PREVIOUSLY...

(HW #3 NOW AVAILABLE!!)

- ELLIPTIC CURVES OVER ARBITRARY (PERFECT) FIELDS
- ELLIPTIC CURVES OVER FINITE FIELDS
- ELLIPTIC CURVES OVER $\mathbb{C}$

~~TODAY~~: ELLIPTIC CURVES OVER ~~LOCAL~~ FIELDS

Recall:

$$\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z} = \left\{ (a_1, a_2, \ldots, a_n, \ldots) : \begin{array}{l} a_n \in \mathbb{Z}/p^n\mathbb{Z} \\ a_{n+1} \equiv a_n \bmod p^n \end{array} \right\}$$

$$\mathbb{Q}_p = \begin{array}{l}\text{field of}\\ \text{fractions}\\ \text{of } \mathbb{Z}_p\end{array} = \mathbb{Z}_p\left[\tfrac{1}{p}\right]$$

) an example of a local field.

(also: $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_q((T))$, extensions of $\mathbb{Q}_p$)

complete field wrt p-adic norm

$$|a|_p := |p^n \cdot m|_p = \frac{1}{p^n} = \frac{1}{p^{v_p(a)}}$$

w/ $\gcd(p,m)=1$

Actually... Today: Formal Groups

- Expansion around $\mathcal{O}$:

Let $E: \left(y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\right)$ (*)

$\{[x,y,1]\} = \{z=1\}$ ← $y=1$

at $\mathcal{O} = [0,1,0]$

$\{y=1\}$ ←

and change vars: $z = -\frac{x}{y}$, $w = -\frac{1}{y}$

so now $\mathcal{O}$ is now $(z,w) = (0,0)$ and z is a uniformizer at $\mathcal{O}$.

(Recall: $\mathrm{ord}_{\mathcal{O}}(x) = -2$, $\mathrm{ord}_{\mathcal{O}}(y) = -3$ $\Rightarrow \mathrm{ord}_{\mathcal{O}}(z) = -2 - (-3) = 1$

$\Rightarrow \mathrm{ord}_{\mathcal{O}}\left(\frac{1}{y}\right) = 3$)

(*) becomes:

$$w = z^3 + a_1zw + a_2z^2w + a_3w^2 + a_4zw^2 + a_6w^3 = f(z,w)$$

Trick: Substitute recursively so we get to $w = w(z)$

- $w = f(z,w) \Rightarrow f_1(z,w) = f(z,w)$

$f_2(z,w) = f_1(z, f(z,w))$

$f_3(z,w) = f_2(z, f(z,w))$

In the limit ... $w = z^3(1 + A_1 z + A_2 z^2 + \dots)$

$w = w(z)$, $A_1 = a_1$, $A_2 = a_1^2 + a_2$, $A_3 = a_1^3 + 2a_1a_2 + a_3$ ...

$$w(z) \in \left(\mathbb{Z}[a_1, \dots, a_4, a_6]\right)[[z]]$$

- Need to show convergence! Also $w(z) = f(z, w(z))$

Our candidate: $w(z) = \lim_{m \to \infty} f_m(z, 0) \overset{?}{\in} \mathbb{Z}[a_1, \dots, a_6][[z]]$.

Prop (a) $w(z)$ is a power series in $\mathbb{Z}[a_1, \dots, a_6][[z]]$.

(b) $w(z)$ is unique w/ $w(z) = f(z, w(z))$.

(c) If $\mathbb{Z}[a_1, \dots, a_6]$ is made into a graded ring with weights $\mathrm{wt}(a_i) = i$, then A_n is a homogeneous polynomial of deg n.

ex $A_1 = a_1$, $A_2 = a_1^2 + a_2$, $A_3 = a_1^3 + 2a_1a_2 + a_3$

$3 \cdot 1 = 3$, $1 + 2 = 3$, 3

Lemma (Hensel's Lemma)

R a complete ring wrt. $I \subseteq R$ ideal, $F(w) \in R[w]$ a polynomial.

Suppose there is $a \in R$: $F(a) \in I^n$, $F'(a) \in R^*$, for some $n \geq 1$.

Then, for any $\alpha \in R$, with $\alpha \equiv F'(a) \bmod I$, the sequence

$$w_0 = a, \quad w_{m+1} = w_m - F(w_m)/\alpha$$

converges to $b \in R$ w/ $F(b) = 0$, st. $b \equiv a \bmod I^n$.

(If R is an int. domain, then b is unique.)

Proof of Prop: Let $R = \mathbb{Z}[a_1, \ldots, a_b][[z]]$, $I = (z)$.

$F(w) = f(z, w) - w$, $a = 0$, $\alpha = -1$.

(NOTE: $F'(0) = a_1 z + a_2 z^2 - 1 \equiv -1 \bmod z$)

Hensel $\Longrightarrow \exists!\ b = b(z)$ st. $F(b) = 0 \Rightarrow b = f(z, b)$. ▨

QUESTION

$W = f(z,w)$ (cubic in z,w) over, say, $\mathbb{Q}_p$

Given $z \in p\mathbb{Z}_p$, there are 3 options for w.

Which of the 3 roots is $W(z)$?

ex $E: y^2 = x^3 + 1 \longrightarrow W = z^3 + w^3 \quad / \mathbb{Q}_5$

$$w^3 - w + z^3 = 0$$

Take $z = 5 \in 5\mathbb{Z}_5$, then $w^3 - w + 5^3 = 0$

has solutions $W(z) \equiv 0 \bmod 5^3$

$w \equiv 1$

$w \equiv -1$

$W(z)$ was built as the Hensel's thm solution to $F(w) = f(z,w) - w$ w/ $a = 0$

$\Rightarrow W(z) \equiv 0 \bmod z$

In fact, there is only one root of $w^3 - w + 5^3 = 0$ which is $\equiv 0 \bmod z$

ex

In this case: $w_1 \equiv 91554687625$

$= (0, 0, 0, 125, 125, \dots)$

$w_2 \equiv 6182707757751$

$= (1, 1, 1, 251, 1501, \dots)$

$w_3 \equiv -627426244375$

$= (4, 24, 124, 249, 1499, \dots$

$E : y^2 + a_1 xy + a_3 y = \cdots$

$\hookrightarrow w = z^3 + \cdots = f(z, w)$

(z, w)

$z \longmapsto w(z)$ s.t. $w(z) = f(z, w(z))$

$z \longmapsto (z, w) = (z, w(z))$ formal point on E.

$$W(z) = z^3\left(1 + A_1 z + A_2 z^2 + \cdots\right) \qquad \left(z = -\frac{x}{y},\ w = -\frac{1}{y}\right)$$

$$X(z) = \frac{z}{w} = \frac{z}{W(z)} = \frac{1}{z^2} - \frac{a_1}{z} - a_2 - a_3 z - (a_4 + a_1 a_3) z^2 + \cdots$$

$$y(z) = -\frac{1}{w} = -\frac{1}{W(z)} = -\frac{1}{z^3} + \frac{a_1}{z^2} + \frac{a_2}{z} + a_3 + (a_4 + a_1 a_3) z + \cdots$$

$$\omega(z) = \left(1 + a_1 z + (a_1^2 + a_2) z^2 + \cdots\right) dz$$

$\omega(z)$ inv. diff.

} in $\mathbb{Z}[a_1, \ldots, a_6][[z]]$

The pair $(x(z), y(z))$ provides a "formal" solution to $y^2 + a_1 xy + a_3 y = x^3 + \cdots$ in the (quot. field of $\mathbb{Z}[a_1, \ldots, a_6][[z]]$) $= K$ $\rightarrow$ $P \in E(K)$.

Q. E/K, $z \in K$ s.t. $x(z)$, $y(z)$ converge??

$K = \mathbb{Q}_p$
$R = \mathbb{Z}_p$
$\mathcal{M} = p\mathbb{Z}_p$

If K is a complete local field, $R, \mathcal{M}$, $a_i \in R$, $z \in \mathcal{M}$
then $(x(z), y(z)) \in E(K)$. (Gouvêa "p-adic Numbers")

We obtain: (K, R, m)

$$m \hookrightarrow E(K)$$

$$z \longmapsto (z, w) = (z, w(z))$$

$$\longmapsto (x(z), y(z))$$

- image

  (x, y) s.t. $xy^{-1} \in m$

  $x = \frac{z}{w}$, $y = -\frac{1}{w}$

  so $\frac{x}{y} = -z \in m$

- Addition on (z, w) plane.

  $P = (z_1, w_1)$, $Q = (z_2, w_2)$

  Find line $L = \overline{PQ}$, $w = \lambda z - v$

- injective

  $x = \frac{z}{w} = \frac{z'}{w'} = x'$ $\Rightarrow z = z'$

  $y = -\frac{1}{w} = -\frac{1}{w'} = y'$ $\Rightarrow w = w'$

Find $E \cap L$:

$$\begin{cases} z_1 \\ z_2 \\ z_3 = z_3(z_1, z_2) = -z_1 - z_2 + \dfrac{a_1\lambda + a_3\lambda^2 - a_2 v - 2a_4\lambda v - 3a_6\lambda^2 v}{1 + a_2\lambda + a_4\lambda^2 + a_6\lambda^3} \end{cases}$$

$$\in \mathbb{Z}[a_1, \dots, a_6][z_1, z_2]$$

- inverse $(x, y) \mapsto (x, -y - a_1 x - a_3)$

$$i(z) = \frac{x(z)}{y(z) + a_1 x(z) + a_3}$$

$$\Rightarrow \boxed{F(z_1, z_2) = i(z_3(z_1, z_2)) \in \mathbb{Z}[a_1, \dots, a_6][z_1, z_2]}$$

We have built: $F(z_1, z_2) \in \mathbb{Z}[a_1, \ldots, a_6][\![z_1, z_2]\!]$

(a) $F(z_1, z_2) = F(z_2, z_1)$ (add. is comm.)

(b) $F(z_1, F(z_2, z_3)) = F(F(z_1, z_2), z_3)$ (add. is associative)

NOTE. Define $z_1 +_F z_2 := F(z_1, z_2)$

↳ (a) $z_1 +_F z_2 = z_2 +_F z_1$

(b) $z_1 +_F (z_2 +_F z_3) = (z_1 +_F z_2) +_F z_3$

(c) $F(z, i(z)) = 0$ $(z +_F i(z) = 0)$

"A group law without any group elements"

↳ Formal group.

Formal Groups

Let R be a ring.

Def A (one-parameter, commutative) formal group $\mathcal{F}$ defined over R is a power series $F(X,Y) \in R[[X,Y]]$ satisfying:

(a) $F(X,Y) = X + Y + (\text{terms of deg} \geq 2)$

(b) $F(X, F(Y,Z)) = F(F(X,Y), Z)$ (assoc.)

(c) $F(X,Y) = F(Y,X)$ (comm.)

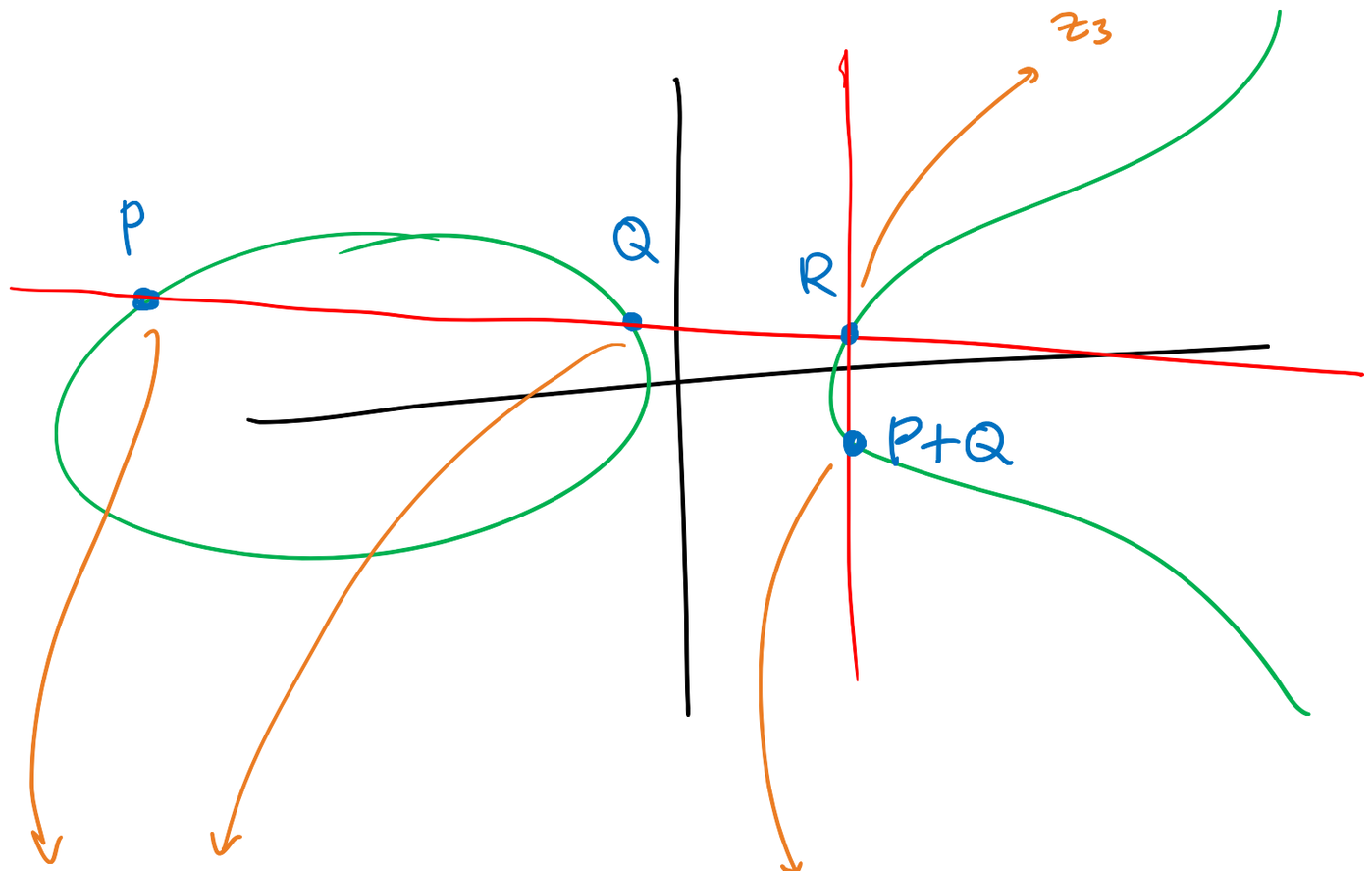
(d) $\exists!\, i(T) \in R[[T]]$ s.t. $F(T, i(T)) = 0$

(e) $F(X,0) = X$, $F(0,Y) = Y$.

We call F the formal gp law of $\mathcal{F}$. $(\mathcal{F}, F)$

Rmk (a) + (b) $\Rightarrow$ (d) + (e)

$\mathcal{M} \hookrightarrow E(K)$



$z_1 + z_2 \quad = \quad i(z_3) = z_1 +_E z_2$

$= F(z_1, z_2)$