Elliptic Curves: a Jewel of Modern Mathematics

By: Jacob White

◄ | ►

How Would You Like to Win $1,000,000?

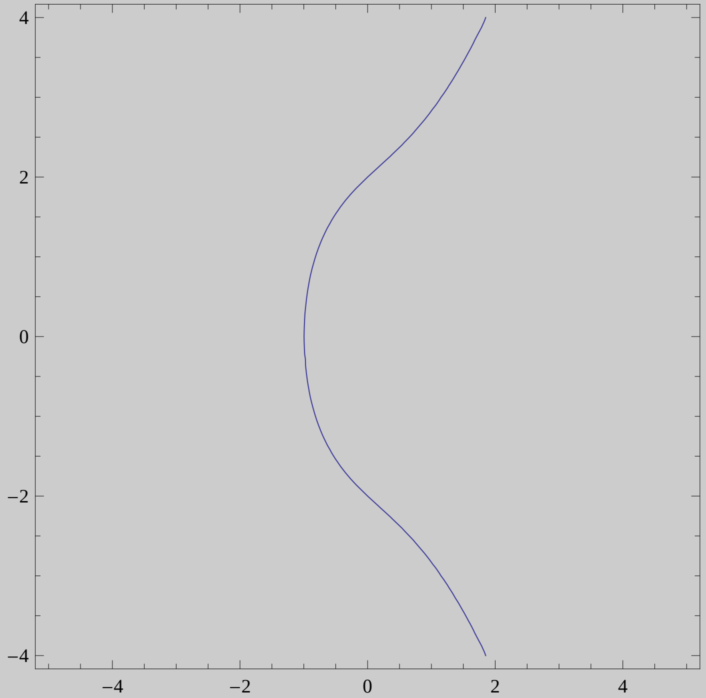
- Become famous like Andrew Wiles!
- Taniyama-Shimura Conjecture and Fermat's Last Theorem
- Birch and Swinnerton-Dyer Conjecture

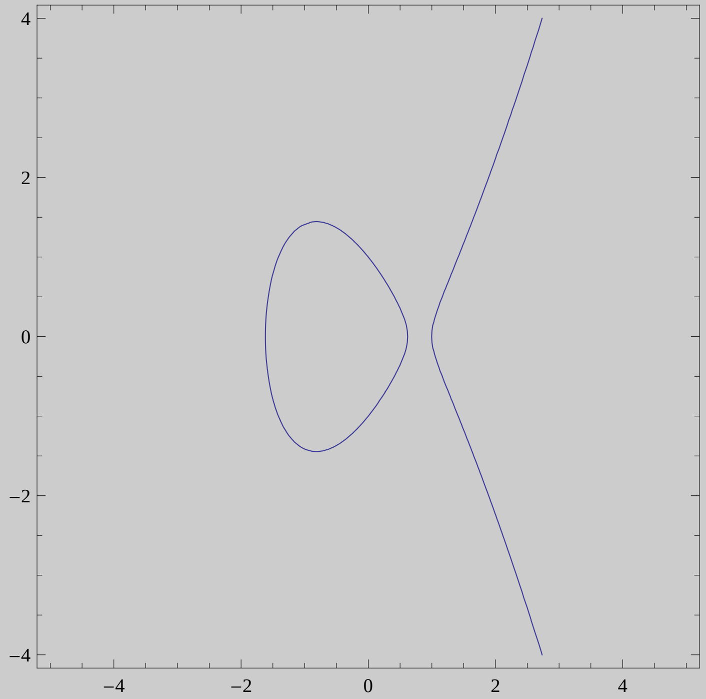
◀ | ▶

What does an Elliptic Curve Look Like?

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

$y^2 = x^3 - 2x + 1$


4
2
0
−2
−4
−4
−2
0
2
4

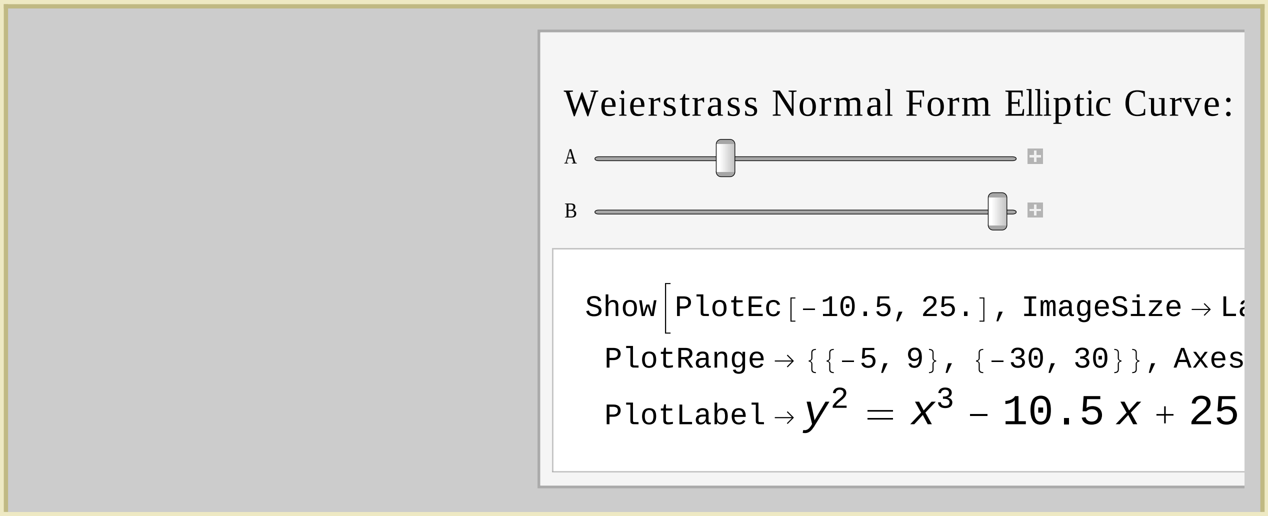

4
2
0
−2
−4
−4
−2
0
2
4

The General Form of an Elliptic Curve

- Complete general form : $y^2 + ay = x^3 + bx^2 + cxy + dx + e$, together with a special point, O

- Typical form: $y^2 = x^3 + ax + b$ (occurs when characteristic of field is neither 2 nor 3, and is called Weierstrass Normal Form)

More Examples



Weierstrass Normal Form Elliptic Curve:

```
Show[PlotEc[-10.5, 25.], ImageSize → La
 PlotRange → {{-5, 9}, {-30, 30}}, Axes
 PlotLabel → y^2 == x^3 - 10.5 x + 25
```

Show::gtype : PlotEc is not a type of graphics. ≫

What do these Curves have to do with Ellipses?

- Wallis - English Mathematician studying arclength of an ellipse
  Parameterize ellipse using x = acos(θ), y = bsin(θ)

- $a\int\sqrt{1-\frac{(1-b^2)}{a^2}\cos^2(\theta)}\,d\theta$

  Let $e^2 = 1 - \frac{b^2}{a^2}$, x = cos($\theta$) and the integral becomes: $-a\int\sqrt{\frac{1-(e^2x^2)}{1-x^2}}\,dx$

- Let y denote the integrand, and note that $y^2(1-x^2) = 1 - e^2x^2$

  Now let $u = \frac{1}{1+x}$, $v = y\,\frac{(1-x)}{(1+x)}$ and you can get $v^2 = 2(u^3)(1-e^2) + u^2(5e^2-1) - 4e^2u + e^2$

  And now we have an elliptic curve!

◄ | ►

Elliptic Integrals

- Does this integral look familiar? $\int \frac{1}{\sqrt{1-x^2}} \, dx$
- That's the Arcsine function!
- Arises from arclength of a circle rather than ellipse
- Example: -a $\int \sqrt{1 - \frac{\left(e^2 x^2\right)}{1-x^2}} \, dx$
- Generalization of inverse trigonometric functions

◄ | ►

Elliptic Functions

- Sine versus Arcsine
- Inversion of elliptic integrals!
- y=Sin(x) has period 2π...
- Definition: in the complex plane, an elliptic function is a *doubly* periodic function that is analytic and without singularities, where the ratio of the periods cannot be real
- Arise in differential equations, applications in engineering and physics
- Weierstrass elliptic functions

◄ | ►

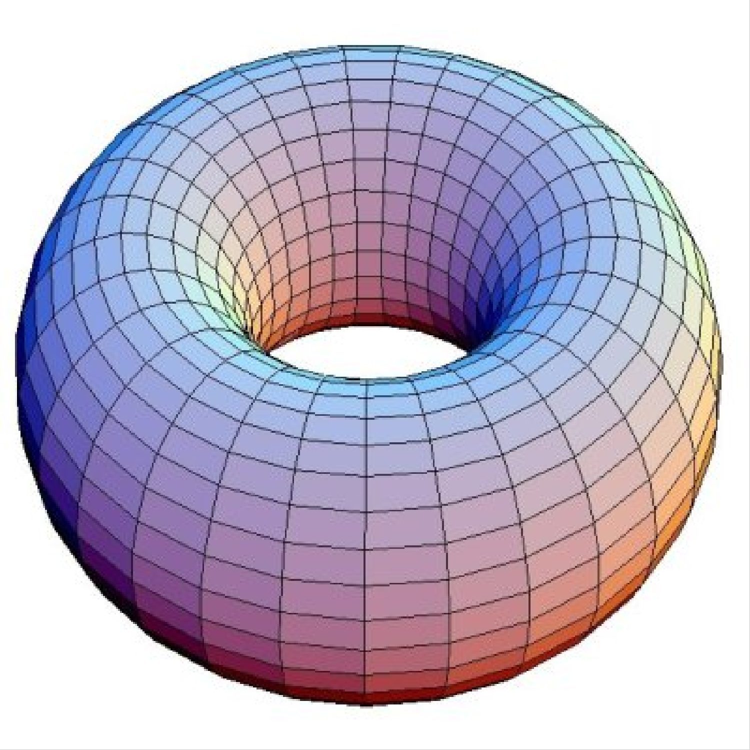
Gauss, Jacobi, and Abel

- Gauss - arclength of the lemniscate: $\frac{1}{\sqrt{2}}\int_0^1 \frac{1}{\sqrt{1-x^4}}\,dx$
- Jacobi's incomplete elliptic integral of the first kind:
  $$\int_0^X \frac{1}{\sqrt{\left(1-x^2\right)\left(1-k^2\,x^2\right)}}\,dx$$
  k^2 is called the modulus of the function.
- Gauss and Abel: if $k^2 \neq 1$, then inversion gives an elliptic function!

◂ | ▸

A torus on C/L

- Definition: The lattice L formed by x and y is the set {ax + by | a,b ϵ Z}
  Example: the Gaussian Integers {a + bi | a,b ϵ Z}!
- Form lattice with periods of elliptic function
- C/L is a torus!



◄ | ►

An Informal Definition of an Elliptic Curve

- A cubic curve whose solutions fall within a region topologically equivalent to a torus.

- Where did that come from?

- The Weierstrass elliptic functions tell us how to go from a given torus to an equation of the curve

◀ | ▶

Summary and Explanation

- Starting with an elliptic integral, take the inverse to get to an elliptic function.

- The resulting function has two complex periods, and by creating a lattice L out of these points we can use C/L to define an elliptic curve.

- Weierstrass elliptic functions again

$$y^2 + ay = x^3 + bx^2 + cxy + dx + e.$$

◀ | ▶

Introduction to the Projective Plane

- Special point on all elliptic curves?
- Definition: The real projective plane is the set of all lines through the origin.
- Ratios [X:Y:Z], where X,Y,Z ϵ R. (2,3,5) ~ (4,6,10)
- Identify lines of R_3 with their slope

◄ | ►

Projective Plane (Continued)

- $P_R{}^2$ (the projective plane): {[X:Y:Z] | X, Y, Z ϵ R, and X,Y,Z not all zero}.
- Line at infinity (Z = 0 yields [1:y:0])
- XY-plane hidden in projective plane (Z ≠ 1 yields [x:y:1])
- Equation for elliptic curve including special point: $Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3$
- Intersection of equation with projective plane?

Point at infinity and Weierstrass Equation ($y^2 = x^3$ + ax + b)

◀ | ▶

Finally, a Formal Definition

- An elliptic curve over a field K is the set of all solutions in K of a nonsingular projective algebraic curve over K with genus 1, together with a given point defined over K.

- Nonsingular - if f(x) is the equation of the curve, -f'(x) and $2\sqrt{f(x)}$ don't vanish at the same point

- Topologically equivalent to a torus

Point at infinity

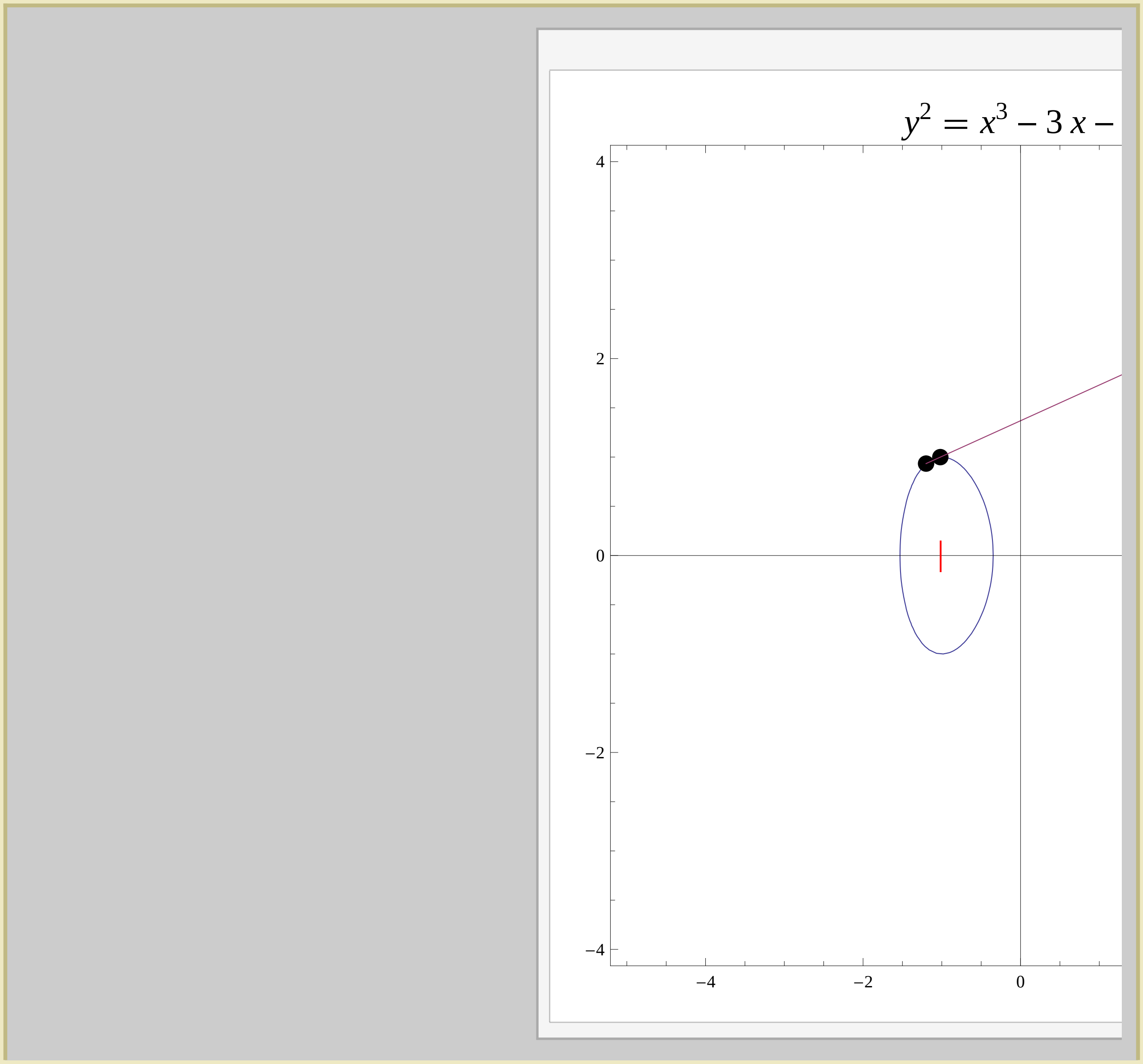
◄ | ►

Addition?

- We must be able to add points - C/L
- Geometric way: take two points on the curve, construct the line between them. If the line intersects a third point (almost always the case), reflect this point through the horizontal axis of symmetry to find the sum.
- Special cases...
- Abel's proof

◂ | ▸

Demonstration of Addition



What Properties Hold for this Addition?

- Additive inverse of a point (x,y) is (x, -y)

- Identity: point at infinity

- Associativity holds

- Even commutativity holds!

◀ | ▶

A Group is Born!

- Abelian group

- Geometry, Complex Analysis, and Abstract Algebra meet one another

- Applications of this remarkable fact

◀ | ▶

Subgroups

- **Poincare studied elliptic curves in depth**
- **Subgroup for the form $y^2 = x^3 + ax + b$**
- **Let a, b ϵ K for some field K. The set of all solutions with coordinates in K forms a subgroup of the entire curve**

◂ | ▸

Finite Fields and Cryptography

- The field K doesn't have to be infinite
- Applications to cryptography enjoy the field Z_p, where p is prime
- We can't view the curve geometrically over Z_p, but we can still add

◀ | ▶

Birch and Swinnerton-Dyer

- What if K is the rational numbers?

- The conjecture is that there is a simple way to tell whether an elliptic curve over Q has a finite or infinite number of solutions whose coordinates are also rational.

- Has been proven in special cases, still huge amount of research

◄ | ►

Final Thoughts

- Elliptic Curves are of vital importance in modern number theory

- Studying them *could* net you money

- Applications in computer science, engineering, and physics

◀ | ▶

Special Thanks To:

- **Wolfram and *Mathematica* for demonstrations and insight**

- **Dr. Lunsford for helping me choose an interesting and challenging topic**

◀ | ▶

Works Cited

- Koblitz, Neal. Introduction to Elliptic Curves and Modular Forms. New York: Springer, 1984.
- McKean, Henry and Moll, Victor. Elliptic Curves. Cambridge University Press, 1997.
- Charlap, Leonard S., and Robbins, David P. “An Elementary Introduction to Elliptic Curves.” December 1988. <www.idaccr.org/reports/reports.html>
- Akhtar, Reza. “An Introduction to Elliptic Curves.” Summer 2002. <calico.mth.muohio.edu/reza/sumsri/2002/notes.pdf>
- Silverman, Joseph H. “An Introduction to the Theory of Elliptic Curves.” July 2006. <www.math.brown.edu/~jhs/Presentations/WyomingEllipticCurve.pdf>
- Hewitt, Paul. “A Brief History of Elliptic Curves.” December 2005. <livetoad.org/Courses/Documents/132d/…/history_of_elliptic_curves.pdf>
- www.wikipedia.org
- mathworld.wolfram.com

◄ | ►