p-ADIC APPROACHES TO RATIONAL AND INTEGRAL POINTS ON CURVES

BJORN POONEN

Abstract. We give an introduction to two p-adic methods that aim to prove the finiteness of the set of rational or integral points on hyperbolic curves. The first is Kim's method, generalizing Chabauty's method, which in turn was inspired by a method of Skolem. The second is the method of Lawrence and Venkatesh, which uses p-adic period maps to give a new proof of the theorems of Siegel and Faltings.

1. The theorems of Siegel and Faltings

1.1. **Rational points on projective curves.** Let K be a number field. Call a curve over K nice if it is smooth, projective, and geometrically integral. The following theorem was originally conjectured by Mordell [Mor22].

Theorem 1.1 (Faltings). *Let X be a nice curve of genus g over K. If $g > 1$, then $X(K)$ is finite.*

There exist several proofs, all difficult:

- Faltings [Fal83], via Arakelov methods.
- Vojta [Voj91], via diophantine approximation. A more elementary variant of Vojta's proof was given by Bombieri [Bom90].
- Lawrence–Venkatesh [LV18], via p-adic period maps.

There is also a much older result of Chabauty [Cha41], who adapted a p-adic method of Skolem to prove that if the Jacobian J of X satisfies $\operatorname{rank} J(K) < g$, then $X(K)$ is finite.

1.2. **Integral points on curves.** Let S be a finite set of places of K containing all the archimedean places. Then the ring of S-integers in K is

$$\mathcal{O} = \mathcal{O}_{K,S} := \{x \in K : v(x) \geq 0 \text{ for all } v \notin S\}.$$

Date: March 7, 2020.
These are updated versions of notes for lectures given July 1–10, 2019 during the "Reinventing rational points" trimester at the Institut Henri Poincaré and on March 7, 2020 at the 2020 Arizona Winter School on "Nonabelian Chabauty". The writing of these notes was supported in part by the Université de Paris-Sud, National Science Foundation grant DMS-1601946, and Simons Foundation grants #402472 (to Bjorn Poonen) and #550033.

Let X be a nice curve of genus g over K. Let Z be a nonempty 0-dimensional subscheme of X. Let $r = \#Z(\overline{K})$, where $\overline{K}$ denotes an algebraic closure of K. Let $U = X - Z$. Then one may define the topological Euler characteristic $\chi(U) = \chi(X) - r = (2-2g) - r$.

Theorem 1.2 (Siegel). *Let $U = X - Z$ as above. Let $\mathcal{U}$ be any finite-type $\mathcal{O}$-scheme such that $\mathcal{U}_K \simeq U$. If $\chi(U) < 0$, then $\mathcal{U}(\mathcal{O})$ is finite.*

Again there are a few proofs:

- Siegel [Sie29], via diophantine approximation.
- Baker–Coates [BC70] gave a proof when either $g \le 1$ or X is hyperelliptic and Z contains a Weierstrass point, via linear forms in logarithms. This proof, when it applies, is the only one that is *effective*, giving a computable upper bound on the height of the integral points.
- Lawrence–Venkatesh [LV18], via p-adic period maps, gave a new proof of the case $U = \mathbb{P}^1 - \{0, 1, \infty\}$.

Also, Skolem [Sko34] invented a p-adic method that in some situations would determine $U(\mathcal{O})$.

Remark 1.3. Theorem 1.1 implies Theorem 1.2, even if U has genus ≤ 1, because one can use descent to replace U by a finite étale cover (and its twists) of genus > 1.

Remark 1.4. If one allowed $Z = \emptyset$ in Theorem 1.2, then one would obtain a statement that included also Theorem 1.1: if $Z = \emptyset$, then the condition $\chi(U) < 0$ becomes $g > 1$ and the valuative criterion for properness yields $\mathcal{U}(\mathcal{O}) = X(K)$. In this combined statement, the hypothesis $\chi(U) < 0$ amounts to being in one of the following situations:

- $g = 0$ and $r \ge 3$ (e.g., $\mathbb{P}^1 - \{0, 1, \infty\}$);
- $g = 1$ and $r \ge 1$ (e.g., an elliptic curve with the point at infinity removed);
- $g \ge 2$ and r is arbitrary.

1.3. **Goals of these lecture notes.** Sections 2 and 3 give an introduction to Kim's non-abelian generalization of Chabauty's p-adic method.

The remaining sections give an introduction to the article by Lawrence and Venkatesh [LV18]. We present their general method, and sketch how they use it to prove Siegel's theorem for $\mathbb{P}^1 - \{0, 1, \infty\}$, also known as the S-unit equation.

2. Kim's rewriting of Chabauty in terms of étale homology of the curve

2.1. **Chabauty's method.** Here we give only a quick review of Chabauty's method; for more details, see [MP12], for example.

Let K be a number field. Let X be a nice (i.e., smooth, projective, and geometrically integral) curve of genus g over K. Let $\mathfrak{p}$ be a prime of K at which X has good reduction. Let

p be the prime of $\mathbb{Q}$ below $\mathfrak{p}$. Let $K_\mathfrak{p}$ be the completion of K at $\mathfrak{p}$. Let J be the Jacobian of X. Let r be the rank of $J(K)$. We have a commutative diagram

$$\begin{tikzcd} X(K) \arrow[r] \arrow[d] & X(K_\mathfrak{p}) \arrow[d] & \\ J(K) \arrow[r] & J(K_\mathfrak{p}) \arrow[r, "\log"] & \operatorname{Lie} J_{K_\mathfrak{p}}. \end{tikzcd} \tag{1}$$

Chabauty's approach is to understand the images of $J(K)$ and $X(K_\mathfrak{p})$ in $\operatorname{Lie} J_{K_\mathfrak{p}}$. Specifically, the image of $J(K)$ in the g-dimensional space $\operatorname{Lie} J_{K_\mathfrak{p}}$ spans a $K_\mathfrak{p}$-subspace of dimension at most r, so if $r < g$, then there is a nonzero $K_\mathfrak{p}$-linear functional on $\operatorname{Lie} J_{K_\mathfrak{p}}$ vanishing on the image of $J(K)$, and one shows that it pulls back to a nonzero locally analytic function on $X(K_\mathfrak{p})$ vanishing on $X(K)$, which proves that $X(K)$ is finite.

2.2. **Summary of the rewriting.** Minhyong Kim found a way to rewrite (1) so that all references to J are replaced by references to X and its various homology groups. This enabled him to generalize, by replacing homology by deeper quotients of the fundamental group of X. Our exposition of this mainly follows [Cor19], but without going into as much detail.

The rewriting can be summarized by the following diagram, which will be explained in later sections; the red items are to be replaced by the green ones. We assume from now on that X has good reduction at all places above p.

$$\begin{tikzcd} X(K) \arrow[rr] \arrow[d] & & X(K_\mathfrak{p}) \arrow[d] & \\ J(K) \arrow[rr] \arrow[d] & & J(K_\mathfrak{p}) \arrow[r, "\log"] \arrow[d] & \operatorname{Lie} J_{K_\mathfrak{p}} \\ \widehat{J(K)}\left[\frac{1}{p}\right] \arrow[rr] \arrow[d, "\simeq?"'] & & \widehat{J(K_\mathfrak{p})}\left[\frac{1}{p}\right] \arrow[ur, "\simeq"'] \arrow[d] & \\ \operatorname{Sel}_{\mathbb{Q}_p} J \arrow[r, equal] \arrow[d, hook] & \mathrm{H}^1_f(K, V) \arrow[r] & \mathrm{H}^1_f(K_\mathfrak{p}, V) \arrow[r, "\log_{\mathrm{BK}}", "\simeq"'] \arrow[d, hook] & \mathrm{H}_1^{\mathrm{dR}}(X_{K_\mathfrak{p}})/\operatorname{Fil}^0 \arrow[uu, "\simeq"'] \\ \mathrm{H}^1(K, V) \arrow[rr] & & \mathrm{H}^1(K_\mathfrak{p}, V). & \end{tikzcd} \tag{2}$$

2.3. ***p*-adic completions.** Let M be an abelian group. We can form a $\mathbb{Z}_p$-module by taking the p-adic completion $\widehat{M} := \varprojlim_n M/p^n M$. Next, we can form a $\mathbb{Q}_p$-vector space by localizing the module by inverting p, to obtain $\widehat{M}\left[\frac{1}{p}\right] \simeq M \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. These constructions are functorial in M.

The group $J(K_\mathfrak{p})$ is compact, so the images of $p^n J(K_\mathfrak{p})$ in $\operatorname{Lie} J_{K_\mathfrak{p}}$ tend to 0 p-adically as $n \to \infty$. Therefore the homomorphism $J(K_\mathfrak{p}) \to \operatorname{Lie} J_{K_\mathfrak{p}}$ factors through $\widehat{J(K_\mathfrak{p})}$ and hence also through $\widehat{J(K_\mathfrak{p})}\left[\frac{1}{p}\right]$. Using that log is a local diffeomorphism with finite kernel, one can prove that the $\mathbb{Q}_p$-linear map $\widehat{J(K_\mathfrak{p})}\left[\frac{1}{p}\right] \to \operatorname{Lie} K_\mathfrak{p}$ is an isomorphism.

This explains up to the third row of (2).

2.4. **Étale homology.** If $J = \operatorname{Jac} X$ for some curve X over $\mathbb{C}$, then $J(\mathbb{C}) \simeq \mathbb{C}^g/\Lambda$ for some lattice $\Lambda \simeq \mathrm{H}_1(J(\mathbb{C}), \mathbb{Z})$, and

$$J[p] \simeq \frac{p^{-1}\Lambda}{\Lambda} \simeq \frac{\Lambda}{p\Lambda} \simeq \mathrm{H}_1(J(\mathbb{C}), \mathbb{Z}/p\mathbb{Z}) \simeq \mathrm{H}_1(X(\mathbb{C}), \mathbb{Z}/p\mathbb{Z}).$$

Similarly, for our curve X over K, one can define $\mathrm{H}_1^{\mathrm{et}}(X_{\overline{K}}, \mathbb{Z}/p\mathbb{Z})$ as the $\mathbb{Z}/p\mathbb{Z}$-dual of the étale cohomology group $\mathrm{H}^1_{\mathrm{et}}(X_{\overline{K}}, \mathbb{Z}/p\mathbb{Z})$, and then

$$J[p] \simeq \mathrm{H}_1^{\mathrm{et}}(X_{\overline{K}}, \mathbb{Z}/p\mathbb{Z})$$

as $\mathfrak{G}_K$-modules, where $\mathfrak{G}_K := \operatorname{Gal}(\overline{K}/K)$. Likewise, for $n \geq 1$ one has

$$J[p^n] \simeq \mathrm{H}_1^{\mathrm{et}}(X_{\overline{K}}, \mathbb{Z}/p^n\mathbb{Z}).$$

Take inverse limits to define the $\mathbb{Z}_p$ and $\mathbb{Q}_p$ Tate modules

$$T := \varprojlim_n J[p^n] \simeq \mathrm{H}_1^{\mathrm{et}}(X_{\overline{K}}, \mathbb{Z}_p)$$
$$V := T\left[\frac{1}{p}\right] = T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \simeq \mathrm{H}_1^{\mathrm{et}}(X_{\overline{K}}, \mathbb{Q}_p)$$

in terms of X. We have $\dim_{\mathbb{Q}_p} V = 2g$.

Finally, let us associate to V an algebraic group $\mathcal{V}$. Over any field F, the additive group variety $\mathbb{G}_a$, defined as $\mathbb{A}^1_F := \operatorname{Spec} F[t]$ equipped with the group law given by addition, is such that $\mathbb{G}_a(F) = F$. More generally, any finite-dimensional F-vector space W can be viewed as $\mathcal{W}(F)$ for a canonically-associated group variety $\mathcal{W}$ isomorphic to a power of $\mathbb{G}_a$. In particular, V is $\mathcal{V}(\mathbb{Q}_p)$ for some $\mathcal{V}$ isomorphic to $\mathbb{G}_a^{2g}$.

2.5. **Selmer groups.** Taking cohomology of the Kummer sequence

$$0 \longrightarrow J[p] \longrightarrow J \xrightarrow{p} J \longrightarrow 0$$

yields an injection

$$\frac{J(K)}{pJ(K)} \hookrightarrow \mathrm{H}^1(K, J[p]).$$

(Note: Before we were using étale cohomology of a variety, but now we are using Galois cohomology.) The $\mathbb{F}_p$-vector space $\mathrm{H}^1(K, J[p])$ is infinite-dimensional if $\dim J > 0$, but $J(K)/pJ(K)$ injects into a finite-dimensional subspace $\operatorname{Sel}_p J$ defined as the set of classes that are "locally in the image"; more precisely, if α and β are the homomorphisms in the diagram

$$\begin{tikzcd}
\dfrac{J(K)}{pJ(K)} \arrow[r, hook] \arrow[d] & \mathrm{H}^1(K, J[p]) \arrow[d, "\beta"] \\
\prod_v \dfrac{J(K_v)}{pJ(K_v)} \arrow[r, hook, "\alpha"] & \prod_v \mathrm{H}^1(K_v, J[p]),
\end{tikzcd}$$

then $\mathrm{Sel}_p J := \beta^{-1}(\mathrm{im}\,\alpha)$.

A similar square with p^n in place of p yields

$$\frac{J(K)}{p^n J(K)} \hookrightarrow \mathrm{Sel}_{p^n} J \subset \mathrm{H}^1(K, J[p^n]).$$

The inverse limit of these square diagrams yields

$$\widehat{J(K)} \hookrightarrow \mathrm{Sel}_{\mathbb{Z}_p} J \subset \mathrm{H}^1(K, T),$$

and inverting p yields

$$\widehat{J(K)}\left[\frac{1}{p}\right] \hookrightarrow \mathrm{Sel}_{\mathbb{Q}_p} J \subset \mathrm{H}^1(K, V).$$

Let Ш be the Shafarevich–Tate group of J. The standard exact sequence

$$0 \longrightarrow \frac{J(K)}{pJ(K)} \longrightarrow \mathrm{Sel}_p J \longrightarrow Ш[p] \longrightarrow 0$$

and its analogue for p^n lead to the exact sequence

$$0 \longrightarrow \widehat{J(K)}\left[\frac{1}{p}\right] \longrightarrow \mathrm{Sel}_{\mathbb{Q}_p} J \longrightarrow \left(\varprojlim Ш[p^n]\right)\left[\frac{1}{p}\right] \longrightarrow 0.$$

If $Ш[p^\infty]$ is finite, as is conjectured, then $\varprojlim Ш[p^n] = 0$, so $\widehat{J(K)}\left[\frac{1}{p}\right] \simeq \mathrm{Sel}_{\mathbb{Q}_p} J$.

We have now explained all of (2) except for the green terms and homomorphisms involving them.

2.6. **Crystalline representations and cohomology classes.** Let us temporarily forget X and J, and work with the following type of local Galois representation: a finite-dimensional $\mathbb{Q}_p$-vector space V with a continuous action of a local Galois group $\mathfrak{G}_{K_v}$, where $v|p$. Fontaine defined a certain ring B_{cris} equipped with a $\mathfrak{G}_{K_v}$-action, and then defined $D_{\mathrm{cris}}(V) := (B_{\mathrm{cris}} \otimes_{\mathbb{Q}_p} V)^{\mathfrak{G}_{K_v}}$; see [BC09] for an extended exposition. Then $\dim_{K_v} D_{\mathrm{cris}}(V) \le \dim_{\mathbb{Q}_p} V$, and V is called crystalline if equality holds.

Example 2.1. Fix an abelian variety A over K_v, where v is a finite place that may or may not divide p. Let V be the $\mathbb{Q}_p$ Tate module of A.

- For $v \nmid p$, the abelian variety A has good reduction if and only if V is unramified (Néron–Ogg–Shafarevich criterion).
- For $v|p$, the abelian variety A has good reduction if and only if V is *crystalline.*

The notion of crystalline can be extended to cohomology classes $\xi \in \mathrm{H}^1(K_v, V)$: the space of crystalline classes is

$$\mathrm{H}^1_f(K_v, V) := \ker\left(\mathrm{H}^1(K_v, V) \to \mathrm{H}^1(K_v, B_{\mathrm{cris}} \otimes_{\mathbb{Q}_p} V)\right).$$

For crystalline V, the following is an equivalent definition: a class $\xi \in \mathrm{H}^1(K_v, V)$ corresponds to an isomorphism class of extensions $0 \to V \to E \to \mathbb{Q}_p \to 0$, and ξ is crystalline if and only if E is crystalline.

Theorem 2.2 (Bloch–Kato)**.** *Let A be an abelian variety with good reduction over K_v, where $v|p$. Let V be the $\mathbb{Q}_p$ Tate module of A. Then the image of the injection $\widehat{A(K_v)}\left[\frac{1}{p}\right] \to \mathrm{H}^1(K_v, V)$ equals $\mathrm{H}^1_f(K_v, V)$.*

2.7. **The Bloch–Kato Selmer group.** Now let V be a global Galois representation: a finite-dimensional $\mathbb{Q}_p$-vector space with a continuous action of a global Galois group $\mathfrak{G}_K$. Given $\xi \in \mathrm{H}^1(K, V)$, let ξ_v be its image in $\mathrm{H}^1(K_v, V)$. Define the Bloch–Kato Selmer group $\mathrm{H}^1_f(K, V)$ as $\{\xi \in \mathrm{H}^1(K, V) : \xi_v \text{ is crystalline for every } v|p\}$.

Let us specialize this definition to the situation where J is an abelian variety over K with good reduction at all $v|p$, and V is its $\mathbb{Q}_p$ Tate module. Using Theorem 2.2, Bloch and Kato were able to prove that $\mathrm{H}^1_f(K, V)$ coincides with $\mathrm{Sel}_{\mathbb{Q}_p} J$ in $\mathrm{H}^1(K, V)$, and hence gives a Jacobian-free way to define the Selmer group.

Let $\mathrm{H}^1_{\mathrm{dR}}(X_{K_\mathfrak{p}})$ be the (algebraic) de Rham cohomology group; it is a finite-dimensional $K_\mathfrak{p}$-vector space equipped with a descending chain $\mathrm{Fil}^\bullet$ of subspaces called the Hodge filtration. Define the de Rham homology group $\mathrm{H}_1^{\mathrm{dR}}(X_{K_\mathfrak{p}})$ as the dual vector space with the dual filtration. Bloch and Kato showed that the $\mathbb{Q}_p$-linear isomorphism $\widehat{J(K_\mathfrak{p})}\left[\frac{1}{p}\right] \to \operatorname{Lie} J_{K_\mathfrak{p}}$ induced by log is isomorphic to a $\mathbb{Q}_p$-linear isomorphism $\mathrm{H}^1_f(K_\mathfrak{p}, V) \to \mathrm{H}_1^{\mathrm{dR}}(X_{K_\mathfrak{p}})/\mathrm{Fil}^0$ that can be defined without reference to J.

This completes the explanation of the diagram (2).

2.8. **Conclusion.** The upshot is that we obtain a diagram

$$\begin{tikzcd}
X(K) \arrow[r] \arrow[d] & X(K_\mathfrak{p}) \arrow[d] \arrow[dr, "p\text{-adic integrals}"] & \\
\mathrm{H}^1_f(K, V) \arrow[r] & \mathrm{H}^1_f(K_\mathfrak{p}, V) \arrow[r, "\simeq"] & \mathrm{H}_1^{\mathrm{dR}}(X_{K_\mathfrak{p}})/\mathrm{Fil}^0
\end{tikzcd} \tag{3}$$

that contains the same information as Chabauty's diagram (1) (at least if $\text{Ш}[p^\infty]$ is finite) and that is expressed purely in terms of X and its homology group V.

3. Kim's nonabelian generalization of Chabauty's method

3.1. **Lower central series.** Let G be a group (resp., topological group). For subgroups $A, B \subset G$, let (A, B) denote (the closure of) the subgroup generated by the elements $aba^{-1}b^{-1}$ for $a \in A$ and $b \in B$.

Define $C^1 G := G$ and $C^n G := (G, C^{n-1}G)$ for $n \geq 2$, where Then $(C^n G)$ is a descending chain of normal subgroups of G called the lower central series of G. Define the quotient $G_n = G/C^{n+1}G$. For example, $G_1 = G/C^2 G = G/(G,G)$ is the abelianization G^{ab} of G. For $n \geq 2$, the group G_n is an n-step nilpotent group that is typically nonabelian.

3.2. **The abelianized fundamental group.** A connected real manifold M equipped with a basepoint m has a fundamental group $\pi_1(M, m)$ and homology group $\mathrm{H}_1(M, \mathbb{Z})$, which are canonically related as follows: $\pi_1(M,m)^{\mathrm{ab}} \simeq \mathrm{H}_1(M, \mathbb{Z})$.

Now let us return to our genus g curve X over K, and assume that X is equipped with a K-point x. Then one can define the geometric étale fundamental group $\pi_1^{\mathrm{et}}(X_{\overline{K}}, x)$, a profinite group such that $\pi_1^{\mathrm{et}}(X_{\overline{K}}, x)^{\mathrm{ab}} \simeq \mathrm{H}_1^{\mathrm{et}}(X_{\overline{K}}, \widehat{\mathbb{Z}})$. Then
(4)
$$\pi_1^{\mathrm{et}}(X_{\overline{K}}, x)_1 = \pi_1^{\mathrm{et}}(X_{\overline{K}}, x)^{\mathrm{ab}} \simeq \mathrm{H}_1^{\mathrm{et}}(X_{\overline{K}}, \widehat{\mathbb{Z}}) \twoheadrightarrow \mathrm{H}_1^{\mathrm{et}}(X_{\overline{K}}, \mathbb{Z}_p) \subseteq \mathrm{H}_1^{\mathrm{et}}(X_{\overline{K}}, \mathbb{Q}_p) =: V = \mathcal{V}(\mathbb{Q}_p),$$
and $\mathfrak{G}_K$ acts continuously on all these groups; in particular, it acts via $\mathbb{Q}_p$-linear automorphisms on $\mathcal{V} \simeq \mathbb{G}_a^{2g}$.

3.3. **Deeper quotients of the fundamental group.** For $n \geq 2$, there is a construction analogous to that embodied in (4) that maps $\pi_1^{\mathrm{et}}(X_{\overline{K}}, x)_n$ to a topological group V_n that is the group of $\mathbb{Q}_p$-points of a unipotent algebraic group $\mathcal{V}_n$ over $\mathbb{Q}_p$ equipped with a $\mathfrak{G}_K$-action.

Kim generalized (3) to a diagram

(5)
$$\begin{tikzcd}
X(K) \arrow[r] \arrow[d] & X(K_\mathfrak{p}) \arrow[d] \arrow[dr, "p\text{-adic iterated integrals}"] & \\
\mathrm{H}^1_f(K, V_n) \arrow[r] & \mathrm{H}^1_f(K_\mathfrak{p}, V_n) \arrow[r, "\simeq"] & \pi_1^{\mathrm{dR}}(X_{K_\mathfrak{p}}, x)_n / \mathrm{Fil}^0
\end{tikzcd}$$

and interpreted the bottom row as being the maps on $\mathbb{Q}_p$-points for morphisms of $\mathbb{Q}_p$-varieties $\mathrm{Sel}^{[n]} \to J^{[n]} \xrightarrow{\sim} L^{[n]}$ (not group varieties for $n > 1$). For example, $\mathrm{Sel}^{[1]} \to J^{[1]}$ is simply a linear morphism between affine spaces over $\mathbb{Q}_p$.

Finally, $X(K_\mathfrak{p}) \to \pi_1^{\mathrm{dR}}(X_{K_\mathfrak{p}}, x)_n / \mathrm{Fil}^0$ is an analytic map whose image turns out to be Zariski dense in $L^{[n]}$; this implies the following generalization of Chabauty's theorem:

Theorem 3.1 (Kim). *If for some $n \geq 1$ we have*
$$\dim \mathrm{Sel}^{[n]} < \dim J^{[n]},$$

then $X(K)$ is contained in the set of zeros of some nonzero locally analytic function on $X(K_{\mathfrak{p}})$, so $X(K)$ is finite.

Various conjectures would imply that $\dim \mathrm{Sel}^{[n]} < \dim J^{[n]}$ holds for sufficiently large n, but this is not yet known in general.

This ends our introduction to Kim's nonabelian Chabauty method.

4. Faltings's finiteness theorem for Galois representations

We now begin assembling the ingredients needed for the method of Lawrence and Venkatesh.

Let K be a number field. Fix an algebraic closure $\overline{K}$ of K, and let $\mathfrak{G}_K := \mathrm{Gal}(\overline{K}/K)$. Let S be a finite set of places of K containing all archimedean places.

Theorem 4.1 (Hermite [Ser97, §4.1]). *Fix a number field K, a finite set of places S of K, and a positive integer d. Then the set of isomorphism classes of degree d field extensions of K unramified outside S is finite.*

For each nonarchimedean place v of K, let $\mathrm{Frob}_v \in \mathfrak{G}_K$ be a Frobenius automorphism, and let $I_v \subseteq \mathfrak{G}_K$ be the inertia subgroup associated to an extension of v to $\overline{K}$. Call a homomorphism h from $\mathfrak{G}_K$ to a group G **unramified outside** S if $h(I_v) = 1$ for all $v \notin S$.

Lemma 4.2 (Weak Chebotarev). *Given a number field K and a finite set of places S of K, for any discrete finite group G and continuous homomorphism $h\colon \mathfrak{G}_K \to G$ unramified outside S, there exists a finite set T of primes of K disjoint from S such that $\{\mathrm{Frob}_v : v \in T\}$ has the same image under h as the whole group $\mathfrak{G}_K$.*

Proof. Factor h as $\mathfrak{G}_K \twoheadrightarrow \mathrm{Gal}(L/K) \hookrightarrow G$, and apply the Chebotarev density theorem to the finite Galois extension $L \supseteq K$. □

Lemma 4.3 (Uniform weak Chebotarev). *Given a number field K, a finite set S of places of K, and a positive integer n, there exists a finite set T of primes of K disjoint from S such that for any discrete group G of order $\leq n$ and any continuous homomorphism $h\colon \mathfrak{G}_K \to G$ unramified outside S, the subset $\{\mathrm{Frob}_v : v \in T\}$ has the same image under h as the whole group $\mathfrak{G}_K$.*

Proof. By Theorem 4.1, there are only finitely many possible h up to isomorphism, say $h_i\colon \mathfrak{G}_K \to G_i$. Let T be as in Lemma 4.2 for the product $\prod h_i \colon \mathfrak{G}_K \to \prod G_i$. □

A $\mathbb{Z}_\ell$-**lattice** is a finite-dimensional $\mathbb{Q}_\ell$-vector space V is a finitely generated (hence free) $\mathbb{Z}_\ell$-submodule L such that $\mathbb{Q}_\ell L = V$.

Lemma 4.4. *Let $\mathfrak{G}$ be a compact topological group (e.g., any Galois group). Any finite dimensional $\mathbb{Q}_\ell$-representation V of $\mathfrak{G}$ contains a $\mathfrak{G}$-stable $\mathbb{Z}_\ell$-lattice.*

Proof. Let L_0 be any $\mathbb{Z}_\ell$-lattice in V. Let L be the $\mathbb{Z}_\ell$-span of the lattices gL_0 for all $g \in \mathfrak{G}$, so L is $\mathfrak{G}$-stable and $\mathbb{Q}_\ell L = V$.

The image of the compact space $\mathfrak{G} \times L_0$ under the action map $\mathfrak{G} \times V \to V$ is compact, hence contained in a finitely generated $\mathbb{Z}_\ell$-submodule M of V. By construction, $L \subseteq M$, so L is finitely generated too. $\square$

Lemma 4.5. *Given a number field K, a finite set of places S of K, a rational prime ℓ, and a nonnegative integer d, there exists a finite set of primes T of K disjoint from S such that if ρ and ρ' are d-dimensional $\mathbb{Q}_\ell$-representations of $\mathfrak{G}_K$ unramified outside S and $\operatorname{tr}\rho(\mathrm{Frob}_v) = \operatorname{tr}\rho'(\mathrm{Frob}_v)$ for all $v \in T$, then $\operatorname{tr}\rho(g) = \operatorname{tr}\rho'(g)$ for all $g \in \mathfrak{G}_K$.*

Proof. Let T be as in Lemma 4.3 with $n := \ell^{2d^2}$. Suppose that ρ and ρ' are d-dimensional $\mathbb{Q}_\ell$-representations of $\mathfrak{G}_K$ unramified outside S such that $\operatorname{tr}\rho(\mathrm{Frob}_v) = \operatorname{tr}\rho'(\mathrm{Frob}_v)$ for all $v \in T$.

By Lemma 4.4, we may assume that ρ and ρ' take values in $\mathrm{GL}_d(\mathbb{Z}_\ell)$. Let $R \subseteq \mathrm{M}_d(\mathbb{Z}_\ell) \times \mathrm{M}_d(\mathbb{Z}_\ell)$ be the $\mathbb{Z}_\ell$-module spanned by $\{(\rho(g), \rho'(g)) : g \in \mathfrak{G}_K\}$; in fact, R is a $\mathbb{Z}_\ell$-subalgebra. Let h be the composition

$$\mathfrak{G}_K \longrightarrow R^\times \longrightarrow (R/\ell R)^\times,$$

and for each $v \in T$, let $r_v \in R^\times$ and $r_{v,\ell} \in (R/\ell R)^\times$ denote the images of Frob_v:

$$\mathrm{Frob}_v \longmapsto r_v \longmapsto r_{v,\ell}.$$

(i) We have $\#(R/\ell R)^\times \le n$. (Proof: As a $\mathbb{Z}_\ell$-module, $\mathrm{M}_d(\mathbb{Z}_\ell) \times \mathrm{M}_d(\mathbb{Z}_\ell)$ is free of rank $2d^2$, so R is free of rank $\le 2d^2$, so $\#(R/\ell R)^\times \le \#(R/\ell R) \le \ell^{2d^2} = n$.)

(ii) The homomorphism h is unramified outside S. (Proof: $(\rho, \rho') \colon \mathfrak{G}_K \to R^\times$ is unramified outside S.)

(iii) The set $\{r_{v,\ell} : v \in T\}$ equals $h(\mathfrak{G}_K)$, which spans $R/\ell R$ as an $\mathbb{F}_\ell$-vector space. (Proof: By (i) and (ii), the T in Lemma 4.3 is such that $\{r_{v,\ell} : v \in T\} = h(\mathfrak{G}_K)$. The image of $\mathfrak{G}_K \to R^\times$ spans R as a $\mathbb{Z}_\ell$-module by construction, so the image $h(\mathfrak{G}_K)$ of $\mathfrak{G}_K \to (R/\ell R)^\times$ spans $R/\ell R$ as an $\mathbb{F}_\ell$-vector space.)

(iv) The set $\{r_v : v \in T\}$ spans R as a $\mathbb{Z}_\ell$-module. (Proof: Combine (iii) with Nakayama's lemma.)

By hypothesis on ρ and ρ', each r_v has the property that its two projections in $\mathrm{M}_d(\mathbb{Z}_\ell)$ have the same trace. Since the r_v span R, *every* element of R has this property. In particular, if $g \in \mathfrak{G}_K$, then $(\rho(g), \rho'(g))$ has the property; i.e., $\operatorname{tr}\rho(g) = \operatorname{tr}\rho'(g)$. $\square$

Corollary 4.6. *In the setting of Lemma 4.5, if in addition ρ and ρ' are semisimple, then $\rho \simeq \rho'$.*

Proof. Over a characteristic 0 field, such as $\mathbb{Q}_\ell$, a semisimple representation is determined by its trace. $\square$

Let ρ be a $\mathbb{Q}_\ell$-representation of $\mathfrak{G}_K$ unramified outside S. Call ρ pure of weight i if for every $v \notin S$, every eigenvalue of $\rho(\mathrm{Frob}_v)$ is an algebraic integer all of whose conjugates have complex absolute value $q_v^{i/2}$, where q_v is the size of the residue field at v.

Theorem 4.7 (Faltings)**.** *Fix a number field K, a finite set S of places of K, a rational prime ℓ, a nonnegative integer d, and an integer i. Then the set of equivalence classes of semisimple d-dimensional $\mathbb{Q}_\ell$-representations ρ of $\mathfrak{G}_K$ that are unramified outside S and pure of weight i is finite.*

Proof. Let T be as in Lemma 4.5. If ρ is pure of weight i and $v \notin S$, then there are only finitely many possibilities for the eigenvalues of $\rho(\mathrm{Frob}_v)$, so there is a finite set $Z_v \subseteq \mathbb{Q}_\ell$ that contains all possibilities for $\operatorname{tr}\rho(\mathrm{Frob}_v)$. By Corollary 4.6, $\rho \mapsto (\operatorname{tr}\rho(\mathrm{Frob}_v))_{v\in T}$ defines an *injection* from the set of classes of representations in question to the finite set $\prod_{v\in T} Z_v$. $\square$

5. Cohomology theories

Let K be any field. Let X be a smooth proper variety over K. Let i be a nonnegative integer.

5.1. **Betti cohomology.** If $K = \mathbb{C}$, one has the Betti cohomology group (also called singular cohomology group) $\mathrm{H}^i_B(X(\mathbb{C}), \mathbb{Z})$. It is a finitely generated $\mathbb{Z}$-module.

5.2. **Étale cohomology.** Choose a prime $\ell \neq \operatorname{char} K$. After base changing X to $\overline{K}$ (to have a geometric object more analogous to a variety over $\mathbb{C}$), one forms the étale cohomology group (also called ℓ-adic cohomology group) $\mathrm{H}^i_{\mathrm{et}}(X_{\overline{K}}, \mathbb{Z}_\ell)$. It is a finitely generated $\mathbb{Z}_\ell$-module equipped with a continuous $\mathfrak{G}_K$-action.

5.3. **De Rham cohomology.** Define $\mathrm{H}^i_{\mathrm{dR}}(X) := \mathbb{H}^i(X, \Omega^\bullet)$ (hypercohomology of the algebraic de Rham complex). This is a finite-dimensional K-vector space equipped with a descending filtration

$$\mathrm{Fil}^0\,\mathrm{H}^i_{\mathrm{dR}}(X) \supseteq \mathrm{Fil}^1\,\mathrm{H}^i_{\mathrm{dR}}(X) \supseteq \mathrm{Fil}^2\,\mathrm{H}^i_{\mathrm{dR}}(X) \supseteq \cdot$$

of subspaces called the Hodge filtration. We have $\mathrm{Fil}^0\,\mathrm{H}^i_{\mathrm{dR}}(X) = \mathrm{H}^i_{\mathrm{dR}}(X)$, and $\mathrm{Fil}^p\,\mathrm{H}^i_{\mathrm{dR}}(X) = 0$ if p is sufficiently large.

5.4. **Crystalline cohomology.** Suppose that K is a perfect field of characteristic p. Let $W := W(K)$ be the ring of Witt vectors, which is the unique complete discrete valuation ring with residue field K and maximal ideal (p). There is a Frobenius automorphism $F\colon W \to W$, but it is not the pth power map. For example, if $K = \mathbb{F}_{p^n}$, and L_n is the degree n unramified extension of $\mathbb{Q}_p$, and σ is the automorphism in $\mathrm{Gal}(L_n/\mathbb{Q}_p)$ inducing the pth power map on the residue field $\mathbb{F}_{p^n}$, then W is the valuation ring of L_n and $F = \sigma|_W$. A semilinear operator ϕ on a W-module H is a homomorphism of abelian groups $\phi\colon H \to H$ such that $\phi(av) = F(a)\,\phi(v)$ for all $a \in W$ and $v \in H$. (Linear would mean $\phi(av) = a\,\phi(v)$ instead.)

Sheaf cohomology on the crystalline site lets one define $\mathrm{H}^i_{\mathrm{cris}}(X/W)$. This is a finitely generated W-module equipped with a semilinear operator ϕ called Frobenius (because it is induced by the absolute Frobenius morphism of X).

6. Comparisons

Remark 6.1 (Changing the coefficient ring). If a cohomology theory $\mathrm{H}^i_\bullet(X, R)$ above produces an R-module, and R' is a flat R-algebra (e.g., a field extension of $\operatorname{Frac} R$), then it is reasonable to define $\mathrm{H}^i_\bullet(X, R')$ as $R' \otimes_R \mathrm{H}^i_\bullet(X, R)$ if it is not already defined directly.

6.1. **Étale and Betti.** If $K = \mathbb{C}$, then $\mathrm{H}^i_{\mathrm{et}}(X, \mathbb{Z}_\ell) \simeq \mathrm{H}^i_B(X(\mathbb{C}), \mathbb{Z}_\ell)$. (As explained above, $\mathrm{H}^i_B(X(\mathbb{C}), \mathbb{Z}_\ell) = \mathbb{Z}_\ell \otimes \mathrm{H}^i_B(X(\mathbb{C}), \mathbb{Z})$.)

6.2. **De Rham and Betti.** If $K = \mathbb{C}$, then integration of differential forms defines an isomorphism $\mathrm{H}^i_{\mathrm{dR}}(X) \xrightarrow{\sim} \mathrm{H}^i_B(X(\mathbb{C}), \mathbb{C})$.

6.3. **Étale, de Rham, and crystalline.** Let K be a finite unramified extension of $\mathbb{Q}_p$. Let $\mathcal{O}$ be its valuation ring. Let k be its residue field. Thus k is a finite field, and $\mathcal{O} \simeq W(k)$.

A filtered ϕ-module over K is a triple $(D, \phi, \mathrm{Fil}^\bullet)$, consisting of a finite-dimensional K-vector space D, a semilinear map $\phi\colon D \to D$ and a descending filtration $\mathrm{Fil}^\bullet$ of subspaces of D indexed by integers such that $\mathrm{Fil}^i = D$ for $i \ll 0$ and $\mathrm{Fil}^i = 0$ for $i \gg 0$.

Let $\mathrm{Rep}_{\mathbb{Q}_p}(\mathfrak{G}_K)$ be the category of finite-dimensional $\mathbb{Q}_p$-vector spaces equipped with a continuous $\mathfrak{G}_K$-action. Let MF^ϕ_K denote the category of filtered ϕ-modules. Then there exists a functor

$$\begin{aligned} D_{\mathrm{cris}}\colon \mathrm{Rep}_{\mathbb{Q}_p}(\mathfrak{G}_K) &\to \mathrm{MF}^\phi_K \\ V &\mapsto (B_{\mathrm{cris}} \otimes_{\mathbb{Q}_p} V)^{\mathfrak{G}_K}. \end{aligned}$$

(This is the same functor as in Section 2.6, although there we were not concerned with the semilinear operator and filtration on the output.) Recall that $\dim_K D_{\mathrm{cris}}(V) \le \dim_{\mathbb{Q}_p} V$, and that V is called crystalline if equality holds. Let $\mathrm{Rep}^{\mathrm{cris}}_{\mathbb{Q}_p}(\mathfrak{G}_K) \subseteq \mathrm{Rep}_{\mathbb{Q}_p}(\mathfrak{G}_K)$ denote the full subcategory of crystalline representations.

Theorem 6.2.

(a) *The functor D_{cris} restricts to a fully faithful functor $\mathrm{Rep}^{\mathrm{cris}}_{\mathbb{Q}_p}(\mathfrak{G}_K) \hookrightarrow \mathrm{MF}^\phi_K$.*

(b) *If X is a smooth proper $\mathcal{O}$-scheme, then*

  (i) *The representation $\mathrm{H}^i_{\mathrm{et}}(X_{\overline{K}}, \mathbb{Q}_p)$ is crystalline.*

(ii) *There is a canonical isomorphism* $\mathrm{H}^i_{\mathrm{dR}}(X_K) \simeq \mathrm{H}^i_{\mathrm{cris}}(X_k/K)$ *of* K*-vector spaces, making either vector space into a filtered* ϕ*-module (the filtration is the Hodge filtration on* $\mathrm{H}^i_{\mathrm{dR}}(X_K)$*, and the* ϕ *is the Frobenius on* $\mathrm{H}^i_{\mathrm{cris}}(X_k/K)$*).*

(iii) *The functor* D_{cris} *maps* $\mathrm{H}^i_{\mathrm{et}}(X_{\overline{K}}, \mathbb{Q}_p)$ *to* $\mathrm{H}^i_{\mathrm{dR}}(X_K) \simeq \mathrm{H}^i_{\mathrm{cris}}(X_k/K)$*.*

7. Cohomology in a family; period maps

Let B be a smooth variety over a field K. Let $f\colon X \to B$ be a smooth proper morphism. For each $b \in B$, the fiber $X_b := f^{-1}(b)$ is a smooth proper variety (over the residue field of b).

In the following table, each entry in the first column refers to a single variety Z, and each entry in the second column is the analogue for a family $f\colon X \to B$.

$\Gamma(Z, -)$	f_*
$\mathrm{H}^i(Z, -)$	$\mathrm{R}^i f_*$
$\mathbb{H}^i(Z, -)$	$\mathbb{R}^i f_*$
$\mathrm{H}^i_{\mathrm{dR}}(Z)$	$\mathbb{R}^i f_* \Omega^\bullet_{X/B}$.

The relative de Rham cohomology $\mathbb{R}^i f_* \Omega^\bullet_{X/B}$ is a vector bundle on B whose fiber above each point b is the de Rham cohomology group $\mathrm{H}^i_{\mathrm{dR}}(X_b)$.

7.1. Complex setting.

Let $K = \mathbb{C}$. Let $\Omega \subset B(\mathbb{C})$ be a simply connected open subset. Normally, given a vector bundle on B, there is no canonical way to identify the nearby fibers (fibers above points of Ω). But for $\mathbb{R}^i f_* \Omega^\bullet_{X/B}$ there is a way, which admits two descriptions:

7.1.1. *Description 1.* Ehresmann's theorem says that $f^{-1}\Omega \to \Omega$ viewed a map of C^∞ manifolds is diffeomorphic to a constant family $X_0 \times \Omega \to \Omega$, so the spaces $\mathrm{H}^i_B(X_b(\mathbb{C}), \mathbb{C})$ for $b \in \Omega$ are canonically identified — the fancy way to say this is to say that $\mathrm{R} f_* \underline{\mathbb{C}}$ is a local system of $\mathbb{C}$-vector spaces on B. By comparison, it follows that $\mathrm{H}^i_{\mathrm{dR}}(X_b)$ for $b \in \Omega$ are canonically identified as vector spaces (without filtration).

7.1.2. *Description 2.* The operator d on differential forms induces a rule for taking directional derivatives of sections of $\mathbb{R}^i f_* \Omega^\bullet_{X/B}$. The fancy way to say this is to say that the vector bundle $\mathbb{R}^i f_* \Omega^\bullet_{X/B}$ comes equipped with a connection ∇, called the Gauss–Manin connection — this connection is algebraic, defined over K; it is also integrable (i.e., flat): see [KO68]. A section s of $\mathbb{R}^i f_* \Omega^\bullet_{X/B}$ is called horizontal if $\nabla s = 0$. If a local basis of the vector bundle is chosen, then $\nabla s = 0$ amounts to a system of linear differential equations whose coefficients are algebraic functions on B; because the connection is integrable, there exists a basis of *analytic* solutions on Ω. Fibers above points of Ω can be identified by following these horizontal sections.

7.1.3. *Equality of descriptions.* It turns out that the two descriptions give the *same* identification of fibers.

7.1.4. *Period map.* As hinted above, the identification does not respect the fiberwise Hodge filtrations $\operatorname{Fil}^\bullet$. To measure the variation of the Hodge filtration, fix a point $0 \in \Omega$, let $\mathcal{F}$ be the flag variety parametrizing chains of subspaces in $\mathrm{H}^i_{\mathrm{dR}}(X_0)$ of dimensions agreeing with the spaces in $\operatorname{Fil}^\bullet \mathrm{H}^i_{\mathrm{dR}}(X_0)$, and define the complex period map

$$\begin{aligned} \Omega &\stackrel{\mathrm{Period}_{\mathbb{C}}}{\longrightarrow} \mathcal{F}(\mathbb{C}) \\ b &\longmapsto \left(\operatorname{Fil}^\bullet \mathrm{H}^i_{\mathrm{dR}}(X_b) \text{ transported to } \mathrm{H}^i_{\mathrm{dR}}(X_0)\right). \end{aligned}$$

This is an analytic map.

Remark 7.1. If $X \to B$ is defined over a subfield of $K \subseteq \mathbb{C}$ and $0 \in B(K)$, then $\mathcal{F}$ is a K-variety and $\mathrm{Period}_{\mathbb{C}}$ near 0 is given by power series with coefficients in K, because ∇ is defined over K.

7.2. ***p*-adic setting.** Let K_v be a finite unramified extension of $\mathbb{Q}_p$. Let $\mathcal{O}_v$ be its valuation ring. Let k_v be its residue field. Let B be a smooth scheme over $\mathcal{O}_v$. Let $\bar{0} \in B(k_v)$. Let $\Omega_v = \{b \in B(\mathcal{O}_v) \text{ reducing to } \bar{0}\}$. Fix $0 \in \Omega_v$. Again we have a canonical identification of the fibers of $\mathbb{R}^i f_* \Omega^\bullet_{X/B}$ above K-points in Ω_v, as we now explain.

7.2.1. *Description 1.* The K_v-vector spaces $\mathrm{H}^i_{\mathrm{dR}}(X_b)$ for $b \in \Omega_v$ are canonically identified since they are all canonically isomorphic to $\mathrm{H}^i_{\mathrm{cris}}(X_{\bar{0}}/K_v)$.

7.2.2. *Description 2.* Use p-adic analytic solutions to $\nabla s = 0$.

7.2.3. *Equality of descriptions.* Again it turns out that the two descriptions give the *same* identification of fibers.

7.2.4. *Period map.* Define the p-adic period map

$$\begin{aligned} \Omega_v &\stackrel{\mathrm{Period}_v}{\longrightarrow} \mathcal{F}(K_v) \\ b &\longmapsto \left(\operatorname{Fil}^\bullet \mathrm{H}^i_{\mathrm{dR}}(X_b) \text{ transported to } \mathrm{H}^i_{\mathrm{dR}}(X_0)\right). \end{aligned}$$

This is a p-adic analytic map.

7.3. **Comparison.** If $X \to B$ is over a ring of S-integers $\mathcal{O}_{K,S}$ in a number field K, then $\mathrm{Period}_{\mathbb{C}}$ and Period_v both come from the formal solutions to $\nabla s = 0$, so they are given by the same power series with coefficients in K. It follows that the Zariski closures $(\operatorname{im} \mathrm{Period}_{\mathbb{C}})^{\mathrm{Zar}}$ and $(\operatorname{im} \mathrm{Period}_v)^{\mathrm{Zar}}$ in $\mathcal{F}$ are equal.

8. Rational/integral points and period maps

8.1. **General setup.** Let K be a number field. Let S be a finite set of places of K containing all archimedean places and all ramified places. Let $\mathcal{O} := \mathcal{O}_{K,S}$, the ring of S-integers in K. Let $v \notin S$. Let K_v be the completion of K at v. Let $\mathcal{O}_v$ be the valuation ring in K_v. Let k_v be the residue field of $\mathcal{O}_v$. Let Y be a smooth separated finite-type $\mathcal{O}$-scheme such that Y_K

is a smooth geometrically integral curve that is hyperbolic, meaning that $\chi(Y_K) < 0$ (if $Y_{\overline{K}}$ is expressed as a smooth projective curve of genus g minus r points, then $\chi(Y_K) := 2 - 2g - r$).

The goal is to prove that $Y(\mathcal{O})$ is finite. It suffices to consider one residue disk in $Y(\mathcal{O}_v)$ at a time, so without loss of generality, remove all but one k_v-point from Y; now $Y(\mathcal{O}_v)$ is a single residue disk. Assume that $y_0 \in Y(\mathcal{O})$.

8.2. **Rough strategy.**

1. Choose a smooth proper family $f\colon X \to Y$ and a nonnegative integer i.
2. For each $y \in Y(\mathcal{O})$, we get $V_y := \mathrm{H}^i_{\mathrm{et}}((X_y)_{\overline{K}}, \mathbb{Q}_p) \in \mathrm{Rep}_{\mathbb{Q}_p}(\mathfrak{G}_K)$.
3. Use Faltings's finiteness theorem for semisimple Galois representations to prove that there are only finitely many possibilities for the isomorphic type of V_y. (One challenge here is that we do not know a priori that the V_y are semisimple.)
4. Prove that V_y varies enough with y (even when restricted to a representation of $\mathfrak{G}_{K_v}$) that each isomorphism type arises from only finitely many y.

8.3. **Additional notation.** Let $V := \mathrm{H}^i_{\mathrm{dR}}((X_{y_0})_{K_v})$; this is a finite-dimensional K_v-vector space, and it has a Frobenius operator ϕ and Hodge filtration $\mathrm{Fil}^\bullet$. Let $d := \dim_{K_v} V$, which also equals $\dim_{\mathbb{Q}_p} V_y$ for any $y \in Y(\mathcal{O}_v)$.

Let $Y(\mathcal{O})^{\mathrm{ss}} := \{y \in Y(\mathcal{O}) : V_y \text{ is semisimple}\}$.

Let $\mathrm{Rep}^{\text{cris at } v}_{\mathbb{Q}_p}(\mathfrak{G}_K)$ be the category of $\mathbb{Q}_p$-representations of $\mathfrak{G}_K$ that are crystalline at v (i.e., the restriction to $\mathfrak{G}_{K_v}$ is crystalline). Let $\mathrm{Rep}^{\mathrm{Faltings}}_{\mathbb{Q}_p}(\mathfrak{G}_K)$ be the category of semisimple d-dimensional $\mathbb{Q}_p$-representations of $\mathfrak{G}_K$ that are unramified and pure of weight i outside S and crystalline at v.

Let $\mathrm{MF}^{\phi,\mathrm{framed}}_{K_v}$ be the category of tuples $(D, \varphi, \mathrm{Fil}^\bullet, \iota)$ where $(D, \varphi, \mathrm{Fil}^\bullet) \in \mathrm{MF}^{\phi}_{K_v}$ and the "framing" $\iota\colon (D, \varphi) \xrightarrow{\sim} (V, \phi)$ is a K_v-linear isomorphism $D \to V$ under which φ and ϕ correspond.

8.4. **The big diagram.** One should interpret each category in the following commutative diagram as its set of isomorphism classes.

(6)

$$\begin{tikzcd}
Y(\mathcal{O})^{\mathrm{ss}} \arrow[r, hook] \arrow[dd, "\mathrm{H}^i_{\mathrm{et}}"'] & Y(\mathcal{O}) \arrow[rr, hook] \arrow[dd, "\mathrm{H}^i_{\mathrm{et}}"'] & & Y(\mathcal{O}_v) \arrow[d, "\mathrm{H}^i_{\mathrm{dR}}+\mathrm{GM}"] \arrow[ddl, bend right, "\mathrm{H}^i_{\mathrm{et}}"'] \arrow[dr, bend left, "\mathrm{Period}_v"] & \\
& & & \mathrm{MF}^{\phi,\mathrm{framed}}_{K_v} \arrow[r] \arrow[d, "\text{forget frame}"] & \mathcal{F}(K_v) \\
\mathrm{Rep}^{\mathrm{Faltings}}_{\mathbb{Q}_p}(\mathfrak{G}_K) \arrow[r, hook] & \mathrm{Rep}^{\text{cris at v}}_{\mathbb{Q}_p}(\mathfrak{G}_K) \arrow[r] & \mathrm{Rep}^{\mathrm{cris}}_{\mathbb{Q}_p}(\mathfrak{G}_{K_v}) \arrow[r, hook, "D_{\mathrm{cris}}"] & \mathrm{MF}^{\phi}_{K_v} . &
\end{tikzcd}$$

The first two maps labelled $\mathrm{H}^i_{\mathrm{et}}$ send y to $\mathrm{H}^i_{\mathrm{et}}((X_y)_{\overline{K}}, \mathbb{Q}_p)$; the third sends y to $\mathrm{H}^i_{\mathrm{et}}((X_y)_{\overline{K}_v}, \mathbb{Q}_p)$. The map $\mathrm{H}^i_{\mathrm{dR}} + \mathrm{GM}$ sends y to $(\mathrm{H}^i_{\mathrm{dR}}(X_y), \varphi, \mathrm{Fil}^\bullet, \mathrm{GM})$, where φ is the Frobenius operator coming from comparison with $\mathrm{H}^i_{\mathrm{cris}}((X_y)_{k_v}/K_v)$, and $\mathrm{Fil}^\bullet$ is the Hodge filtration, and GM is the isomorphism $\mathrm{H}^i_{\mathrm{dR}}(X_y) \to V = \mathrm{H}^i_{\mathrm{dR}}((X_{y_0})_{K_v})$ coming from the Gauss–Manin connection. The map $\mathrm{MF}^{\phi,\mathrm{framed}}_{K_v} \to \mathcal{F}(K_v)$ takes $(D, \varphi, \mathrm{Fil}^\bullet, \iota)$ to the filtration $\iota(\mathrm{Fil}^\bullet)$ of V.

Let $\mathrm{Aut}(V, \phi)$ be the set of K_v-linear automorphisms of V that commute with the operator ϕ. Let $\Phi = \phi^{[K_v:\mathbb{Q}_p]}$, so $\mathrm{Aut}(V, \phi) \subseteq \mathrm{Aut}(V, \Phi)$. Then Φ is K_v-linear, so $\mathrm{Aut}(V, \Phi)$ is (the set of K_v-points of) an algebraic subgroup of $\mathrm{GL}(V)$.

The group $\mathrm{Aut}(V, \phi)$ acts on $\mathrm{MF}^{\phi,\mathrm{framed}}_K$; namely, α maps $(D, \varphi, \mathrm{Fil}^\bullet, \iota)$ to $(D, \varphi, \mathrm{Fil}^\bullet, \alpha\iota)$. The group $\mathrm{GL}(V)$ acts on $\mathcal{F}(K_v)$; namely $g \in \mathrm{GL}(V)$ maps $(\mathrm{Fil}^j)_{j\in\mathbb{Z}}$ to $(g\,\mathrm{Fil}^j)_{j\in\mathbb{Z}}$. These two actions are compatible with respect to the map $\mathrm{MF}^{\phi,\mathrm{framed}}_K \to \mathcal{F}(K_v)$ and inclusion $\mathrm{Aut}(V, \phi) \subseteq \mathrm{GL}(V)$.

Each nonempty fiber of the "forget frame" map is an $\mathrm{Aut}(V, \phi)$-orbit in $\mathrm{MF}^{\phi,\mathrm{framed}}_{K_v}$, and such an orbit maps into an $\mathrm{Aut}(V, \Phi)$-orbit in $\mathcal{F}(K_v)$. Thus the diagram shows

Proposition 8.1. *The set $Y(\mathcal{O})^{\mathrm{ss}}$ is mapped by Period_v into finitely many $\mathrm{Aut}(V, \Phi)$-orbits in $\mathcal{F}(K_v)$.*

Proof. By Theorem 4.7, $\mathrm{Rep}^{\mathrm{Faltings}}_{\mathbb{Q}_p}(\mathfrak{G}_K)$ has only finitely many isomorphism classes. The diagram (6) then shows that the image of $Y(\mathcal{O})^{\mathrm{ss}}$ in $\mathrm{MF}^{\phi}_{K_v}$ is finite, so the image of $Y(\mathcal{O})^{\mathrm{ss}}$ in $\mathrm{MF}^{\phi,\mathrm{framed}}_{K_v}$ is contained in finitely many $\mathrm{Aut}(V, \phi)$-orbits, and these map into finitely many $\mathrm{Aut}(V, \Phi)$-orbits in $\mathcal{F}(K_v)$. $\square$

Corollary 8.2. *If $\dim_{K_v} \mathrm{Aut}(V, \Phi) < \dim \mathrm{im}(\mathrm{Period}_v)^{\mathrm{Zar}}$, then $Y(\mathcal{O})^{\mathrm{ss}}$ is contained in the set of zeros of some nonzero analytic function on $Y(\mathcal{O}_v)$, and hence is finite.*

8.5. **Period maps and the monodromy group.** Let $\widetilde{Y(\mathbb{C})}$ be the universal cover of $Y(\mathbb{C})$. Analytically continue $\mathrm{Period}_{\mathbb{C}} \colon \Omega \to \mathcal{F}(\mathbb{C})$ to obtain $\widetilde{\mathrm{Period}}_{\mathbb{C}} \colon \widetilde{Y(\mathbb{C})} \to \mathcal{F}(\mathbb{C})$. Let $V_{\mathbb{C}} = \mathrm{H}^i_B(X_{y_0}(\mathbb{C}), \mathbb{C}) \simeq \mathrm{H}^i_{\mathrm{dR}}(X_{y_0,\mathbb{C}})$. If γ is a loop in $Y(\mathbb{C})$ based at y_0, then following horizontal sections above γ gives a $\mathbb{C}$-linear identification of $V_{\mathbb{C}}$ with itself, i.e., an element of $\mathrm{GL}(V_{\mathbb{C}})$, and this defines the monodromy representation $\pi_1(Y, y_0) \to \mathrm{GL}(V_{\mathbb{C}})$. The Zariski closure of the image of this representation is called the monodromy group Γ. We obtain a commutative diagram

$$\begin{tikzcd}
\pi_1(Y, y_0) \arrow[r] \arrow[d, hook] & \Gamma \subseteq \mathrm{GL}(V_{\mathbb{C}}) \arrow[d] \\
\widetilde{Y(\mathbb{C})} \arrow[r, "\widetilde{\mathrm{Period}}_{\mathbb{C}}"] & \mathcal{F}(\mathbb{C}),
\end{tikzcd}$$

in which the right vertical map sends $g \in \mathrm{GL}(V_{\mathbb{C}})$ to $g(\mathrm{Fil}^\bullet V_{\mathbb{C}})$.

Now

$$\mathrm{im}(\mathrm{Period}_v)^{\mathrm{Zar}} = \mathrm{im}(\mathrm{Period}_{\mathbb{C}})^{\mathrm{Zar}} = \mathrm{im}(\widetilde{\mathrm{Period}}_{\mathbb{C}})^{\mathrm{Zar}} \supseteq (\Gamma.\, \mathrm{Fil}^\bullet V_{\mathbb{C}})^{\mathrm{Zar}}.$$

Combining this with Corollary 8.2 yields

Corollary 8.3. *If* $\dim_{K_v} \operatorname{Aut}(V, \Phi) < \dim \left(\Gamma. \operatorname{Fil}^\bullet V_{\mathbb{C}}\right)^{\mathrm{Zar}}$*, then* $Y(\mathcal{O})^{\mathrm{ss}}$ *is finite.*

9. The S-unit equation

9.1. **Setup.** Now we specialize to the case $Y = \mathbb{P}^1 - \{0, 1, \infty\}$, which is isomorphic to the curve $t + u = 1$ in $\mathbb{G}_m \times \mathbb{G}_m$. (More formally, $Y = \operatorname{Spec} \mathcal{O}[t, 1/t, 1/(t-1)]$.) The goal is the following:

Theorem 9.1. *The set* $Y(\mathcal{O}) = \{t \in \mathcal{O}^\times : 1 - t \in \mathcal{O}^\times\}$ *is finite.*

We may assume that $y_0 \in Y(\mathcal{O})$; identify this point with a number $t_0 \in \mathcal{O}^\times$.

9.2. **First attempt.** Let $X \to Y$ be the Legendre family of elliptic curves, whose fiber above t is the elliptic curve $E_t \colon y^2 = x(x-1)(x-t)$ (i.e., the smooth projective model of this affine curve). Let $i = 1$. Then $\dim V = 2$.

9.2.1. *Left hand side.* On the left of the inequality in Corollary 8.3 is $\dim \operatorname{Aut}(V, \Phi)$, which could be as large as 4 (e.g., if $\Phi = -p$, which could happen if the mod p reduction of E_{t_0} is a supersingular elliptic curve over $\mathbb{F}_{p^2}$).

9.2.2. *Right hand side.* On the right is $\dim \left(\Gamma. \operatorname{Fil}^\bullet V_{\mathbb{C}}\right)^{\mathrm{Zar}}$, which is at most 1, since the Zariski closure is taken inside $\mathcal{F} = \{\text{1-dimensional subspaces of } V\} \simeq \mathbb{P}^1$. In fact, the image of the monodromy representation $\pi_1(Y(\mathbb{C}), t_0) \to \mathrm{GL}(V_{\mathbb{C}}) = \mathrm{GL}_2(\mathbb{C})$ is a finite-index subgroup of $\mathrm{SL}_2(\mathbb{Z})$, so $\Gamma = \mathrm{SL}_2$ and $\dim \left(\Gamma. \operatorname{Fil}^\bullet V_{\mathbb{C}}\right)^{\mathrm{Zar}} = 1$.

9.2.3. *Conclusion.* The inequality $4 < 1$ does not hold, so we cannot apply Corollary 8.3 to deduce finiteness. We need to start over with a different family $X \to Y$.

9.3. **Second attempt.** Choose $m \geq 1$, and let $Y' = \mathbb{P}^1 - \{0, \mu_m, \infty\}$ be the inverse image of Y under the mth power map $\mathbb{P}^1 \to \mathbb{P}^1$. Let z be the coordinate on Y', so $z^m = t$. Let $X \to Y'$ be the family whose fiber above $z \in Y'$ is E_z. Thus the fiber X_t of the composition $X \to Y' \to Y$ above t is a smooth proper geometrically *disconnected* curve with $(X_t)_{\overline{K}} = \coprod_{z^m = t} E_z$.

The group $\mu_{2^\infty}(K)$ of roots of unity of 2-power order in K is a finite cyclic group. Let m be its order, and let ζ be a generator. Without loss of generality, enlarge K and S (this only makes $Y(\mathcal{O})$ larger) so that $m \geq 8$ and S contains all the places above 2 and ∞, and all the places ramified in $K/\mathbb{Q}$.

Let $U := \{t \in Y(\mathcal{O}) : t \notin K^{\times 2}\}$.

Lemma 9.2. *We have* $Y(\mathcal{O}) = U \cup U^2 \cup U^4 \cup \cdots \cup U^m$.

Proof. First, if $t, 1 - t \in \mathcal{O}^\times$ and $\sqrt{t} \in K$, then $\sqrt{t}, 1 - \sqrt{t} \in \mathcal{O}^\times$ too, because $1 - t = (1 + \sqrt{t})(1 - \sqrt{t})$. Let $t \in Y(\mathcal{O})$.

- If $t^{1/m} \notin K$, then repeatedly taking square roots until no longer possible shows that $t \in U \cup U^2 \cup \cdots \cup U^{m/2}$.
- If $t^{1/m} \in K$, then $t = (t^{1/m})^m = (\zeta t^{1/m})^m$, and either $t^{1/m}$ or $\zeta t^{1/m}$ is in U (since $\zeta \notin K^{\times 2}$). $\square$

By Lemma 9.2, it will suffice to prove that U is finite. We may also assume that U is nonempty, so assume $t_0 \in U$.

By Hermite's theorem (Theorem 4.1), there are only finitely many possibilities for the field $K(t^{1/m})$ as t ranges over U. Therefore it will suffice to fix one of them, say L, and prove that the set of $t \in U$ such that $K(t^{1/m}) \simeq L$ is finite. Since $t \notin K^{\times 2}$, the field L is a Kummer extension of K, with $\operatorname{Gal}(L/K) \simeq \mathbb{Z}/m\mathbb{Z}$.

Choose a place $v \notin S$ such that Frob_v is a generator of $\operatorname{Gal}(L/K)$. Then v is inert in L/K, and the completion L_v at the place of L above v is a $\mathbb{Z}/m\mathbb{Z}$-extension of K_v.

9.3.1. *Left hand side.* Let $V = \mathrm{H}^1_{\mathrm{dR}}((X_{t_0})_{K_v})$. Then V is a $2m$-dimensional K_v-vector space with K_v-linear operator Φ, but $(X_{t_0})_{K_v}$ can also be viewed as an elliptic curve over L_v, so V can also be viewed as a 2-dimensional L_v-vector space $\mathcal{V}$ with L_v-linear operator Φ^m. An elementary linear algebra lemma (Lemma 2.1 in [LV18]) shows that $\dim_{K_v} \operatorname{Aut}(V, \Phi) = \dim_{L_v} \operatorname{Aut}(\mathcal{V}, \Phi^m)$, and the latter is at most $\dim_{L_v} \mathrm{GL}_2(L_v) = 4$.

9.3.2. *Right hand side.* A monodromy calculation (Lemma 4.3 in [LV18]) shows that the image of the monodromy representation contains a finite index subgroup of $\prod_{z^m=t_0} \mathrm{SL}_2(\mathbb{Z}) \subseteq \mathrm{GL}\left(\bigoplus_{z^m=t_0} \mathrm{H}^1(E_z(\mathbb{C}), \mathbb{C})\right)$, so Γ contains $\prod_{z^m=t_0} \mathrm{SL}_2$. Thus $(\Gamma. \operatorname{Fil}^\bullet V_{\mathbb{C}})^{\mathrm{Zar}} = \prod_{z^m=t_0} \mathbb{P}^1$, so $\dim (\Gamma. \operatorname{Fil}^\bullet V_{\mathbb{C}})^{\mathrm{Zar}} = m \geq 8$.

9.3.3. *Conclusion.* We have $\dim_{K_v} \operatorname{Aut}(V, \Phi) \leq 4 < 8 \leq m = \dim (\Gamma. \operatorname{Fil}^\bullet V_{\mathbb{C}})^{\mathrm{Zar}}$, so Corollary 8.3 shows that the set $U^{\mathrm{ss}} := U \cap Y(\mathcal{O})^{\mathrm{ss}}$ is finite.

9.3.4. *Handling points with non-semisimple representations.* It remains to show that the set $U^{\text{non-ss}} := U - U^{\mathrm{ss}}$ is finite. In fact, we will prove that $Y(\mathcal{O})^{\text{non-ss}} := Y(\mathcal{O}) - Y(\mathcal{O})^{\mathrm{ss}}$ is finite.

Recall that an elliptic curve E over a field L is called non-CM if $\operatorname{End} E_{\overline{L}} = \mathbb{Z}$.

We use Serre's open image theorem:

Theorem 9.3 ([Ser72, statement (2)])**.** *If E is a non-CM elliptic curve over a number field L, then the image of $\mathfrak{G}_L \to \operatorname{Aut} \mathrm{H}^1_{\mathrm{et}}(E_{\overline{L}}, \mathbb{Z}_p) \simeq \mathrm{GL}_2(\mathbb{Z}_p)$ is an open subgroup of finite index.*

Corollary 9.4. *Under the hypotheses of Theorem 9.3, the 2-dimensional representation $\mathrm{H}^1_{\mathrm{et}}(E_{\overline{L}}, \mathbb{Q}_p) \in \operatorname{Rep}_{\mathbb{Q}_p}(\mathfrak{G}_L)$ is simple.*

Proof. A finite-index subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$ does not stabilize any 1-dimensional subspace of $\mathbb{Q}_p^2$. $\square$

Corollary 9.5. *Let $t \in Y(\mathcal{O})$. Suppose that for all $z \in \overline{K}$ with $z^m = t$, the elliptic curve E_z is non-CM. Then the representation $V_t \in \operatorname{Rep}_{\mathbb{Q}_p}(\mathfrak{G}_K)$ is semisimple.*

Proof. For a representation over a field of characteristic 0, semisimplicity is unaffected by restricting to a finite index subgroup. The restriction of V_t to a representation of $\mathfrak{G}_{K(z)}$ is a direct sum of m simple representations of the type in Corollary 9.4. □

Corollary 9.6. *The set $Y(\mathcal{O})^{\text{non-ss}}$ is finite.*

Proof. There are only finitely many CM j-invariants of any fixed degree, and the j-invariant of E_z is a rational function of z, so there are only finitely many $z \in \overline{K}$ of degree $\leq m[K : \mathbb{Q}]$ such that E_z has CM, and hence there are only finitely many t that violate the hypothesis of Corollary 9.5. □

This completes the proof of Theorem 9.1.

Remark 9.7. One can prove Corollary 9.6 without using Serre's open image theorem, by using Hodge–Tate weights: see [LV18, Lemma 4.2]. This is important for the application of the method in other situations where the analogue of Serre's theorem is unknown or false.

10. The Mordell conjecture

The proof of the Mordell conjecture in [LV18] follows similar lines, but everything is more complicated, especially the method for handling non-semisimple representations and the computation of the monodromy group.

Acknowledgments

I thank David Corwin, Olivier Wittenberg, and Zijian Yao for sharing their notes on these subjects. Part of the present exposition is adapted from their presentations. I also thank Zhiyu Zhang for spotting some typos.

References

[BC70] A. Baker and J. Coates, *Integer points on curves of genus 1*, Proc. Cambridge Philos. Soc. **67** (1970), 595–602, DOI 10.1017/s0305004100045904. MR256983 ↑1.2

[Bom90] Enrico Bombieri, *The Mordell conjecture revisited*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) **17** (1990), no. 4, 615–640. MR1093712 (92a:11072) ↑1.1

[BC09] Oliver Brinon and Brian Conrad, *CMI Summer School notes on p-adic Hodge theory (preliminary version)*, June 24, 2009. Preprint, `http://math.stanford.edu/~conrad/papers/notes.pdf` . ↑2.6

[Cha41] Claude Chabauty, *Sur les points rationnels des courbes algébriques de genre supérieur à l'unité*, C. R. Acad. Sci. Paris **212** (1941), 882–885 (French). MR0004484 (3,14d) ↑1.1

[Cor19] David Corwin, *From Chabauty's method to Kim's non-abelian Chabauty method*, July 4, 2019. Preprint, `https://math.berkeley.edu/~dcorwin/files/ChabautytoKim.pdf`. ↑2.2

[Fal83] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), no. 3, 349–366 (German). English translation: Finiteness theorems for abelian varieties over number fields, 9–27 in *Arithmetic Geometry (Storrs, Conn., 1984)*, Springer, New York, 1986. Erratum in: Invent. Math. **75** (1984), 381. MR718935 (85g:11026a) ↑1.1

[KO68] Nicholas M. Katz and Tadao Oda, *On the differentiation of de Rham cohomology classes with respect to parameters*, J. Math. Kyoto Univ. **8** (1968), 199–213, DOI 10.1215/kjm/1250524135. MR0237510 ↑7.1.2

[LV18] Brian Lawrence and Akshay Venkatesh, *Diophantine problems and p-adic period mappings*, August 30, 2018. Preprint, `arXiv:1807.02721v2` . ↑1.1, 1.2, 1.3, 9.3.1, 9.3.2, 9.7, 10

[MP12] William McCallum and Bjorn Poonen, *The method of Chabauty and Coleman*, Explicit Methods in Number Theory: Rational Points and Diophantine Equations, Panoramas et Synthèses, vol. 36, Société Mathématique de France, Paris, 2012, pp. 99–117. ↑2.1

[Mor22] L. J. Mordell, *On the rational solutions of the indeterminate equations of the third and fourth degrees*, Proc. Cambridge Phil. Soc. **21** (1922), 179–192. ↑1.1

[Ser72] Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331 (French). MR0387283 (52 #8126) ↑9.3

[Ser97] Jean-Pierre Serre, *Lectures on the Mordell-Weil theorem*, 3rd ed., Aspects of Mathematics, Friedr. Vieweg & Sohn, Braunschweig, 1997. Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt; With a foreword by Brown and Serre. MR1757192 (2000m:11049) ↑4.1

[Sie29] Carl Ludwig Siegel, *Über einige Anwendungen diophantischer Approximationen*, Abh. Preuß. Akad. Wissen. Phys.-math. Klasse (1929), 41–69. English translation: *On some applications of diophantine approximations*, edited by Umberto Zannier, Scuola Normale Superiore Pisa, 2014. ↑1.2

[Sko34] Th. Skolem, *Ein Verfahren zur Behandlung gewisser exponentialer Gleichungen und diophantischer Gleichungen*, 8. Skand. Mat.-Kongr., Stockholm, 1934, pp. 163–188 (German). ↑1.2

[Voj91] Paul Vojta, *Siegel's theorem in the compact case*, Ann. of Math. (2) **133** (1991), no. 3, 509–548. MR1109352 (93d:11065) ↑1.1

Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139-4307, USA

Email address: `poonen@math.mit.edu`

URL: `http://math.mit.edu/~poonen/`