Introduction to Elliptic Curves

Ilias S. Kotsireas[1]

[1]Director, CARGO Lab

Wilfrid Laurier University
Waterloo, Ontario, Canada

http://www.cargo.wlu.ca

May 13, 2018

Finding integer/rational solutions to polynomial equations

Finding integer/rational solutions to polynomial equations

Diophantus, Pythagoras

find integer/rational solutions to polynomial equations:

$$x^2 + y^2 = 100, \qquad x^2 + y^2 + 2z^2 = 7$$

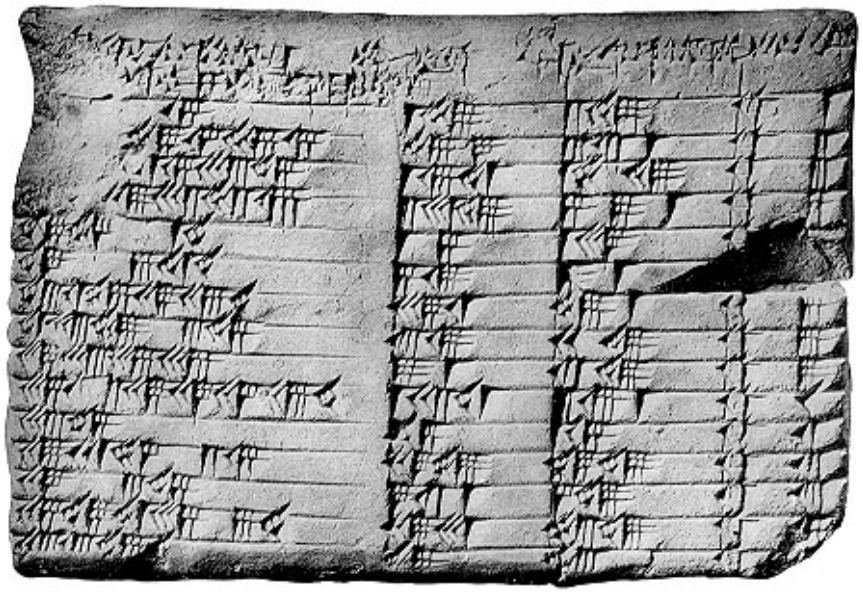
Finding integer/rational solutions to polynomial equations

Diophantus, Pythagoras

find integer/rational solutions to polynomial equations:

$$x^2 + y^2 = 100, \qquad x^2 + y^2 + 2z^2 = 7$$

Babylonian tablet Plimpton 322



Mathematical Cuneiform Tablets

Otto Neugebauer & Abraham Sachs, 1945

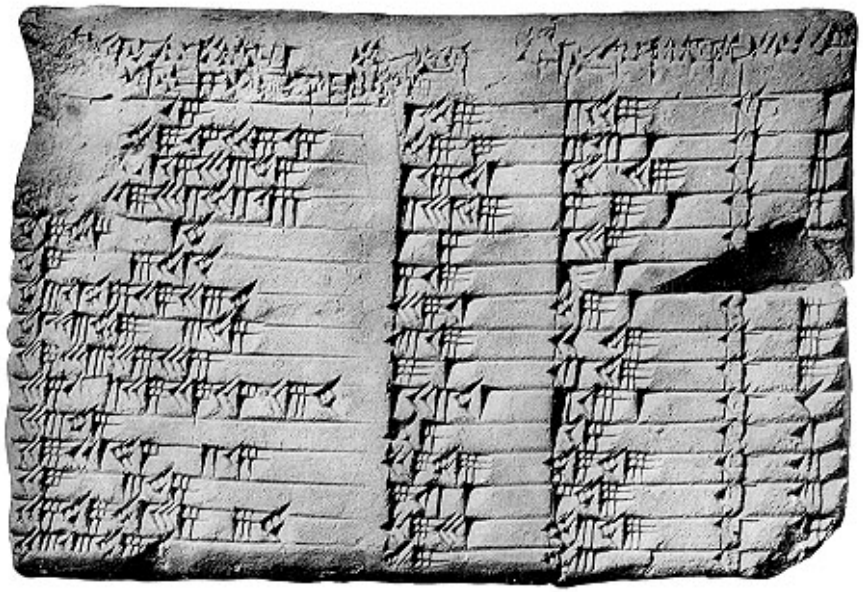
Finding integer/rational solutions to polynomial equations

Diophantus, Pythagoras

find integer/rational solutions to polynomial equations:

$$x^2 + y^2 = 100, \qquad x^2 + y^2 + 2z^2 = 7$$

Babylonian tablet Plimpton 322



Mathematical Cuneiform Tablets

Otto Neugebauer & Abraham Sachs, 1945

N.A.B.U. (Nouvelles Assyriologiques Brèves et Utilitaires) Sept 2017

The case of one-variable polynomial equations

The case of one-variable polynomial equations

The case of one-variable polynomial equations is well-known:

$$a_n x^n + a_{n-1} x^{n-1} + \cdots a_1 x + a_0 = 0$$

(with all a_i integers)

The case of one-variable polynomial equations

The case of one-variable polynomial equations is well-known:

$$a_n x^n + a_{n-1} x^{n-1} + \cdots a_1 x + a_0 = 0$$

(with all a_i integers)

Fundamental Theorem of Algebra

There are n roots.

The case of one-variable polynomial equations

The case of one-variable polynomial equations is well-known:

$$a_n x^n + a_{n-1} x^{n-1} + \cdots a_1 x + a_0 = 0$$

(with all a_i integers)

Fundamental Theorem of Algebra

There are n roots.

Rational Roots Theorem

If $a_0 \neq 0$, $a_n \neq 0$, $x = \frac{p}{q}$, $(p, q) = 1$, then p/a_0 and q/a_n.

The case of one-variable polynomial equations

The case of one-variable polynomial equations is well-known:

$$a_n x^n + a_{n-1} x^{n-1} + \cdots a_1 x + a_0 = 0$$

(with all a_i integers)

Fundamental Theorem of Algebra
There are n roots.

Rational Roots Theorem
If $a_0 \neq 0$, $a_n \neq 0$, $x = \frac{p}{q}$, $(p, q) = 1$, then p/a_0 and q/a_n.

$\rightsquigarrow$ algorithm that tests a finite number of candidate rational roots

The case of two-variable polynomial equations

The case of two-variable polynomial equations

Degree 1

Find all rational solutions to a two-variable polynomial equation of degree 1

$$y = ax + b, \quad a, b \text{ rationals}$$

The case of two-variable polynomial equations

Degree 1

Find all rational solutions to a two-variable polynomial equation of degree 1

$$y = ax + b, \quad a, b \text{ rationals}$$

Every rational value of x gives a rational value of y.

The case of two-variable polynomial equations

Degree 1

Find all rational solutions to a two-variable polynomial equation of degree 1

$$y = ax + b, \quad a, b \text{ rationals}$$

Every rational value of x gives a rational value of y.

Degree 2

Find all rational solutions to a two-variable polynomial equation of degree 2
(full theory is available)
Illustration by:

The case of two-variable polynomial equations

Degree 1

Find all rational solutions to a two-variable polynomial equation of degree 1

$$y = ax + b, \quad a, b \text{ rationals}$$

Every rational value of x gives a rational value of y.

Degree 2

Find all rational solutions to a two-variable polynomial equation of degree 2
(full theory is available)
Illustration by:

Example

Find all rational solutions of $x^2 + y^2 = 1$

Find all points in the unit cirle, that have rational coordinates

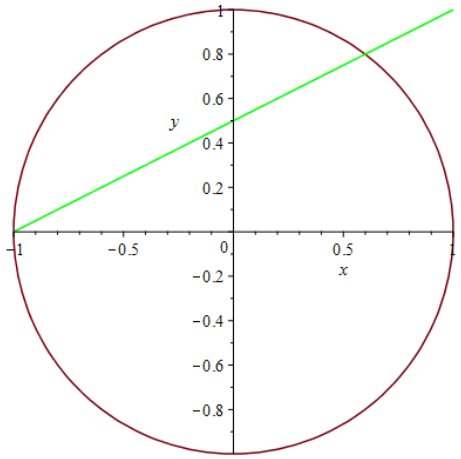
Find all points in the unit cirle, that have rational coordinates

Rational Point == point each of whose coordinates are rational

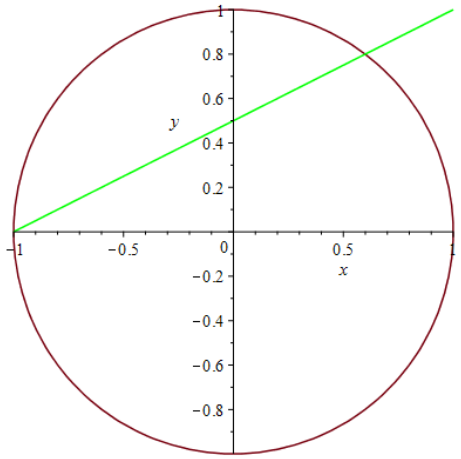
Find all points in the unit cirle, that have rational coordinates

Rational Point == point each of whose coordinates are rational

Obvious rational points: (-1,0) (left-most point on the unit circle)



Find all points in the unit cirle, that have rational coordinates
Rational Point == point each of whose coordinates are rational
Obvious rational points: (-1,0) (left-most point on the unit circle)



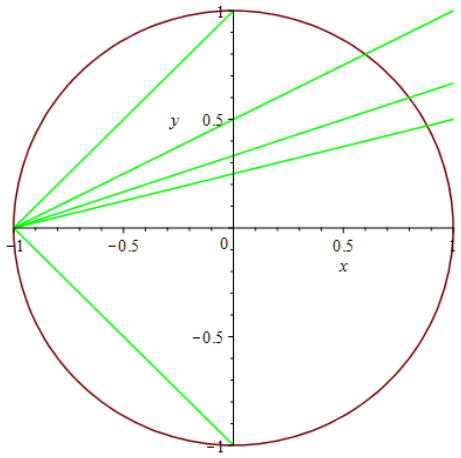
Key observation I If $P = (x, y)$ is another rational point on the unit circle, then the slope s of the line joining $(-1, 0)$ and P is rational.

Key observation II: The converse is also true!

If you take a line with rational slope through $(-1, 0)$ that intersects the unit circle, then the point of intersection is a rational point.

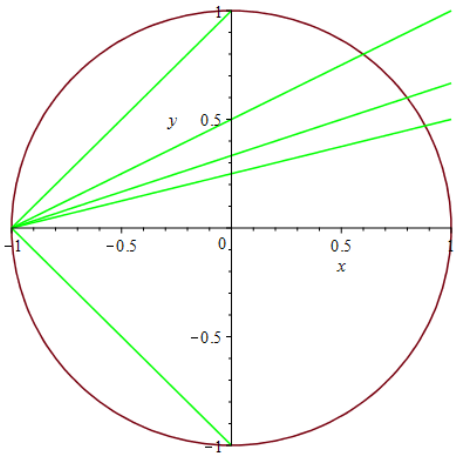
Key observation II: The converse is also true!

If you take a line with rational slope through $(-1, 0)$ that intersects the unit circle, then the point of intersection is a rational point.



Key observation II: The converse is also true!

If you take a line with rational slope through $(-1, 0)$ that intersects the unit circle, then the point of intersection is a rational point.

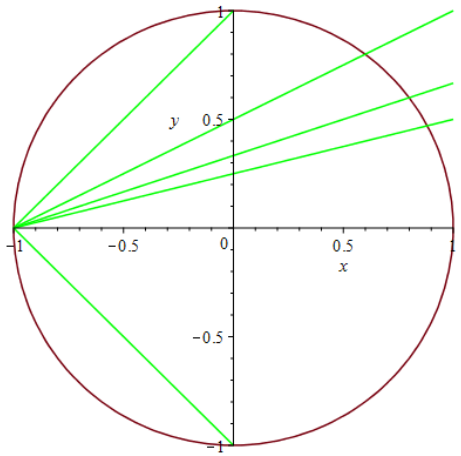


Proof Suppose we take a line of rational slope s through $(-1, 0)$,

$$y = s(x + 1) \tag{1}$$

Key observation II: The converse is also true!

If you take a line with rational slope through $(-1, 0)$ that intersects the unit circle, then the point of intersection is a rational point.



Proof Suppose we take a line of rational slope s through $(-1, 0)$,

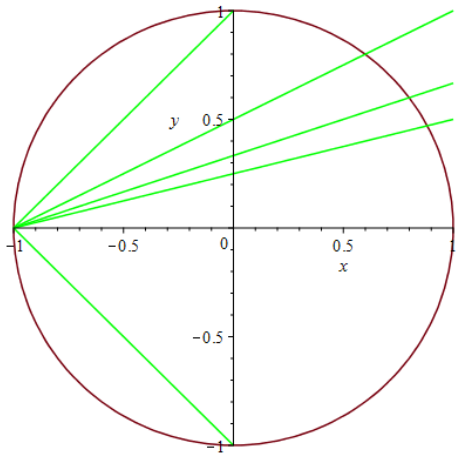
$$y = s(x + 1) \tag{1}$$

We need to find the intersection of this line with the unit circle

$$x^2 + y^2 = 1 \tag{2}$$

Key observation II: The converse is also true!

If you take a line with rational slope through $(-1, 0)$ that intersects the unit circle, then the point of intersection is a rational point.



Proof Suppose we take a line of rational slope s through $(-1, 0)$,

$$y = s(x + 1) \tag{1}$$

We need to find the intersection of this line with the unit circle

$$x^2 + y^2 = 1 \tag{2}$$

Substitution of (1) in (2) yields the quadratic equation

$$x^2 + s^2(x + 1)^2 = 1 \tag{3}$$

The roots are: $x = -1, x = -\frac{s^2-1}{s^2+1}$

The roots are: $x = -1, x = -\frac{s^2-1}{s^2+1}$

The corresponding y-values are $y = 0, y = \frac{2s}{s^2+1}$

The roots are: $x = -1, x = -\frac{s^2-1}{s^2+1}$

The corresponding y-values are $y = 0, y = \frac{2s}{s^2+1}$

Since s is rational, the point of intersection $P(x, y) = (-\frac{s^2-1}{s^2+1}, \frac{2s}{s^2+1})$ is also a rational point

The roots are: $x = -1, x = -\frac{s^2-1}{s^2+1}$

The corresponding y-values are $y = 0, y = \frac{2s}{s^2+1}$

Since s is rational, the point of intersection

$P(x, y) = (-\frac{s^2-1}{s^2+1}, \frac{2s}{s^2+1})$ is also a rational point

Observation 1

Since the sum/product of the roots of (3) are rational numbers, and one root is -1, the other root would have to be rational

The roots are: $x = -1, x = -\frac{s^2-1}{s^2+1}$

The corresponding y-values are $y = 0, y = \frac{2s}{s^2+1}$

Since s is rational, the point of intersection $P(x, y) = (-\frac{s^2-1}{s^2+1}, \frac{2s}{s^2+1})$ is also a rational point

Observation 1

Since the sum/product of the roots of (3) are rational numbers, and one root is -1, the other root would have to be rational

Observation 2

We have a complete parameterization of all rational points in the unit circle

The roots are: $x = -1, x = -\frac{s^2-1}{s^2+1}$

The corresponding y-values are $y = 0, y = \frac{2s}{s^2+1}$

Since s is rational, the point of intersection $P(x, y) = (-\frac{s^2-1}{s^2+1}, \frac{2s}{s^2+1})$ is also a rational point

Observation 1

Since the sum/product of the roots of (3) are rational numbers, and one root is -1, the other root would have to be rational

Observation 2

We have a complete parameterization of all rational points in the unit circle

Theorem

The rational points (x,y) on the unit circle $x^2 + y^2 = 1$ are in 1-1 correspondence with the elements s of the set $\mathbb{Q} \cup \infty$.

The roots are: $x = -1, x = -\frac{s^2-1}{s^2+1}$

The corresponding y-values are $y = 0, y = \frac{2s}{s^2+1}$

Since s is rational, the point of intersection $P(x, y) = (-\frac{s^2-1}{s^2+1}, \frac{2s}{s^2+1})$ is also a rational point

Observation 1

Since the sum/product of the roots of (3) are rational numbers, and one root is -1, the other root would have to be rational

Observation 2

We have a complete parameterization of all rational points in the unit circle

Theorem

The rational points (x,y) on the unit circle $x^2 + y^2 = 1$ are in 1-1 correspondence with the elements s of the set $\mathbb{Q} \cup \infty$.

The correspondence between slopes s and points (x,y) is:

$$s \mapsto \left(-\frac{s^2 - 1}{s^2 + 1}, \frac{2s}{s^2 + 1} \right) \tag{4}$$

Summary of the process/result

Summary of the process/result

1. We have explicitly determined all rational points on the unit circle

Summary of the process/result

1. We have explicitly determined all rational points on the unit circle
2. We only used the fact that the equation is quadratic

Summary of the process/result

1. We have explicitly determined all rational points on the unit circle
2. We only used the fact that the equation is quadratic
3. This procedure would work in any quadratic equation in two variables

Summary of the process/result

1. We have explicitly determined all rational points on the unit circle
2. We only used the fact that the equation is quadratic
3. This procedure would work in any quadratic equation in two variables
4. It is easy to see that $x^2 + y^2 = 3$ does not have any rational points

Summary of the process/result

1. We have explicitly determined all rational points on the unit circle
2. We only used the fact that the equation is quadratic
3. This procedure would work in any quadratic equation in two variables
4. It is easy to see that $x^2 + y^2 = 3$ does not have any rational points
5. (think modulo powers of 3)

Fundamental Theorem About Rational Points on Conics

Theorem

Let $f(x,y)$ be a quadratic polynomial in x and y with rational coefficients.

Fundamental Theorem About Rational Points on Conics

Theorem

Let $f(x,y)$ be a quadratic polynomial in x and y with rational coefficients.
Then the set of all rational points (x,y) on the conic $f(x,y)=0$ is either:

Fundamental Theorem About Rational Points on Conics

Theorem

Let $f(x,y)$ be a quadratic polynomial in x and y with rational coefficients.
Then the set of all rational points (x,y) on the conic $f(x,y)=0$ is either:
(1) empty

Fundamental Theorem About Rational Points on Conics

Theorem

Let f(x,y) be a quadratic polynomial in x and y with rational coefficients.
Then the set of all rational points (x,y) on the conic f(x,y)=0 is either:
(1) empty
(2) in 1-1 correspondence with slopes in $\mathbb{Q} \cup \infty$

Fundamental Theorem About Rational Points on Conics

Theorem

Let f(x,y) be a quadratic polynomial in x and y with rational coefficients.
Then the set of all rational points (x,y) on the conic f(x,y)=0 is either:
(1) empty
(2) in 1-1 correspondence with slopes in $\mathbb{Q} \cup \infty$
In case (2) above, we can find explicitly all rational points as follows:

Fundamental Theorem About Rational Points on Conics

Theorem

Let f(x,y) be a quadratic polynomial in x and y with rational coefficients.
Then the set of all rational points (x,y) on the conic f(x,y)=0 is either:
(1) empty
(2) in 1-1 correspondence with slopes in $\mathbb{Q} \cup \infty$
In case (2) above, we can find explicitly all rational points as follows:

- Start with a base rational point P on the conic
- Take all lines of rational slope through P
- Compute the second point of intersection of each of these lines with the conic

Fundamental Theorem About Rational Points on Conics

Theorem

Let f(x,y) be a quadratic polynomial in x and y with rational coefficients.
Then the set of all rational points (x,y) on the conic f(x,y)=0 is either:
(1) empty
(2) in 1-1 correspondence with slopes in $\mathbb{Q} \cup \infty$
In case (2) above, we can find explicitly all rational points as follows:

- Start with a base rational point P on the conic
- Take all lines of rational slope through P
- Compute the second point of intersection of each of these lines with the conic

Observation These is an effective method to determine whether we are in case (1) or (2) above:

Fundamental Theorem About Rational Points on Conics

Theorem

Let f(x,y) be a quadratic polynomial in x and y with rational coefficients.
Then the set of all rational points (x,y) on the conic f(x,y)=0 is either:
(1) empty
(2) in 1-1 correspondence with slopes in $\mathbb{Q} \cup \infty$
In case (2) above, we can find explicitly all rational points as follows:

- Start with a base rational point P on the conic
- Take all lines of rational slope through P
- Compute the second point of intersection of each of these lines with the conic

Observation These is an effective method to determine whether we are in case (1) or (2) above: Hasse-Minkowski theorem

Degree 3 equations in two variables

Degree 3 equations in two variables

Given a two-variable polynomial equation of degree 3, it may have:

Degree 3 equations in two variables

Given a two-variable polynomial equation of degree 3, it may have:

- zero rational points
- a positive finite number of rational points
- an infinite number of rational points

Degree 3 equations in two variables

Given a two-variable polynomial equation of degree 3, it may have:

- zero rational points
- a positive finite number of rational points
- an infinite number of rational points

Open problem: Determine in which case we are in

Degree 3 equations in two variables

Given a two-variable polynomial equation of degree 3, it may have:

- zero rational points
- a positive finite number of rational points
- an infinite number of rational points

Open problem: Determine in which case we are in

Open problem: We do not know how to find all rational solutions

Degree 3 equations in two variables

Given a two-variable polynomial equation of degree 3, it may have:

- zero rational points
- a positive finite number of rational points
- an infinite number of rational points

Open problem: Determine in which case we are in

Open problem: We do not know how to find all rational solutions

This is where BSD comes in!

Degree 3 equations in two variables

Given a two-variable polynomial equation of degree 3, it may have:

- zero rational points
- a positive finite number of rational points
- an infinite number of rational points

Open problem: Determine in which case we are in

Open problem: We do not know how to find all rational solutions

This is where BSD comes in!

If BSD was true, then we would have a method to find all rational solutions to a cubic equation in two variables and determine whether it has finitely many of infinitely many rational solutions.

The structure of rational points on cubic curves

The structure of rational points on cubic curves

1. Assume we have a smooth cubic equation $f(x, y) = 0$ with a base rational point $P = (x_0, y_0)$

The structure of rational points on cubic curves

1. Assume we have a smooth cubic equation $f(x, y) = 0$ with a base rational point $P = (x_0, y_0)$
2. We can always perform a rational change of variables so that P is sent to infinity and the equation of the cubic becomes

$$y^2 = x^3 + Ax + B \tag{5}$$

where A and B are integers and $\Delta = -4A^3 - 27B^2 \neq 0$ (smooth, no repeated roots in x-part)

The structure of rational points on cubic curves

1. Assume we have a smooth cubic equation $f(x, y) = 0$ with a base rational point $P = (x_0, y_0)$
2. We can always perform a rational change of variables so that P is sent to infinity and the equation of the cubic becomes

$$y^2 = x^3 + Ax + B \tag{5}$$

where A and B are integers and $\Delta = -4A^3 - 27B^2 \neq 0$ (smooth, no repeated roots in x-part)

3. An equation of the type (5) is called an elliptic curve, in Weierstrass form.

The structure of rational points on cubic curves

1. Assume we have a smooth cubic equation $f(x, y) = 0$ with a base rational point $P = (x_0, y_0)$
2. We can always perform a rational change of variables so that P is sent to infinity and the equation of the cubic becomes

$$y^2 = x^3 + Ax + B \tag{5}$$

   where A and B are integers and $\Delta = -4A^3 - 27B^2 \neq 0$ (smooth, no repeated roots in x-part)
3. An equation of the type (5) is called an elliptic curve, in Weierstrass form.
4. It is very convenient to use this canonical form

The structure of rational points on cubic curves

1. Assume we have a smooth cubic equation $f(x, y) = 0$ with a base rational point $P = (x_0, y_0)$
2. We can always perform a rational change of variables so that P is sent to infinity and the equation of the cubic becomes

$$y^2 = x^3 + Ax + B \tag{5}$$

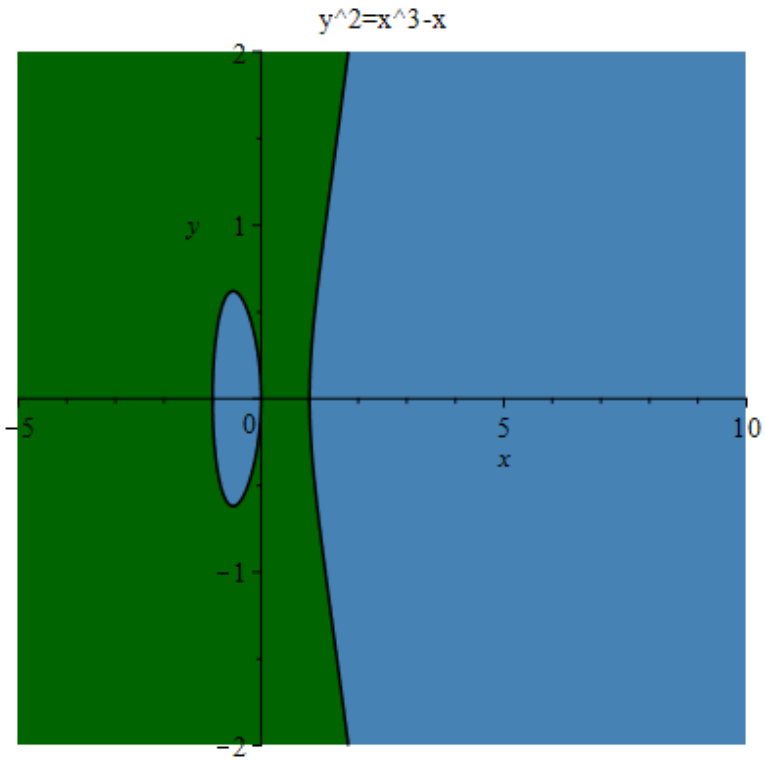
   where A and B are integers and $\Delta = -4A^3 - 27B^2 \neq 0$ (smooth, no repeated roots in x-part)
3. An equation of the type (5) is called an elliptic curve, in Weierstrass form.
4. It is very convenient to use this canonical form
5. It is now easy to describe an amazing structure, exhibited by the set of rational points on an elliptic curve

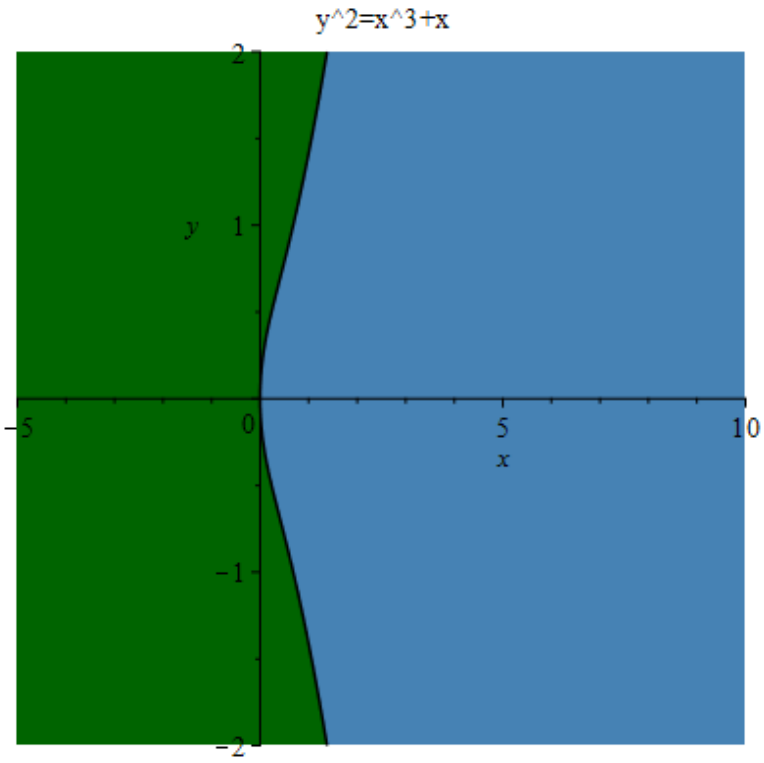
The graph of an elliptic curve

Typical graphs of elliptic curves in $\mathbb{R}^2$:

The graph of an elliptic curve

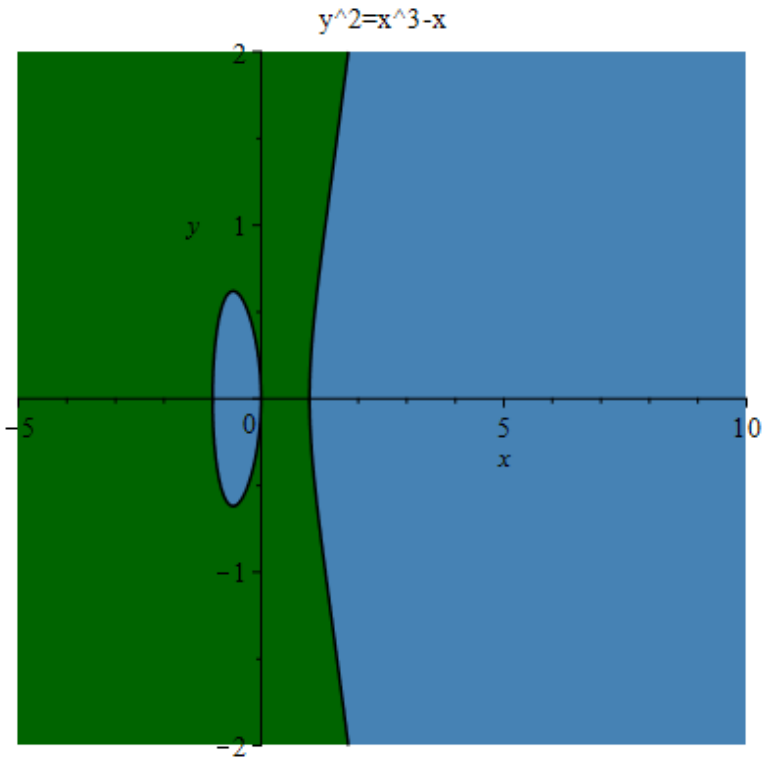
Typical graphs of elliptic curves in $\mathbb{R}^2$:

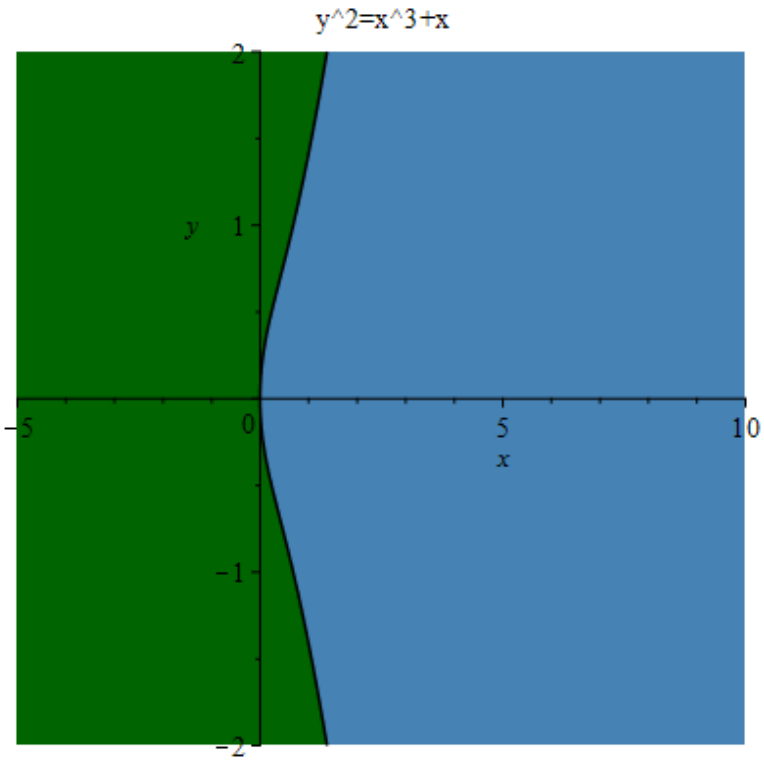




The graph of an elliptic curve

Typical graphs of elliptic curves in $\mathbb{R}^2$:





(depending on whether the x-part has 1 real root or 3 real roots)

The group law on elliptic curves

The group law on elliptic curves

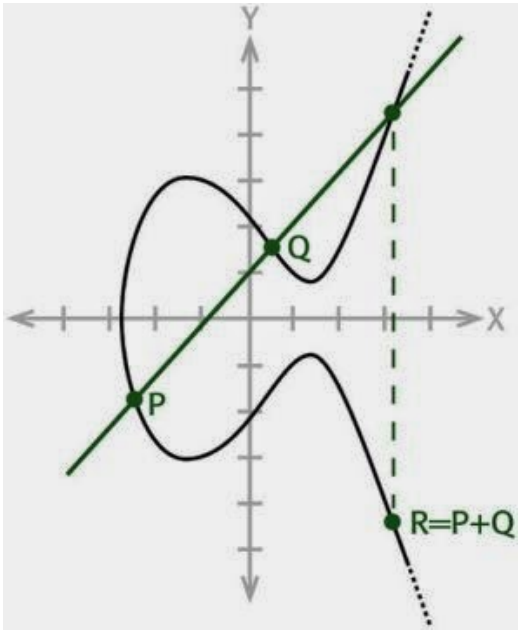
1. If we have 2 r.p. on a plane elliptic curve E, then the line connecting those two r.p. intersects E in a 3rd r.p.

The group law on elliptic curves

1. If we have 2 r.p. on a plane elliptic curve E, then the line connecting those two r.p. intersects E in a 3rd r.p.
2. Given rational points P and Q on E, we can define a rational point $R = P + Q$ on E as follows:

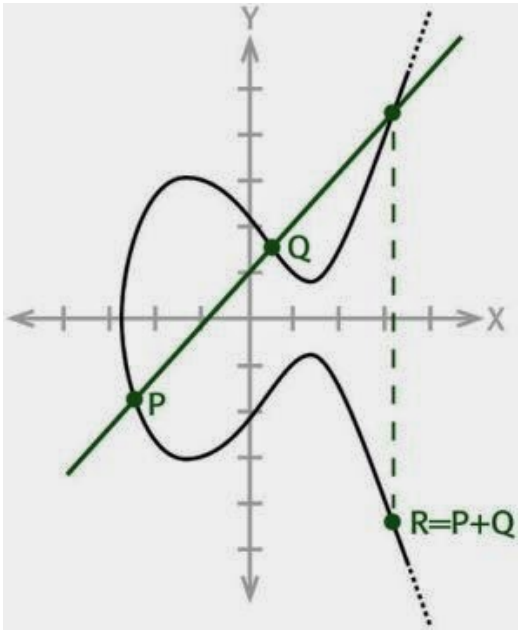
The group law on elliptic curves

1. If we have 2 r.p. on a plane elliptic curve E, then the line connecting those two r.p. intersects E in a 3rd r.p.
2. Given rational points P and Q on E, we can define a rational point $R = P + Q$ on E as follows:



The group law on elliptic curves

1. If we have 2 r.p. on a plane elliptic curve E, then the line connecting those two r.p. intersects E in a 3rd r.p.
2. Given rational points P and Q on E, we can define a rational point $R = P + Q$ on E as follows:



Fact

This law of addition endows the set of r.p. on E, together with the point at ∞, with the structure of an abelian group.

Mordell's theorem

Mordell's theorem

Notation

For an elliptic curve E, the group of rational points is denoted by $E(\mathbb{Q})$

Mordell's theorem

Notation

For an elliptic curve E, the group of rational points is denoted by $E(\mathbb{Q})$

Mordell's theorem

For any elliptic curve E, the group $E(\mathbb{Q})$ is finitely generated

Mordell's theorem

Notation

For an elliptic curve E, the group of rational points is denoted by $E(\mathbb{Q})$

Mordell's theorem

For any elliptic curve E, the group $E(\mathbb{Q})$ is finitely generated

Consequence of the fundamental thm of finitely generated abelian groups:

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus T$$

for some $r \geq 0$ and T a finite abelian group, (torsion).

Mordell's theorem

Notation

For an elliptic curve E, the group of rational points is denoted by $E(\mathbb{Q})$

Mordell's theorem

For any elliptic curve E, the group $E(\mathbb{Q})$ is finitely generated

Consequence of the fundamental thm of finitely generated abelian groups:

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus T$$

for some $r \geq 0$ and T a finite abelian group, (torsion).

Mazur's theorem

T is bounded in size by 16

Mordell's theorem

Notation

For an elliptic curve E, the group of rational points is denoted by $E(\mathbb{Q})$

Mordell's theorem

For any elliptic curve E, the group $E(\mathbb{Q})$ is finitely generated

Consequence of the fundamental thm of finitely generated abelian groups:

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus T$$

for some $r \geq 0$ and T a finite abelian group, (torsion).

Mazur's theorem

T is bounded in size by 16 (usually it is just $\{1\}$)

The rank of the elliptic curve

The rank of the elliptic curve

Thus r measures how big the group of rational points is, it is a fundamental invariant.

The rank of the elliptic curve

Thus r measures how big the group of rational points is, it is a fundamental invariant.

- $r = 0 \rightsquigarrow$ finitely many rational points
- $r > 0 \rightsquigarrow$ infinitely many rational points

The rank of the elliptic curve

Thus r measures how big the group of rational points is, it is a fundamental invariant.

- $r = 0 \rightsquigarrow$ finitely many rational points
- $r > 0 \rightsquigarrow$ infinitely many rational points

Definition

The quantity r is called the rank of the elliptic curve E.

The rank of the elliptic curve

Thus r measures how big the group of rational points is, it is a fundamental invariant.

- $r = 0 \rightsquigarrow$ finitely many rational points
- $r > 0 \rightsquigarrow$ infinitely many rational points

Definition

The quantity r is called the rank of the elliptic curve E.

- The rank is a fundamental arithmetic invariant of an elliptic curve

The rank of the elliptic curve

Thus r measures how big the group of rational points is, it is a fundamental invariant.

- $r = 0 \rightsquigarrow$ finitely many rational points
- $r > 0 \rightsquigarrow$ infinitely many rational points

Definition

The quantity r is called the rank of the elliptic curve E.

- The rank is a fundamental arithmetic invariant of an elliptic curve
- The rank of E measures the number of points needed to generate all rational points on the curve. (by Mordell's theorem this number is always finite)

The rank of the elliptic curve

Thus r measures how big the group of rational points is, it is a fundamental invariant.

- $r = 0 \rightsquigarrow$ finitely many rational points
- $r > 0 \rightsquigarrow$ infinitely many rational points

Definition

The quantity r is called the rank of the elliptic curve E.

- The rank is a fundamental arithmetic invariant of an elliptic curve
- The rank of E measures the number of points needed to generate all rational points on the curve. (by Mordell's theorem this number is always finite)
- In Number Theory, we are interested in the behavior of the rank

Open questions

Open questions

1. What is the maximum value of r? (is there a maximum value?)

Open questions

1. What is the maximum value of r? (is there a maximum value?)
2. current record: $r = 28$, Noam Elkies, 2006

Open questions

1. What is the maximum value of r? (is there a maximum value?)
2. current record: $r = 28$, Noam Elkies, 2006

$$y^2 + xy + y = x^3 - x^2 - 2006776241557552658503320820933854275093023031217895650 2x +$$

$$3448161179503055646703298569039072037485594435931918036126600829629193944873224342 9$$

Open questions

1. What is the maximum value of r? (is there a maximum value?)
2. current record: $r = 28$, Noam Elkies, 2006

$$y^2 + xy + y = x^3 - x^2 - 2006776241557552658503320820933854275093023031217895650 2x +$$

$$3448161179503055646703298569039072037485594435931918036126600829629193944873224342 9$$

$$2 \cdot 2161 \cdot 194083 \cdot 2392360876634196152809896070161520193495865117 7$$

Open questions

1. What is the maximum value of r? (is there a maximum value?)
2. current record: $r = 28$, Noam Elkies, 2006

$$y^2 + xy + y = x^3 - x^2 - 2006776241557552658503320820933854275093023031217895650 2x +$$

$$344816117950305564670329856903907203748559443593191803612660082962919394487322434 29$$

$$2 \cdot 2161 \cdot 194083 \cdot 23923608766341961528098960701615201934958651177$$

$$45317 \cdot 34460641 \cdot 1508741780415612155069 \cdot 14634845362034056885106572128327924482438697644053$$

Open questions

1. What is the maximum value of r? (is there a maximum value?)
2. current record: $r = 28$, Noam Elkies, 2006

$$y^2 + xy + y = x^3 - x^2 - 20067762415575526585033208209338542750930230312178956502x +$$

$$3448161179503055646703298569039072037485594435931918036126600829629193944873224342 9$$

$$2 \cdot 2161 \cdot 194083 \cdot 2392360876634196152809896070161520193495865117 7$$

$$45317 \cdot 34460641 \cdot 1508741780415612155069 \cdot 14634845362034056885106572128327924482438697644053$$

3. What is the average size of the rank? (distribution?)

Open questions

1. What is the maximum value of r? (is there a maximum value?)
2. current record: $r = 28$, Noam Elkies, 2006

$$y^2 + xy + y = x^3 - x^2 - 20067762415575526585033208209338542750930230312178956502x +$$

$$3448161179503055646703298569039072037485594435931918036126600829629193944873224342 9$$

$$2 \cdot 2161 \cdot 194083 \cdot 23923608766341961528098960701615201934958651177$$

$$45317 \cdot 34460641 \cdot 1508741780415612155069 \cdot 14634845362034056885106572128327924482438697644053$$

3. What is the average size of the rank? (distribution?)
4. Do most elliptic curves have rank 0 or 1?

Open questions

1. What is the maximum value of r? (is there a maximum value?)
2. current record: $r = 28$, Noam Elkies, 2006

$$y^2 + xy + y = x^3 - x^2 - 20067762415575526585033208209338542750930230312178956502x +$$

$$3448161179503055646703298569039072037485594435931918036126600829629193944873224342 9$$

$$2 \cdot 2161 \cdot 194083 \cdot 2392360876634196152809896070161520193495865117 7$$

$$45317 \cdot 34460641 \cdot 1508741780415612155069 \cdot 14634845362034056885106572128327924482438697644053$$

3. What is the average size of the rank? (distribution?)
4. Do most elliptic curves have rank 0 or 1?
5. Is there an algorithm to determine the rank of an elliptic curve, that will provably terminate with the correct answer?

Open questions

1. What is the maximum value of r? (is there a maximum value?)
2. current record: $r = 28$, Noam Elkies, 2006

$$y^2 + xy + y = x^3 - x^2 - 20067762415575526585033208209338542750930230312178956502x +$$

$$3448161179503055646703298569039072037485594435931918036126600829629193944873224342 9$$

$$2 \cdot 2161 \cdot 194083 \cdot 23923608766341961528098960701615201934958651177$$

$$45317 \cdot 34460641 \cdot 1508741780415612155069 \cdot 14634845362034056885106572128327924482438697644053$$

3. What is the average size of the rank? (distribution?)
4. Do most elliptic curves have rank 0 or 1?
5. Is there an algorithm to determine the rank of an elliptic curve, that will provably terminate with the correct answer?
6. The BSD conjecture would give such an algorithm.

The Birch and Swinnerton-Dyer (BSD) Conjecture

The Birch and Swinnerton-Dyer (BSD) Conjecture

1. Key Idea look at solutions mod p

The Birch and Swinnerton-Dyer (BSD) Conjecture

1. Key Idea look at solutions mod p
2. In 1960, Birch and Swinnerton-Dyer did some computations of ranks of elliptic curves and of the number of solutions mod p (up to 53) on these elliptic curves

The Birch and Swinnerton-Dyer (BSD) Conjecture

1. Key Idea look at solutions mod p
2. In 1960, Birch and Swinnerton-Dyer did some computations of ranks of elliptic curves and of the number of solutions mod p (up to 53) on these elliptic curves
3. They produced a lot of theoretical and algorithmic breakthroughs

The Birch and Swinnerton-Dyer (BSD) Conjecture

1. Key Idea look at solutions mod p
2. In 1960, Birch and Swinnerton-Dyer did some computations of ranks of elliptic curves and of the number of solutions mod p (up to 53) on these elliptic curves
3. They produced a lot of theoretical and algorithmic breakthroughs
4. In general, for a random elliptic curve $E : y^2 = x^3 + Ax + B$ we expect about p points mod p

The Birch and Swinnerton-Dyer (BSD) Conjecture

1. Key Idea look at solutions mod p
2. In 1960, Birch and Swinnerton-Dyer did some computations of ranks of elliptic curves and of the number of solutions mod p (up to 53) on these elliptic curves
3. They produced a lot of theoretical and algorithmic breakthroughs
4. In general, for a random elliptic curve $E : y^2 = x^3 + Ax + B$ we expect about p points mod p
5. Denote by N_p the number of points mod p of an elliptic curve E.

The Birch and Swinnerton-Dyer (BSD) Conjecture

1. Key Idea look at solutions mod p
2. In 1960, Birch and Swinnerton-Dyer did some computations of ranks of elliptic curves and of the number of solutions mod p (up to 53) on these elliptic curves
3. They produced a lot of theoretical and algorithmic breakthroughs
4. In general, for a random elliptic curve $E : y^2 = x^3 + Ax + B$ we expect about p points mod p
5. Denote by N_p the number of points mod p of an elliptic curve E.
6. Thus N_p/p should be one most of the time

The Birch and Swinnerton-Dyer (BSD) Conjecture

1. Key Idea look at solutions mod p
2. In 1960, Birch and Swinnerton-Dyer did some computations of ranks of elliptic curves and of the number of solutions mod p (up to 53) on these elliptic curves
3. They produced a lot of theoretical and algorithmic breakthroughs
4. In general, for a random elliptic curve $E : y^2 = x^3 + Ax + B$ we expect about p points mod p
5. Denote by N_p the number of points mod p of an elliptic curve E.
6. Thus N_p/p should be one most of the time
7. However, if E has lot of rational point on it, then reducing these mod p would give a lot of points mod p on the elliptic curve.

The Birch and Swinnerton-Dyer (BSD) Conjecture

1. Key Idea look at solutions mod p
2. In 1960, Birch and Swinnerton-Dyer did some computations of ranks of elliptic curves and of the number of solutions mod p (up to 53) on these elliptic curves
3. They produced a lot of theoretical and algorithmic breakthroughs
4. In general, for a random elliptic curve $E : y^2 = x^3 + Ax + B$ we expect about p points mod p
5. Denote by N_p the number of points mod p of an elliptic curve E.
6. Thus N_p/p should be one most of the time
7. However, if E has lot of rational point on it, then reducing these mod p would give a lot of points mod p on the elliptic curve.
8. BSD hypothesized that if the rank of an elliptic curve E is large, then on the average (as p varies) one should notice E having more than p points modulo p.

The rank of the elliptic curve

The rank of the elliptic curve

Their computations in this direction led them to the observation that N_p/p is bigger than 1 for many primes p.

The rank of the elliptic curve

Their computations in this direction led them to the observation that N_p/p is bigger than 1 for many primes p.
They expressed this information with the following spectacular conjecture:

The rank of the elliptic curve

Their computations in this direction led them to the observation that N_p/p is bigger than 1 for many primes p.
They expressed this information with the following spectacular conjecture:

Conjecture (Birch and Swinnerton-Dyer)

The rank of the elliptic curve

Their computations in this direction led them to the observation that N_p/p is bigger than 1 for many primes p.
They expressed this information with the following spectacular conjecture:

Conjecture (Birch and Swinnerton-Dyer)

Let E be an elliptic curve of rank r and denote by N_p the number of points on E (mod p).

The rank of the elliptic curve

Their computations in this direction led them to the observation that N_p/p is bigger than 1 for many primes p.
They expressed this information with the following spectacular conjecture:

Conjecture (Birch and Swinnerton-Dyer)

Let E be an elliptic curve of rank r and denote by N_p the number of points on $E \pmod p$. Then

$$\prod_{p \leq X} \frac{N_p}{p}$$

The rank of the elliptic curve

Their computations in this direction led them to the observation that N_p/p is bigger than 1 for many primes p.
They expressed this information with the following spectacular conjecture:

Conjecture (Birch and Swinnerton-Dyer)

Let E be an elliptic curve of rank r and denote by N_p the number of points on $E \pmod p$. Then

$$\prod_{p \leq X} \frac{N_p}{p} \sim c$$

The rank of the elliptic curve

Their computations in this direction led them to the observation that N_p/p is bigger than 1 for many primes p.
They expressed this information with the following spectacular conjecture:

Conjecture (Birch and Swinnerton-Dyer)

Let E be an elliptic curve of rank r and denote by N_p the number of points on $E \pmod p$. Then

$$\prod_{p \leq X} \frac{N_p}{p} \sim c \cdot (\log X)^r$$

The rank of the elliptic curve

Their computations in this direction led them to the observation that N_p/p is bigger than 1 for many primes p.
They expressed this information with the following spectacular conjecture:

Conjecture (Birch and Swinnerton-Dyer)

Let E be an elliptic curve of rank r and denote by N_p the number of points on $E \pmod p$. Then

$$\prod_{p \leq X} \frac{N_p}{p} \sim c \cdot (\log X)^r$$

Birch and Swinnerton-Dyer also gave an explicit expression for c in terms of E (c.f. Don Zagier 1991)

The rank of the elliptic curve

Their computations in this direction led them to the observation that N_p/p is bigger than 1 for many primes p.
They expressed this information with the following spectacular conjecture:

Conjecture (Birch and Swinnerton-Dyer)

Let E be an elliptic curve of rank r and denote by N_p the number of points on $E \pmod p$. Then

$$\prod_{p \leq X} \frac{N_p}{p} \sim c \cdot (\log X)^r$$

Birch and Swinnerton-Dyer also gave an explicit expression for c in terms of E (c.f. Don Zagier 1991)
This is called the strong form of the BSD conjecture

The rank of the elliptic curve

Their computations in this direction led them to the observation that N_p/p is bigger than 1 for many primes p.
They expressed this information with the following spectacular conjecture:

Conjecture (Birch and Swinnerton-Dyer)

Let E be an elliptic curve of rank r and denote by N_p the number of points on E (mod p). Then

$$\prod_{p \leq X} \frac{N_p}{p} \sim c \cdot (\log X)^r$$

Birch and Swinnerton-Dyer also gave an explicit expression for c in terms of E (c.f. Don Zagier 1991)
This is called the strong form of the BSD conjecture
Remark If you prove BSD (weak/strong), you win a million $!

BSD = fundamental problem in NT

BSD = Birch and Swinnerton-Dyer conjecture

Named after Bryan Birch and Peter Swinnerton-Dyer, who developed it in the 1960's with the help of machine computation

- Describe BSD in elementary terms
- Explain why BSD is so important
- Mention what is known about it

The 7 Clay Millennium Prize Problems

Posed in 2000, in celebration of the new millennium

$ 1 M prize (each)

- Birch and Swinnerton-Dyer conjecture (BSD)
- Hodge conjecture
- Navier-Stokes existence and smoothness
- P versus NP
- Riemann Hypothesis
- Poincaré conjecture
- Yang-Mills existence and mass gap

The 7 Clay Millennium Prize Problems

Posed in 2000, in celebration of the new millennium

$ 1 M prize (each)

- Birch and Swinnerton-Dyer conjecture (BSD)
- Hodge conjecture
- Navier-Stokes existence and smoothness
- P versus NP
- Riemann Hypothesis
- Poincaré conjecture
- Yang-Mills existence and mass gap

In 2002 Grigori Perelman solved the Poincaré conjecture.
refused the 1M prize, (IHP, Paris, France)

The 7 Clay Millennium Prize Problems

Posed in 2000, in celebration of the new millennium

$ 1 M prize (each)

- Birch and Swinnerton-Dyer conjecture (BSD)
- Hodge conjecture
- Navier-Stokes existence and smoothness
- P versus NP
- Riemann Hypothesis
- Poincaré conjecture
- Yang-Mills existence and mass gap

In 2002 Grigori Perelman solved the Poincaré conjecture.
refused the 1M prize, (IHP, Paris, France)
BSD was discovered in its elementary formulation.

Claude Gaspard Bachet's pearl

Claude Gaspard Bachet's pearl

Consider the family of elliptic curves

$$y^2 = x^3 + k, \qquad k \neq 0 \tag{6}$$

Claude Gaspard Bachet's pearl

Consider the family of elliptic curves

$$y^2 = x^3 + k, \qquad k \neq 0 \tag{6}$$

Example

For $k = 17$, there are obvious integer/rational points:

Claude Gaspard Bachet's pearl

Consider the family of elliptic curves

$$y^2 = x^3 + k, \qquad k \neq 0 \tag{6}$$

Example

For $k = 17$, there are obvious integer/rational points:
$(2, 5)$, $(2, -5)$,

Claude Gaspard Bachet's pearl

Consider the family of elliptic curves

$$y^2 = x^3 + k, \qquad k \neq 0 \tag{6}$$

Example

For $k = 17$, there are obvious integer/rational points:
$(2, 5)$, $(2, -5)$, $\left(-\frac{64}{25}, -\frac{59}{125}\right)$

Claude Gaspard Bachet's pearl

Consider the family of elliptic curves

$$y^2 = x^3 + k, \qquad k \neq 0 \tag{6}$$

Example

For $k = 17$, there are obvious integer/rational points:
$(2, 5)$, $(2, -5)$, $\left(-\frac{64}{25}, -\frac{59}{125}\right)$
There are some less obvious rational points:

Claude Gaspard Bachet's pearl

Consider the family of elliptic curves

$$y^2 = x^3 + k, \qquad k \neq 0 \tag{6}$$

Example

For $k = 17$, there are obvious integer/rational points:
$(2, 5)$, $(2, -5)$, $\left(-\frac{64}{25}, -\frac{59}{125}\right)$
There are some less obvious rational points:
$\left(\frac{38194304}{87025}, -\frac{236046706033}{25672375}\right)$,

Claude Gaspard Bachet's pearl

Consider the family of elliptic curves

$$y^2 = x^3 + k, \qquad k \neq 0 \tag{6}$$

Example

For $k = 17$, there are obvious integer/rational points:
$(2, 5)$, $(2, -5)$, $\left(-\frac{64}{25}, -\frac{59}{125}\right)$
There are some less obvious rational points:
$\left(\frac{38194304}{87025}, -\frac{236046706033}{25672375}\right)$,
$\left(\frac{5320270475899308970040873195264}{484886307751129385591167022 5}, \frac{3880640057843875523189162704075133227405322 87}{337644656448214941842939018840311120390375}\right)$

Claude Gaspard Bachet's pearl

Consider the family of elliptic curves

$$y^2 = x^3 + k, \qquad k \neq 0 \tag{6}$$

Example

For $k = 17$, there are obvious integer/rational points:
$(2, 5)$, $(2, -5)$, $\left(-\frac{64}{25}, -\frac{59}{125}\right)$
There are some less obvious rational points:
$\left(\frac{38194304}{87025}, -\frac{236046706033}{25672375}\right)$,
$\left(\frac{5320270475899308970040873195264}{484886307751129385591167022 5}, \frac{3880640057843875523189162704075133227405322 87}{337644656448214941842939018840311120390375}\right)$

Bachet duplication formula (1621)

If (x, y) is a rational point on the curve (6), with $y \neq 0$, then another rational point on the curve (6) is given by:

Claude Gaspard Bachet's pearl

Consider the family of elliptic curves

$$y^2 = x^3 + k, \qquad k \neq 0 \tag{6}$$

Example

For $k = 17$, there are obvious integer/rational points:
$(2, 5)$, $(2, -5)$, $\left(-\frac{64}{25}, -\frac{59}{125}\right)$
There are some less obvious rational points:
$\left(\frac{38194304}{87025}, -\frac{236046706033}{25672375}\right)$,
$\left(\frac{5320270475899308970040873195264}{484886307751129385591167025}, \frac{3880640057843875523189162704075133227405322 87}{337644656448214941842939018840311120390375}\right)$

Bachet duplication formula (1621)

If (x, y) is a rational point on the curve (6), with $y \neq 0$, then another rational point on the curve (6) is given by:

$$\left(\frac{x^4 - 8kx}{4y^2}, \frac{-x^6 - 20kx^3 + 8k^2}{8y^3}\right)$$

Questions on Bachet's formula

Questions on Bachet's formula

Main Idea

If we start with a point (a, b) on the elliptic curve (6), then the formula gives, as the next point, the point of intersection of the curve with the tangent line to the curve (6)

- Do you think this sequence of points can be periodic?
- Is it always the case that the tangent intersects the curve at exactly one point?
- What is going on with the bad case $y = 0$?

Elliptic Curves over $\mathbb{F}_p$

Elliptic Curves over $\mathbb{F}_p$

- Elliptic Curves over finite fields are useful for cryptographic applications. Elliptic Curves Cryptography ECC

Elliptic Curves over $\mathbb{F}_p$

- Elliptic Curves over finite fields are useful for cryptographic applications. Elliptic Curves Cryptography ECC
- Consider curves $y^2 = x^3 + Ax + B$, with $A, B \in \mathbb{F}_7$, $\Delta = 4A^3 + 27B^2 \neq 0$ over the field $\mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$

Elliptic Curves over $\mathbb{F}_p$

- Elliptic Curves over finite fields are useful for cryptographic applications. Elliptic Curves Cryptography ECC
- Consider curves $y^2 = x^3 + Ax + B$, with $A, B \in \mathbb{F}_7$, $\Delta = 4A^3 + 27B^2 \neq 0$ over the field $\mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$
- There are at most 49 possible elliptic curves of this form over $\mathbb{F}_7$. (definitely fewer, since Δ can be 0)

Elliptic Curves over $\mathbb{F}_p$

- Elliptic Curves over finite fields are useful for cryptographic applications. Elliptic Curves Cryptography ECC
- Consider curves $y^2 = x^3 + Ax + B$, with $A, B \in \mathbb{F}_7$, $\Delta = 4A^3 + 27B^2 \neq 0$ over the field $\mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$
- There are at most 49 possible elliptic curves of this form over $\mathbb{F}_7$. (definitely fewer, since Δ can be 0)
- For a fixed such curve, $\exists$ 7 possible values for x and $\forall\, x \,\exists\, 0, 1, 2$ values of y, plus the point at ∞,

Elliptic Curves over $\mathbb{F}_p$

- Elliptic Curves over finite fields are useful for cryptographic applications. Elliptic Curves Cryptography ECC
- Consider curves $y^2 = x^3 + Ax + B$, with $A, B \in \mathbb{F}_7$, $\Delta = 4A^3 + 27B^2 \neq 0$ over the field $\mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$
- There are at most 49 possible elliptic curves of this form over $\mathbb{F}_7$. (definitely fewer, since Δ can be 0)
- For a fixed such curve, $\exists$ 7 possible values for x and $\forall\, x \,\exists\, 0, 1, 2$ values of y, plus the point at ∞, $\rightsquigarrow |E(\mathbb{F}_7)| \leq 15$

Elliptic Curves over $\mathbb{F}_p$

- Elliptic Curves over finite fields are useful for cryptographic applications. Elliptic Curves Cryptography ECC
- Consider curves $y^2 = x^3 + Ax + B$, with $A, B \in \mathbb{F}_7$, $\Delta = 4A^3 + 27B^2 \neq 0$ over the field $\mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$
- There are at most 49 possible elliptic curves of this form over $\mathbb{F}_7$. (definitely fewer, since Δ can be 0)
- For a fixed such curve, $\exists$ 7 possible values for x and $\forall\, x \,\exists\, 0, 1, 2$ values of y, plus the point at ∞, $\rightsquigarrow |E(\mathbb{F}_7)| \leq 15$

Example

$E : y^2 = x^3 + 5x + 2$ over the field $\mathbb{F}_7$

Elliptic Curves over $\mathbb{F}_p$

- Elliptic Curves over finite fields are useful for cryptographic applications. Elliptic Curves Cryptography ECC
- Consider curves $y^2 = x^3 + Ax + B$, with $A, B \in \mathbb{F}_7$, $\Delta = 4A^3 + 27B^2 \neq 0$ over the field $\mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$
- There are at most 49 possible elliptic curves of this form over $\mathbb{F}_7$. (definitely fewer, since Δ can be 0)
- For a fixed such curve, $\exists$ 7 possible values for x and $\forall x \exists 0, 1, 2$ values of y, plus the point at ∞, $\rightsquigarrow |E(\mathbb{F}_7)| \leq 15$

Example

$E : y^2 = x^3 + 5x + 2$ over the field $\mathbb{F}_7$

$\Delta = 4 \cdot 5^3 + 27 \cdot 2^2 \equiv 4 \cdot (-2)^3 + 6 \cdot 2^2 \equiv -8 \equiv 6 \neq 0 (mod 7)$

Elliptic Curves over $\mathbb{F}_p$

- Elliptic Curves over finite fields are useful for cryptographic applications. Elliptic Curves Cryptography ECC
- Consider curves $y^2 = x^3 + Ax + B$, with $A, B \in \mathbb{F}_7$, $\Delta = 4A^3 + 27B^2 \neq 0$ over the field $\mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$
- There are at most 49 possible elliptic curves of this form over $\mathbb{F}_7$. (definitely fewer, since Δ can be 0)
- For a fixed such curve, $\exists$ 7 possible values for x and $\forall\, x \,\exists\, 0, 1, 2$ values of y, plus the point at ∞, $\rightsquigarrow |E(\mathbb{F}_7)| \leq 15$

Example

$E : y^2 = x^3 + 5x + 2$ over the field $\mathbb{F}_7$

$\Delta = 4 \cdot 5^3 + 27 \cdot 2^2 \equiv 4 \cdot (-2)^3 + 6 \cdot 2^2 \equiv -8 \equiv 6 \neq 0 (mod 7)$

$E(\mathbb{F}_7) = \{\mathbf{0}, \underbrace{[0,3], [0,4]}_{[0,\pm 3]}, \underbrace{[1,1], [1,6]}_{[1,\pm 1]}, \underbrace{[3,3], [3,4]}_{[3,\pm 3]}, \underbrace{[4,3], [4,4]}_{[4,\pm 3]}\}$

Elliptic Curves over $\mathbb{F}_p$

- Elliptic Curves over finite fields are useful for cryptographic applications. Elliptic Curves Cryptography ECC
- Consider curves $y^2 = x^3 + Ax + B$, with $A, B \in \mathbb{F}_7$, $\Delta = 4A^3 + 27B^2 \neq 0$ over the field $\mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$
- There are at most 49 possible elliptic curves of this form over $\mathbb{F}_7$. (definitely fewer, since Δ can be 0)
- For a fixed such curve, $\exists$ 7 possible values for x and $\forall\, x \,\exists\, 0, 1, 2$ values of y, plus the point at ∞, $\rightsquigarrow |E(\mathbb{F}_7)| \leq 15$

Example

$E : y^2 = x^3 + 5x + 2$ over the field $\mathbb{F}_7$

$\Delta = 4 \cdot 5^3 + 27 \cdot 2^2 \equiv 4 \cdot (-2)^3 + 6 \cdot 2^2 \equiv -8 \equiv 6 \neq 0 (mod 7)$

$E(\mathbb{F}_7) = \{\mathbf{0}, \underbrace{[0,3], [0,4]}_{[0,\pm 3]}, \underbrace{[1,1], [1,6]}_{[1,\pm 1]}, \underbrace{[3,3], [3,4]}_{[3,\pm 3]}, \underbrace{[4,3], [4,4]}_{[4,\pm 3]}\}$

$E(\mathbb{F}_7)$ is an abelian group of order 9, isomorphic $\mathbb{Z}_3 \times \mathbb{Z}_3, \mathbb{Z}_9$

Elliptic Curves over $\mathbb{F}_p$

- Elliptic Curves over finite fields are useful for cryptographic applications. Elliptic Curves Cryptography ECC
- Consider curves $y^2 = x^3 + Ax + B$, with $A, B \in \mathbb{F}_7$, $\Delta = 4A^3 + 27B^2 \neq 0$ over the field $\mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$
- There are at most 49 possible elliptic curves of this form over $\mathbb{F}_7$. (definitely fewer, since Δ can be 0)
- For a fixed such curve, $\exists$ 7 possible values for x and $\forall x \exists 0, 1, 2$ values of y, plus the point at ∞, $\rightsquigarrow |E(\mathbb{F}_7)| \leq 15$

Example

$E : y^2 = x^3 + 5x + 2$ over the field $\mathbb{F}_7$

$\Delta = 4 \cdot 5^3 + 27 \cdot 2^2 \equiv 4 \cdot (-2)^3 + 6 \cdot 2^2 \equiv -8 \equiv 6 \neq 0 (mod 7)$

$E(\mathbb{F}_7) = \{\mathbf{0}, \underbrace{[0,3], [0,4]}_{[0,\pm 3]}, \underbrace{[1,1], [1,6]}_{[1,\pm 1]}, \underbrace{[3,3], [3,4]}_{[3,\pm 3]}, \underbrace{[4,3], [4,4]}_{[4,\pm 3]}\}$

$E(\mathbb{F}_7)$ is an abelian group of order 9, isomorphic $\mathbb{Z}_3 \times \mathbb{Z}_3, \mathbb{Z}_9$

Verify that $[4, 4]$ is of order 9,

Elliptic Curves over $\mathbb{F}_p$

- Elliptic Curves over finite fields are useful for cryptographic applications. Elliptic Curves Cryptography ECC
- Consider curves $y^2 = x^3 + Ax + B$, with $A, B \in \mathbb{F}_7$, $\Delta = 4A^3 + 27B^2 \neq 0$ over the field $\mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$
- There are at most 49 possible elliptic curves of this form over $\mathbb{F}_7$. (definitely fewer, since Δ can be 0)
- For a fixed such curve, $\exists$ 7 possible values for x and $\forall\, x \,\exists\, 0, 1, 2$ values of y, plus the point at ∞, $\rightsquigarrow |E(\mathbb{F}_7)| \leq 15$

Example

$E : y^2 = x^3 + 5x + 2$ over the field $\mathbb{F}_7$

$\Delta = 4 \cdot 5^3 + 27 \cdot 2^2 \equiv 4 \cdot (-2)^3 + 6 \cdot 2^2 \equiv -8 \equiv 6 \neq 0 (mod 7)$

$E(\mathbb{F}_7) = \{\mathbf{0}, \underbrace{[0,3], [0,4]}_{[0,\pm 3]}, \underbrace{[1,1], [1,6]}_{[1,\pm 1]}, \underbrace{[3,3], [3,4]}_{[3,\pm 3]}, \underbrace{[4,3], [4,4]}_{[4,\pm 3]}\}$

$E(\mathbb{F}_7)$ is an abelian group of order 9, isomorphic $\mathbb{Z}_3 \times \mathbb{Z}_3, \mathbb{Z}_9$

Verify that $[4,4]$ is of order 9, $\rightsquigarrow E(\mathbb{F}_7) \cong \mathbb{Z}_9$

The number of integer points on an elliptic curve

The number of integer points on an elliptic curve

The number of integer points on an elliptic curve

- Important question (for ECC): how large $E(\mathbb{F}_p)$ can be?

The number of integer points on an elliptic curve

- Important question (for ECC): how large $E(\mathbb{F}_p)$ can be?
- ECC == Elliptic Curves Cryptography

The number of integer points on an elliptic curve

- Important question (for ECC): how large $E(\mathbb{F}_p)$ can be?
- ECC == Elliptic Curves Cryptography
- A heuristic estimate (based on the uniform distribution) yields $p+1$ rational points

The number of integer points on an elliptic curve

- Important question (for ECC): how large $E(\mathbb{F}_p)$ can be?
- ECC == Elliptic Curves Cryptography
- A heuristic estimate (based on the uniform distribution) yields $p+1$ rational points
- $|E(\mathbb{F}_p)| = p + 1 + \text{error term}$

The number of integer points on an elliptic curve

- Important question (for ECC): how large $E(\mathbb{F}_p)$ can be?
- ECC == Elliptic Curves Cryptography
- A heuristic estimate (based on the uniform distribution) yields $p+1$ rational points
- $|E(\mathbb{F}_p)| = p+1+$error term

Theorem (Hasse)

$$-2\sqrt{p} < |E(\mathbb{F}_p)| - (p+1) < 2\sqrt{p}$$

The number of integer points on an elliptic curve

- Important question (for ECC): how large $E(\mathbb{F}_p)$ can be?
- ECC == Elliptic Curves Cryptography
- A heuristic estimate (based on the uniform distribution) yields $p+1$ rational points
- $|E(\mathbb{F}_p)| = p+1$+error term

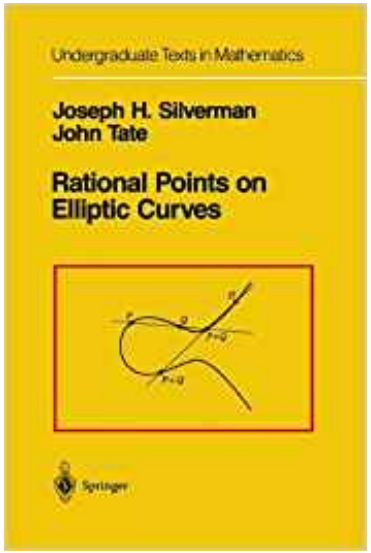
Theorem (Hasse)

$$-2\sqrt{p} < |E(\mathbb{F}_p)| - (p+1) < 2\sqrt{p}$$

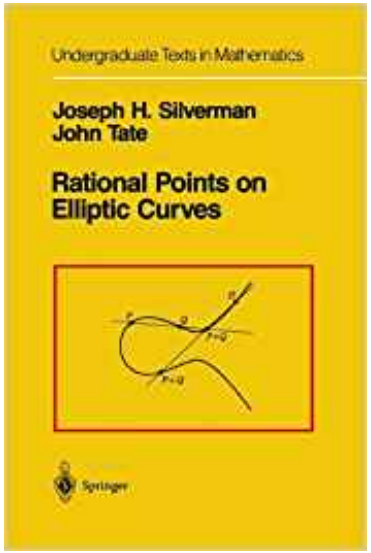
- The error term is bounded in absolute value by $2\sqrt{p}$

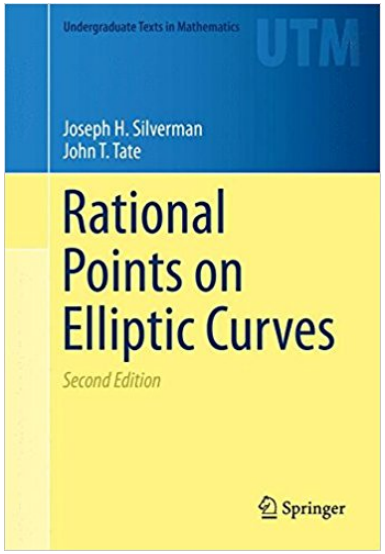
Useful bibliographical references

Useful bibliographical references

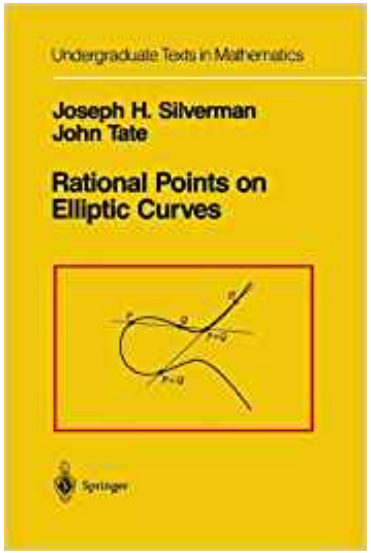


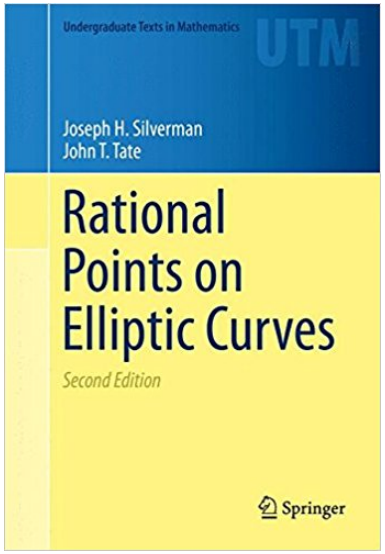
Useful bibliographical references

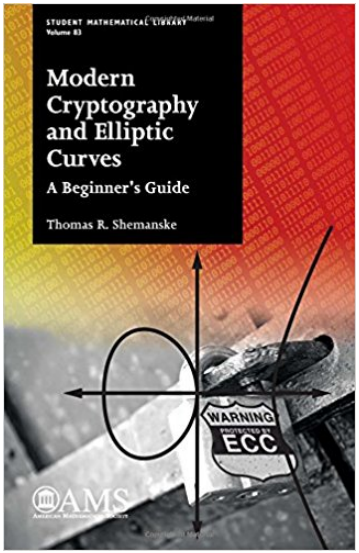




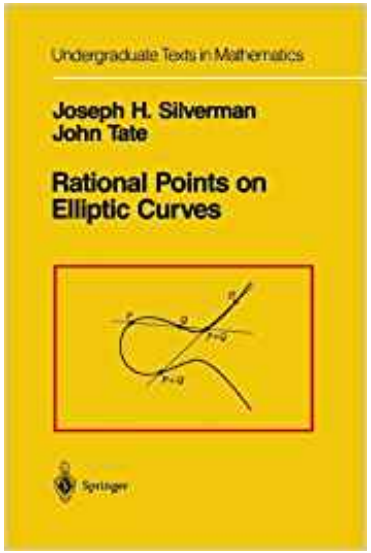
Useful bibliographical references

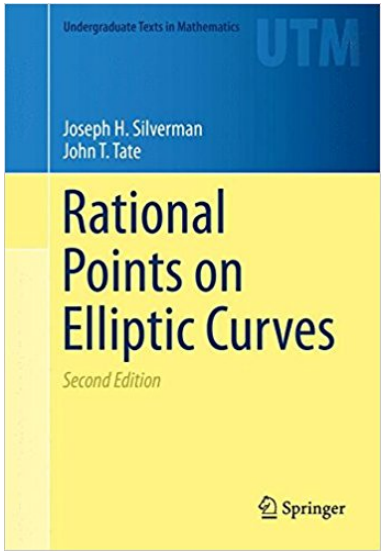


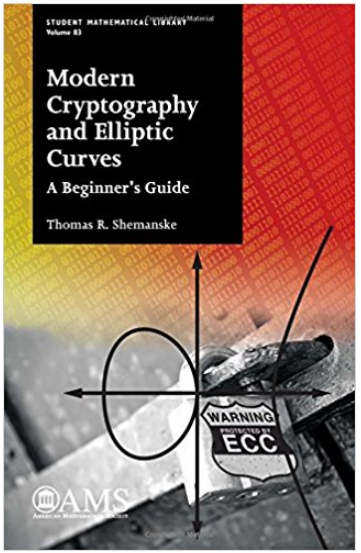


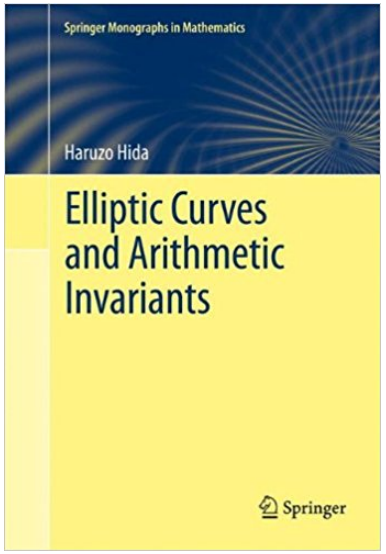


Useful bibliographical references

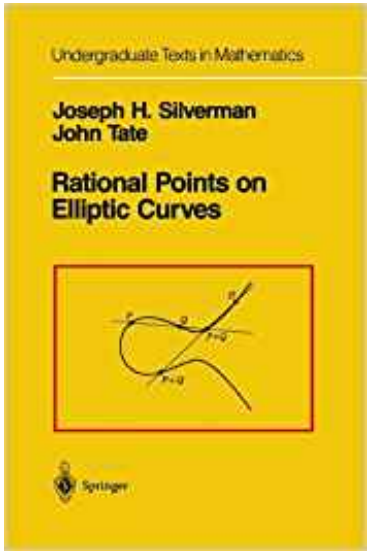


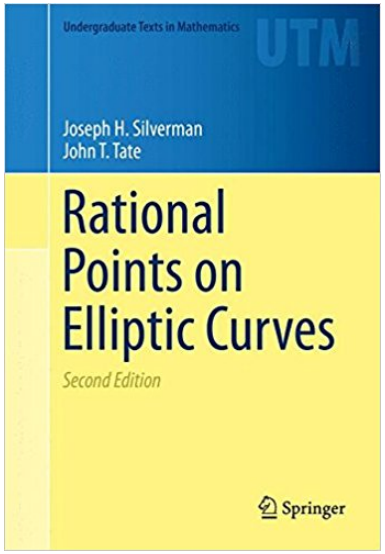


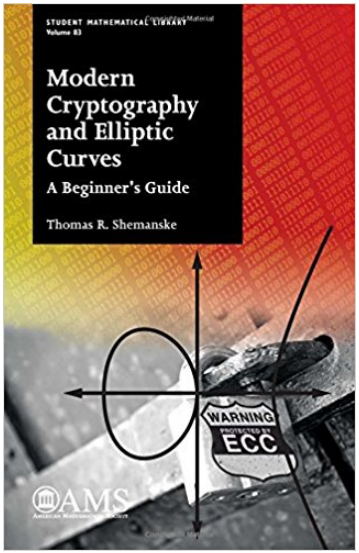


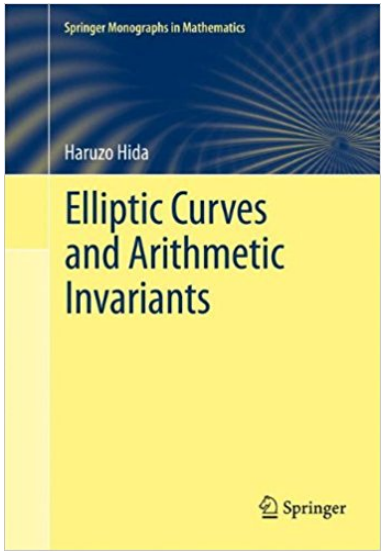


Useful bibliographical references









- Panorama of Mathematics: Manjul Bhargava 2015 Hausdorff Center for Mathematics, YouTube Video
  `https://www.youtube.com/watch?v=9popVxuvLEE`