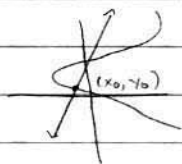


18.781

30 Apr 2003

$C: ax^2 + by^2 = 0 \quad a, b \in \mathbb{Q}$

$(x_0, y_0) \in C(\mathbb{Q})$



line through pt hits curve in one other pt.

{slopes m_3 } \leftrightarrow {pts. on C } (bij.)

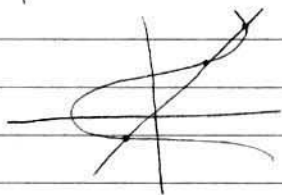
Homework to show rat'l pts. correspond to rat'l slopes

$\mathbb{Q} \cup \{\infty\} \leftrightarrow C(\mathbb{Q})$

Cubic curves:

$E: y^2 = x^3 - Ax - B$ smooth if $\Delta = 16(4A^3 - 27B^2) \neq 0$ (Δ is discriminant)

(from homework)



$P_1, P_2 \in E(\mathbb{Q})$

want to define commutative op. " $P_1 + P_2$ " $\in E(\mathbb{Q})$

Lemma: $P_1 = [a:b:c]$ $P_2 = [a':b':c']$ distinct.

Then there exists unique nonzero expression

$L: \alpha x + \beta y + \gamma z = 0$

so that $P_1, P_2 \in L(\mathbb{Q})$. (A line)

Pr: Without loss of generality, assume $c=1$ (since symmetric in a, b, c)

$L: (b-bc')(x-az) - (a'-ac')(y-bz) = 0$

If both $b-bc'$ and $a'-ac'$ are 0, we have

$b'=bc'$, $a'=ac'$ and $c'=c'$, so $[a':b':c'] = c'[a:b:c] = [a:b:c]$

By changing variable, we can always get $P_1 = [a:b:1]$, $P_2 = [a',b',1]$ in which case the line is just the reg. line b/w two pts, and so thus is unique.

Lemma: $P_1, P_2 \in E(\mathbb{Q})$. Then the line through P_1, P_2 intersects $E(\mathbb{Q})$

in exactly one other point, P_3 . Moreover, if $P_1, P_2 \in E(\mathbb{Q})$, then $P_3 \in E(\mathbb{Q})$

(Assume $A, B \in \mathbb{Q}$)

Proof: $P_i = [a_i:b_i:1] \quad i=1,2$

$L: (b_2-b_1)(x-a_1) - (a_2-a_1)(y-b_1) = 0 \Rightarrow$

$y = \frac{b_2-b_1}{a_2-a_1}(x-a_1) + b_1$ (if $a_2 \neq a_1$)

$E: \left(\frac{b_2-b_1}{a_2-a_1}(x-a_1) + b_1\right)^2 - x^3 + Ax + B = 0$

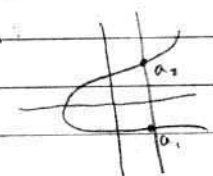
$\Rightarrow c(x-a_1)(x-a_2)(x-a_3)$, and $c = -1$

so we have $-(x-a_1)(x-a_2)(x-a_3)$

and a_3 is the x-coord. of P_3 , so the third pt is

$(a_3, \frac{b_2-b_1}{a_2-a_1}(a_3-a_1) + b_1)$ (Note this may be the same as P_1, P_2)

$a_2 = a_1$ (since P_1, P_2 distinct)
 $L: x = a_1$ $[0:1:0]$ works.



For pts $[a:b:1]$.

$$L: x = a, \quad E: y^2 = x^2 - Ax - B \Rightarrow F: y^2 = a^2 - Aa - B$$

which is quadratic, so it only has 2 sol'ns

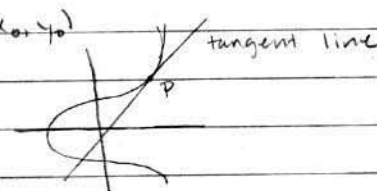
since we already have two sol'n, there are no more sol'n of the form $[a:b:1]$.

If $[a:b:0]$, the only sol'n to L is $[0:1:0]$.

To get general case, make linear change of variable.

What if $P_1 = P_2 = P$? Want L through P that hits $E(\mathbb{C})$ in 1 other pt
 $L: y = mx + b, \quad (mx + b)^2 = x^2 - Ax - B \leftarrow$ want x_0 to be a double root

$P = (x_0, y_0)$
 concretely:



Tangent line at $P \in E(\mathbb{C})$.

$$F = y^2 z - x^3 + Axz^2 + Bz^3$$

Tangent line at $P = [a:b:1]$

$$\frac{\partial F}{\partial x}(P)(x - az) - \frac{\partial F}{\partial y}(P)(y - bz) = 0$$

When we solve for y then plug into F , factor in F and P is a double root.

Define " $P_1 + P_2$ ": First draw line L through P_1 and P_2 and let P_3 be the third pt. of intersection of L with $E(\mathbb{C})$.

Define $P_1 + P_2$ to be third pt of intersection of the line through P_3 and $[0:1:0]$.

Thm: Let $O = [0:1:0]$.

1) $P_1 + P_2 = P_2 + P_1$

2) $O + P = P$

3) $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$

4) for all P there exists point " $-P$ " s.t. $P + -P = O$.