Lecture VI — B. Conrad

Elliptic curves and group law.

1. Some integrals

The unit circle is a commutative group in two ~~commutative~~ equivalent ways

Multiplication in $\{z \in \mathbb{C} : |z| = 1\}$ = Addition of angles mod (2π)

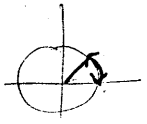
Algebraic version

$$(u,v)(u',v') = (uu' + vv', uv' + vu')$$

$$(u,v)^{-1} = (u, -v) \quad \text{(inflection in } u\text{-axis)}$$

(There's a group law defined in the locus $\{u^2+v^2=1\}$ using an algebraic expression in the coordinates)

Analytic version $\theta_0(u,v)$



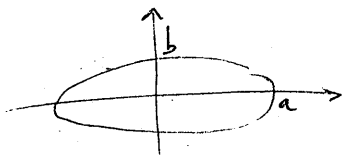
$v = \sqrt{1-u^2} \Rightarrow \theta_0(u,v) = -\int_1^u \frac{dx}{\sqrt{1-x^2}}$

(computes the arc) $(x = \cos\theta)$

$I(t) = -\int_1^t \frac{dx}{\sqrt{1-x^2}}$ $\rightsquigarrow$ invert this function we get cos and define sin $:= -\cos'$

then these are periodic mod $2\pi\mathbb{Z}$

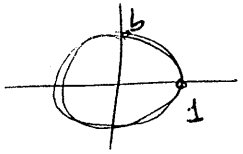
what happens with an ellipse ≠ circle.



$\frac{u^2}{a^2} + \frac{v^2}{b^2} = 1 \quad (0 < b < a)$

(Area is nab) and circumference?
(that is perimeter !!)

Scaling by $\frac{1}{a}$ we get



$b < 1$

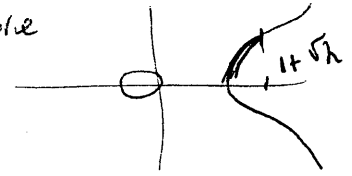
Let $k = \sqrt{1-b^2} > 0$

$$\lambda = \left(\frac{1+k}{1-k}\right)^2 > 1$$

Perimeter is an integral along the path:

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

(the wire



So these curve appear historically because
the study of the perimeter of ellipse.

Study of these integrals led to the discovery that these curves have a "group law", both algebraic and analytic descriptions.

Analytic group law best seen on $\mathbb{C}$-solutions to

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

(can be presented as a $\mathbb{C}/\Lambda$ with Λ a lattice,
this is a 2-dimensional picture of $\{u^2+v^2=1\} = \mathbb{R}/2\pi\mathbb{Z}$.

We will stay at the algebraic side

Algebraic viewpoint works over many fields: $\mathbb{C}, \mathbb{Q}, \mathbb{F}_p$.

2. Elliptic curves

F = field $\mathrm{char}(F) \neq 2, 3$

$\mathbb{Q}$, $\mathbb{F}_p$, $\mathbb{C}$ ...

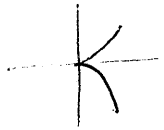
Suppose given a field $F' \supset F$ where F' is algebraically closed, that is, every positive degree polynomial in F' has a full set of roots in F'.

Ex: $F = \mathbb{Q}$ $F' = \mathbb{C}$

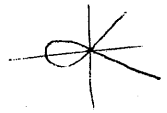
Def: An elliptic curve (over F) is the set of solutions

$$E = \{(x,y) \in (F')^2 \mid y^2 = f(x)\} \cup \{\infty\}$$

with $f(x)$ a cubic polynomial over F with distinct roots in F'.



$y^2 = x^3$



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

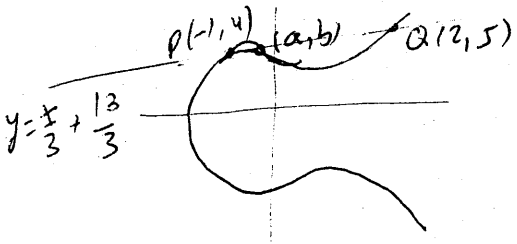
"Distinct roots" guarantees that every point on E

We're most interested in

$E(F) = \{$ points of E with coordinates in $F\} \cup \{\infty\}$

$E_1 = \{y^2 = x^3 + 17\}/\mathbb{Q}$

∞.



Intersects the line and the ubc (get the other solutions)

$$\left(\frac{x}{3} + \frac{13}{3}\right)^2 = x^3 + 17$$

$$0 = x^3 - \frac{x^2}{9} + \cdots$$

$$= (x+1)(x-2)(x-a)$$

$$-1 + 2 + a = \frac{1}{9} \Rightarrow a = \frac{-3}{9}$$

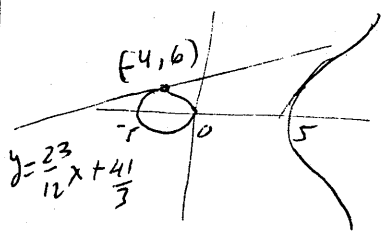
$$b = \frac{109}{27}$$

(and using the eq. line)

(In general the third point will not be integral)

$E_2 = \{y^2 = x^3 - 25x\}/\mathbb{Q}$

∞.



Taking the tangent line

$$2yy' = 3x^2 - 25$$

plugging in the function

$$(\ )^2 = x^3 - 25x$$

$$x^3 - \left(\frac{23}{12}\right)^2 x^2 + (\ ) = 0$$

$$= (x+41)^2(x-a)$$

(double root.)

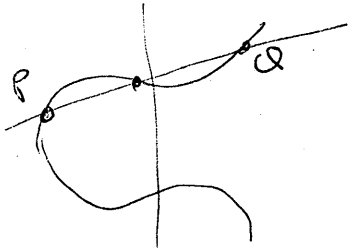
$$\Rightarrow 82 + a = \left(\frac{23}{12}\right)^2$$

$$\Rightarrow a = \frac{1681}{144} \quad b = \frac{41\,1519}{2^6 3^3}$$

10/11 From 2 point + line $\Rightarrow$ get another point

Note that we can define the tangent line in a purely algebraic way.

Miracle:



$E \cap \overline{PQ} = \{P, Q, R\}$

If $R = (a, b)$

define $P \oplus Q = (a, -b)$

This is in fact a commutative group law in $\mathcal{C}$ with inverse $(x,y) \mapsto (x,-y)$ and identity ∞. (preserving $E(F)$)

Hard point: associativity. (easy using analytic !!)

Ex $[2][P] = 0$ $(P \neq 0)$ that means that $P = -P$ $(a,b) \quad (a,-b)$

but it's implies $b = 0$

no point where $f(x) = 0$

Ex $[3][P] = 0 \iff [2][P] = -P$ $P \neq 0$

take the tanget line $T_P E$, see whee it meets E and flip that aroun x-axes.

$\iff T_P(E)$ melts E at P to 3 order

For example $y^2 = x^3 + 16 \quad P = (0, 4)$

$T_P(E) = \{y = 4\}$

plugin $y = 4$ in the eqution get $x^3 = 0$

In the example before

$E_1 \quad (2,5) \oplus (4,9) = (-2,3)$

$[2](-1,4) = \left(\frac{137}{64}, -\frac{2651}{512}\right)$

Question 1: Is $E_1(\mathbb{Q})$ finite or not?

If infinite, is the group has finite generated?

$E_1(\mathbb{Z})$ finite?

VI.5

Question 2: $E(\mathbb{F}_p)$ is finite group.

Does $\{E_2(\mathbb{F}_p)\}_{p \geq 5}$

"control" $E_2(\mathbb{Q})$.