Examples Class 1

Elliptic Curves

28/10/2019

Q1: Work with this equation:

$$Dw^2 = uv(u-v)(u+v).$$

D	u	v	w	$\frac{u^2-v^2}{w}$	$\frac{2uv}{w}$	$\frac{u^2+v^2}{w}$
6						
15						
21						
210						

Q2: $x^2 + xy + 3y^2 = 1$

Pick a point $(x, y) = (-1, 0)$. $y = t(x+1)$.

$$(x, y) = \left(\frac{1-3t^2}{1+t+3t^2}, \frac{2t+t^2}{1+t+3t^2}\right)$$

Vertical line?

$$(x, y) = (t^2-1, t^3-t).$$

Rational means: rational curve (genus 0 curve)

(Manins):

Q3:

(a) Given $F(u,v,w) = u^3 + v^3 - w^3$

Inflection points: $\det(\partial^2 F) = 0$

$$\begin{vmatrix} 6u & 0 & 0 \\ 0 & 6v & 0 \\ 0 & 0 & 6w \end{vmatrix} = 0 \quad \Rightarrow uvw = 0$$

This gives the points of inflection are:
$[0:1:1]$, $[1:0:1]$, $[1:-1:0]$

(these are rational pts.

But over alg. closed field: There are nine.
(including reals of cuspy).

$P = [0:1:1]$: $T_P C = \{(u,v,w) \mid v - w = 0\}$

$(0,1,1) \longrightarrow (0,1,0)$

$(0,1,-1) \longrightarrow (0,0,1)$ $\quad \hookrightarrow z = 0$

$x^3 = u$, $y^3 = v$, $z^3 = w - v$.

$F = (x')^3 + (y')^3 - (z' + y')^3$

$= (x')^3 - (z')^3 - 3(y')^2 z' - 3y'(z')^2$.

$F = 0$: $y'^2 z^3 + y^3 (z')^2 = -\frac{1}{3}(x')^3 + \frac{1}{3}(z')^3$.

$$\left.\begin{array}{l} z = z' \\ y = y'/3 \\ x = x'/3 \end{array}\right\} \Rightarrow \boxed{y^2 z - \frac{1}{3} y z^2 = x^3 + \frac{1}{3} z^3.}$$

Note: $T_P C = \left\{(u,v,w) \mid \frac{\partial F}{\partial u}\Big|_P \cdot u + \frac{\partial F}{\partial v}\Big|_P \cdot v + \frac{\partial F}{\partial w}\Big|_P \cdot w = 0\right\}$

(iii) Just do it.
(Verify that tedious direct proof Fermat Last Th for $n=4$).

[(i): Also can do: $Y^2Z + 9YZ^2 = X^3 + \frac{1}{17}Z^3$
or $y^2 = x^3 - \underbrace{432}_{2^4 \cdot 3^3}$]

(Richard)

Q4: $C_0 = \{y^2 = f(x)\}$
$C = \{y^2 z^{n-2} = z^n f(\frac{x}{z})\}$ $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$.

$Z = 0 \Rightarrow X = 0$ $P_\infty = [0:1:0]$. point at infinity.

C_0: $P = (x_0, y_0)$ is singular $\iff \frac{\partial}{\partial y}(y^2 - f(x)) = \frac{\partial}{\partial x}(y^2 - f(x))$
$= 0$
$\iff y = 0$ & $f'(x) = 0$ at P.
$\iff f(x_0) = f'(x_0) = 0$.
$\iff f$ has repeated root

(note this argument is valid for all n).

What about $P_\infty = [0:1:0]$?
P_∞ when $n = 3$. Dehomogenize at $Y \neq 0$.
$z - z^3 f(\frac{x}{z}) = 0$.

$\frac{\partial}{\partial z}$ $1 - 3z^2 f(\frac{x}{z}) + z f'(\frac{x}{z})$ at $(0,0)$.
This point is non-singular

At ∞: $\frac{\partial}{\partial z} = 0$ for $n \neq 4$.
Also check partials at x

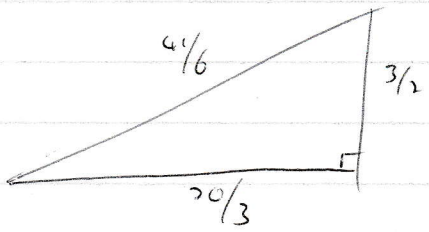
If we have alg. curve, it is birational to a smooth projective curve.

Q5: Multiples of $P = (0,0)$

$(0,0)$, $(1,0)$ $(-1,-1)$, $(2,-2)$, $(\frac{1}{4}, -\frac{5}{8})$, $(0,4)$, $(-\frac{5}{9}, \frac{8}{27})$, $(\frac{21}{25}, -\frac{69}{125})$

Denominators: Notice squares and cubes. Just plug into Weierstrass equation →

Q6: Note that



is one solution →

First need to homogenize:

$E: Dy^2 = x^3 - x$

Homogenize: $Dy^2z = x^3 - xz^2$.

$Y \longmapsto \frac{1}{D}Y$

$Z \longmapsto DZ$

$(X:Y:Z) \longmapsto (X:DY:\frac{1}{D}Z)$

$y^2z = x^3 - D^2xz$.

$E^1: y^2 = x^3 - D^2x$ Just double the point →

If $(x,y) \in E'$, then $\left(\frac{x}{D}, \frac{y}{D^2}\right) \in E$

Find a, v, w s.t. (a, v coprime.) (don't actually need coprime.)

$\frac{x}{D} = \frac{u}{v}$, $\frac{y}{D^2} = \frac{w}{v^2}$. Then the triple with sides

$a = u^2 - v^2$

$b = 2uv$

$c = u^2 + v^2$

has area Dw^2 $\longrightarrow$

"Almost" the case that torsion points have integer co-ordinates.

Q7: c) $dy^2 = x^3 + a_2x^2 + a_4x + a_6$.

Replace x & y by $\frac{x}{d}$ and $\frac{y}{d^2}$

$\therefore d\left(\frac{y}{d^2}\right)^2 = \left(\frac{x}{d}\right)^3 + a_2\left(\frac{x}{d}\right)^2 + a_4\left(\frac{x}{d}\right) + a_6$

$\Rightarrow y^2 = x^3 + da_2x^2 + d^2a_4x + d^3a_6$ →

(what quadratic twists look like)

Depends only on $d \in \mathbb{Q}^*/(\mathbb{Q}^*)^2$.

Now $j(E) \neq 0, 1728$, $ab \neq 0$

when $y^2 = x^3 + ax + b$.

If $E \cong E'$ over $\bar{\mathbb{Q}}$, then:

$a' = u^4a$

$b' = u^6b$ for some $u \in \bar{\mathbb{Q}}^*$.

$\therefore u^2 = \frac{ab'}{a'b} \in \mathbb{Q}$

d (say)

Note: $\mathbb{Q}^*/(\mathbb{Q}^*)^2$, a famous set of coset representatives is the square-free integers →

Q8:

Over $\mathbb{C}$: $y^2 = (x-e_1)(x-e_2)(x-e_3)$

$x \mapsto x + e_1$: $y^2 = x(x + e_1 - e_2)(x + e_1 - e_3)$

Rescaling: $y^2 = x(x-1)\left(x + \frac{e_1 - e_3}{e_2 - e_1}\right)$

$\therefore$ $y^2 = x(x-1)(x-\lambda)$ is justified!

Note: $E_\lambda \cong E_{1/\lambda}$, $E_\lambda \cong E_{1-\lambda}$.

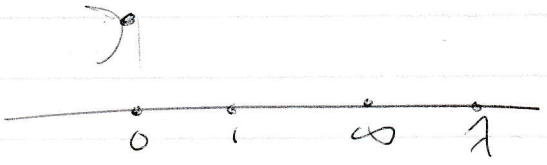
So we get $\lambda' \in \{\lambda, \frac{1}{\lambda}, 1-\lambda, \ldots$ any others$\}$.

Yes, Equality invariants: $\left[\lambda, \frac{1}{\lambda}, 1-\lambda, \frac{1}{1-\lambda}, \frac{\lambda-1}{\lambda}, \frac{\lambda}{\lambda-1}\right]$

Get 6 solutions.

Note $j(\lambda) = j(\lambda')$ yields 6^{th} order polynomial. $\circlearrowleft S_3$

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



For cross-ratio,

Q9: $P = (x, y)$ — the expected answer ☺

$$2P = \left(\frac{g(x)}{(2y)^2}, \frac{h(x)}{(2y)^3} \right) \quad \text{where} \quad \begin{aligned} g(x) &= x^4 - 2ax^2 + \dots \\ h(x) &= x^6 + 5ax^4 + \dots \end{aligned}$$

(ii). $3T = O_E \iff x(2T) = x(-T)$

Why ($\Leftarrow$)? Now, if two pts have same x-coord.
Then $2T = \pm T$ (!!)
But if $2T = T$, $T = O_E$, and we're implicitly assuming $T \neq O_E$.

9 ii) $3x^4 + 6ax^2 + 12bx - a^2 = 0$ ← $g(x)$
Get $2 \cdot 4 = 8$ 3-torsion point $(x, \pm y)$
Adding point at infinity, get 9 3-torsion points!

(iii). Now $g'(x) = 12(x^3 + ax + b)$.
So repeat rots $\Rightarrow$ 3 torsion and 2-torsion.

Q10:

$$C = \{aX^3 + bY^3 + cZ^3 = 0\} \subset \mathbb{P}^2$$

$$\phi : C \longrightarrow \mathbb{P}^3$$
$$(X:Y:Z) \longmapsto (X^3 : Y^3 : Z^3 : XYZ)$$
$$\qquad\qquad\quad u \quad v \quad w \quad t$$

Let $D = \{au + bv + cw = 0 \text{ and } uvw = t^3\} \subset \mathbb{P}^3$.

Steps: (i) Show $\phi(C) = D$.
(ii) D elliptic curve and put in Weierstrass form.
(iii) Compute $\deg(\phi)$.

(ii) Eliminate w gives:
$$uv(au + bv) = -ct^3$$
$$\uparrow -cw$$

Cannot just say this is Weierstrass eqn
Must put it in actual form:

$u \sim y$, $v \sim z$, $t \sim x$ gives:
$$ay^2z + byz^2 = -cx^3$$
$$\downarrow$$
$$y^2z - \frac{bc}{a^2} yz^2 = x^3$$

Put: $z = 1$: $y^2 - \frac{bc}{a^2} y = x^3$
$\qquad\qquad\qquad\quad \uparrow a_1$

To reflect symmetry: we can multiply by a^3:
$$y^2 - (abc)y = x^3$$
complete the square
OR: $y^2 = x^3 + \frac{1}{4}(abc)^2$
or $y^2 = x^3 + (4abc)^2$

That completes step 2.

We associate the curve with its $\bar{K}$ points (always over alg. closed field).

E.g. $C = \{3x^3 + 4y^3 + 5z^3 = 0\} \subset \mathbb{P}^2$

Selmer: $C(\mathbb{Q}) = \emptyset$ (no $\mathbb{Q}$ solutions).

Yet: $C(\mathbb{Q}_p) \neq \emptyset$ $\forall$ primes p.
(e.g. of failure of Hasse principle)

and $C(\mathbb{R}) \neq \emptyset$

Degree is geometric object (over alg. closed!!)

Degree: Degree is 3. (always over alg. clos.)

$\phi : C \longrightarrow D$, $P = (x:y:z) \in C$

$\phi^{-1}(\phi(P)) = \{(x:y:z), (x:\zeta_3^r y:\zeta_3^s z) : s = 2r, \quad r = 0,1,2\}$.

Thus, with finitely many exceptions, fibres have size 3.

Fibres easiest method

OR: Can do extension of function field.

$C \circlearrowleft \alpha$ $\qquad \alpha : (X_1 : Y_1 : Z) \longmapsto (X_1 : \zeta_3 Y_1 : \zeta_3^2 Z)$

$\downarrow \phi$ $\qquad$ order 3 automorphism.

E

Get: $K(C) \circlearrowleft \alpha^*$

$\Big|$

$K(E)$

As we saw for order 3 automorph of $K(C)$, this implies degree is at least 3.

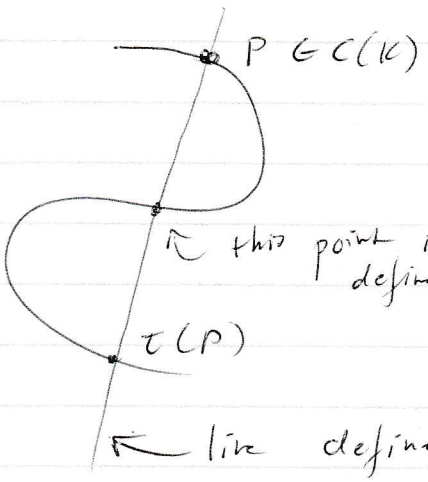
$\therefore \; [K(C) : K(E)] \geq 3.$

To prove $= 3$, go to affine, find an element generating $K(C)$ with min poly of deg ≤ 3.

To get rational functions, need to go to affine space, can't just use X from projective space.

Q12: $[K:\mathbb{Q}] = 2$.

$\mathrm{Gal}(K/\mathbb{Q}) = \{1, \epsilon\}$



Can do similar thing for chord-tangent process.

this gives us over $\mathbb{Q}$ point.