Lectures notes on "Classical and quadratic Chabauty"

Samuel Le Fourn
ICTS 2023

September 11, 2023

A short introduction to the principles of the methods

In these lectures, I will talk about Chabauty methods to determine rational points on an algebraic projective curve of genus at least 2.

I will use throughout the following notation:

Notation

- C is a smooth algebraic projective curve over $\mathbb{Q}$, with genus $g \geq 2$. By the famous Faltings' theorem, $C(\mathbb{Q})$ is then finite, but this theorem does not give a way to determine this finite set (in fact, the methods employed, apart from a quite large bound on the size of $C(\mathbb{Q})$, cannot say much more).
- J is the jacobian of C, thus a principally polarised abelian variety over $\mathbb{Q}$ of dimension g.
- We fix a base point $b \in C(\mathbb{Q})$, thanks to which we define the embedding from C to J

$$\iota : \left| \begin{array}{ccc} C & \longrightarrow & J \\ P & \longmapsto & \mathrm{cl}([P]-[b]) \end{array} \right. .$$

- For any scheme $\mathcal{X}$ over some $\operatorname{Spec} A$ with A a ring and any A-algebra B, we denote by $\mathcal{X}_B$ the fiber product $\mathcal{X} \times_{\operatorname{Spec} A} \operatorname{Spec} B$ (in other words extension of scalars from A to B).
- p is a prime number at which C has good reduction (i.e. there exists a smooth algebraic projective curve $\mathscr{C}$ over $\mathbb{Z}_{(p)}$ such that $\mathscr{C}_{\mathbb{Q}}$ is isomorphic to C). This model is unique (up to $\mathbb{Z}_{(p)}$-isomorphism), so we fix it and by abuse of notation, we will write $C_{\mathbb{F}_p} := \mathscr{C}_{\mathbb{F}_p}$ and $C(\mathbb{F}_p) := \mathscr{C}(\mathbb{F}_p)$.
- As $\mathscr{C}$ is proper, every point P in $C(\mathbb{Q}_p)$ extends to a unique morphism $\operatorname{Spec} \mathbb{Z}_p \to \mathscr{C}$ and thus defines the *reduction modulo p of P*, i.e. a point of $C(\mathbb{F}_p)$, denoted by $\overline{P}$ (f).
- For any point $x \in C(\mathbb{F}_p)$, we denote $D_x \subset C(\mathbb{Q}_p)$ the (p-adic) *residue disk* of x, i.e. the set of points of $C(\mathbb{Q}_p)$ whose reduction modulo p is exactly x (this terminology will be justified later).

  Remark 0.1. Everything works out in a very similar way for finite extensions of $\mathbb{Q}$ (resp. $\mathbb{Q}_p$), but I preferred to keep it simple.

Main idea of classical Chabauty

The idea of Chabauty's method can be summed up in the following diagram.

$$\begin{array}{ccc} C(\mathbb{Q}) & \xrightarrow{\ \iota\ } & J(\mathbb{Q}) \\ \downarrow \subset & & \downarrow \subset \\ C(\mathbb{Q}_p) & \xrightarrow{\ \iota\ } & J(\mathbb{Q}_p) \end{array}$$

This allows us to "see" $C(\mathbb{Q})$ as included in $C(\mathbb{Q}_p) \cap J(\mathbb{Q})$ inside $J(\mathbb{Q}_p)$. More precisely,

$$\iota(C(\mathbb{Q})) \subset \iota(C(\mathbb{Q}_p)) \cap J(\mathbb{Q}).$$

Now, by p-adic Lie theory $J(\mathbb{Q}_p) \cong \mathbb{Z}_p^g \oplus H$, with H some finite abelian group, imagine $J(\mathbb{Q}_p) \cong \mathbb{Z}_p^g$ for simplicity. We are thus looking up to torsion at an intersection inside $\mathbb{Z}_p^g$, to fix the ideas. Furthermore, by Mordell-Weil theorem, we can write

$$J(\mathbb{Q}) \cong \mathbb{Z}^r \oplus T, \quad r := \operatorname{rank} J(\mathbb{Q}) < +\infty$$

with T the finite torsion subgroup of $J(\mathbb{Q})$, and r called the Mordell-Weil rank of $J(\mathbb{Q})$. Here is where Chabauty's idea comes into play:

If $r < g$, $J(\mathbb{Q})$ is contained in an hyperplane of $J(\mathbb{Q}_p)$, i.e. is contained in the set of zeroes of a nontrivial linear equation $\ell : J(\mathbb{Q}_p) \to \mathbb{Q}_p$.

Remark 0.2. This is not true in archimedean topology and the initial reason why we use p-adic numbers here. More explicitly, if $P_1, \cdots, P_r$ generate $J(\mathbb{Q})$ up to torsion, one can define $\mathbb{Z}_p P_1 + \cdots \mathbb{Z}_p P_r$ a p-adic closed analytic subgroup of $J(\mathbb{Q}_p)$ containing $J(\mathbb{Q})$, obviously of rank at most r.

Theorem (Chabauty, 1941)**.** *If $r < g$ (*Chabauty hypothesis*), $C(\mathbb{Q})$ is finite.*

Proof's idea (based on Coleman's 1985 version). Assuming $r < g$, let ℓ be a nontrivial linear equation on $J(\mathbb{Q}_p)$ whose zero locus contains $J(\mathbb{Q})$, so that $C(\mathbb{Q}) \subset (\ell \circ \iota)^{-1}(0)$ on $C(\mathbb{Q}_p)$. On each residue disk (isomorphic to $p\mathbb{Z}_p$) (f), this function can be expressed by p-adic power series (f). Now, we have a *logarithm map* of p-adic Lie groups to the tangent space at 0 (o)

$$\log : J(\mathbb{Q}_p) \to T_0 J_{\mathbb{Q}_p} \cong \mathbb{Q}_p^g$$

who has the property that $\log \circ \iota$ is transcendent on each residue disk (f)**??**. This imposes that for each $x \in C(\mathbb{F}_p)$, $\iota(D_x)$ is not contained in an hyperplane of $J(\mathbb{Q}_p)$, so the p-adic power series defined on D_x by $\ell \circ \iota$ is not 0, and thus has finitely many zeroes (which we can bound) (f).

Gathering bounds on all residue disks, we obtain the finiteness of $C(\mathbb{Q})$. □

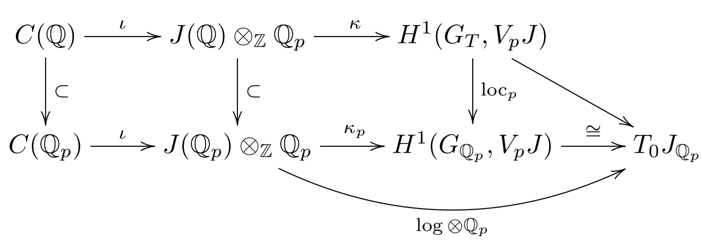
To be precise, we have proven that we always have

$$C(\mathbb{Q}) \subset C(\mathbb{Q}_p)_1 := \bigcap_{\substack{\ell \\ \ell_{|J(\mathbb{Q})}=0}} (\ell \circ \iota)^{-1}(0).$$

(more on the nature of those ℓ's later) and that if $r < g$, $C(\mathbb{Q}_p)_1$ (the *first obstruction* for rational points) is finite and hopefully small enough to be exactly $C(\mathbb{Q})$.

The inspiration for quadratic Chabauty

Let us first complicate a bit the first diagram (even though it starts off the same !)



A bit of explanation here (more later): G_T is the Galois group of the maximal extension of $\mathbb{Q}$ unramified everywhere outside p, $G_{\mathbb{Q}_p}$ is the absolute Galois group of $\mathbb{Q}_p$, κ and κ_p are Kummer maps (which are injective [f]) [o], loc_p is the localisation map of cohomology (I will not explain the cohomology choice), $V_pJ = T_pJ \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ with T_pJ the Tate module [o]and the isomorphism is given by p-adic Hodge theory [f].

With this cohomological construction (over V_pJ the Tate vector space), now we want to "replace" V_pJ by some nonabelian algebraic group. In fact, we will pick a unipotent group U [o]over $\mathbb{Q}_p$ endowed with a Galois action (of G_T) on its $\mathbb{Q}_p$-points and a surjective morphism $U \to V_pJ \cong (\mathbb{G}_a)^g_{\mathbb{Q}_p}$ as an algebraic group with G_T-action.

In an analogous way, we have

$$\begin{array}{ccc} C(\mathbb{Q}) & \xrightarrow{\kappa} & \mathrm{Sel}(U) \\ \downarrow & & \downarrow{\scriptstyle \mathrm{loc}_p} \\ C(\mathbb{Q}_p) & \xrightarrow{\kappa_p} & H^1(G_{\mathbb{Q}_p}, U) \end{array}$$

where $\mathrm{Sel}(U) \subset H^1(G_T, U)$ is defined by localisation conditions.

Here comes the main point: Kim's results [f][Kim05] prove that $\mathrm{Sel}(U)$ and $H^1(G_{\mathbb{Q}_p}, U)$ are not only pointed sets, but the sets of $\mathbb{Q}_p$ points of affine schemes of finite type over $\mathbb{Q}_p$, with loc_p an algebraic map!

Now, we will "only" need to prove two things to obtain finiteness of $C(\mathbb{Q})$: first, that the localisation map loc_p is not dominant and second that κ_p is analytic and transcendental (for the p-adic analytic topology). The second always holds, for the first one, we can "simply" find conditions for which $\dim \mathrm{Sel}(U) < \dim H^1(G_{\mathbb{Q}_p}, U)$, and this is where the *quadratic Chabauty condition* will appear. To give some spoilers, its simplest form is as follows: instead of $r < g$, we need to have

$$r < g + \rho - 1$$

where $\rho = \mathrm{rank}\, \mathrm{NS}(J)$ with $\mathrm{NS}(J)$ the Néron-Severi subgroup [o].

Remark 0.3. Why "quadratic Chabauty"? If you recall, the classical case can also be called linear as it relies on a "linear equation" isolating $J(\mathbb{Q})$ in $J(\mathbb{Q}_p)$.

Here, thinking with maps to $\mathbb{Q}_p$, the equations involved will appear ultimately given by "quadratic equations on $J(\mathbb{Q}_p)$". On another hand, they correspond to the "smallest" non abelian unipotent group above V_pJ, and in Kim's terminology to the second obstruction $C(\mathbb{Q}_p)_2$.

The interpretation of quadratic Chabauty for these lectures

We will study here quadratic Chabauty method with an alternative description recently devised by Besser, Müller and Srinivasan in [BMS21]. That preprint will thus be our main reference for the second part. Let us give its main ideas here:

• After some choices of auxiliary data, one can define for every line bundle L a "canonical" p-adic height $h_L : J(\mathbb{Q}) \to \mathbb{Q}_p$, with $L \to h_L$ linear. Furthermore, for each L, h_L as built will be a quadratic function on $J(\mathbb{Q})/J(\mathbb{Q})_{\mathrm{tors}}$.

• Using this construction, considering the pullback morphism $\iota^*_{\mathrm{NS}} : \mathrm{NS}(J) \to \mathrm{NS}(X) \cong \mathbb{Z}$. Its kernel V' is a $\mathbb{Z}$-module of rank $\rho - 1$, and together with the logarithm and the construction of heights, this defines a map

$$\varphi : J(\mathbb{Q}) \to T_0 J_{\mathbb{Q}_p} \oplus (V')^* \otimes \mathbb{Q}_p \cong \mathbb{Q}_p^{g+\rho-1}$$

by the logarithm map for the first summand and evaluation at D of the global heights for the second, and this extends to a polynomial map on $J(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{Q}_p \cong \mathbb{Q}_p^{r'}$ ($r' \leq r$) of degree at most 2 by construction. By a dimension argument, assuming $r < g + \rho - 1$, there must be a polynomial Q with coefficient in $\mathbb{Q}_p$ and $g + \rho - 1$ variables such that $Q(\varphi) = 0$ on $J(\mathbb{Q})$.

Now, we have to go back to how our heights are defined. As we have taken classes of $L \in \mathrm{Ker}\, \iota^*_{\mathrm{NS}}$, one can consider L's such that $\iota^* L$ is trivial, and then by functoriality this gives for each L a canonical height on $C(\mathbb{Q})$, built as a sum of local heights. The local heights at $q \neq p$ will have finitely many possible values, and each local height at p will be a special kind of locally analytic function built with p-adic integration, so in total we will have something like

$$C(\mathbb{Q}) \subset \bigcup_{t \in T} \{P \in C(\mathbb{Q}) \mid f_t(P) = t\}$$

with $T \subset \mathbb{Q}_p s$ finite and f_t a Vologosdky function on $C(\mathbb{Q}_p)$ obtained with the heights h_L and Q. The definition techniques employed will then allow to prove that none of these functions is locally constant (which means in other words that the p-adic iterated integrals that we build for such a family are algebraically independent on every residue disk $C(\mathbb{Q}_p)$), so on every small open f_t has only finitely many zeroes. This allows to conclude that $C(\mathbb{Q})$ is finite.

Geometric quadratic Chabauty version

1 Classical Chabauty method

The valuation v on $\mathbb{Q}_p$ is normalised by $v(p) = 1$, and we extend it to a valuation on $\overline{\mathbb{Q}_p}$ (by convention $v(0) = +\infty$).

1.1 Reminders on p-adic power series

This paragraph is based on [Kob77, §IV.4].

Definition 1.1 (Newton polygon)**.** Let

$$f(T) := \sum_{n=0}^{+\infty} a_n T^n \in \mathbb{Q}_p[[T]]$$

be a nonzero power series.

The *Newton polygon* of f is the lower convex envelop of the set of points $(n, v(a_n))_{n \geq 0}$ in the plane.

It is made up with possibly infinitely many segments (the last one being vertical infinite if f is a polynomial), one of them (the rightmost one) possibly infinite. The sequence of slopes of those segments (from left to right) is thus a strictly increasing sequence of real numbers. The *length* of a segment of the Newton polygon is its horizontal length (i.e. difference of x-coordinates of its endpoints).

To be more precise, three cases can happen [(E)]:

(a) there are infinitely many segments all of finite length (e.g. $f(T) = \sum^{n=0} p^{n^2} T^n$) [(E)].

(b) there are finitely many segments of finite length at first and then an infinitely long segment passing through infinitely many points $(n, v(a_n))$ (e.g. $f(T) = p^2 + \sum_{n \geq 1} pT^n$ [(E)].

(c) Same as (b) but the infinite segment does not pass through infinitely many points, although if its slope was higher it would be above infinitely many points $(n, v(a_n))$ (e.g. $f(T) = 1 + \sum_{n \geq 1} pT^n$) [(E)].

Many things can be said about the Newton polygon, but we will focus on the following.

Theorem 1.1 (Weierstrass preparation theorem)**.** *Assume that $f(T) \in \mathbb{Q}_p[[T]]$ converges on $D(0, p^\lambda)$ the closed disk of radius p^λ. Then:*

(a) The Newton polygon of f has only a finite total length of segments with slopes $< \lambda$[(E)].

(b) Defining N the total length of segments with slopes $\leq \lambda$ (if the infinite segment has slope λ, define N as the last n such that $(n, v(a_n))$ does belong to this segment), we can write

$$f = gh$$

with $g \in \mathbb{Q}_p[T]$ of degree N and $h \in \mathbb{Q}_p[[T]]$ converging and with no zeroes on $D(0, p^\lambda)$ and g, h are uniquely determined by these properties.

(*c*) *Furthermore, the Newton polygons of* f *and* g *truncated over* $[0, N]$ *are the same.*

(*d*) *If* S *is a segment of this truncated Newton polygon of length* ℓ *and slope* α, g *(and therefore* f*) has exactly* ℓ *roots in* $\overline{\mathbb{Q}_p}$ *of valuation* $-\alpha$ *with multiplicity.*

Proof. All this can be found in [Kob77]: (a) is Lemma IV.4.5, (b) (most generally referred to as the preparation theorem itself) and (c) are Theorem IV.4.14 and (d) is Lemma IV.3.4 (we can assume $f(0) = 1$ after dividing by some uT^k, which only translates the Newton polygon). □

Remark 1.2. When we are given a specific (converging) p-adic power series, this theorem is very precise regarding the sizes of roots, and that is exactly what we will be able to use later. We want nevertheless a theoretical result, so let us dive directly into a special case which we have a very good (later) reason to study.

Corollary 1.3. *Let* $f = \sum_{n\geq 0} \frac{a_n}{n+1} T^{n+1} \in \mathbb{Q}_p[[T]]$ *with* $a_n \in \mathbb{Z}_p$ *for all* $n \in \mathbb{N}$.

Let us assume that for some $n \in \mathbb{N}$ $v(a_n) = 0$ *and consider the smallest possible such* n.

(*a*) *If* $n < p-2$, *there are at most* $n+1$ *roots of* f *(counting 0) in* $D_{\overline{\mathbb{Q}_p}}(0, 1/p)$.

(*b*) *If* $n = p-2$, *there are at most* $n+1$ *or* $n+2$ *roots of* f *(counting 0) in* $D_{\overline{\mathbb{Q}_p}}(0, 1/p)$ *with the extra root (of norm* $1/p$*) coming up when* $v(a_{p-1}) = 0$.

(*c*) *If* $v(a_0) = 0$, *if* $p > 2$ *the unique root of* f *in* $D_{\overline{\mathbb{Q}_p}}(0, 1/p)$ *is 0, if* $p = 2$ *there is another root in that disk if* $v(a_1) = 0$, *of norm* $1/2$.

Proof. First, notice that f converges on the closed disk $D_{\overline{\mathbb{Q}_p}}(0, 1/p)$. and that for every $n \leq p-2$ and every index $i \geq n+1$, $v(i+1) \leq i-n$. Indeed, this is trivially true for $i = n+1$ $(1 \leq 1)$ and for $i \in [p, 2p-2]$, and for $i \geq 2p-1$,

$$v(i+1) \leq \frac{\log(i+1)}{\log(p)} \leq i+1-(p-1) \leq i+1-(n+1) = i-n$$

by real analysis for the middle term $^{(E)}$. Notice furthermore that if $n < p-2$, the proven inequality is always strict if again $i \geq n+1$.

Now, denote by P_k the point $(k+1, v(\frac{a_k}{k+1}))$ for all $k \in \mathbb{N}$.

By hypothesis, the slope of any segment between P_k $(k < n)$ and P_i $(i > n)$ is

$$\frac{v(a_i) - v(i+1) - v(a_k)}{i-k} \geq \frac{n-i-v(a_k)}{i-k}.$$

The same computation between P_k $(k < n)$ and P_n gives a slope $-v(a_k)/(n-k)$. There are thus two cases: if $v(a_k) > n-k$, the segment $[P_k P_n]$ has a lower slope than any segment $[P_k P_i]$ with $i > n$, so P_n is one of the vertices of the Newton polygon. If $v(a_k) \leq n-k$, the above inequality shows that

$$\frac{v(a_i) - v(i+1) - v(a_k)}{i-k} \geq \frac{n-i-v(a_k)}{i-k} \geq \frac{n-i-(n-k)}{i-k} = -1.$$

In case (a), this even gives a strict inequality, which implies that in both situations the last segment of the Newton polygon which originates in some P_k $(k \leq n)$ must have a slope > -1, so all following segments of the Newton polygon also do. Therefore, all segments of the polygon with slopes ≤ -1 are contained in the truncated Newton polygon above $[0, n+1]$ and their total length is at most n, from which we can conclude by Theorem 1.1 (b).

Case (b) is similar but we can have such a segment of slope -1 when $k = n$ and the equality case $v(i+1) = i-n$, which happens only when $i = p-1$. In that situation, the segment $[P_{p-2} P_{p-1}]$ has slope -1 exactly if $v(a_p) = 0$, but then the following segments don't, so it is enough to consider the Newton polygon truncated over $[0, n+2]$ and the result follows.

Case (c) is now an immediate conclusion based on those two cases. □

1.2 The setup of Chabauty's method

1.2.1 Local rings and parameters

Let us now start with our curve $C/_{\mathbb{Q}}$, base point $b \in C(\mathbb{Q})$ and jacobian J of C and a choice of prime number p. The main reference for the algebraic geometry arguments here is [Liu02].

Fix a smooth projective model $\mathscr{C}$ of C over $\mathbb{Z}_{(p)}$ such that $\mathscr{C}_{\mathbb{Q}} \cong C$ (and it is then unique up to isomorphism by [Liu02, Proposition 10.1.21]), we fix such a model, identify $\mathscr{C}_{\mathbb{Q}}$ with C and by abuse of notation, write $C_{\mathbb{F}_p} := \mathscr{C} \times \operatorname{Spec} \mathbb{F}_p$ the fiber of $\mathscr{C}$ at p and $C(\mathbb{F}_p) := \mathscr{C}(\mathbb{F}_p)$.

This model extends to $\operatorname{Spec} \mathbb{Z}_p$, and for $C(\mathbb{Q}_p) = \mathscr{C}(\mathbb{Q}_p) = \mathscr{C}(\mathbb{Z}_p)$ by the valuative criterion of properness [Liu02, Corollary 3.3.26].

Definition 1.4. For any point $P \in C(\mathbb{Q}_p)$, the *reduction of P modulo p*, denoted by $\overline{P} \in C(\mathbb{F}_p)$ is the image of the extension of P to $\operatorname{Spec} \mathbb{Z}_p \to \mathscr{C}$ at the special fiber.

The *residue disk* D_x of $x \in C(\mathbb{F}_p)$ is

$$D_x := \{P \in C(\mathbb{Q}_p) \,|\, \overline{P} = x\}.$$

Remark 1.5. These reduction maps can actually be defined more generally for any proper scheme over a Dedekind scheme, see [Liu02, Definition 10.1.31].

Definition 1.6 (Systems of local parameters)**.** Let $\mathcal{X}$ be a projective scheme of relative dimension d over $\mathbb{Z}_p$, smooth over $\mathbb{Q}_p$.

- For any smooth point $x \in \mathcal{X}(\mathbb{F}_p)$ seen as a closed point of $\mathcal{X}$, the maximal ideal $\mathfrak{m}_{X,x}$ of $\mathcal{O}_{\mathcal{X},x}$ can be generated by p together with d other elements $t_1, \cdots, t_d$ such their reductions modulo p generate the maximal idea of $\mathcal{O}_{\mathcal{X}_{\mathbb{F}_p},x}$. In this case we call $(p, t_1, \cdots, t_d)$ a *system of local parameters at x*.
- If furthermore $P \in \mathcal{X}(\mathbb{Q}_p)$ is a point whose reduction modulo p is x and $t_1(P) = 0, \cdots, t_d(P) = 0$ (this is well-defined through the canonical injection $\mathcal{O}_{\mathcal{X},x} \to \mathcal{O}_{\mathcal{X},P}$), then we call $(p, t_1, \cdots, t_d)$ a *system of good local parameters at P*.

Proof. By smooothness of $\mathcal{X}_{\mathbb{F}_p}$ at x, $\overline{A} := \mathcal{O}_{\mathcal{X}_{\mathbb{F}_p},x}$ is a regular local ring with characteristic p and of dimension d. We can thus fix $\overline{t_1}, \cdots, \overline{t_d}$ in $\mathfrak{m}_{\overline{A}}$ whose classes give a basis of the $k(x)$-vector space $\mathfrak{m}_{\overline{A}}/\mathfrak{m}_{\overline{A}}^2$, and by Nakayama's Lemma, $\overline{t_1}, \cdots, \overline{t_d}$ then generate $\mathfrak{m}_{\overline{A}}$ itself.

Now, $\mathcal{O}_{\mathcal{X},x}$ is a ring whose tensor product with $\mathbb{F}_p$ is $\overline{A}$, so we can fix elements $t_1, \cdots, t_d$ of $\mathcal{O}_{\mathcal{X},x}$ whose images modulo p are $\overline{t_1}, \cdots, \overline{t_d}$, so that now $(p, \overline{t_1}, \cdots, \overline{t_d})$ generate $\mathfrak{m}_{\mathcal{X},x}$ by Nakayama's lemma again. □

The following fundamental result is based on [Liu02, Proposition 10.1.40].

Proposition 1.7. *With those definitions and $(p, t_1, \cdots, t_d)$ a system of local parameters at x, we have an isomorphism*

$$\mathbb{Z}_p[[T_1, \cdots, T_d]] \overset{\varphi}{\cong} \widehat{\mathcal{O}_{\mathcal{X},x}}$$

sending each T_i on t_i and it induces a bijection between D_x and $(p\mathbb{Z}_p)^d$ via

$$D_x \cong \operatorname{Hom}_{\mathrm{loc}}(\widehat{\mathcal{O}_{\mathcal{X},x}}, \mathbb{Z}_p) \overset{\varphi^*}{\cong} (p\mathbb{Z}_p)^d.$$

where to each morphism $F : \widehat{\mathcal{O}_{\mathcal{X},x}} \to \mathbb{Z}_p$ we associate its images on the $\varphi(t_1), \cdots \varphi(t_d)$ and $\operatorname{Hom}_{\mathrm{loc}}$ *means morphisms of local rings. This bijection will be called "evaluation of the parameters at points of the residue disk", and the image of $P \in D_x$ denoted by $(t_1(P), \cdots, t_d(P))$.*

Furthermore, for $P \in X(\mathbb{Q}_p)$ reducing to x and assuming $t_1(P), \cdots, t_d(P) = 0$, we have a commutative diagram

$$\begin{array}{ccc}
\mathbb{Q}_p[[T_1, \cdots, T_d]] & \xrightarrow{\varphi \otimes_{\mathbb{Z}_p} \mathbb{Q}_p} & \widehat{\mathcal{O}_{X,P}} \\
\uparrow {\scriptstyle \mathrm{Id} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p} & & \uparrow {\scriptstyle \mathrm{Id} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p} \\
\mathbb{Z}_p[[T_1, \cdots, T_d]] & \xrightarrow{\varphi} & \widehat{\mathcal{O}_{\mathcal{X},x}} \\
\downarrow {\scriptstyle \mathrm{Id} \otimes_{\mathbb{F}_p} \mathbb{Q}_p} & & \downarrow {\scriptstyle \mathrm{Id} \otimes_{\mathbb{Z}_p} \mathbb{F}_p} \\
\mathbb{F}_p[[T_1, \cdots, T_d]] & \xrightarrow{\varphi \otimes \mathbb{F}_p} & \widehat{\mathcal{O}_{\mathcal{X}_{\mathbb{F}_p},x}}
\end{array}$$

where horizontal arrows are isomorphisms.

Proof. First, notice that each t_i belongs to $\mathfrak{m}_{\mathcal{X},x}$ by construction, so φ is actually a well-defined morphism of complete local rings. For the surjectivity, we have $k(x) = \mathbb{F}_p$ and $\mathfrak{m}_{\mathcal{X},x}$ is generated by $(p, t_1, \cdots, t_d)$ so we have

$$\mathcal{O}_{\mathcal{X},x} = \mathbb{Z}_p + (t_1, \cdots, t_d) \subset \mathbb{Z}_p[t_1, \cdots, t_d] + (t_1, \cdots, t_d)^m$$

for all $m \geq 1$ by immediate induction, which leads to the surjectivity of φ. Now, x being a smooth point in the special fiber and $\mathcal{X}$ of relative dimension d, $\widehat{\mathcal{O}_{\mathcal{X},x}}$ is a complete (integral) regular local ring of dimension $d+1$ so φ must be an isomorphism.

With similar arguments, as $(\overline{t_1}, \cdots, \overline{t_d})$ is a system of local parameters at $x \in \mathcal{X}_{\mathbb{F}_p}$ and $(t_1, \cdots, t_d)$ is a system of local parameters at P by construction, we also obtain

$$\mathbb{Q}_p[[t_1, \cdots, t_d]] = \widehat{\mathcal{O}_{X,P}}, \qquad \mathbb{F}_p[[\overline{t_1}, \cdots, \overline{t_d}]] = \widehat{\mathcal{O}_{\mathcal{X}_{\mathbb{F}_p},x}},$$

in a compatible way with the canonical morphisms given, which proves that the diagram is well-defined and commutes.

Then, we have the sequence of standard identifications

$$\begin{array}{rcl}
D_x & = & \{f : \operatorname{Spec} \mathbb{Z}_p \to \mathcal{X} \mid f(p\mathbb{Z}_p) = x\} \\
& \cong & \{f : \operatorname{Spec} \mathbb{Z}_p \to \operatorname{Spec} \mathcal{O}_{\mathcal{X},x}\} \\
& \cong & \mathrm{Hom}_{\mathrm{loc}}(\mathcal{O}_{\mathcal{X},x}, \mathbb{Z}_p) \\
& \cong & \mathrm{Hom}_{\mathrm{loc}}(\widehat{\mathcal{O}_{\mathcal{X},x}}, \mathbb{Z}_p) \\
& \cong & \mathrm{Hom}_{\mathrm{loc}}(\mathbb{Z}_p[[T_1, \cdots, T_d]], \mathbb{Z}_p) \\
& \cong & (p\mathbb{Z}_p)^d,
\end{array}$$

the latter bijection simply given by choosing the images of the generators T_i (they have to be in $p\mathbb{Z}_p$ to obtain a morphism of local rings). □

The following Corollary can also be found as [Sik09, Lemma 2.3].

Corollary 1.8 (Case of curves)**.** *If $x \in \mathscr{C}(\mathbb{F}_p)$, we can fix $t \in \mathcal{O}_{\mathscr{C}_{\mathbb{Z}_p},x}$ whose reduction modulo p is a uniformizer in $\mathscr{C}_{\mathbb{F}_p}$. The residue disk D_x is then in bijection with $p\mathbb{Z}_p = D_{\mathbb{Q}_p}(0, 1/p)$ through "evaluation of t". Furthermore, considering t as rational function in $\mathbb{Q}_p(C)$, for a point $P \in C(\mathbb{Q}_p)$ reducing to x modulo p, $s_P := t - t(P)$ has the following properties:*

(a) s_P is a uniformizer at P.

(b) the reduction of s_P modulo p (seen as a rational function in $\mathbb{F}_p(\mathscr{C}_{\mathbb{F}_p})$) is a uniformizer at x.

(*c*) *We have*

$$\begin{array}{ccc}
\widehat{\mathcal{O}_{C_{\mathbb{Q}_p},P}} & \xrightarrow{\cong} & \mathbb{Q}_p[[s_P]] \\
\uparrow & & \uparrow \\
\widehat{\mathcal{O}_{\mathscr{C}_{\mathbb{Z}_p},x}} & \xrightarrow{\cong} & \mathbb{Z}_p[[s_P]] \\
\downarrow & & \downarrow \\
\widehat{\mathcal{O}_{\mathscr{C}_{\mathbb{F}_p},x}} & \xrightarrow{\cong} & \mathbb{F}_p[[\overline{s_P}]].
\end{array}$$

where vertical arrows are the reduction mod p (i.e. tensoring by $\mathbb{F}_p$).

(*d*) *The "evaluation of s_P at x" is a bijection between the residue disk D_P and $p\mathbb{Z}_p$, sending P to 0.*

Definition 1.9 (Good uniformizer)**.** For a given $P \in C(\mathbb{Q}_p)$ as above, a function s_P thus obtained will be called a *good uniformizer at P*.

References

[BMS21] Amnon Besser, J. Steffen Müller, and Padmavathi Srinivasan, *p-adic adelic metrics and quadratic chabauty i*, 2021.

[Kim05] Minhyong Kim, *The motivic fundamental group of* $\mathbb{P}^1\{0, 1, \infty\}$ *and the theorem of Siegel*, Invent. Math. **161** (2005), no. 3, 629–656.

[Kob77] Neal Koblitz, *P-adic numbers, p-adic analysis, and zeta-functions*, Graduate texts in mathematics, Springer-Verlag, 1977.

[Liu02] Qing Liu, *Algebraic Geometry and Arithmetic Curves*, Oxford University Press, 2002.

[Sik09] Samir Siksek, *Chabauty for symmetric powers of curves*, Algebra Number Theory **3** (2009), no. 2, 209–236.