Elliptic Curves over p-adic Fields

Robert L. Benedetto
Amherst College

University of Connecticut

Saturday, May 17, 2014

Quick review of p-adic numbers

The p-adic absolute value $|\cdot|_p$ on $\mathbb{Q}$ has $|0|_p = 0$ and

$$\left|\frac{r}{s}p^n\right|_p = p^{-n} \quad \text{for } r, s \in \mathbb{Z} \text{ not divisible by } p.$$

$|\cdot|_p$ is non-archimedean:

- $|x|_p \geq 0$, with equality **iff** $x = 0$,
- $|xy|_p = |x|_p \cdot |y|_p$,
- $|x + y|_p \leq \max\{|x|_p, |y|_p\}$.

$\mathbb{Q}_p$ is the *completion* of $\mathbb{Q}$ w.r.t. $|\cdot|_p$.
(All $|\cdot|_p$-Cauchy sequences converge in $\mathbb{Q}_p$).

Fun Fact: Let $\{a_n\}_{n\geq 0}$ be a sequence in $\mathbb{Q}_p$. Then

$$\sum_{n\geq 0} a_n \text{ converges} \qquad \text{if and only if} \qquad \lim_{n\to\infty} a_n = 0.$$

The Residue Field and Value Group

The ring of integers and (unique) maximal ideal of $\mathbb{Q}_p$ are

$$\mathcal{O}_p = \mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$$

and

$$\mathcal{M}_p = p\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p < 1\}.$$

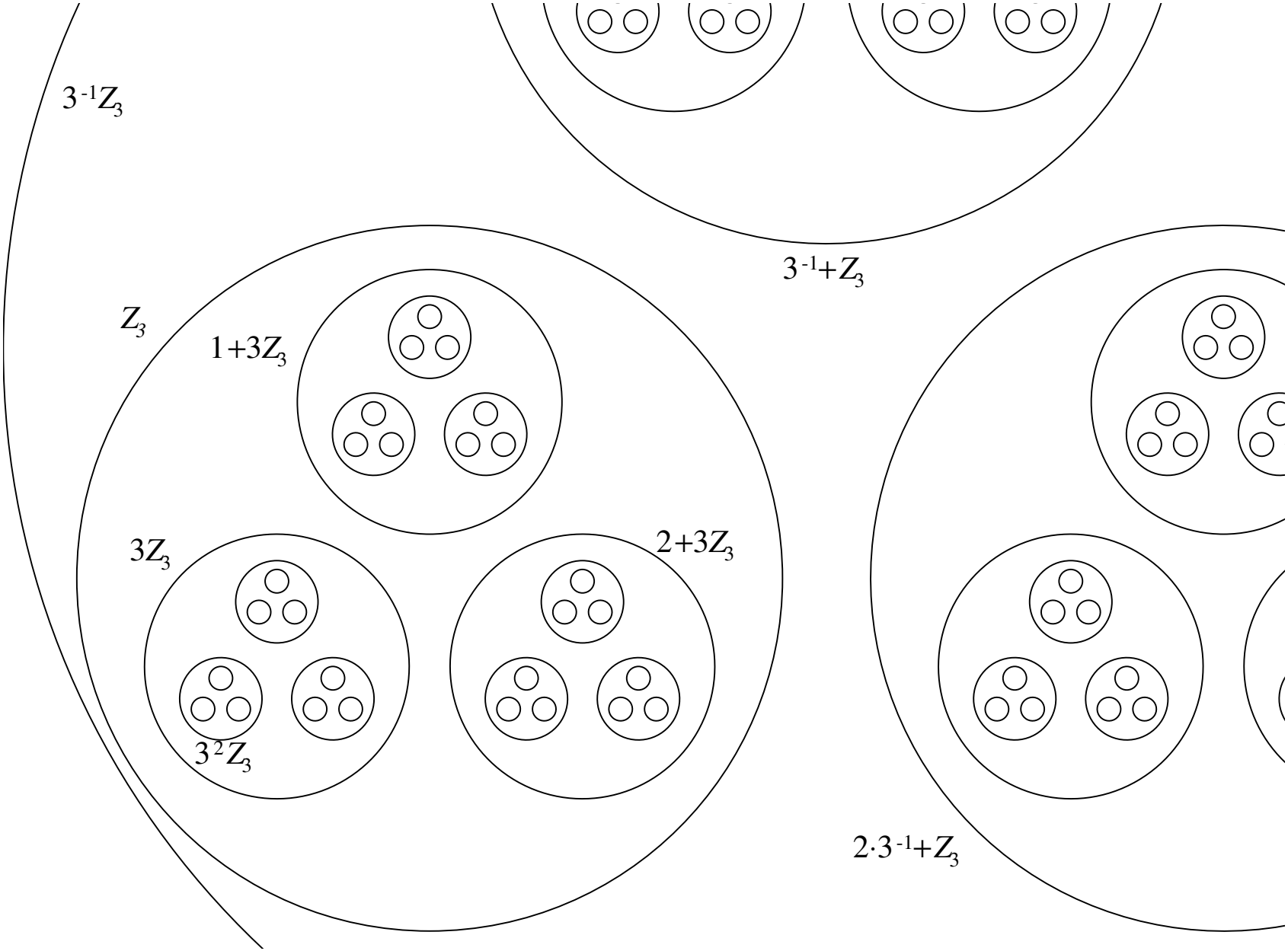
The *residue field* of $\mathbb{Q}_p$ is

$$\mathcal{O}_p/\mathcal{M}_p = \mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p.$$

The *value group* of K is

$$|\mathbb{Q}_p^\times|_p = p^{\mathbb{Z}} \subseteq (0, \infty).$$

A Sketch of $\mathbb{Q}_3$



Extension Fields

Let K be a finite (or more generally, algebraic) extension of $\mathbb{Q}_p$. Then $|\cdot|_p$ extends uniquely to K.

The new value group $|K^\times|$ contains $|\mathbb{Q}_p^\times|$ as a subgroup. The *ramification degree* is $e = [|K^\times| : |\mathbb{Q}_p^\times|]$.

If $e < \infty$, a *uniformizer* $\pi \in \mathcal{M}_K = \{x \in K : |x|_p < 1\}$ is an element of maximum absolute value less than 1.

$$\mathcal{M}_K = \pi\mathcal{O}_K, \quad \text{where } \mathcal{O}_K = \{x \in K : |x|_p \leq 1\}.$$

The new residue field k is a finite (respectively, algebraic) extension of $\mathbb{F}_p$. The *residue field extension degree* is $f = [k : \mathbb{F}_p]$.

Fact: $[K : \mathbb{Q}_p] = ef$.

Examples

$K = \mathbb{Q}_p(\sqrt[n]{p})$ has $e(K/\mathbb{Q}_p) = n$, $f(K/\mathbb{Q}_p) = 1$.

$K = \mathbb{Q}_p(\zeta_{p^n-1})$ has $e(K/\mathbb{Q}_p) = 1$, $f(K/\mathbb{Q}_p) = n$.

$K = \mathbb{Q}_p^{\mathrm{ur}}$, the *unramified closure* of $\mathbb{Q}_p$, has $e = 1$ and $f = \infty$.
In fact, $k \cong \overline{\mathbb{F}}_p$.

$K = \overline{\mathbb{Q}}_p$, the algebraic closure of $\mathbb{Q}_p$, has $e = \infty$ and $f = \infty$.
In fact, $|\overline{\mathbb{Q}}_p^{\times}|_p = p^{\mathbb{Q}}$ and $k \cong \overline{\mathbb{F}}_p$.

$K = \mathbb{C}_p$, the completion of $\overline{\mathbb{Q}}_p$, has $e = \infty$ and $f = \infty$.
In fact, $|\overline{\mathbb{Q}}_p^{\times}|_p = p^{\mathbb{Q}}$ and $k \cong \overline{\mathbb{F}}_p$.

Elliptic Curves over p-adic fields

Let $K/\mathbb{Q}_p$ be a p-adic field with $e(K/\mathbb{Q}_p)$ finite, so K has a uniformizer π.

For this talk, an elliptic curve over K is given by a Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

After a change of coordinates, we may assume this is an *integral model*, i.e., $|a_i|_p \leq 1$.

Mod out by $\pi\mathcal{O}_K = \mathcal{M}_K$, (giving coefficients $\overline{a}_i \in k$),
$\overline{E}$ may or may not still be an elliptic curve. (May be singular.)

If it's still an elliptic curve: good reduction.

Otherwise: bad reduction

Examples: Good Reduction

$p \neq 2$, and $E : y^2 = x^3 + Ax + B$, where
$|\Delta|_p = |-16(4A^3 + 27B^2)|_p = 1$.

Then $\overline{E} : y^2 = x^3 + \overline{A}x + \overline{B}$ has $\overline{\Delta} \neq 0$ and hence is nonsingular.
So good reduction.

---

p anything, and $E : y^2 + a_1xy = x^3 + a_6$,

has $\Delta = -a_6(a_1^6 + 2^4 3^3 a_6)$.

Again, $|\Delta|_p = 1$ implies good reduction.

An Example of Multiplicative Reduction

p anything and $E : y^2 + xy = x^3 + \pi^n$

has $\Delta = -\pi^n(1 + 2^4 3^3 \pi^n)$, so $|\Delta|_p = |\pi|_p^n < 1$.

$\overline{E} : y^2 + xy = x^3$ is singular at $(0, 0)$.

Note: Node, not cusp, because near $(0, 0)$ it looks like $y^2 + xy = 0$, i.e. $y(x + y) = 0$: two crossing lines.

Multiplicative Reduction Example: Part 2

$E : y^2 + xy = x^3 + \pi^n$ reduces to $\overline{E} : y^2 + xy = x^3$.

"Blow up" $\overline{E}$ at $(0, 0)$ via $y = tx$, giving $\overline{E}' : t^2x^2 + tx^2 = x^3$,

i.e. $x = t^2 + t$, $y = tx = t^3 + t^2$. [Note: bad at $t = 0, -1$.]

So $\overline{E}_{\text{ns}}$ is a copy of $\mathbb{P}^1$ with two points missing.

But that was blowing up $\overline{E}$ at the point $x = 0, y = 0$
in Spec $k[x, y]$.

Instead, let's blow up E at the point $x = 0, y = 0, \pi = 0$
in Spec $\mathcal{O}_K[x, y]$.

Multiplicative Reduction Example: Part 3

Blowing up $E : y^2 + xy = x^3 + \pi^n$ at $x = 0, y = 0, \pi = 0$:

We've already seen one "component" on the "special fiber" is $\overline{E} : y^2 + xy = x^3$, i.e. $x = t(t+1)$. [Via $y = tx$.]

If $n \geq 2$, blowing up via $x = \pi x_1$ and $y = \pi y_1$ [and cancelling π^2] gives $\quad E_1 : y_1^2 + x_1 y_1 = \pi x_1^3 + \pi^{n-2}$

which reduces (mod π) to $y_1(x_1 + y_1) = 0$, i.e., two lines.

And each of those points really should have two points removed:

- $(0, 0)$, where they cross, and
- each one's point at ∞, where it meets the original component.

Multiplicative Reduction Example: Part 4

Blowing up $E : y^2 + xy = x^3 + \pi^n$ at $x = 0, y = 0, \pi = 0$:

Component 0: $\overline{E} : y^2 + xy = x^3$, i.e. $x = t(t+1)$.

Components 1 and $n-1$: $E_1 : y_1^2 + x_1 y_1 = \pi x_1^3 + \pi^{n-2}$,
with $\overline{E}_1 : y_1(x_1 + y_1) = 0$, where $x = \pi x_1$, $y = \pi y_1$.

If $n \geq 4$, blowing up via $x_1 = \pi x_2$ and $y_1 = \pi y_2$ [and cancelling π^2]
gives $\quad E_2 : y_2^2 + x_2 y_2 = \pi^2 x_2^3 + \pi^{n-4}$

And so on, until we stop at

$E_m : y_m^2 + x_m y_m = \pi^m x_m^3 + \pi$ (if $n = 2m+1$ is odd)

or $E_m : y_m^2 + x_m y_m = \pi^m x_m^3 + 1$ (if $n = 2m$ is even)

Néron Models over a p-adic field K

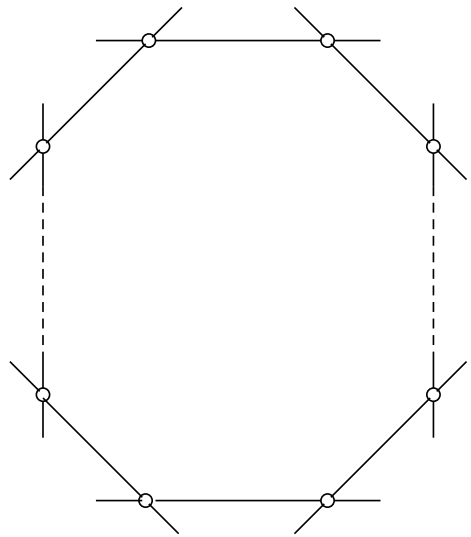
The set of all the equations $E, E_1, \ldots, E_m$, with the understanding that the singular points on the special fiber have been removed, is the **Néron Model** $\mathcal{E}$ for E/K.

Key properties:

- Each equation E_i/K is simply a change of coordinates of E/K. That is, the generic fiber of $\mathcal{E}$ is E.
- $\mathcal{E}$ is **smooth**: any singular points, even on the special fiber (i.e., mod π), have been removed.
- Every K-rational point $P \in E(K)$ has a reduction $\overline{P}$ on one of the $\overline{E}_i$.
- If we replace K by an unramified extension L/K, like $L = K^{\mathrm{ur}}$, the Néron model doesn't change.
  (Well, technically it base-changes to $\mathcal{E} \times \operatorname{Spec} \mathcal{O}_L$.)
- But if we replace K by a **ramified** extension L/K, $\mathcal{E}$ is usually **not** a Néron model for E/L.

$E : y^2 + xy = x^3 + \pi^n$ Revisited

Special fiber of $\mathcal{E}$ has n components (called "type I_n"):



but if we work over $L = K(\sqrt{\pi})$, then points (x, y) with, say, $|x|_p = |\sqrt{\pi}|_p$, will want to reduce to those missing singular points.

Instead, $\mathcal{E}_L$ should have $2n$ components on the special fiber, since equation is $E : y^2 + xy = x^3 + \sqrt{\pi}^{2n}$.

Another Example: Additive Reduction

Consider $p \neq 2$, and $E : y^2 = x^3 - \pi^2 x$.
$\Delta = 64\pi^6$, so $|\Delta|_p < 1$.

$\overline{E} : y^2 = x^3$ is singular at $(0, 0)$.

(Cusp, not node, because near $(0, 0)$ it looks like $y^2 = 0$, i.e., doubled line.)

Blowing up $y = tx$ gives $t^2 = x$.

So again reduced curve is $\mathbb{P}^1$, but this time with only one bad point ($t = 0$) removed.

$E : y^2 = x^3 - \pi^2 x$, Part 2

Let's blow up in $\operatorname{Spec} \mathcal{O}_K[x, y]$ more at $x = 0, y = 0, \pi = 0$:

$x = \pi x_1$ and $y = \pi y_1$ gives

$$E_1 : y_1^2 = \pi x_1^3 - \pi x_1 = \pi x_1(x_1 + 1)(x_1 - 1).$$

Reduction: $\overline{E}_1 : y_1^2 = 0$; double copy of $\mathbb{P}^1$

But there are K-rational points with $|y_1|_p < 1$ and $|x_1^3 - x_1|_p < 1$.
We need to blow up more:

$(0, 0)$: $x_1 = \pi x_{2,0}$, $y_1 = \pi y_2$ gives $E_{2,0} : y_2^2 = \pi^2 x_{2,0}^3 - x_{2,0}$.
Reduction: $\overline{E}_{2,0} : y_2^2 = -x_{2,0}$; single $\mathbb{P}^1$.

$(1, 0)$: $x_1 = 1 + \pi x_{2,1}$, $y_1 = \pi y_2$ gives
$E_{2,1} : y_2^2 = x_{2,1}(1 + \pi x_{2,1}^2)(2 + \pi x_{2,1}^2)$
Reduction: $\overline{E}_{2,1} : y_2^2 = 2x_{2,1}$; single $\mathbb{P}^1$.

$(-1, 0)$: $x_1 = -1 + \pi x_{2,-1}$, $y_1 = \pi y_2$ gives
$E_{2,-1} : y_2^2 = x_{2,-1}(-1 + \pi x_{2,-1}^2)(-2 + \pi x_{2,-1}^2)$
Reduction: $\overline{E}_{2,-1} : y_2^2 = 2x_{2,-1}$; single $\mathbb{P}^1$.

$E : y^2 = x^3 - \pi^2 x$, Part 3

The Néron model for E consists of the four copies of $\mathbb{P}^1$:
E, $E_{2,0}$, $E_{2,1}$, and $E_{2,-1}$.

The double copy of $\mathbb{P}^1$ (from E_1) is entirely singular, so remove it.

[E_1 is part of the "minimal proper regular model," but **not** part of the Néron model.]

$E : y^2 = x^3 - \pi^2 x$ is said to have type I_0^* reduction.
(Recall $p \neq 2$.)

Note: over $L = K(\sqrt{\pi})$, E becomes $y^2 = x^3 - \pi_L^4 x$.

The change of coordinates $x = \pi_L^2 \tilde{x}$, $y = \pi_L^3 \tilde{y}$ gives

$E : \tilde{y}^2 = \tilde{x}^3 - \tilde{x}$, which has good reduction (type I_0).

The Tate Curve

Let's now view $\mathbb{Q}_p \subseteq K \subseteq \mathbb{C}_p$. $D(a, r)$ denotes the open disk

$$D(a, r) = \{x \in \mathbb{C}_p : |x - a|_p < r\}.$$

Theorem (Tate)

There are power series $a_4(q) = q + O(q^2)$ and $a_6(q) = -q + O(q^2)$ in $\mathbb{Z}[[q]]$ converging for $q \in D(0, 1)$, so that for $q \neq 0$,

$$E_q : y^2 + xy = x^3 + a_4(q)x + a_6(q)$$

has multiplicative reduction, with $\Delta = q + O(q^2)$.
Moreover, for fixed q, there is a map $\phi_q : \mathbb{C}_p^\times / q^{\mathbb{Z}} \xrightarrow{\sim} E_q(\mathbb{C}_p)$.
If $q \in K$, then $\phi_q : K^\times / q^{\mathbb{Z}} \xrightarrow{\sim} E_q(K)$.

The Tate Curve, Continued

Idea: For fixed $q \in K$ with $0 < |q|_p < 1$, consider the "annulus"

$$A_q = \{x \in \mathbb{C}_p : |q|_p \leq |x|_p \leq 1\},$$

and glue the two "ends" of the annulus to each other:

$$\text{for } |y|_p = 1, \text{ glue } y \text{ to } qy.$$

We get a p-adic analog of a torus.

In fact, any elliptic curve E/K of (split) multiplicative reduction is isomorphic to the Tate curve for a unique q.

If E has reduction type I_n, then $|q|_p = |\pi|_p^n$, and the n components of the Néron model $\mathcal{E}$ correspond to the sets:

$$C_i = \{x \in \mathbb{C}_p : |x|_p = |\pi|_p^i\}, \quad \text{for } i = 0, 1, \ldots, n-1.$$

Each would be a copy of all of $\mathbb{P}^1(\mathbb{C}_p)$, except it is missing two residue classes: at 0 and ∞.

Hence the two missing points on each component of $\mathcal{E}$.

Berkovich Disks

Idea: Make a bigger space containing the disk

$$\overline{D}(a,r) = \{x \in \mathbb{C}_p : |x-a|_p \leq r\} \subseteq \mathbb{C}_p.$$

The new space $\overline{D}_{\mathrm{Ber}}(a,r)$ will include all the points of $\overline{D}(a,r)$, **plus** one point $\zeta(b,s)$ for each closed disk $\overline{D}(b,s) \subseteq \overline{D}(a,r)$.

In particular, the Berkovich version $A_{q,\mathrm{Ber}}$ of the annulus

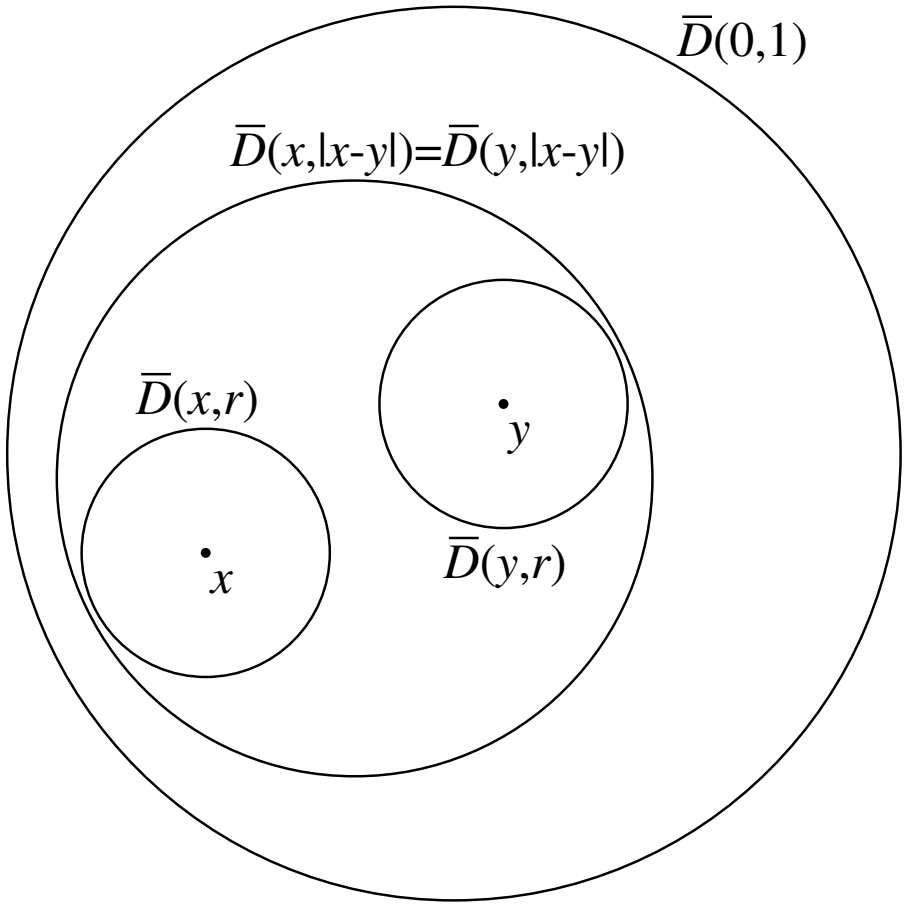
$$A_q = \{x \in \mathbb{C}_p : |q|_p \leq |x|_p \leq 1\}$$

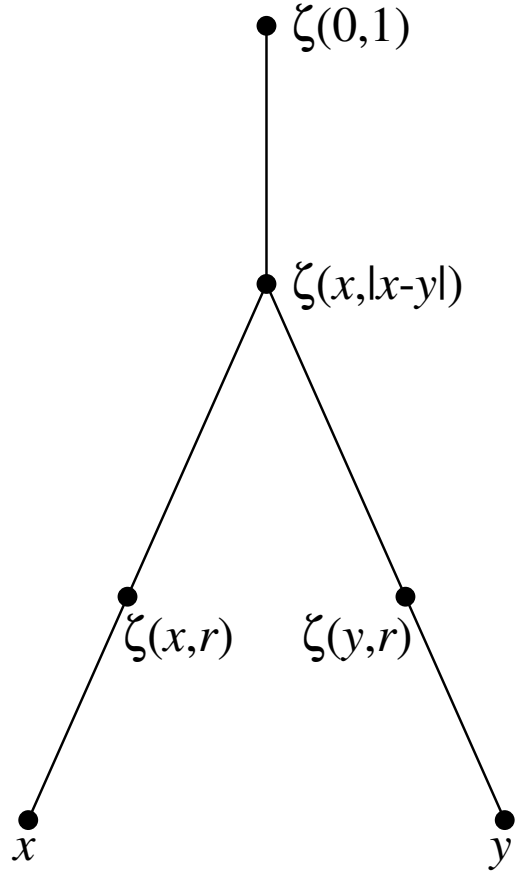
is

$$A_{q,\mathrm{Ber}} = \overline{D}_{\mathrm{Ber}}(0,1) \smallsetminus D_{\mathrm{Ber}}(0,|q|).$$

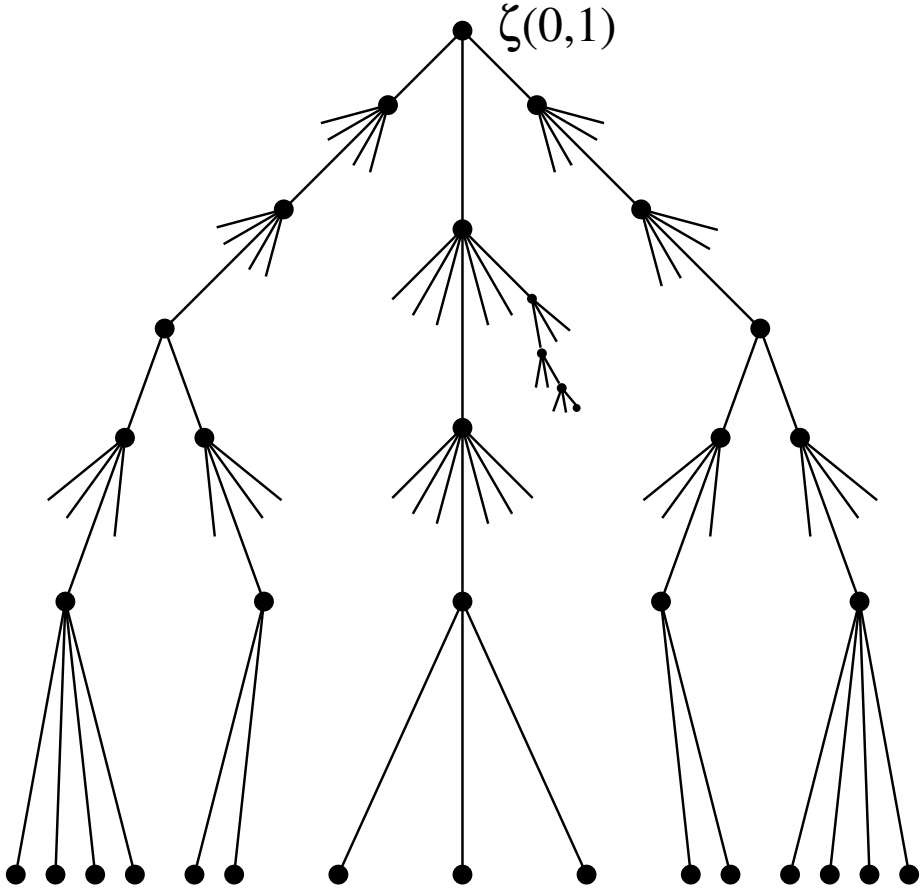
The Tate curve glueing will glue $\zeta(0,|q|)$ to $\zeta(0,1)$.

Berkovich Disks Are Connected





The Berkovich Unit Disk



Berkovich Elliptic Curves: Good Reduction

Any algebraic variety over K can be Berkovichized; the construction is functorial.

If E has good reduction, then E_{Ber} has one special point ζ_0:

- The branches emanating from ζ_0 are in natural one-to-one correspondence with the points of $\overline{E}(\overline{\mathbb{F}}_p)$
- Each branch is a copy of the open Berkovich disk $D_{\mathrm{Ber}}(0,1)$.

Berkovich Elliptic Curves: Multiplicative Reduction

If E has multiplicative reduction, then the Tate curve for E glues the two endpoints of the line segment

$$\zeta(0,1) \quad \text{to} \quad \zeta(0,|q|),$$

producing a circle.

For each point $\zeta(0,r)$ on this circle, with $r \in |\mathbb{C}_p|^\times$:

- There are two branches, towards zero and ∞, pointing around the circle,
- The other branches emanating from $\zeta(0,r)$ are in natural one-to-one correspondence with the points of $\overline{\mathbb{F}}_p^\times$,
- Each such branch is a copy of the open Berkovich disk $D_{\mathrm{Ber}}(0,1)$.

Moreover, the "K-rational" points on this circle, i.e., the ones of the form $\zeta(0,|\pi|^i)$, correspond to the components C_i of the Néron model.

Moral:

A Berkovich point ζ is a choice of coordinates for the defining equation of E.

and

The topology of E_{Ber} determines the reduction type of E (over a large enough extension of K).