

18.781

28 Apr 2003

$$\mathbb{P}^2(\mathbb{Q}) \subset \mathbb{P}^2(\mathbb{R}) \subset \mathbb{P}^2(\mathbb{C})$$

$$C: F(x, y) = \sum a_{ij} x^i y^j \quad a_{ij} \in \mathbb{Q} \quad \text{degree } d$$

$$\text{Homogeneous eq: } F(x, y, z) = \sum a_{ij} x^i y^j z^{d-i-j}$$

$$C(\mathbb{Q}) \subset \mathbb{P}^2(\mathbb{Q})$$

Thm: If $d \geq 4$ and C is smooth, then $C(\mathbb{Q})$ is finite.

Proof omitted.

C is smooth (calc. def.)

$P = (a, b)$ satisfies $f(x, y) = 0$.

P is smooth if $\frac{\partial f}{\partial x}(P)$ and $\frac{\partial f}{\partial y}(P)$ are not both zero.

Def: $P \in C(\mathbb{Q})$ is a smooth point iff at least one of $\frac{\partial F}{\partial x}, \frac{\partial F}{\partial y}, \frac{\partial F}{\partial z}$ is non-zero at P .

Lemma: $P = [a:b:1] \in C(\mathbb{Q})$. Then P is smooth iff at least one of $\frac{\partial F}{\partial x}, \frac{\partial F}{\partial y}$ is nonzero at (a, b) .

Sublemma: For any poly all of whose monomial terms have same degree d

$$x \frac{\partial F}{\partial x} + y \frac{\partial F}{\partial y} + z \frac{\partial F}{\partial z} = d \cdot (F)$$

Pr: Since diff. & mult. by d are linear operations,

enough to check $x^i y^j z^{d-i-j}$

$$x \frac{\partial F}{\partial x} + y \frac{\partial F}{\partial y} + z \frac{\partial F}{\partial z} = i x^i y^j z^{d-i-j} + j x^i y^j z^{d-i-j} + (d-i-j) x^i y^j z^{d-i-j}$$

$$(i+j+d-i-j) x^i y^j z^{d-i-j} = d x^i y^j z^{d-i-j} = d(F)$$

Proof of Lemma: Smooth at $P \Leftrightarrow$ one of $\frac{\partial F}{\partial x}(P), \frac{\partial F}{\partial y}(P), \frac{\partial F}{\partial z}(P)$ nonzero.

$$\frac{\partial F}{\partial x}(a, b) = \frac{\partial F}{\partial x}(P) \quad \frac{\partial F}{\partial y}(a, b) = \frac{\partial F}{\partial y}(P), \text{ so "} \leftarrow \text{" obvious.}$$

$$\text{From sublemma: } a \frac{\partial F}{\partial x}(a, b) + b \frac{\partial F}{\partial y}(a, b) + \frac{\partial F}{\partial z}(P) = 0 \quad (\text{since } [a:b:1] \in C(\mathbb{Q}))$$

$$\text{Thus, we cannot have } \frac{\partial F}{\partial z}(P) \neq 0 \text{ and } \frac{\partial F}{\partial x} = \frac{\partial F}{\partial y} = 0.$$

Def: C is smooth iff every pt $P \in C(\mathbb{Q})$ is smooth.

Ex: Find singular pts (not smooth pts) $C: xy^2 - 1 = 0$.

Look at points $[a:b:1]$

$$\frac{\partial F}{\partial x} = y^2, \quad \frac{\partial F}{\partial y} = 2xy, \quad \text{so if both are zero at } [a:b:1],$$

$$b=0 \text{ but then } ab^2 - 1 \neq 0.$$

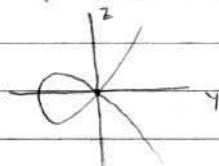
$$F(x, y, z) = xy^2 - z^3$$

$$\frac{\partial F}{\partial x} = y^2 \quad \frac{\partial F}{\partial y} = 2xy \quad \frac{\partial F}{\partial z} = -3z^2$$

so singular pt when $y = z = 0$. $[1:0:0]$ ($F([1:0:0]) = 0$)

Look at $\mathbb{R}^2 \subset \mathbb{P}^2(\mathbb{R})$

$$\{[1:a:b]\}$$



deg 1, 2 understandable
 deg 3 elliptic curves
 deg ≥ 4 finitely many rational pts

Equations in 1-variable:

Galois Theory

$$f(x) = \sum a_i x^i$$

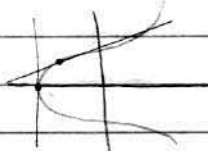
defines a finite set in $\mathbb{P}^1(\mathbb{Q})$

Elliptic curves: cubic poly. in two variables

$$E: y^2 = x^3 + Ax + B \quad A, B \in \mathbb{Q}$$

(can always complete square + make line change of var. to get this form)

Ex: $E: x^3 + y^3 - 9 = 0$ has infinitely many rat'l pts.



The tangent line at any pt hits the curve at one other pts.

$$y = ax + b$$

If the pt of tangency is rat'l, then so must be the third root.

$$[x_n : y_n : z_n] \quad x_0 = 2 \quad y_0 = 1 \quad z_0 = 1$$

$$x_{n+1} = x_n(x_n^2 + 2y_n^2)$$

$$y_{n+1} = -y_n(2x_n^2 - y_n^2)$$

$$z_{n+1} = z_n(x_n^2 - y_n^2)$$

y_n, z_n always odd.

power of 2 in x_n is 2^{n+1} . Thus pts. are distinct.