

The Iwasawa theoretic version of the conjecture
of Birch and Swinnerton-Dyer

Peter Schneider

This talk is a report on some recent work in the algebraic p-adic theory of abelian varieties over number fields. Detailed proofs are contained in the series of papers [5]-[7]. Let me begin by recalling the main problems of that theory.

We start with
a number field k/\mathbb{Q} ,
an abelian variety A/k ,
and a prime number p

which, for simplicity, we assume to be odd. The most important arithmetic invariants of A are the group of k -rational points $A(k)$ and the Tate-Safarevič group $\mathbb{W}_k(A)$.

Basic problem :

How are $A(k_n)$ and $\mathbb{W}_{k_n}(A)$ ($= p$ -component of $\mathbb{W}_{k_n}(A)$) behaved if k_n varies through the intermediate layers of the cyclotomic \mathbb{Z}_p -extension k_∞/k ?

(For simplicity we will consider here only the cyclotomic case although the theory works for other \mathbb{Z}_p -extensions as well).

The method due to Iwasawa to handle problems of that type is to study the natural action of $\Gamma := \text{Gal}(k_\infty/k)$ on $A(k_\infty)$ resp. $\mathbb{W}_{k_\infty}(A)$ (p). But if A has good reduction at the primes above p these Γ -modules fit together into the flat cohomology group $H^1(\mathbb{Q}_\infty, A(p))$; here \mathbb{Q}_∞ denotes the ring of integers in k_∞ and $A(p)$ is the ind- p -subgroup scheme of the Néron model A of A over the ring of integers \mathbb{O} in k . We then namely have the exact "Kummer" sequence

$$0 \rightarrow A(K_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p \rightarrow H^1(0_\infty, A(p)) \rightarrow H^1(0_\infty, A)(p) \rightarrow 0,$$

and $\mathbb{H}_{K_\infty}(A)(p)$ is contained in $H^1(0_\infty, A)(p)$ with finite index. One therefore has to study the Pontrjagin dual

$$H := H^1(0_\infty, A(p))^*$$

which is a compact module over the completed group ring $\mathbb{Z}_p[[\Gamma]]$. The weak Mordell-Weil theorem implies that H is even finitely generated as $\mathbb{Z}_p[[\Gamma]]$ -module.

Problem 1 : (conjecture of Mazur)

Is H a $\mathbb{Z}_p[[\Gamma]]$ -torsion module if A has ordinary good reduction at the primes above p ? (A consequence would be that $A(K_\infty)$ is finitely generated as abelian group).

In that case $H \otimes \mathbb{Q}_p$ is a finite-dimensional vector space and we put

$$F(t) := p^{\mu(H)} \cdot \det(t - (\gamma - 1); H \otimes \mathbb{Q}_p)$$

where $\mu(H) \geq 0$ is a certain invariant describing the \mathbb{Z}_p -torsion submodule of H and γ is a fixed topological generator of Γ ; furthermore

$$L_p(A, s) := F(k(\gamma)^{1-s} - 1), \quad s \in \mathbb{Z}_p,$$

where $k: \Gamma \rightarrow \mathbb{Z}_p^*$ denotes the cyclotomic character is called the Iwasawa L -function of A (with respect to p).

Problem 2 :

Prove a formula of the Birch/Swinnerton-Dyer type for $L_p(A, s)$ at $s = 1$ (if A is "ordinary at p ") !

But already in order to formulate this problem more precisely one first has to solve the following one.

Problem 3 :

Define a p -adic height for A !

Although we will not discuss it here I finally want to mention the following question.

Problem 4 :

What is the $\mathbb{Z}_p[[\Gamma]]$ -rank of H in the nonordinary case ?

(A discussion of that problem with some partial results is contained in [7]).

From now on we always assume that A has ordinary good reduction at the primes above p ! I want to describe in this talk a partial solution of Problem 2. But I should emphasize that in the case of elliptic curves with complex multiplication similar results were obtained by B. Perrin-Riou [4] and J. Coates [1].

1 - The descent diagram

A first important task is to see the precise relationship between H and the invariants $A(k)$ and $\mathbb{H}_k(A)(p)$. We have two spectral sequences

$$\begin{aligned} H^i(\Gamma, H^j(0_\infty, A(p))) &\implies H^{i+j}(0_\infty/0, A(p)) \\ H^i(0, R^j \pi_{\Gamma*} A(p)) &\implies H^{i+j}(0_\infty/0, A(p)) \end{aligned}$$

where the abutment is a cohomology theory for sheaves with Γ -action.

Basic fact : $\pi_{\Gamma*} A(p) = A(p)$.

Using that and the fact that $cd_{\mathbb{Z}_p} \Gamma = 1$ we get the exact diagram

$$\begin{array}{ccccccc} & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \\ & & H^1(0, A(p)) & & H^1(0, A(p)) & & \\ & & \downarrow & & \downarrow & & \\ 0 & \rightarrow & H^1(\Gamma, A(K_\infty)(p)) & \rightarrow & H^1(0_\infty/0, A(p)) & \rightarrow & (H_\Gamma^1)^* \rightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ & & H^0(0, R^1 \pi_{\Gamma*} A(p)) & & H^0(0, R^1 \pi_{\Gamma*} A(p)) & & \downarrow \\ & & \downarrow & & \downarrow & & \downarrow \\ & & H^2(0, A(p)) & & H^2(0, A(p)) & & \downarrow \\ 0 & \leftarrow & H^2(0_\infty, A(p))^{\Gamma} & \leftarrow & H^2(0_\infty/0, A(p)) & \leftarrow & (H_\Gamma^2)^* \rightarrow 0 \end{array}$$

furthermore f^* denotes the map which is induced by the identity on H .

2 - "Local analysis"

By local considerations one proves the following result.

Proposition :

- i) $H^0(O, R^1 \pi_{T_p} A(p))$ is finite of order $(\prod A(k_p)(p))^2$ where k_p denotes the residue class field of O at p ;
- ii) the map $H^2(O, A(p)) \rightarrow H^2(O_\infty/O, A(p))$ is surjective.

Here our assumption "A ordinary at p " is used in an essential way. Apart from our ignorance of $H^2(O_\infty, A(p))^\Gamma$ (which can be circumvented lateron) we thus have solved our first task.

3 - The algebraic p-adic height pairing

Let \tilde{A} , resp. \tilde{A} , denote the dual abelian variety, resp. its Néron model over O . We put $H^1(O, T_p(A)) := \varprojlim_p H^1(O, A_{\nu^p})$. The sequence of maps

$$\begin{array}{ccc}
 H^1(O, T_p(\tilde{A})) & & \text{Hom}_{\mathbb{Z}_p} (H^1(O, T_p(A)), \mathbb{Z}_p) \\
 \parallel \text{ global duality} & & \downarrow \\
 H^2(O, A(p))^* & & H^1(O, A(p))^* \\
 \uparrow \text{ injective with} & & \uparrow \\
 \text{finite cokernel} & & \\
 H^2(O_\infty/O, A(p))^* & & \\
 \downarrow & & \\
 H^1 T & \xrightarrow{f} & H^1 T
 \end{array}$$

then determines a pairing

$$\langle\langle, \rangle\rangle : H^1(O, T_p(\tilde{A})) \times H^1(O, T_p(A)) \rightarrow \mathbb{Q}_p ;$$

furthermore, the modified pairing

$$\langle\langle, \rangle\rangle_p := \log_p K(\gamma) \cdot \langle\langle, \rangle\rangle$$

does not depend on the special choice of the generator $\gamma \in \Gamma$! Using the exact sequences

$$\begin{array}{ccccccc}
 0 & \longrightarrow & A^0(O) \otimes \mathbb{Z}_p & \longrightarrow & H^1(O, T_p(A)) & \longrightarrow & T_p(\mathbb{W}_K(A)) \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 0 & \longrightarrow & \tilde{A}^0(O) \otimes \mathbb{Z}_p & \longrightarrow & H^1(O, T_p(\tilde{A})) & \longrightarrow & T_p(\mathbb{W}_K(\tilde{A})) \longrightarrow 0
 \end{array}$$

we get, by restriction of $\langle\langle, \rangle\rangle_p$, a pairing

$$\langle, \rangle_p : \tilde{A}(K) \times A(K) \longrightarrow \mathbb{Q}_p$$

which we call the algebraic p-adic height pairing:

Theorem I :

Under the assumption that $\langle\langle, \rangle\rangle_p$ is nondegenerate we have :

- i) $H^2(O_\infty, A(p)) = 0$;
- ii) H is a \mathbb{Z}_p [[Γ]]-torsion module ;
- iii) $L_p(A, s)$ has a zero at $s = 1$ of multiplicity $\rho := \text{rank}_{\mathbb{Z}_p} H^1(O, T_p(A))$ with leading coefficient

$$|L_p(A, s) \cdot (s-1)^{-\rho}|_{s=1}^{-1} = \frac{\#\mathbb{W}_K(A)(p) \cdot \text{Div}}{\#A(K)(p) \cdot \#\tilde{A}(K)(p)} \cdot \frac{|\det \langle\langle, \rangle\rangle_p|^{-1}}{I \cdot \tilde{I}} \cdot \prod_{p|p} \#\pi_p(A)(p) \cdot (\prod_{p|p} \#A(k_p)(p))^2$$

where $\pi_p(A)$ denotes the group of rational connected components of the reduction of A at p and I is defined to be the order of the kernel of the map

$$\text{Div } H^1(O, A^0(p)) \longrightarrow \text{Div } H^1(O, A(p)) ,$$

resp. \tilde{I} analogously for \tilde{A} . (For any abelian group M we denote by $\text{Div } M$ the maximal divisible subgroup and we put $M_{\text{Div}} := M/\text{Div } M$).

The proof of that theorem consists in a careful study of the descent diagram. The main difficulty is to show the vanishing of $H^2(O_\infty, A(p))$ which requires additional "local analysis" using a relative cohomology sequence

4 - The comparison theorem and its consequence

There is a canonical (or analytic) p-adic height pairing (see [5]) :
 For any $\tilde{a} = (0 \rightarrow \mathbb{G}_m \rightarrow X \rightarrow A^0 \rightarrow 0) \in \text{Ext}_0^1(A^0, \mathbb{G}_m) = \tilde{A}(K)$ we have the exact sequence of points in the finite adèles A of K

$$0 \rightarrow \mathbb{G}_m(A) \rightarrow X(A) \rightarrow A^0(A) \rightarrow 0.$$

The homomorphism $v := \log_p \circ \kappa \circ \text{reciprocity} : \mathbb{G}_m(A) \rightarrow \mathbb{Z}_p$ extends in a natural way to a homomorphism $v_{\tilde{a}} : X(A) \rightarrow \mathbb{Q}_p$. By restriction to global points $v_{\tilde{a}}$ induces a map $v_{\tilde{a}} : A(K) \rightarrow \mathbb{Q}_p$ and we put

$$\begin{aligned} (\cdot, \cdot)_p : \tilde{A}(K) \times A(K) &\rightarrow \mathbb{Q}_p \\ (\tilde{a}, a) &\longmapsto v_{\tilde{a}}(a). \end{aligned}$$

Theorem II :

$$\langle \cdot, \cdot \rangle_p = (\cdot, \cdot)_p.$$

For the proof of this result we have to develop a modified flat cohomology theory for rings of integers which has a "degree map" into \mathbb{Z}_p (like in the function field case) and in which $(\cdot, \cdot)_p$ has an interpretation as a certain Yoneda pairing followed by that degree map. The comparison then consists in long and complicated cohomological computations which in the essential step are based on a result of Serre about the vanishing of the congruence kernel for abelian varieties.

Theorems I and II together imply the promised partial solution of Problem 2.

Theorem III :

Assume that $\prod_k(A)(p)$ is finite and that $(\cdot, \cdot)_p$ is nondegenerate. Then $L_p(A, s)$ has a zero at $s = 1$ of multiplicity $\rho := \text{rank}_{\mathbb{Z}} A(K)$ with

$$|L_p(A, s) \cdot (s-1)^{-\rho}|_{s=1}^{-1} = \frac{\# \prod_k(A)(p) \cdot |\det(\cdot, \cdot)_p|^{-1}}{\# A(K)(p) \cdot \# \tilde{A}(K)(p)}$$

$$\cdot \prod_{\mathfrak{p} \mid p} \# \pi_{\mathfrak{p}}(A)(p) \cdot \left(\prod_{\mathfrak{p} \mid p} \# A(K_{\mathfrak{p}})(p) \right)^2.$$

Of course, we conjecture that $(\cdot, \cdot)_p$ always is nondegenerate (in the cyclotomic case).

BIBLIOGRAPHY

- [1] J. Coates.- Infinite Descent on Elliptic Curves with Complex Multiplication. In *Arithmetic and Geometry*, Papers Dedicated to I.R. Shafarevich, vol. I. Progress in Math. vol. 35, 107-137. Boston-Basel-Stuttgart : Birkhäuser 1985.
- [2] B. Mazur.- Rational points of abelian varieties with values in towers of number fields. *Invent. Math.* 18, 183-266 (1972).
- [3] B. Mazur.- Canonical Heights via Biextensions. In *Arithmetic and Geometry*, Papers Dedicated to I.R. Shafarevich, vol. I. Progress in Math. vol. 35, 195-237. Boston-Basel-Stuttgart : Birkhäuser 1985.
- [4] B. Perrin-Riou.- Descente infinie et hauteur p-adique sur les courbes elliptiques à multiplication complexe. *Invent. Math.* 70, 369-398 (1982).
- [5] P. Schneider.- p-Adic Height Pairings I. *Invent. Math.* 69, 401-409 (1982).
- [6] P. Schneider.- Iwasawa L-Functions of Varieties over Algebraic Number Fields. A First Approach. *Invent. Math.* 71, 251-293 (1983).
- [7] P. Schneider.- p-Adic Height Pairings II. To appear.
- [8] J.-P. Serre.- Sur les groupes de congruence des variétés abéliennes I, II. *Izv. Akad. Nauk SSSR* 28, 3-20 (1964) and 35, 731-737 (1971).

Peter Schneider
 Fakultät für Mathematik
 Universitätsstrasse 31
 D-8400 REGENSBURG
 BUNDESREPUBLIK DEUTSCHLAND