A WHIRLWIND TOUR BEYOND QUADRATICS

Steven J. Wilson, JCCC Professor of Mathematics
KAMATYC, Wichita, March 4, 2017

POLYNOMIAL ROOTS

Degree	Formula	History
1, linear $ax+b=0$	$x=\frac{-b}{a}$	
2, quadratic $ax^2+bx+c=0$	$x=\frac{-b\pm\sqrt{b^2-4ac}}{2a}$	Known to the Babylonians
3, cubic $ax^3+bx^2+cx+d=0$		del Ferro (1515), Tartaglia (1535) Cardano (published 1545)
4, quartic $ax^4+bx^3+\ \ldots\ =0$	even worse, but it is still algebraic	Ferrari (c1543) Cardano (published 1545)
5, quintic $ax^5+bx^4+\ \ldots\ =0$	requires hypergeometric functions	Abel (1826, no algebraic solution) Klein (1877)

THE CUBIC SOLUTION

$$ax^3+bx^2+cx+d=0$$

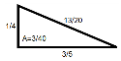
$$\begin{cases} x_1=\frac{-b}{3a}+u+v \\ x_2=\frac{-b}{3a}+\left(\frac{-1+i\sqrt{3}}{2}\right)u+\left(\frac{-1-i\sqrt{3}}{2}\right)v \\ x_3=\frac{-b}{3a}+\left(\frac{-1-i\sqrt{3}}{2}\right)u+\left(\frac{-1+i\sqrt{3}}{2}\right)v \end{cases} \text{ where } \begin{cases} u=\sqrt[3]{\frac{9abc-2b^3-27a^2d}{54a^3}+\sqrt{\frac{27a^2d^2-b^2c^2+4ac^3+4b^3d-18abcd}{108a^4}}} \\ v=\sqrt[3]{\frac{9abc-2b^3-27a^2d}{54a^3}-\sqrt{\frac{27a^2d^2-b^2c^2+4ac^3+4b^3d-18abcd}{108a^4}}} \end{cases}$$

DIOPHANTINE EQUATIONS

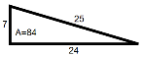
Degree	Solutions	History
1, linear $x + y = z$	Choose any 2 integers, the third will also be an integer.	
2, quadratic $x^2 + y^2 = z^2$	**Pythagorean Triples** Infinitely many non-trivial solutions, but not all integers can be used.	Known to Greeks, and before that, the Babylonians
3, cubic $x^3 + y^3 = z^3$	Trivial solutions only: At least one variable is zero. Same for higher degrees.	Fermat's Last Theorem (1637) Andrew Wiles (1995)

RATIONAL TRIPLES

- Can we construct right triangles with rational number (non-integer) sides?
  - Yes. Example:

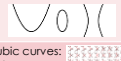


- Will the areas of Pythagorean triangles be integers?
  - For integer sides, yes, always.
  - For rational number sides, maybe.



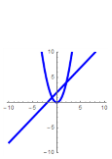
- Which integers can be areas of rational-sided right triangles?
  - Such integers are called **congruent numbers**.
  - **Unsolved problem**: How to find congruent numbers efficiently.

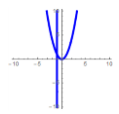
ALGEBRAIC CURVES

Degree	Solutions	History
1, linear $ax + by + c = 0$	Lines	
2, quadratic $ax^2 + bxy + cy^2 + dx + ey + f = 0$	Conic sections: 3 types 	Known to Greeks
3, cubic $ax^3 + bx^2y + cxy^2 + dy^3 + \ \ldots \ = 0$	Cubic curves: 78 types 	Newton (c1667)
4, quartic $ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4 + \ \ldots \ = 0$		Zeuthen (1874), Bullard (1899), and others …

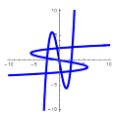
BEZOUT'S THEOREM

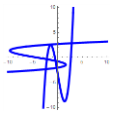
- Given 2 algebraic curves of degrees **m** and **n** having no common factors, then they intersect in exactly **mn** points, counting multiplicities, in the projective complex plane.





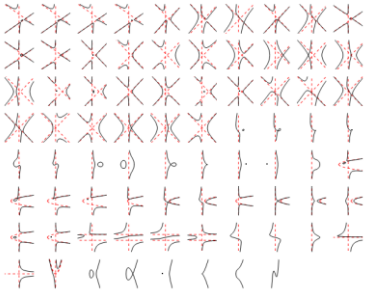
One at infinity





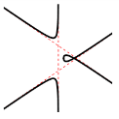
One double
Two nonreal

NEWTON'S 72 (78) SPECIES

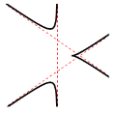


STRANGE BEHAVIORS

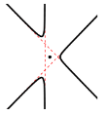
- Some curves have **singularities**.



Node



Cusp



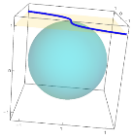
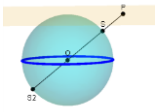
Isolated Point

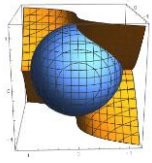
- A point on a curve $P(x,y)=0$ is singular when $P=\frac{\partial P}{\partial x}=\frac{\partial P}{\partial y}=0$ at that point.
- Sometimes the singularity is at infinity.

POINTS AT INFINITY

In 3D space:

- Sketch the graph of $P(x, y) = 0$ on the $z = 1$ plane.
- Project each point P onto the unit sphere (S, S2).
- Points at infinity are projected onto the equator.
- The projection lines form a surface.

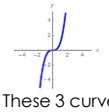





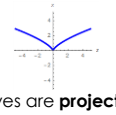
HOMOGENEOUS POLYNOMIALS

- Every term in a **homogeneous polynomial** has the same degree.
- Example: $x^3 - y = 0$, when homogenized, is $x^3 - yz^2 = 0$.
- Can dehomogenize in three ways:

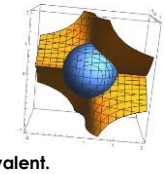
$z = 1$ $x^3 - y = 0$



$y = 1$ $x^3 - z^2 = 0$



$x = 1$ $1 - yz^2 = 0$



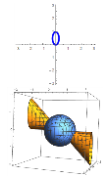
- These 3 curves are **projectively equivalent.**

EQUIVALENCE OF CONICS

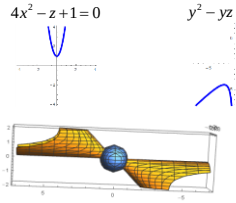
All 3 conic sections are projectively equivalent.

- Example: $4x^2 + y^2 - yz = 0$, when dehomogenized, gives:

$z = 1$ $4x^2 + y^2 - y = 0$

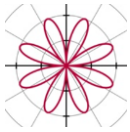


$y = 1$ $4x^2 - z + 1 = 0$

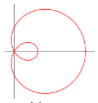


$x = 1$ $y^2 - yz + 4 = 0$

SPECIAL PLANE CURVES



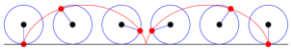
Roses
degree 8



Many Limacons
degree 4

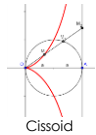
Lemniscates
degree 4

Trisectrix of Maclaurin
degree 3



Many Cycloids
non-algebraic

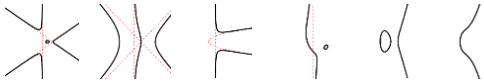
Folium of Descartes
degree 3



Cissoid of Diocles
degree 3

ELLIPTIC CURVES

- An **elliptic curve** is a non-singular cubic curve.



- Of Newton's 78 species, 38 are singular (8 at infinity), and 40 are elliptic curves.
- Projectively, they come in exactly 2 canonical types:

$$y^2 = x^3 \pm px$$

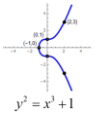
RATIONAL POINTS

- A **rational point** is a point where every coordinate is a rational number.

Degree of a Nonsingular Curve	Finite Rational Points
1, linear $ax+by+c=0$	0, 1, or infinite
2, quadratic $ax^2+bxy+cy^2+dx+ey+f=0$	0 or infinite (If you have 1, draw lines through it with rational slope and get more.)
3, cubic $ax^3+bx^2y+cxy^2+dy^3+\ \ldots\ =0$	0, finite nonzero, or infinite **Major Area of Current Research**
4, quartic $ax^4+bx^3y+cx^2y^2+dxy^3+ey^4+\ \ldots\ =0$	0 or finite nonzero, but never infinite

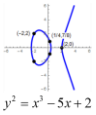
RATIONAL POINTS ON ELLIPTIC CURVES

- Elliptic curves may or may not have (finite) rational points.



$y^2 = x^3 + 1$

Exactly 5 rational points



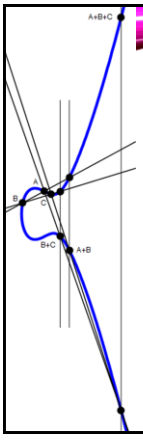
$y^2 = x^3 - 5x + 2$

Infinite number of rational points

$y^2 = x^3 + x + 5$

No rational points

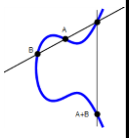
- If a line intersects an elliptic curve with rational coefficients in 3 points, and 2 of those points are rational points, then the third is also a rational point.



ADDING RATIONAL POINTS

For a canonical elliptic curve:

- Select 2 rational points, A and B.
- Draw a line through them, it intersects the curve 3 times.
- Draw a vertical line through the third point.
- The vertical line intersects the curve in one additional finite point, the sum A+B.
- The set of rational points on an elliptic curve with this addition operation form an **abelian group**.

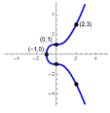


ORDER OF A POINT

- If $A + A + ... + A = nA = \infty$, then the order of point A is n.

Assuming an elliptic curve has integer coefficients:

- **Nagell-Lutz Theorem** (1935): If a rational point has finite order, then both coordinates are integers.



- **Mazur's Theorem** (1982): If a rational point has finite order, then the order is at most 12, but not 11.

FERMAT'S LAST THEOREM

- **Fermat's Last Theorem** (conjectured 1637): There are no non-trivial integer solutions of $a^n + b^n = c^n$ when $n \geq 3$.

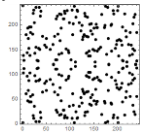

$$\left(\frac{a}{c}\right)^n + \left(\frac{b}{c}\right)^n = 1$$
$$x^n + y^n = 1$$

- Andrew Wiles proved (1995) that every semistable elliptic curve is modular (which was enough to imply Fermat's Last Theorem is true).

CRYPTOGRAPHY

- **Elliptic curve discrete logarithmic problem** (ECDLP): Given an elliptic curve on a finite field, and two points in that field, find the exponent (or multiple) needed on one point to obtain the other point.

$$y^2 = x^3 + 4 \mod 241$$



- The ECDLP is thought to be even harder then factoring very large integers.
- Bitcoin uses elliptic curve cryptography, specifically $y^2 = x^3 + 7$ over the integers mod

115792089237316195423570985008687907853269984665640564039457584007908834671663

BSD CONJECTURE

- **Birch and Swinnerton-Dyer Conjecture** (1965): The multiplicity of the L-function of a rational elliptic curve is equal to the rank of the group of rational points on the curve.


- This is one of the seven **Millennium Problems** identified by the Clay Mathematics Institute. Its proof is worth $1,000,000.

CONGRUENT NUMBER PROBLEM

- **Congruent Number Problem** (currently unsolved): Find all integers which are areas of right triangles where all three sides are rational numbers.

$$a^2 + b^2 = c^2 \quad \text{and} \quad \frac{1}{2}ab = n$$

- There is a one-to-one correspondence between congruent numbers and rational points on the elliptic curve $y^2 = x^3 - n^2 x$.

$$\begin{cases} x = n(a+c)/b \\ y = 2n^2(a+c)/b^2 \end{cases} \qquad \begin{cases} a = (x^2 - n^2)/y \\ b = 2nx/y \\ c = (x^2 + n^2)/y \end{cases}$$

- Tunnell's Theorem (1983) plus BSD Conjecture would prove it.

SUMMARY

Elliptic curves

- were at the heart of the proof of Fermat's Last Theorem
- can be used to encrypt electronic commerce
- are the focus of a $1,000,000 Millennium Problem
- would crack a unsolved question about Pythagorean triples

Not to mention the shear beauty in the 40 non-singular species of Newton's classification of 72 (78) cubic curves.

EXCITED?

- We live in exciting times (mathematically speaking).
- Can we infect our students with that excitement?
- These slides:

http://www.milefoot.com/about/presentations/BeyondQuadratics.pdf

- Related slides:

http://www.milefoot.com/about/presentations/EllipticCurves1.pdf

…/EllipticCurves6.pdf