

An elliptic curve (over \mathbb{C}) is an algebraic curve whose rational function field is equivalent over \mathbb{C} to the field of all elliptic functions with some given proper period lattice.

—Patrick Du Val, *Elliptic Functions and Elliptic Curves*, Cambridge 1973, p.185.

Curves of genus 1 are called elliptic curves.

—Robin Hartshorne, *Algebraic Geometry*, Springer 1977, p.56.

An irreducible curve is said to be elliptic if it is birationally equivalent to a plane non-singular cubic.

—J.G.Semple & G.T.Kneebone, *Algebraic Curves*, Oxford 1959, p.177.

Informally, an elliptic curve is a type of cubic curve whose solutions are confined to a region of space that is topologically equivalent to a torus.

Formally, an elliptic curve over a field K is a nonsingular cubic curve in two variables, $f(X, Y) = 0$, with a K -rational point (which may be a point at infinity).

—<http://mathworld.wolfram.com/EllipticCurve.html>

If $y^2 = P(x)$, where P is any polynomial of degree three or four in x with no repeated roots, then we obtain a nonsingular plane curve of genus one, which is also called an elliptic curve.

—http://en.wikipedia.org/wiki/Elliptic_curve

Arc length of an ellipse of eccentricity k :

$$u = \int \sqrt{1 - k^2 \sin^2 \theta} \, d\theta$$

This is an elliptic integral of the *second* kind.

If this formula is inverted, so that we regard θ as a function of u , then it is clearly periodic, with period the length of the ellipse.

Now consider

$$u = \int \frac{d\theta}{\sqrt{1 - k^2 \sin^2 \theta}}$$

This is an elliptic integral of the *first* kind.

Substituting $x = \sin^2 \theta$ (sic!) puts it in the form

$$u = \int \frac{dx}{\sqrt{\text{cubic in } x}}$$

Weierstrass' \wp -function: $\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Omega'} \left(\frac{1}{(z - \omega)^2} - \frac{1}{\omega^2} \right)$.

Ω is a lattice; $\Omega' = \Omega \setminus \{0\}$. (\wp depends on Ω , as well as z ; and $\wp(z + \omega) = \wp(z)$, all $\omega \in \Omega$: \wp is doubly periodic—an elliptic function.)

$$\wp^{-1}(x) = \int \frac{dx}{\sqrt{4x^3 - ax - b}}$$

where $a = 60 \sum_{\Omega'} \omega^{-4}$ and $b = 140 \sum_{\Omega'} \omega^{-6}$, and $a^3 \neq 27b^2$.

The curve

$$y^2 = 4x^3 - ax - b$$

is parametrised by $(x, y) = (\wp(z), \wp'(z))$.

(Here I was just trying to get an elliptic function, an elliptic integral, and an elliptic curve, onto the same slide!)

Let the non-singular cubic curve Γ be given by the equation

$$y^2 = x(x - 1)(x - \lambda)$$

where $\lambda \neq 0, 1$. [In fact every non-singular cubic is projectively equivalent (over \mathbb{C}) to the above, for some such $\lambda \in \mathbb{C}$.]

We shall show that Γ is not a rational curve, that is, it cannot be parametrised by rational functions.

(The argument is adapted from Miles Reid, *Undergraduate Algebraic Geometry*, CUP 1988.)

Suppose to the contrary, that there are polynomials

$$p = p(t), \quad q = q(t), \quad r = r(t), \quad s = s(t)$$

such that

$$x = \frac{p}{q}, \quad y = \frac{r}{s}$$

is a parametrisation of the curve, that is,

$$\left(\frac{r}{s}\right)^2 = \frac{p}{q} \left(\frac{p}{q} - 1\right) \left(\frac{p}{q} - \lambda\right).$$

We assume $q \neq 0$ and $s \neq 0$, of course, and also that p, q are coprime (and not both constant), and likewise r, s .

Clearing denominators, we have

$$r^2q^3 = s^2p(p - q)(p - \lambda q).$$

Thus $s^2 \mid r^2q^3$; but r, s are coprime, so $s^2 \mid q^3$.

Next, $q^3 \mid s^2p(p - q)(p - \lambda q)$; but p, q are coprime, so $q^3 \mid s^2$.

We deduce that $s^2 = \alpha q^3$ for some non-zero $\alpha \in \mathbb{C}$, and so, writing $\alpha = \beta^2$ for some $\beta \in \mathbb{C}$, we have

$$q = \left(\frac{s}{\beta q} \right)^2,$$

so that q is a square in the polynomial ring $\mathbb{C}[t]$. (OK?)

From

$$r^2q^3 = s^2p(p - q)(p - \lambda q)$$

we obtain, on substituting $s^2 = \alpha q^3$ and $\alpha = \beta^2$, and cancelling,

$$r^2 = \beta^2p(p - q)(p - \lambda q).$$

Now because p and q are coprime, it follows that the polynomials p , $p - q$, $p - \lambda q$ are pairwise coprime, and since their product is a square in $\mathbb{C}[t]$, so each one of them is itself a square in $\mathbb{C}[t]$.

We already know that q is a square, so now we have that all four of p , q , $p - q$, $p - \lambda q$ are squares in $\mathbb{C}[t]$, where p , q are coprime, not both constant, and $\lambda \neq 0, 1$.

We use the method of descent to show that this is impossible: we shall find p_1, q_1, λ_1 satisfying the same conditions, but with

$$0 < \max(\deg(p_1), \deg(q_1)) < \max(\deg(p), \deg(q)).$$

Repeating the argument eventually gives a contradiction, because one cannot have an infinite decreasing sequence of positive integers.

So write $p = u^2$ and $q = v^2$ for some $u, v \in \mathbb{C}[t]$; note that u, v must be coprime, with

$$0 < \max(\deg(u), \deg(v)) < \max(\deg(p), \deg(v)).$$

Then

$$p - q = u^2 - v^2 = (u - v)(u + v),$$

so, since this is a square and $u \pm v$ are coprime (OK?) then $u \pm v$ are squares. Likewise, writing $\lambda = \mu^2$ for some $\mu \in \mathbb{C}$, $\mu \neq -1, 0, 1$,

$$p - \lambda q = u^2 - \mu^2 v^2 = (u - \mu v)(u + \mu v),$$

and so $u \pm \mu v$ are also squares.

Now put $p_1 = (\mu + 1)(u - v)$ and $q_1 = (\mu - 1)(u + v)$, noting that p_1, q_1 are squares since $u \mp v$ are squares—and so are $\mu \pm 1$ of course, since they are in \mathbb{C} . Also p_1, q_1 are coprime, with

$$\max(\deg(p_1), \deg(q_1)) = \max(\deg(u), \deg(v)),$$

and so

$$0 < \max(\deg(p_1), \deg(q_1)) < \max(\deg(p), \deg(v)),$$

as required.

It remains to show that $p_1 - q_1$ and $p_1 - \lambda_1 q_1$ are squares, for some $\lambda_1 \in \mathbb{C}$, $\lambda_1 \neq 0, 1$.

Then

$p_1 - q_1 = (\mu + 1)(u - v) - (\mu - 1)(u + v) = 2(u - \mu v)$,
which is a square, since $u - \mu v$ is—and so is 2, of course!

Finally, putting $\lambda_1 = \left(\frac{1 + \mu}{1 - \mu}\right)^2$ ($\neq 0, 1$), we have

$$\begin{aligned} p_1 - \lambda_1 q_1 &= (1 + \mu)(u - v) + \frac{(1 + \mu)^2}{1 - \mu}(u + v) \\ &= \left(\frac{1 + \mu}{1 - \mu}\right) \left((1 - \mu)(u - v) + (1 + \mu)(u + v) \right) \\ &= 2 \left(\frac{1 + \mu}{1 - \mu}\right) (u + \mu v), \end{aligned}$$

which is another square, since $u + \mu v$ is a square—and the rest is in \mathbb{C} so is a square; and we have finished.