Elliptic curves: what they are, why they are called elliptic, and why topologists like them, I

Wayne State University Mathematics Colloquium
February 26, 2007

Doug Ravenel

Early history of elliptic curves

In the 18th century it was natural to ask about the arc length of an ellipse.

Early history of elliptic curves

In the 18th century it was natural to ask about the arc length of an ellipse. This question led to the study of integrals involving $\sqrt{f(x)}$ where $f(x)$ is a polynomial of degree 3 or 4.

Early history of elliptic curves

In the 18th century it was natural to ask about the arc length of an ellipse. This question led to the study of integrals involving $\sqrt{f(x)}$ where $f(x)$ is a polynomial of degree 3 or 4.

We know now that such integrals cannot be described in terms of familiar functions that we teach in calculus. They came to be known as *elliptic integrals*.

Early history of elliptic curves

If the ellipse is a circle, then one can simplify things and replace $f(x)$ by a quadratic polynomial. We teach our calculus students how to handle these "circular integrals," for example we know that

$$\int \frac{\mathrm{d}x}{\sqrt{1-x^2}} = \sin^{-1} x.$$

Early history of elliptic curves

If the ellipse is a circle, then one can simplify things and replace $f(x)$ by a quadratic polynomial. We teach our calculus students how to handle these “circular integrals,” for example we know that

$$\int \frac{\mathrm{d}x}{\sqrt{1-x^2}} = \sin^{-1} x.$$

Experience has taught us that the inverse of this function, namely $\sin x$, is much easier to deal with. Thus circular integrals lead to trigonometric functions $g(x)$, many of which are periodic in the sense that

$$g(x+2\pi) = g(x).$$

Early history of elliptic curves

Experience has taught us that the inverse of this function, namely $\sin x$, is much easier to deal with. Thus circular integrals lead to trigonometric functions $g(x)$, many of which are periodic in the sense that

$$g(x + 2\pi) = g(x).$$

This means that as a function of a complex variable, $g(x)$ is well defined on the quotient $\mathbf{C}/2\pi\mathbf{Z}$, which is topologically a cylinder.

Early history of elliptic curves

Similarly, it is convenient to replace certain elliptic integrals by their inverses, which came to be known as *elliptic functions*.

Early history of elliptic curves

Similarly, it is convenient to replace certain elliptic integrals by their inverses, which came to be known as *elliptic functions*. This insight was originally due to Abel.

Early history of elliptic curves

Similarly, it is convenient to replace certain elliptic integrals by their inverses, which came to be known as *elliptic functions*. This insight was originally due to Abel.

It turns out that an elliptic function $g(x)$ is doubly periodic in the following sense. There are nonzero complex numbers ω_1 and ω_2 (whose ratio is not real) such that

$$g(x + \omega_1) = g(x + \omega_2) = g(x).$$

Early history of elliptic curves

It turns out that an elliptic function $g(x)$ is doubly periodic in the following sense. There are nonzero complex numbers ω_1 and ω_2 (whose ratio is not real) such that

$$g(x+\omega_1) = g(x+\omega_2) = g(x).$$

This means that $g(x)$ factors through the quotient $\mathbf{C}/\Lambda$, where $\Lambda \subset \mathbf{C}$ is the lattice (additive subgroup) generated by ω_1 and ω_2. Topologically, $\mathbf{C}/\Lambda$ is a torus, and it is by definition an *elliptic curve over* $\mathbf{C}$. It is also an Abelian group since it is a quotient of the additive group $\mathbf{C}$.

Early history of elliptic curves

There are nonzero complex numbers ω_1 and ω_2 (whose ratio is not real) such that

$$g(x+\omega_1) = g(x+\omega_2) = g(x).$$

One can assume without loss of generality that $\tau = \omega_1/\omega_2$ has positive imaginary part (permuting ω_1 and ω_2 if necessary), and by a simple rescaling, we can replace ω_2 by 1. Thus every elliptic curve is isomorphic to one associated with the lattice generated by 1 and τ, where τ lies in the upper half plane.

Elliptic curves as plane cubics

Weierstrass determined the field of meromorphic functions that are doubly periodic with respect to a given lattice. His work led to a description of the corresponding elliptic curve as a cubic curve in the complex projective plane $\mathbf{C}P^2$.

Elliptic curves as plane cubics

Weierstrass determined the field of meromorphic functions that are doubly periodic with respect to a given lattice. His work led to a description of the corresponding elliptic curve as a cubic curve in the complex projective plane $\mathbf{C}P^2$.

Recall that $\mathbf{C}P^2$ is the space of complex lines through the origin in the complex vector space $\mathbf{C}^3$. A nonzero point (x, y, z) determines such a line, which we denote by $[x, y, z]$. Note that

$$[\lambda x, \lambda y, \lambda z] = [x, y, z]$$

for any nonzero scalar λ, and there is no line with coordinates $[0, 0, 0]$.

Elliptic curves as plane cubics

Now let $h(x, y, z)$ be a homogeneous polynomial of degree d. This means that

$$h(\lambda x, \lambda y, \lambda z) = \lambda^d h(x, y, z).$$

Hence h does *not* give a complex valued function on $\mathbf{C}P^2$, although it can be shown that is corresponds to a section of a certain line bundle over $\mathbf{C}P^2$.

Elliptic curves as plane cubics

Now let $h(x, y, z)$ be a homogeneous polynomial of degree d. This means that

$$h(\lambda x, \lambda y, \lambda z) = \lambda^d h(x, y, z).$$

Hence h does *not* give a complex valued function on $\mathbf{C}P^2$, although it can be shown that is corresponds to a section of a certain line bundle over $\mathbf{C}P^2$. However the set of points in $\mathbf{C}P^2$ where h vanishes is well defined and is called a *projective plane curve of degree d*, which we will denote by V_h. For "most" polynomials h, V_h is an embedded Riemann surface of genus $\binom{d-1}{2}$.

Elliptic curves as plane cubics

By "most" I mean the following. The set of homogeneous polynomials of degree d is a complex vector space of dimension $\binom{d+2}{2}$. It is known to have an open dense subset of polynomials h for which V_h is as above. It is also clear that this is not true for all h. For example of $h(x, y, z)$ is a product of d distinct linear factors, then V_h will be the union of d projective lines instead of a surface of the required genus.

Elliptic curves as plane cubics

Weierstrass showed that every elliptic curve $\mathbf{C}/\Lambda$ is equivalent (in the appropriate sense) to a projective plane curve E of degree 3. He gave formulas for the coefficients of the polynomial in terms of the lattice Λ which I will not go into here. This geometric description leads to the following way to describe the Abelian groups structure induced by complex addition.

The sum of any three colinear points in E is zero.

Elliptic curves as plane cubics

Note that finding the intersection of E with a projective line L boils down to finding the roots of a cubic equation in one variable. The Fundamental Theorem of Algebra tells us that one of three things will happen.

(i) There are three distinct roots, which means that L meets E at three distinct points, say A, B and C.

Elliptic curves as plane cubics

Note that finding the intersection of E with a projective line L boils down to finding the roots of a cubic equation in one variable. The Fundamental Theorem of Algebra tells us that one of three things will happen.

(ii) There are two distinct roots, which means that L meets E at two distinct points A and B. In this case the line is tangent to the point A correspsonding to the repeated root, and $2A + B = 0$.

Elliptic curves as plane cubics

Note that finding the intersection of E with a projective line L boils down to finding the roots of a cubic equation in one variable. The Fundamental Theorem of Algebra tells us that one of three things will happen.

(iii) There is a single root with multiplicity three. In this case L meets E tangentially at a single point of inflection A, and $3A = 0$.

Elliptic curves as plane cubics

The colinear rule is not quite enough to determine the group structure on E because it does not determine which point $e \in E$ is the identity. Since $3e = 0$, e must be a point of inflection, and it is known that there are 9 of them. This can be seen from the lattice point of view as follows.

Elliptic curves as plane cubics

Suppose the lattice Λ is generated by 1 and τ. Then each of the 9 points points in the set

$$\{(a + b\tau)/3 \colon 0 \leq a, b < 3\}$$

has order dividing 3 in $\mathbf{C}/\Lambda$. Similarly, there are n^2 points with order dividing n.
Once we have chosen one of the 9 points of inflection as the identity element, the group structure on E is determined by the colinear rule

The formal group law

Suppose that

$$h(x, y, z) = x^3 + axy^2 + by^3 - yz^2$$

for some constants a and b. This defines an elliptic curve provided that

$$4a^3 + 27b^2 \neq 0.$$

The formal group law

We can choose $[0, 0, 1]$ to be our identity element. There is an embedding of the affine plane $\mathbf{C}^2$ into the projective plane given by

$$(x, y) \mapsto [x, y, 1].$$

Let E' denote the intersection of this plane with the elliptic curve E defined by the equation $h(x, y, z) = 0$, so E' is the affine plane curve defined by

$$y = x^3 + axy^2 + by^3.$$

The identity element of E lies in E' at the origin.

The formal group law

The following facts are easily verified.

(i) Near the origin there is an odd power series expansion for y, namely

$$y = y(x) = x^3 + ax^7 + bx^9 + 2a^2x^{11} + \dots,$$

so a point on E' near the origin is determined by its first coordinate. This power series has coefficients in the ring $R = \mathbf{Z}[a, b]$.

The formal group law

The following facts are easily verified.

(ii) $(x, y) \in E'$ iff $(-x, -y) \in E'$, so the group theoretic inverse of the point (x, y) is $(-x, -y)$.

The formal group law

The following facts are easily verified.

(ii) $(x, y) \in E'$ iff $(-x, -y) \in E'$, so the group theoretic inverse of the point (x, y) is $(-x, -y)$.

(iii) Given two points (x_1, y_1) and (x_2, y_2) near the origin, let (x_3, y_3) denote their group theoretic sum. Then there is a power series expansion $F(x_1, x_2)$ for x_3 in terms of x_1 and x_2 with coefficients in R.

The formal group law

In addition to having a positive radius of convergence, F must satisfy the following three conditions.

(i) $F(u,0) = F(0,u) = u$ since $(0,0)$ is the identity element.

(ii) $F(v,u) = F(u,v)$ since the group is Abelian.

(iii) $F(F(u,v),w) = F(u,F(v,w))$ by associativity.

The oddness of the series for y above implies additionally that $F(u,-u) = 0$.

The formal group law

We define a *commutative 1-dimensional formal group law over a ring* R to be a power series $F \in R[[u, v]]$ satisfying the three conditions above, but without any convergence requirement. A commutative n-dimensional formal group law is a collection of n power series in $2n$ variable satsifying similar conditions. For a much more thorough discussion [Rav04, Appendix 2].

The choice of $h(x, y, z)$ above is convenient but not essential. The variable x could be replaced by a local coordinate at the identity, and we would still get a formal group law.

References

[Hus87] Dale Husemoller. *Elliptic curves*, volume 111 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1987. With an appendix by Ruth Lawrence.

[Kna92] Anthony W. Knapp. *Elliptic curves*, volume 40 of *Mathematical Notes*. Princeton University Press, Princeton, NJ, 1992.

[Kob84] N. Koblitz. *Introduction to Elliptic Curves and Modular Forms*. Graduate Texts in Mathematics. Springer-Verlag, New York, 1984.

References

[Rav04] D. C. Ravenel. *Complex Cobordism and Stable Homotopy Groups of Spheres, Second Edition*. American Mathematical Society, Providence, 2004. Available online.

[Sil86] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.

[ST92] Joseph H. Silverman and John Tate. *Rational points on elliptic curves*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992.