

# Some Highlights along a Path to Elliptic Curves

**Part 2: Conic Sections and Rational Points**  
Steven J. Wilson, Fall 2016

---

---

---

---

---

---

---

---

## Outline of the Series

1. The World of Algebraic Curves
- 2. Conic Sections and Rational Points**
3. Projective Geometry and Bezout's Theorem
4. Solving a Cubic Equation
5. Exploring Cubic Curves
6. Rational Points on Elliptic Curves

---

---

---

---

---

---

---

---

## Sections of a Cone

The diagram illustrates the four types of conic sections based on the angle of a plane intersecting a cone. A legend on the right identifies the sections: Circle (red), Ellipse (green), Parabola (blue), and Hyperbola (orange). The top-left diagram shows a circle as a horizontal cross-section. The top-right diagram shows an ellipse as an inclined cross-section. The bottom-left diagram shows a parabola as a cross-section parallel to the cone's side. The bottom-right diagram shows a hyperbola as a cross-section steeper than the cone's side.

---

---

---

---

---

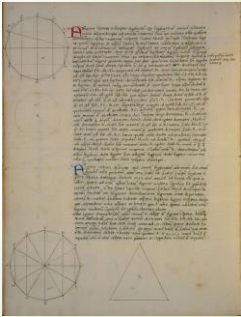
---

---

---

## Early Greek Conic Sections

- Menaechmus was the first to study conics (c350BC)
- Euclid (fl. 300 BC) wrote Conics, but it is now lost
- Archimedes (d. c212 BC) wrote: *On Conoids and Spheroids*
  - Work studied volumes of solids of revolution of conic sections
  - Image from: Piero della Francesca (c1416-1492), who illustrated works of Archimedes.




---

---

---

---

---


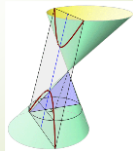
---

---

---

## Apollonius of Perga

- Lived c262-c190 BC
- Conics in 8 "books"
  - Book 8 is lost
  - Image from 9<sup>th</sup> century Arabic translation
- Euclid probably heavily influenced Books 1-3
- He was the first to use oblique cones
- Mentions foci, never directrix


---

---

---

---

---

---

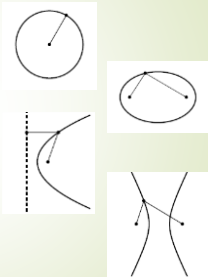
---

---

## Conics Defined as Loci

The set of points whose:

- Circle: Distance to center is constant
- Ellipse: Sum of distances to 2 foci is constant
- Parabola: Distance to focus equals distance to directrix
- Hyperbola: Difference of distances to 2 foci is constant




---

---

---

---

---

---

---

---

## Algebraic Curves of Degree 2

- The general equation:
 
$$ax^2 + bxy + cy^2 + dx + ey + f = 0$$
  - John Wallis was first (1655) to define conics by equations.

- Solve for  $y$  using the quadratic formula:

$$cy^2 + (bx + e)y + (ax^2 + dx + f) = 0$$

- And assuming  $c \neq 0$ :

$$y = \frac{-(bx + e) \pm \sqrt{(bx + e)^2 - 4c(ax^2 + dx + f)}}{2c}$$

$$y = \frac{-(bx + e) \pm \sqrt{(b^2 - 4ac)x^2 + (2be - 4cd)x + (e^2 - 4cf)}}{2c}$$

---

---

---

---

---

---

---

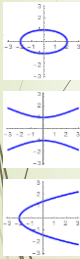
---

## The quadratic cases:

$$y = \frac{-(bx + e) \pm \sqrt{(b^2 - 4ac)x^2 + (2be - 4cd)x + (e^2 - 4cf)}}{2c}$$

Radicand is a quadratic function (parabola):

$$R(x) = (b^2 - 4ac)x^2 + (2be - 4cd)x + (e^2 - 4cf)$$



- If  $R(x)$  opens down, then  $b^2 - 4ac < 0$ , and the domain of  $R(x)$  is finite, which only happens with an ellipse (or circle).
- If  $R(x)$  opens up, then  $b^2 - 4ac > 0$ , and the domain of  $R(x)$  extends to infinity in both directions, which only happens with a hyperbola. [Since  $c \neq 0$ , parabolas with a vertical axis have been excluded.]
- If  $b^2 - 4ac = 0$ , then  $R(x)$  is a linear function, and the domain extends to infinity in only one direction, which only happens with a parabola.

Some "degenerate" cases are also possible.

---

---

---

---

---

---

---

---

## The other cases:

$$cy^2 + (bx + e)y + (ax^2 + dx + f) = 0$$

If  $c = 0$  then  $y = \frac{-(ax^2 + dx + f)}{(bx + e)}$



- If  $b \neq 0$  then the graph is a hyperbola with a vertical asymptote.
- If  $b = 0$  but  $e \neq 0$  then the graph is a parabola with a vertical axis.
- If  $b = e = 0$  then the equation becomes  $ax^2 + dx + f = 0$  whose graph is two vertical lines (or one or zero).

---

---

---

---

---

---

---

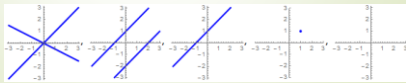
---

## The Discriminant



By defining the discriminant as  $D = b^2 - 4ac$  we have:

Discriminant	Curve	Degenerate Cases
Positive	Hyperbola	Two intersecting lines
Zero	Parabola	Two parallel lines, or One doubled line
Negative	Ellipse	A single point, or The empty set




---

---

---

---

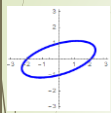
---

---

---

---

## Rotating the general conic



The general equation:

$$ax^2 + bxy + cy^2 + dx + ey + f = 0$$

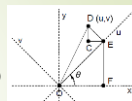
To rotate, let:

$$x = u \cos \theta + v \sin \theta, \quad y = -u \sin \theta + v \cos \theta$$

Then, after a lot of algebra, we find we can "remove"

the  $bxy$  term by using the substitution  $\cot 2\theta = \frac{c-a}{b}$ .

- For  $b \neq 0$ , since the range of the cotangent function is all real numbers, this always has a solution.
- For  $b = 0$ , no rotation is needed.




---

---

---

---

---

---

---

---

## Diophantine Equations

- A **Diophantine equation** is an equation whose solutions are restricted to the set of integers.
- The Diophantine equation  $2x + 3y = 4$  has solutions:  $\dots, (-1, 2), (2, 0), (5, -2), \dots$
- The Diophantine equation  $2x + 2y = 3$  has no solutions:
  - The left side of the equation is even, but the right side is odd.
- In order for the linear Diophantine equation  $ax + by = c$  to have solutions, the constant  $c$  must be a multiple of the greatest common divisor  $\gcd(a, b)$ .

---

---

---

---

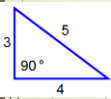
---

---

---

---

## Integer-Sided Right Triangles



- Can a right triangle have all 3 sides be integers?
  - Yes, the most famous example being 3, 4, 5.
- Sides of right triangles satisfy  $a^2 + b^2 = c^2$ .
- Pythagorean Triples** are sets of integers which satisfy the equation  $a^2 + b^2 = c^2$ .
- Finding Pythagorean Triples is a quadratic Diophantine problem.
- Pythagorean Triples are related to points on the unit circle  $x^2 + y^2 = 1$ .
  - Use the substitution  $x = \frac{a}{c}$ ,  $y = \frac{b}{c}$
- Those points will be **rational points**. That is, both coordinates of the point will be rational numbers.




---

---

---

---

---

---

---

---

## Pythagorean Triples

- Every primitive Pythagorean Triple can be expressed as  $(q^2 - p^2, 2pq, q^2 + p^2)$ , where  $q > p > 0$  are integers, have no common factors, and exactly one is odd.



q	p	a	b	c
2	1	3	4	5
3	1	violates "exactly one odd"		
3	2	5	12	13
4	1	15	8	17
4	2	violates "no common factors"		
4	3	7	24	25

---

---

---

---

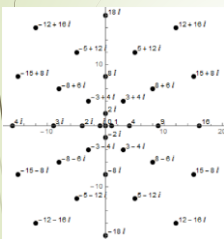
---

---

---

---

## Gaussian Integers



- Every primitive Pythagorean Triple  $(q^2 - p^2, 2pq, q^2 + p^2)$  can be produced by squaring a Gaussian integer.
- Let the Gaussian integer be  $q + pi$ .
- Then  $(q + pi)^2 = (q^2 - p^2) + (2pq)i$ , which gives the first two values in the Pythagorean Triple.
- And the "Pythagorean Theorem" produces the third:

$$\begin{aligned} & \sqrt{(q^2 - p^2)^2 + (2pq)^2} \\ &= \sqrt{q^4 + 2p^2q^2 + p^4} \\ &= q^2 + p^2 \end{aligned}$$

---

---

---

---

---

---

---

---

## Areas of Pythagorean Right Triangles

Some integers are areas of Pythagorean Right Triangles.

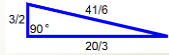
Triple	3,4,5	5,12,13	15,8,17	7,24,25	6,8,10
Area	6	30	60	84	24

The complete list begins: 6, 24, 30, 54, 60, 84, 96, 120, ...

Which integers are areas of rational-sided right triangles?

- Such integers are called **congruent numbers**.
- The smallest congruent number is 5. Note that:

$$\left(\frac{3}{2}\right)^2 + \left(\frac{20}{3}\right)^2 = \left(\frac{41}{6}\right)^2$$



- If denominators were common, the numerators would be the Pythagorean Triple (9, 40, 41).
- Finding congruent numbers efficiently is an unsolved problem.

---

---

---

---

---

---

---

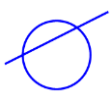
---

---

---

## Some Rational Point Theorems without Proofs

Assuming all given equations have integer coefficients ...



- If a line intersects a circle in two rational points, then the slope of the line is a rational number.
- If a line with rational slope intersects a circle twice, and one of the points is a rational point, then the other point is also a rational point.
- If a circle has one rational point, then it has an infinite number of rational points.
- Every rational point on the unit circle has the form

$$\left(\frac{1-m^2}{1+m^2}, \frac{2m}{1+m^2}\right)$$

where  $m$  is a rational number.

---

---

---

---

---

---

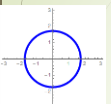
---

---

---

---

## A Circle With No Rational Points



- The circle  $x^2 + y^2 = 3$  has no rational points. Proof by contradiction.
- Assume  $(x, y)$  is a rational point, with coordinates in lowest terms.
- Then integers  $p, q, d$  exist with  $x = \frac{p}{d}$ ,  $y = \frac{q}{d}$ .
- Since we have lowest terms, at least one of  $p, q, d$  is odd.
- By substitution,  $p^2 + q^2 = 3d^2$ .
- If  $p$  is even, then  $p^2 \equiv 0 \pmod{4}$ . If odd, then  $p^2 \equiv 1 \pmod{4}$ .
- Same for  $q, d$ .
- So  $p^2 + q^2 \equiv 0, 1, 2 \pmod{4}$ , and  $3d^2 \equiv 0, 3 \pmod{4}$ .
- So both sides are  $0 \pmod{4}$ , and all variables are even.
- This contradicts the assumption that the fractions were in lowest terms.

---

---

---

---

---

---

---

---

---

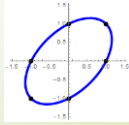
---

## Integer Sided 60° Triangles

- Can a triangle have a 60° angle and 3 integer sides?
  - Yes, equilateral triangles may. Are there others?
- Sides of the triangle satisfy
 
$$c^2 = a^2 + b^2 - 2ab \cos 60^\circ$$

$$c^2 = a^2 + b^2 - ab$$
- Triples solving this equation are called **Eisenstein Triples**.

- Do rational points exist on  $x^2 + y^2 - xy = 1$  ?
- Yes: (0,1), (1,0), (1,1), etc.
- It will have an infinite number of rational points.




---

---

---

---

---

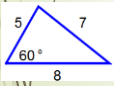
---

---

---

## Eisenstein Triples

- Every rational point on  $x^2 + y^2 - xy = 1$  has the form
 
$$\left( \frac{1-m^2}{1-m+m^2}, \frac{2m-m^2}{1-m+m^2} \right)$$
 where  $m$  is a rational number.
- Every triple  $(q^2 - p^2, 2pq - p^2, p^2 - pq + q^2)$  is an Eisenstein Triple.



q	p	a	b	c
2	1	3	3	3
3	1	8	5	7
4	1	15	7	13
5	1	24	9	21
5	2	21	16	19

---

---

---

---

---

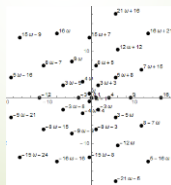
---

---

---

## Eisenstein Integers

- An Eisenstein Integer is a number of the form  $q + p\omega$ , where  $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ 
  - Note:  $\omega$  is one of the cube roots of +1.
- Every primitive Eisenstein Triple can be produced by squaring an Eisenstein integer.




---

---

---

---

---

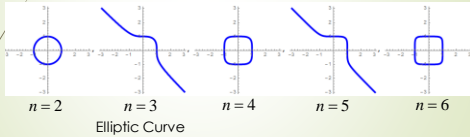
---

---

---

## Fermat's Last Theorem

- For  $n \geq 3$ , the equation  $a^n + b^n = c^n$  has no solutions where all three variables are positive integers.
- Equivalently, for  $n \geq 3$ , the equation  $x^n + y^n = 1$  has no nontrivial rational points.



- Andrew Wiles' proof (1994) of Fermat's Last Theorem (1637) investigated properties of elliptic curves.

---

---

---

---

---

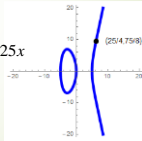
---

---

---

## Congruent Numbers Again

- Congruent numbers satisfy  $a^2 + b^2 = c^2$  and  $ab = 2n$ , where  $a, b, c$  are rational and  $n$  is an integer.
- There is a one-to-one correspondence between congruent numbers and the rational points on the curve  $y^2 = x^3 - n^2x$ .
- For  $n = 5$ , we have  $y^2 = x^3 - 25x$
- The (unsolved) congruent number problem is related to elliptic curves.




---

---

---

---

---

---

---

---

## Challenges:

- Find some more rational points on the unit circle.
- Find some more congruent numbers.
- Can a triangle have a  $120^\circ$  angle and 3 integer sides?

---

---

---

---

---

---

---

---