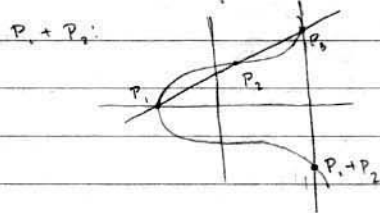


$E: y^2 = x^3 - ax - b \quad 4a^3 + 27b^2 \neq 0$

We define an operation "+" on $E(\mathbb{C})$



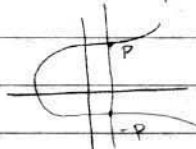
- Let P_3 be the third point of intersection of E + line through $P_1 + P_2$
- Define $P_1 + P_2$ of line through P_3 and O , where $O = [0:1:0]$

Thrm:

- (1) Commutativity: $P_1 + P_2 = P_2 + P_1$
- (2) Identity: $O + P = P$ any P
- (3) Associativity: $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$
- (4) Inverse: For any P , $\exists -P$ s.t. $P + (-P) = O$.

Proof:

- (1) The line through $P_1 + P_2$ is same as line through $P_2 + P_1$, so we construct the same P_3 .
- (2) If $P_1 = O$, then $P_3 =$ third pt of intersection of line through O, P . Then 3rd pt. of intersection of line between $P_3 + O$ must be P

(4)  If P is a point on $E(\mathbb{C})$, then the tangent line at P is $\frac{\partial F}{\partial x}(P)x + \frac{\partial F}{\partial y}(P)y + \frac{\partial F}{\partial z}(P)z = 0$ where $F(x,y,z) = y^2z - x^3 + axz^2 + bz^3$.

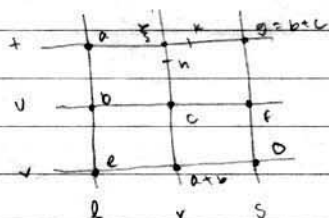
Tangent line at $[0:1:0]$:

$$\begin{aligned} \frac{\partial F}{\partial x}(P) &= 3x^2 + az^2 = 0 \\ \frac{\partial F}{\partial y}(P) &= 2yz = 0 \\ \frac{\partial F}{\partial z}(P) &= y^2 + 2axz + 3bz^2 \end{aligned}$$

so tangent line at $[0:1:0]$: $z=0$ (i.e. $[a:b:0]$)

and we know that $[a:b:0]$ intersects $E(\mathbb{C})$ at only $[0:1:0]$, so in fact $[0:1:0]$ must be a "triple root"

(3) $(a+b)+c = a+(b+c)$.



- n is 3rd pt of intersection of r with E
- $(a+b)+c$ is 3rd pt of intersection of line through $n + O$.
- k is 3rd pt of intersection of t with E .
- $a+(b+c)$ is 3rd pt of intersection of line through $k + O$.

We know: E contains $a, b, e, a+b, O, f, g, c$.

Claim: $h=k=f$.

Look at all cubic polys in x and y with contain these 8 points.

$x^3, y^3, x^2y, y^2x, x^2, xy, y^2, x, y, 1$ span "cubic poly. space"
cubic poly F given by vector $(a_0, a_1, \dots, a_9) \in \mathbb{C}^9$

We're looking at

{set of F 's which vanish on 8 pts} = {cubic polys}

This set is a subspace, since if f, f' vanish at a pt, so does $f+f'$, and so does cf , $c \in \mathbb{C}$.

claim: This subspace has dimension 2

Given a point p , the condition that $F(p)=0$ is a linear condition on coefficients.

($\mathbb{C}^9 \xrightarrow{\text{eval. at } p} \mathbb{C}$, so then the ker has dim 8.)

Then we can solve for one variable in terms of the others, and reduce dimension.

8 such points reduces dimension to 2.

We have two given such cubic polynomials:

$$F_1 = L(u)L(s)L(r)$$

$$F_2 = L(t)L(v)L(w)$$

and these are linearly independent, so we have basis for our set.

(presuming the points are sufficiently distinct).

In particular, $F = y^2 - x^3 - ax - b$ is lin. comb.

$$F = \lambda F_1 + \mu F_2 \quad (\text{and since } F \text{ smooth, } \lambda, \mu \neq 0)$$

$$F(h) = \lambda F_1(h) + \mu F_2(h) = 0$$

$$F_1(h) = 0 \text{ since } h \in r. \Rightarrow \mu F_2(h) = 0 \Rightarrow F_2(h) = 0, \text{ so}$$

$$h = t, v \text{ or } w, \text{ which implies } \xi = h$$

$$\text{By symmetry, } k = \xi, \text{ so } h = k$$

τ on $E(\mathbb{Q})$

(note also operation on $E(\mathbb{Q})$ since line through 2 rat'l pts. intersects E in rat'l pt if coeff of E rat'l).

Want to compute $E(\mathbb{Q}); \approx \mathbb{Z}, \mathbb{Z}/m$