Some Highlights along a Path to Elliptic Curves

Part 1: The World of Algebraic Curves

Steven J. Wilson, Fall 2016

Basic Definitions

- An **elliptic curve** is a nonsingular algebraic curve of degree 3.
- An **algebraic curve** is a graph of the zeros of a polynomial equation in two variables.
- In other words, an **elliptic curve** is the graph of $P(x, y) = 0$, where P is a nonsingular polynomial of degree 3.

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

Definition of a Polynomial

- A **polynomial function** (of one variable) is …
- … a function of the form

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$$
$$= \sum_{i=0}^{n} a_i x^i$$

… where n is a nonnegative integer, and $a_n \neq 0$.

- The value of n is the **degree** of the polynomial.

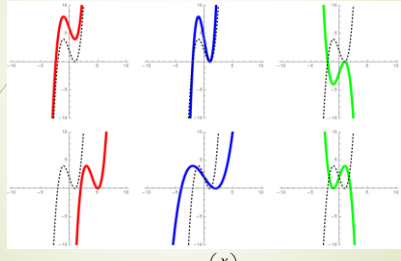
Polynomial Function Graphs

Characteristics of the graph of a polynomial function (of one variable) include:

- Domain is all real numbers
- Continuous
- Smooth (no corners)
- The x-intercepts give the real solutions of the equation $P(x) = 0$
- Number of x-intercepts is at most the degree
- Behavior at the x-intercept is given by multiplicity

Transformations

$y = f(x) + 4$ $y = 2f(x)$ $y = -f(x)$



$y = f(x-4)$ $y = f\left(\frac{x}{2}\right)$ $y = f(-x)$

Bivariate Polynomials

- A **bivariate polynomial** is …
- … a function of the form

$$P(x,y)=\sum_{j=0}^{n-k}\sum_{k=0}^{n}a_{jk}x^j y^k$$

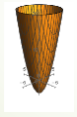
$$=a_{n,0}x^n y^0+\ldots+a_{0,n}x^0 y^n+\ldots\quad\ldots+a_{0,0}x^0 y^0$$

- … where n is a nonnegative integer, and at least one of $a_{n,0}, a_{n-1,1}, a_{n-2,2}, \ldots, a_{0,n}$ is not zero.
- The value of n is the **degree** of the polynomial.

Bivariate Polynomial Graphs

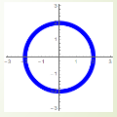
Example: $P(x,y)=x^2+y^2-4$

- We can graph $z=P(x,y)$ as a surface in space.
- Example: $z=x^2+y^2-4$



- Level curves of the 3D surface are algebraic curves.

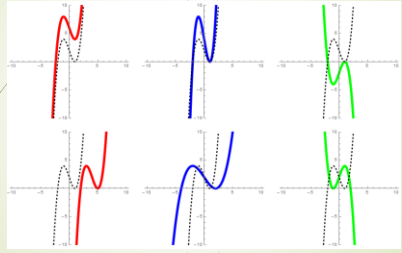
- We can graph $P(x,y)=0$ as a curve in the plane.
- Example: $x^2+y^2-4=0$



- An implicit plotter is useful for graphing algebraic curves.

Transforming Algebraic Curves

$P(x,y-4)=0$ $\quad P\left(x,\frac{y}{2}\right)=0$ $\quad P(x,-y)=0$



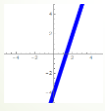
$P(x-4,y)=0$ $\quad P\left(\frac{x}{2},y\right)=0$ $\quad P(-x,y)=0$

Every Polynomial Function gives an Algebraic Curve

- Given the polynomial function (of one variable)
$$y = f(x)$$
- We can always rewrite it as
$$f(x) - y = 0$$
- Which is a bivariate polynomial
$$P(x, y) = f(x) - y$$
- Whose graph is an algebraic curve.

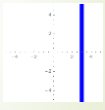
Lines

- Typical Example:
$$y = 3x - 4$$
$$3x - y - 4 = 0$$



- A typical line is an algebraic curve.

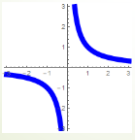
- Vertical Line Example:
$$x = 3$$
$$x - 3 = 0$$



- A vertical line is an algebraic curve.
- Algebraic curves need not pass the Vertical Line Test.

Rational Functions

- Typical Example:
$$y = \frac{1}{x}$$
$$xy - 1 = 0$$

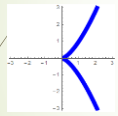


- Every rational function produces an algebraic curve.
$$y = \frac{f(x)}{g(x)}$$
$$f(x) - g(x)y = 0$$
- Algebraic curves may contain asymptotes.
- Holes will be replaced with vertical lines.

More behaviors

$y^2 - x^3 = 0$

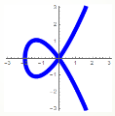
$y = \pm\sqrt{x^3}$



Cusp

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

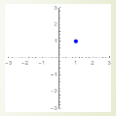
$y = \pm\, x\sqrt{x+2}$



Node
Double Point

$x^2 + y^2 - 2x - 2y + 2 = 0$

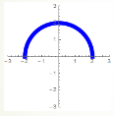
$(x-1)^2 + (y-1)^2 = 0$



Isolated Point

Radical Functions

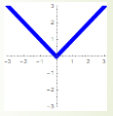
$y = \sqrt{4 - x^2}$



$y^2 = 4 - x^2$

- Subset of $x^2 + y^2 = 4$

$y = |x| = \sqrt{x^2}$



$y^2 = x^2$

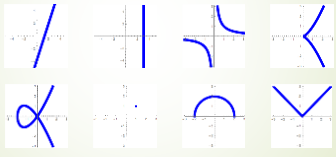
- Subset of $x^2 - y^2 = 0$

$(x-y)(x+y) = 0$

Graphs of Radical Functions are often subsets of algebraic curves.

Singularities

- Cusps, nodes, and isolated points are all examples of **singular points**.
- **A curve is singular** when it has a singular point. Otherwise it is nonsingular.

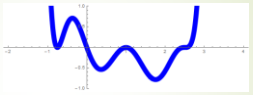


- [Calculus Note:] A point on a curve is **singular** when $\frac{\partial P}{\partial x} = \frac{\partial P}{\partial y} = 0$ at that point.

The Squaring Transformation

$P(x, y) = 0$

$y = f(x)$

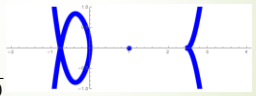


- into

$P(x, y^2) = 0$

$y^2 = f(x)$

$y = \pm\sqrt{f(x)}$



- Can you explain the effect of this transformation?

How to bake a pretzel (curve)

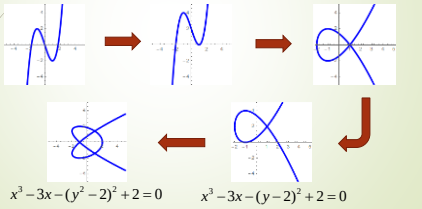
$y = x^3 - 3x$

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

$x^3 - 3x - (y-2) = 0$

$x^3 - 3x - y + 2 = 0$

$x^3 - 3x - y^2 + 2 = 0$



$x^3 - 3x - (y^2 - 2)^2 + 2 = 0$

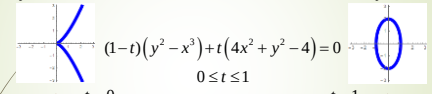
$-y^4 + x^3 + 4y^2 - 3x - 2 = 0$

$x^3 - 3x - (y-2)^2 + 2 = 0$

Morphing Curves

$y^2 - x^3 = 0$

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

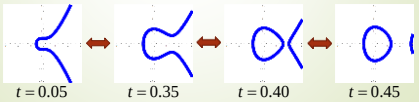


$(1-t)\left(y^2 - x^3\right) + t\left(4x^2 + y^2 - 4\right) = 0$

$0 \le t \le 1$

$t = 0$

$t = 1$



$t = 0.05$

$t = 0.35$

$t = 0.40$

$t = 0.45$

Combining Algebraic Curves

- The union of 2 algebraic curves is an algebraic curve.

$$x^2+y^2-4=0 \quad \cup \quad x+y-1=0$$

$$\left(x^2+y^2-4\right)\left(x+y-1\right)=0$$

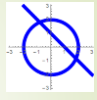
$$x^3+x^2y+xy^2+y^3-x^2-y^2-4x-4y+4=0$$

- Equivalently, if $P(x,y)=0$ factors, then the curve is the union of 2 algebraic curves.
- Factorable polynomials are **composite polynomials**, and those which do not factor are **prime polynomials**.
- Composite polynomials yield **degenerate curves**.

Perturbing Degenerate Curves

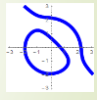
- Begin with a degenerate curve.

$$\left(x^2+y^2-4\right)\left(x+y-1\right)=0$$

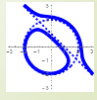


- Change the constant by a small amount.

$$\left(x^2+y^2-4\right)\left(x+y-1\right)=1$$

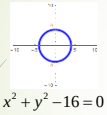


- The new curve is in some sense asymptotic to the original curve.
- Thinking of these as level curves of a 3D surface can explain why this happens.

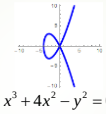


Zooming Out

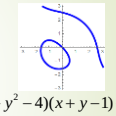
- The highest degree part of $P(x,y)$ describes the general appearance of the curve when we zoom out to infinity.



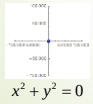
$x^2+y^2-16=0$



$x^3+4x^2-y^2=0$

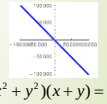


$(x^2+y^2-4)(x+y-1)-4=0$



$x^2+y^2=0$

$x^3=0$



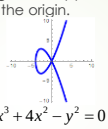
$(x^2+y^2)(x+y)=0$

- When bounded, the highest degree part is a single point.
- Asymptotes will be factors of the highest degree part.

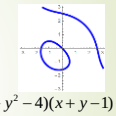
Zooming In

- The lowest degree non-zero part of $P(x, y)$ describes the general appearance of the curve when we zoom in to the origin.

$x^2 + y^2 - 16 = 0$

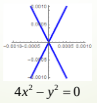


$x^3 + 4x^2 - y^2 = 0$



$(x^2 + y^2 - 4)(x + y - 1) - 4 = 0$

$-16 = 0$



$4x^2 - y^2 = 0$

$(2x - y)(2x + y) = 0$

$-4(x + y) = 0$

- The factors of the lowest degree non-zero part give the tangent lines at the origin.

Customizing a Curve

Create a nondegenerate algebraic curve that has 3 distinct tangents at the point (1,2), and two different linear end behaviors.

- Tangents at *origin* occur from factors of lowest degree part. $xy(x - y) = 0$
- End behaviors occur from factors of highest degree part. $(x + y)^2(x + 2y)^2 + xy(x - y) = 0$
- Move the curve so the multiple point is at (1,2).

$$(x - 1 + y - 2)^2(x - 1 + 2(y - 2))^2 + (x - 1)(y - 2)(x - 1 - (y - 2)) = 0$$

A Challenge

- For next time, create and share your most interesting algebraic curve, and briefly how you obtained it.
- Some references:
  - D2L Community: "Elliptic Curve Colloquia"
  - Kendig, A Guide to Plane Algebraic Curves, chapter 1