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 ... $W = z^3(1 + A_1 z + A_2 z^2 + \cdots)$

$W(z)$ $\quad a_1$ $\quad (a_1^2 + a_2)$ $\quad A_3 = a_1^3 + 2a_1 a_2 + a_3$ ...

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

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

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

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

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

(c) If $\mathbb{Z}[a_1, \ldots, a_6]$ is made into a graded ring with