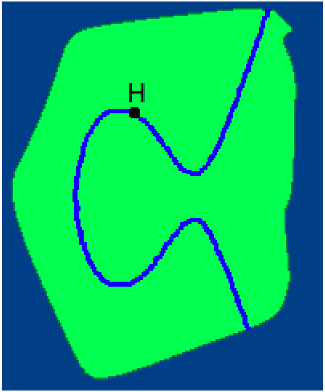
LOST

You have a dream:



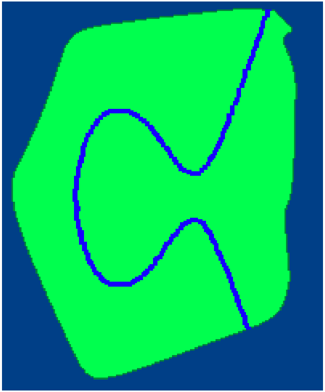
LOST

You have a dream:



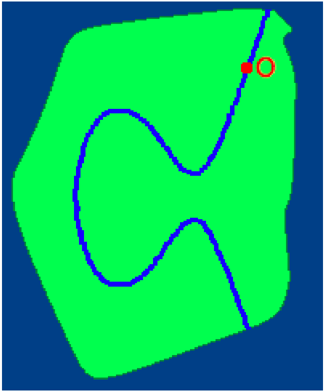
LOST

You have a dream:



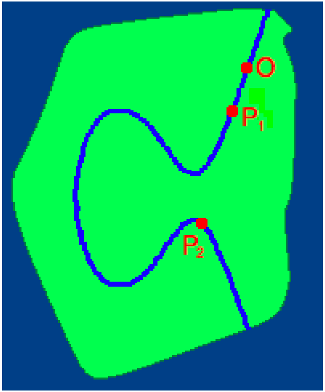
LOST

You have a dream:



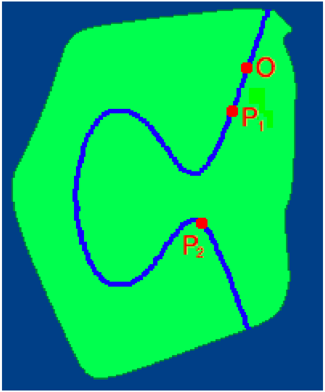
LOST

You have a dream:



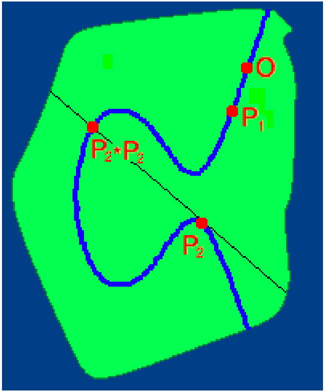
LOST

You wake up:



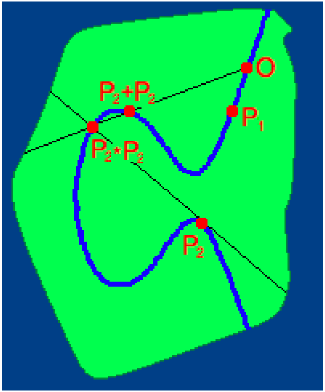
LOST

You try $P_2 + P_2$:



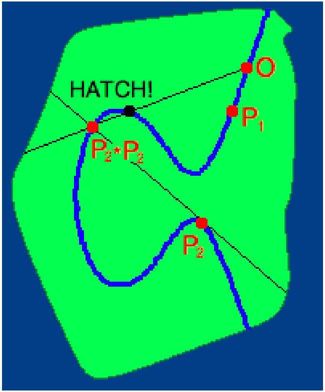
LOST

You try $P_2 + P_2$:



LOST

And you find the hatch!



Open Questions.

- Given a cubic, which are the rational points which compose this finite generating set?
- Given a cubic, what is the minimum number of points needed in a finite generating set?
- It is not yet known how to determine in a finite number of steps whether a given cubic has a rational point at all.

Open Questions.

- Given a cubic, which are the rational points which compose this finite generating set?
- Given a cubic, what is the minimum number of points needed in a finite generating set?
- It is not yet known how to determine in a finite number of steps whether a given cubic has a rational point at all.

Open Questions.

- Given a cubic, which are the rational points which compose this finite generating set?
- Given a cubic, what is the minimum number of points needed in a finite generating set?
- It is not yet known how to determine in a finite number of steps whether a given cubic has a rational point at all.

Open Questions.

- Given a cubic, which are the rational points which compose this finite generating set?
- Given a cubic, what is the minimum number of points needed in a finite generating set?
- It is not yet known how to determine in a finite number of steps whether a given cubic has a rational point at all.

Open Questions.

- Given a cubic, which are the rational points which compose this finite generating set?
- Given a cubic, what is the minimum number of points needed in a finite generating set?
- It is not yet known how to determine in a finite number of steps whether a given cubic has a rational point at all.

THANK YOU!

AND

DON'T STOP BELIEVIN'

THANK YOU!

AND

DON’T STOP BELIEVIN’