p-adic methods for rational points on curves

MA841 at BU Fall 2019

Jennifer Balakrishnan

December 21, 2019

These are notes for Jennifer Balakrishnan's course MA841 at BU, Fall 2019. The course webpage is http://math.bu.edu/people/jbala/841.html.

1 Rational points on curves

Lecture 1 5/9/2019

Main Question: How do we determine $X(\mathbf{Q})$ for X smooth projective of genus ≥ 2? What computational tools are involved?

Topics:

1. Chabauty-Coleman method
2. Coleman integration (p-adic integration)
3. p-adic heights
4. quadratic Chabauty

Evaluation (if you need a grade), TeX 3-4 classes worth of lecture notes.

Detailed list of topics:

- Chabauty-Coleman
- Explicit Coleman integration
- p-adic cohomology, based point counting (Kedlaya + Tuitman)
- Iterated Coleman integration
- Chabauty-Coleman in practice + other tools
- Étale descent
- Covering collections
- Elliptic curve Chabauty
- p-adic heights on elliptic curves
- p-adic heights on Jacobians on curves
- Local heights
- Quadratic Chabauty for integral points on affine hyperelliptic curves
- Kim's nonabelian Chabauty program

- Nekovář's p-adic height
- Quadratic Chabauty for $\mathbf{Q}$-points on curves
- Quadratic Chabauty in practice

References for first two weeks:

- McCallum-Poonen
- Stoll: Arithmetic of Hyperelliptic Curves
- Kedlaya: p-adic cohomology from theory to practice (notes from 2007 AWS)
- Besser: Heidelberg lectures on Coleman integration

For computations

- Sage
- MAGMA

2 The Chabauty-Coleman method

2.1 A question about triangles

Does there exist a rational right triangle and a rational isosceles triangle with with same perimeter and same area? (rational means all side lengths are rational)

Suppose there does exist such a pair, then introducing parameters, k, t for the right triangle, and l, u for the isosceles we can rescale to

$$k, t, u \in \mathbf{Q}$$

$$0 < t, u < 1, \; k > 0$$

an equate areas and perimeters. Areas:

$$\frac{1}{2}(2kt)(k)(1-t^2) = \frac{1}{2}(4u)(1-u^2)$$

$$\implies k^2t^2(1-t^2) = 2u(1-u^2).$$

Perimeters:

$$k(1-t^2) + k(1+t^2) + 2kt = 1 + u^2 + 1 + u^2 + 4u$$

$$\implies k + kt = 1 + 2u + u^2 = (1+u)^2$$

so letting $x = 1 + u$, after some algebra we have $1 < x < 2$ in $\mathbf{Q}$ s.t.

$$2xk^2 + (-3x^3 - 2x^2 + 6x - 4)k + x^5 = 0$$

this is a quadratic in k, and the discriminant is a square in $\mathbf{Q}$. so

$$X\colon\; y^2 = (-3x^3 - 2x^2 + 6x - 4)^2 - 4(2x)x^5$$

$$= x^6 + 12x^5 - 32x^4 + 52x^2 - 48x + 16$$

so this is a genus 2 hyperelliptic curve. We need the $\mathbf{Q}$-points of this.

Facts:. Jac(X) has Mordell-Weil rank 1. The Chabauty-Coleman bound on the size of $X(\mathbf{Q})$ for this curve gives $\#X(\mathbf{Q}) \leq 10$. But we find points

$$\Big\{(0:-4:1)\,, \infty_{\pm}, (0:4:1)\,, (1:-1:1)\,, (1:1:1)\,, \left(\frac{12}{11}:-\frac{868}{1331}:1\right),$$
$$\left(\frac{12}{11}:\frac{868}{1331}:1\right), (2:-8:1)\,, (2:8:1)\Big\}$$

so this set is $X(\mathbf{Q})$.

Back in the original problem we specified $x < 1 < 2$, so there is a unique such pair of triangles:

Theorem 2.1 Hirakawa-Matsumura '18. *Up to similitude there exists a unique pair of a rational right triangle and a rational isosceles triangle that have the same perimeters and areas. The unique pair consists of a right triangle with sides*

$$(377, 135, 352)$$

and the isosceles triangle with sides

$$(366, 366, 132).$$

2.2 Why care about $X(\mathbf{Q})$ for X of genus 2?

Curves of genus 0: have no $\mathbf{Q}$-points or infinitely many, they satisfy a local to global principle so there exists an algorithm to determine the $\mathbf{Q}$-points in finite time.

Curves of genus 1: If we have 1 smooth rational point then we have an elliptic curve, Mordell's theorem implies that $E(\mathbf{Q})$ is a finitely generated abelian group,

$$E(\mathbf{Q}) \simeq \mathbf{Z}^r \oplus T$$

where the possible torsion parts T have been determined by Mazur's theorem. To understand T, and the distribution of T there is work of Harron and Snowden, this often comes down to understanding rational points on $X_1(N)$.

Upshot: to understand $E(\mathbf{Q})$ we want to understand r:

Q1: is there an algorithm to compute r?

Q2: what values of r can occur?

Q3: what is the distribution of r?

A1: n-descent, the obstacle is III, proving finiteness, it is conjectured that $r = \mathrm{ord}_{s=1} L(E, s)$ (BSD).

A2: record due to Noam Elkies an example of E with $r \geq 28$.

A3: minimalist conjecture: 50% of all curves have rank 0, 50% rank 1.

Theorem 2.2 Bhargava-Shankar. *The average rank is* < 1.

Baur Bektemirov, Barry Mazur, William Stein, and Mark Watkins, Average ranks of elliptic curves: tension between data and conjecture, Bull. Amer. Math. Soc. (N.S.) 44 (2007), no. 2, 233–254. MR 2009e:11107 gave average rank graphs, which kept increasing.

Sarnak said there would "obviously be a turn around".

Jennifer S. Balakrishnan, Wei Ho, Nathan Kaplan, Simon Spicer, William Stein, and James Weigandt, Databases of elliptic curves ordered by height and distributions of Selmer groups and ranks, LMS J. Comput. Math. 19 (2016), supp. A, pp. 351-370. MR 3540965

2.3 Coleman's bound

Lecture 2 10/9/2019

Goal today: prove Coleman's refinement of Chabauty's theorem.

Theorem 2.3 Coleman 1985. *Let $X/\mathbf{Q}$ be a curve of genus $g \geq 2$. Suppose the Mordell-Weil rank of $J(\mathbf{Q})$ is less than g. Then if $p > 2g$ is a good prime for X we have*

$$\#X(\mathbf{Q}) \leq \#X_{\mathbf{F}_p}(\mathbf{F}_p) + 2g - 2.$$

Definition 2.4 Differentials. Let X be a curve over a field k. The space of **differentials** on X over k is a 1-dimensional $k(X)$-vector space $\Omega^1_X(k)$.

There is a nontrivial k-linear derivation

$$\mathrm{d}\colon k(X) \to \Omega^1_X(k)$$

i.e. d is k-linear and satisfies the Leibniz rule

$$\mathrm{d}(fg) = g\,\mathrm{d}f + f \cdot \mathrm{d}g$$

for all $f, g \in k(X)$ and there is some $f \in k(X)$ s.t. $\mathrm{d}f \neq 0$.

A general differential can be written as $\omega = f\,\mathrm{d}g$ where $g \in K(X)$ with $\mathrm{d}g \neq 0$. If we fix g this representation is unique. If $\omega, \omega' \in \Omega^1_X(k)$ with $\omega' \neq 0$ then there's a unique $f \in K(X)$ s.t. $\omega = f\omega'$. We may write $\omega/\omega' = f$. ◊

Definition 2.5 Differentials of the first second and third kinds. Let $0 \neq \omega \in \Omega^1_X(k)$ and $P \in X(k)$. Let $t \in k(X)$ be a uniformizer at P. Then $v_P(\omega) = v_P(\omega/\mathrm{d}t)$ is the valuation of ω at P. This valuation is nonzero for only finitely many points $P \in X(\overline{k})$. The divisor

$$\mathrm{div}(\omega) = \sum_{P \in X(\overline{k})} v_P(\omega)P \in \mathrm{Div}_X(k)$$

is the divisor of ω.

If $v_P(\omega) \geq$ then ω is regular at P and ω is said to be regular if it is regular at all points $P \in X(\overline{K})$.

Also called differentials of the **first kind**.

A differential of the **second kind** has residue zero at all points $P \in X(\overline{K})$.

A differential of the **third kind** has at most a simple pole at all points $P \in X(\overline{K})$ (and integer residues there in some references). ◊

Since the quotient of any two non-zero differentials is a function

$$\omega_1 = f_1\,\mathrm{d}g$$
$$\omega_2 = f_2\,\mathrm{d}g$$

so

$$\frac{\omega_1}{\omega_2} = \frac{f_1}{f_2}.$$

The difference of any two divisors of differentials is a principal divisor.

$$\mathrm{div}\left(\frac{\omega_1}{\omega_2}\right) = \mathrm{div}\left(\frac{f_1}{f_2}\right)$$
$$= \mathrm{div}\,\omega_1 - \mathrm{div}\,\omega_2.$$

So the divisors of differentials form one linear equivalence class of divisors, the canonical class.

Recall. Let X/k be a curve and $D \in \mathrm{Div}_X(k)$. The Riemann-Roch space of D is the k-vector space

$$L(D) = \left\{\phi \in k(X)^\times : \operatorname{div}\phi + D \geq 0\right\} \cup \{0\}$$

where we write $D \geq D'$ if $v_P(D) \geq v_P(D')$ for all P.

Theorem 2.6 Riemann-Roch. *Let X/k be a curve of genus g then there is a divisor $W \in \mathrm{Div}_X(k)$ s.t. for every $D \in \mathrm{Div}_X(k)$ w we have $\dim_k L(D)$ is finite and*

$$\dim_k L(D) = \deg D - g + 1 \dim_l L(W - D).$$

In particular, $\dim_k L(W) = g$, $\deg W = 2g - 2$.

The canonical class is exactly the class of the divisor W in Riemann-Roch.

The k-vector space of regular differentials has $\dim L(W) = g$, and is denoted as $H^0(X, \Omega^1_X)$.

Example 2.7 Let $X\colon y^2 = f(x)$ be a hyperelliptic curve of genus g over k. Then $H^0(X, \Omega^1_X)$ has basis

$$\left\{\frac{\mathrm{d}x}{2y}, \dots, \frac{x^{g-1}\,\mathrm{d}x}{2y}\right\}$$

so every regular differential can be written uniquely as

$$\frac{p(x)\,\mathrm{d}x}{2y}$$

with a polynomial p of degree $\leq g - 1$. □

We want to integrate differentials in some p-adic sense, Q: What does a p-adic line integral look like?

Theorem 2.8 *Let $X/\mathbf{Q}_p$ be a curve with good reduction then there is a p-adic integral*

$$\int_P^Q \omega \in \overline{\mathbf{Q}}_p$$

defined for each pair of points $P, Q \in X(\overline{\mathbf{Q}}_p)$ and regular differential $\omega \in H^0(X, \Omega^1_X(\overline{\mathbf{Q}}_p))$ that satisfies the following properties:

1. *The integral is $\overline{\mathbf{Q}}_p$ linear in ω*

2. *If P, Q both reduce to the same point $\bar{P} \in X_{\mathbf{F}_p}(\mathbf{F}_p)$ then the integral can be evaluated by writing*

   $$\omega = \omega(t)\,\mathrm{d}t$$

   with t a uniformizer at P reducing to a uniformizer at $\bar{P}$ and ω a power series. Then integrating formally obtaining a power series l s.t.

   $$\mathrm{d}l(t) = w(t)\,\mathrm{d}t$$

   and $l(0) = 0$ and finally evaluating

   $$l(t(Q))$$

   which converges. This implies that $\int_P^P \omega = 0$.

3. $$\int_P^Q \omega + \int_{P'}^{Q'} \omega = \int_P^{Q'} \omega + \int_{P'}^{Q} \omega$$

so it makes sense to define:

$$\int_D \omega$$

for

$$\sum_{j=1}^{n} Q_j - P_j \in \mathrm{Div}_X^0(\overline{\mathbf{Q}}_p)$$

as

$$\int_D \omega = \sum_{j=1}^{n} \int_{P_j}^{Q_j} \omega$$

4. *If D is principal then* $\int_D \omega = 0$.

5. *The integral commutes with the action of* $\mathrm{Gal}(\overline{\mathbf{Q}_p}/\mathbf{Q}_p)$.

6. *Fix* $P_0 \in X(\overline{\mathbf{Q}}_p)$. *If* $0 \neq \omega \in H^0(X, \Omega_X^1)$, *then the set of points* $P \in X(\overline{\mathbf{Q}}_p)$ *reducing to a fixed point* $P_0 \in X_{\mathbf{F}_p}(\overline{\mathbf{F}}_p)$. *and s.t.*

$$\int_{P_0}^{P} \omega = 0$$

is finite.

Remark 2.9 The statement that the curve has good reduction is not necessary but simplifies the statement of 2.

Remark 2.10 This integral is the Coleman integral [31], other works on p-adic integration include Berkovich [12]. Also there is work of Zarhin, Colmez, Vologodsky, Besser, ...

Remark 2.11 Theory of Coleman integration of forms the second or third kind developed by Coleman-de Shalit [33]. (additivity in endpoints, linearity, change of variables, FTC).

Corollary 2.12 *Given the hypotheses of the previous theorem*

$$P_0 \in X(\mathbf{Q}_p)$$

and J the Jacobian of X let

$$\iota \colon X \to J$$

be the embedding

$$P \mapsto [P - P_0]$$

there is a map

$$J(\mathbf{Q}_p) \times H^0(X, \Omega_X^1) \to \mathbf{Q}_p$$
$$(P, \omega) \mapsto \langle P, \omega \rangle$$

that is additive in P and $\mathbf{Q}_p$ *linear in* ω *which is given by*

$$\langle [D], \omega \rangle = \int_D \omega$$

in particular for

$$P \in X(\mathbf{Q}_p)$$

we have

$$\langle \iota(P), \omega \rangle = \int_{P_0}^{P} \omega.$$

Remark 2.13 If $P \in J(\mathbf{Q}_p)$ has finite order, then

$$\langle P, \omega \rangle = 0,\ \forall \omega \in H^0(X, \Omega^1_X)$$

to see this, if $nP = 0$ then

$$\langle P, \omega \rangle = \frac{1}{n} \langle nP, \omega \rangle = \frac{1}{n} 0 = 0.$$

One can show that torsion points are the only points with this property. On the other hand, if ω has the property that $\langle P, \omega \rangle = 0$ for all $P \in J(\mathbf{Q}_p)$ then $\omega = 0$.

Corollary 2.14 *Let $X/\mathbf{Q}$ be a curve of genus g with Mordell-Weil rank less than g. Then $\#X(\mathbf{Q})$ is finite. Note we don't need $g \geq 2$, in $g = 1$ this applies to rank 0.*

Proof. Pick a prime of good reduction for X let

$$V = \{\omega \in H^0(X, \Omega^1_X) : \forall P \in J(\mathbf{Q}) : \langle P, \omega \rangle = 0\}$$

by additivity in the first argument this condition is equivalent to requiring that $\left\langle P_j, \omega \right\rangle = 0$ for a basis $\{P_j\}_{j=1}^r$ of the free part of $J(\mathbf{Q})$ so it leads to at most r linear constraints, so $\dim V \geq g - r > 0$. So there is some $0 \neq \omega \in V$ pick $P_0 \in X(\mathbf{Q})$, if $X(\mathbf{Q}) = \emptyset$ we are done. To define $\iota \colon X \hookrightarrow J$. Since $\iota(P) \in J(\mathbf{Q})$ for all $P \in X(\mathbf{Q})$ so it follows that $\int_{P_0}^P \omega = 0$ for all $P \in X(\mathbf{Q})$. By the theorem the number of such P is finite in each residue disk of $X(\mathbf{Q})$. Since the number of residue classes is $\#X(\mathbf{F}_p)$ which is finite. The total number of points in $X(\mathbf{Q})$ is finite also.

To get an actual bound we have to bound the number of zeroes of

$$\int_{P_0}^z \omega$$

as a p-adic power series. We can think of $X(\mathbf{Q}_p)$ set theoretically as a finite union of residue disks. Within each residue disk

$$\int_{P_0}^z \omega$$

has finitely many p-adic zeroes. ∎

Lecture 3 10/9/2019

We want to give a more refined version of this result which uses results about zeroes of p-adic power series.

Theorem 2.15 *Let*

$$0 \neq l(t) = \sum_{n=0}^{\infty} a_n t^n \in \mathbf{Q}_p[[t]]$$

such that $a_n \to 0$ as $n \to \infty$ in the p-adic topology. Let

$$v_0 = \min\{v_p(a_n) : n \geq 0\}$$

and

$$N = \max\{n \geq 0, v_p(a_n) = v_0\}$$

then there is a constant

$$c \in \mathbf{Q}_p^\times$$

a monic polynomial

$$q \in \mathbf{Z}_p[t]$$

of degree N, a power series

$$h(t) = \sum_{n=0}^{\infty} b_n t^n \in 1 + pt\mathbf{Z}_p[[t]]$$

with

$$b_n \longrightarrow 0 \text{ as } n \longrightarrow \infty$$

and

$$l(t) = cq(t)h(t).$$

Proof. After rescaling by a_0^{-1} can assume $v_0 = 0$ and $a_N = 1$ so this in particular $l(t) \in \mathbf{Z}_p[[t]]$ the condition $a_n \longrightarrow 0$ means that the image $l_m(t)$ of $l(t)$ in $\mathbf{Z}/p^m\mathbf{Z}[[t]]$ is actually a polynomial for all $m \geq 1$.

The idea is to construct inductively constants $c_m \in (\mathbf{Z}/p^m)^\times$, monic polynomials $q_m(t) \in (\mathbf{Z}/p^m)[t]$ of degree N and polynomials $h_m(t) \in (\mathbf{Z}/p^m)[t]$ with $h_m \equiv 1 \pmod{pt}$ satisfying

$$l_m(t) = c_m q_m(t) h_m(t)$$

and such that

$$(c_{m+1}, q_{m+1}, h_{m+1})$$

reduces $\pmod{p^m}$ to

$$(c_m, q_m, h_m).$$

Then there is a unique c, q, h as above such that

$$(c, q, h)$$

reduces $\pmod{p^m}$ to

$$(c_m, q_m, h_m)$$

for all m.

To start the induction set $c_1 = 1$

$$q_1(t) = l_1(t)$$

$$h_1(t) = 1$$

this is possible since $l_1(t)$ is monic of degree N.

Assume we've constructed c_m, q_m, h_m, let

$$\tilde{c}_{m+1}, \tilde{q}_{m+1}, \tilde{h}_{m+1}$$

be arbitrary lifts of c_m, q_m, h_m to objects over $\mathbf{Z}/p^{m+1}$ with

$$\tilde{q}_{m+1} \text{ monic of degree } N$$

$$\tilde{h}_{m+1}(t) \equiv 1 \pmod{pt}$$

then

$$l_{m+1}(t) - \tilde{c}_{m+1}\tilde{q}_{m+1}\tilde{h}_{m+1} = p^m d(t)$$

with

$$d(t) \in (\mathbf{Z}/p)[t]$$

then we must have

$$c_{m+1} = \tilde{c}_{m+1} + p^m \gamma$$

$$q_{m+1} = \tilde{q}_{m+1} + p^m k(t)$$
$$h_{m+1} = \tilde{h}_{m+1} + p^m \eta(t)$$
with $\gamma \in \mathbf{Z}/p$, $k \in (\mathbf{Z}/p)[t]$ of degree $< N$. and $\eta \in (\mathbf{Z}/p)[t]$ with $\eta(0) = 0$.

For $\gamma \in \mathbf{Z}/p\mathbf{Z}$, $k(t) \in (\mathbf{Z}/p\mathbf{Z})[t]$ of degree less than N, and $\eta(t) \in (\mathbf{Z}/p\mathbf{Z})[t]$ with $\eta(0) = 0$. So the relation $l_{m+1}(t) = c_{m+1}q_{m+1}(t)h_{m+1}(t)$ is equivalent to $d(t) = (\gamma + \eta(t))l_1(t) + k(t)$, and $\gamma, k(t)$, and $\eta(t)$ are uniquely determined through division by $l_1(t)$ with remainder $d(t)$, and this determines c_{m+1}, $q_{m+1}(t)$, and $h_{m+1}(t)$. ∎

Now we apply this to study zeroes of p-adic power series coming from Coleman integrals.

Lemma 2.16 *Let $l(t) \in \mathbf{Q}_p[[t]]$ with formal derivative $w(t) \in \mathbf{Z}_p[[t]]$. Such that the image $\bar{w}(t) \in \mathbf{F}_p[[t]]$ has the form $ut^\nu + \cdots$ with $u \in \mathbf{F}_p^\times$. Then l converges on $p\mathbf{Z}_p$. If $p > \nu + 2$ then*
$$\#\{\tau \in p\mathbf{Z}_p : l(t) = 0\} \leq \nu + 1.$$

Proof. Let
$$w(t) = w_0 + w_1 t + \cdots$$
$$l(t) = l_0 + l_1 t + \cdots$$
then
$$l_{n+1} = \frac{w_n}{n+1} \in \frac{1}{n+1}\mathbf{Z}_p$$
since $v_p(n+1) = O(\log n)$ the assumption that
$$w_n \in \mathbf{Z}_p$$
implies that $v_p(l_n) = v_p(w_n/(n+1)) \geq -c \log n$ for some constant c. If $\tau \in p\mathbf{Z}_p$ so $v_p(\tau) \geq 1$, then
$$v_p(l_n \tau^n) \geq n - c \log n \to \infty$$
as $n \to \infty$, hence $l(\tau)$ converges. Now consider $l(pt) = l_0 + pl_1 t + p^2 l_2 t^2 + \cdots$. The claim is that in the notation of the previous theorem we have $N \leq \nu + 1$.
$$v_p(p^{\nu+1} l_{\nu+1}) = \nu + 1 + v_p(l_{\nu+1})$$
$$= \nu + 1 + v_p\left(\frac{w_\nu}{\nu+1}\right)$$
$$= \nu + 1 + v_p(w_\nu) - v_p(\nu + 1) \leq \nu + 1$$
as by assumption $\bar{w}(t) \in \mathbf{F}_p[[t]]$ has the form $ut^\nu + \cdots$ so that $v_p(w_\nu) = 0$.

For $n > \nu$ we have
$$v_p(p^{n+1} l_{n+1}) = n + 1 + v_p(l_{n+1})$$
$$= n + 1 + v_p(w_n) - v_p(n+1)$$
$$\geq n + 1 - v_p(n+1)$$
since
$$v_p(w_n) \geq 0$$
for $n > \nu$. So it suffices to show that
$$n - v_p(n+1) > \nu$$
This is clear for $v_p(n+1) = 0$. Otherwise suppose $e = v_p(n+1)$ then $p^e | (n+1)$. So $n+1 \geq p^3 > \nu+e+1$, where the second inequality can be shown by induction. For $e = 1$ this is our hypothesis that $p > \nu + 2$, then use $p^{e+1} \geq p^e + 1$. The previous corollary now gives the result. ∎

Theorem 2.17 Coleman '85. *Let $X/\mathbf{Q}$ be a curve of genus g, with Mordell-Weil rank of J less than g. Then*

$$\#X(\mathbf{Q}) \leq \#X(\mathbf{F}_p) + 2g - 2.$$

[32].

Proof. We assume $P_0 \in X(\mathbf{Q})$, now arguing as in the proof of today's first corollary there is a non-zero differential $\omega \in H^0(X, \Omega^1_{X/\mathbf{Q}_p})$ such that

$$\int_{P_0}^{P} \omega = 0$$

for all $P \in X(\mathbf{Q})$. Now consider a point $\bar{Q} \in \overline{X}(\mathbf{F}_p)$ and lift it to Q in $X(\mathbf{Q}_p)$, we can pick a uniformizer $t \in \mathbf{Q}_p(X)^\times$ s.t at Q t reduces to a uniformizer $\bar{t} \in \mathbf{F}_p(\overline{X})^\times$ at $\bar{Q}$. We rescale ω s.t. its reduction $\bar{\omega}$ is defined an non-zero. Then $\bar{\omega} \in H^0(X, \Omega^1_{X/\mathbf{F}_p})$. Recall that $\operatorname{div}(\bar{\omega})$ is effective and has degree $2g-2$. Let $\nu(\bar{Q})$ denote the valuation at $\bar{Q}$ of $\bar{\omega}$. $\nu(\bar{Q}) = \nu_{\bar{Q}}(\bar{\omega})$. We write $\omega(t) = w(t)\,\mathrm{d}t$ with

$$w(t) \in \mathbf{Z}_p[[t]]$$

the coefficients are in $\mathbf{Z}_p$ since $\bar{\omega}$ is defined. Then

$$\bar{\omega} = \bar{w}(t)\,\mathrm{d}\bar{t}$$

$\bar{w}(\bar{t}) = \bar{t}^{\nu(\bar{Q})}(u_0 + u_1\bar{t} + \cdots)$.

$$\int_{P_0}^{P} \omega = l(t(P))$$

for $P \in X(\mathbf{Q}_p)$ such that $\bar{p} = \bar{q}$ and apply previous lemma. Now summing over residue disks we get

$$\begin{aligned}
\#X(\mathbf{Q}) &\leq \#\left\{P \in X(\mathbf{Q}_p) : \int_{P_0}^{P} \omega = 0\right\} \\
&\leq \sum_{\bar{Q} \in \bar{X}(\mathbf{F}_p)} \left(\nu(\bar{Q}) + 1\right) \\
&= \sum_{\bar{Q} \in \bar{X}(\mathbf{F}_p)} \nu(\bar{Q}) + \sum_{\bar{Q} \in \bar{X}(\mathbf{F}_p)} 1 \\
&\leq \deg(\operatorname{div}\omega) + \#\bar{X}(\mathbf{F}_p) \\
&= 2g - 2 + \#\bar{X}(\mathbf{F}_p).
\end{aligned}$$

■

Remark 2.18 Stoll (06) showed that we can choose the best ω in each residue disk, can improve the bound, $r < g$ and $p > 2r + 2$ is a good prime then

$$\#X(\mathbf{Q}) \leq \#\overline{X}(\mathbf{F}_p) + 2r$$

can also weaken the assumption that

$$p > 2r + 2.$$

If $p > 2$ then

$$\#X(\mathbf{Q}) \leq \#\overline{X}(\mathbf{F}_p) + 2r + \left\lfloor \frac{2r}{p-1} \right\rfloor.$$

[87]. Katz-Rabinoff-Zuerieck-Brown (12) extend Stoll's result tot the case of bad reduction, if $p > 2g$ and $\mathcal{X}$ a proper regular model for X over $\mathbf{Z}_p$ then

$$\#X(\mathbf{Q}) \leq \#\mathcal{X}_{sm}(\mathbf{F}_p) + 2r$$

where $\overline{\mathcal{X}}(\mathbf{F}_p)$ is the set of smooth points in the special fiber of minimal proper regular model of X over $\mathbf{Z}_p$. [58].

Lecture 4 17/9/2019

A few results applying Chabauty-Coleman to prove uniform bounds:

Theorem 2.19 Stoll '13. *If $X/\mathbf{Q}$ is hyperelliptic of genus g with Jacobian of Mordell-Weil rank $r \leq g-3$, then*

$$\#X(\mathbf{Q}) \leq 8rg + 33(g-1) + 1$$

[88].

Theorem 2.20 Katz-Rabinoff-Zuerieck-Brown '19. *If $X/\mathbf{Q}$ curves of genus g with $r \leq g-3$.*

$$\#X(\mathbf{Q}) \leq 84g^2 - 98g + 28.$$

Ref KRZB and expository paper.

Suppose $X/\mathbf{Q}$ is genus 3, hyperelliptic curve of rank 0, Stoll's bound gives $\#X(\mathbf{Q}) \leq 67$. Is there a curve meeting this bound? Or even $\#X(\mathbf{Q}) = 10$?

In the LMFDB we find in $g = 2$, $r = 0$ the record seems to be $\#X(\mathbf{Q}) = 8$. For `http://lmfdb.org/Genus2Curve/Q/1116.a.214272.1` we have $\#X(\mathbf{Q}) = 8$.

$$J(\mathbf{Q}) \simeq \mathbf{Z}/39$$

with simple Jacobian (first found by Elkies).

It is possible to use constructions of Howe, Leprevost, Poonen, Elkies, others to construct Jacobians with even larger torsion (and possibly curves of low rank with many rational points? Earlier we talked about computing annihilating differentials in the Chabauty-Coleman method. Here is a concrete example, to motivate a discussion of explicit Coleman integration.

Example 2.21 Consider

$$X\colon y^2 = x^5 - 4x^3 + 3x + 1$$

`http://lmfdb.org/Genus2Curve/Q/3920.b.62720.1`.

$$J(\mathbf{Q}) \simeq \mathbf{Z} \oplus \mathbf{Z}/2.$$

$$N = 3920 = 2^4 \cdot 5 \cdot 7^2.$$

And

$$X(\mathbf{Q}) \supseteq \{\infty, (0, \pm 1), (1, \pm 1), (-1, \pm 1)\}$$

$$\#X_{\mathbf{F}_{11}}(\mathbf{F}_{11}) = 13$$

$$\#X_{\mathbf{F}_{13}}(\mathbf{F}_{13}) = 14$$

so the Chabauty-Coleman bound by itself does not prove that we found all the $\mathbf{Q}$-points already. The point

$$[(1,1) - \infty]$$

is of infinite order in $J(\mathbf{Q})$. We use it to construct an annihilating differential. Let $p = 11$. Then a basis of $H^0(X, \Omega^1)$ is given by

$$\left\{\omega_i = \frac{x^i\,\mathrm{d}x}{2y}\right\}_{i=0,1}$$

so the annihilating differential η is some $\mathbf{Q}_p$-linear combination of ω_0, ω_1. We use the values of

$$\int_\infty^{(1,1)} \omega_0,\ \int_\infty^{(1,1)} \omega_1$$

to compute η. We find

$$\int_\infty^{(1,1)} \omega_0 = 8\cdot 11 + 7\cdot 11^2 + 7\cdot 11^3 + 4\cdot 11^7 + 9\cdot 11^8 + O(11^9) = \alpha$$

$$\int_\infty^{(1,1)} \omega_1 = 3\cdot 11 + 2\cdot 11^2 + 4\cdot 11^3 + 3\cdot 11^4 + 6\cdot 11^5 + 6\cdot 11^6 + 8\cdot 11^7 + 3\cdot 11^8 + O(11^9) = \beta.$$

Then

$$\int_\infty^{(1,1)} \beta\omega_0 - \alpha\omega_1 = 0$$

so take

$$\eta = \beta\omega_0 - \alpha\omega_1.$$

To use η to compute $X(\mathbf{Q})$ or more precisely, a finite subset of $X(\mathbf{Q}_p)$ containing $X(\mathbf{Q})$ we need to compute the collection of indefinite Coleman integrals

$$\left\{\int_\infty^{P_t} \eta\right\}$$

where P_t ranges over all residue disks. And solve for $z \in X(\mathbf{Q}_p)$ such that

$$\int_\infty^{z} \eta = 0.$$

So to compute α, β and the functions we needed Coleman integrals between points not in the same residue disk. $\square$

Goal: show how to compute these p-adic integrals.

Let $X/\mathbf{Q}$ be a curve. Let X^{an} be the associated rigid analytic space. (Let $\mathcal{X}$ be a smooth curve over $\mathbf{Z}_p$ s.t.

$$\mathcal{X} \otimes \mathbf{Q}_p \simeq X \otimes \mathbf{Q}_p,$$

then X^{an} denotes the rigid analytic space over $\mathbf{Q}_p$ which is the generic fibre of $\mathcal{X}$.)

Definition 2.22 A wide open subspace of X^{an} is the complement in X^{an} of the union of a finite collection of disjoint closed disks of radius $\lambda_i < 1$. $\lozenge$

Example 2.23 Let

$$X\colon\ y^2 = \prod_{i=1}^{5}(x - \alpha_i)$$

take out closed disks of radius λ_i for each $P_i = (\alpha_i, 0)$ and ∞. $\square$

Theorem 2.24 Coleman, Coleman-de Shalit. *Let η, ξ be 1-forms on a wide open V of X^{an} and $P, Q, R \in V(\mathbf{Q}_p)$. Let $a, b \in \mathbf{Q}_p$. The definite Coleman integral has the following properties*

1. *Linearity*
$$\int_P^Q \alpha\eta + b\xi = \alpha \int_P^Q \eta + b \int_P^Q \xi$$

2. *Additivity in endpoints*
$$\int_P^Q \eta = \int_P^R \eta + \int_R^Q \eta$$

3. *Change of variables, if $V' \subseteq X'$ is a wide open subspace of a rigid analytic space X' and $\phi\colon V \to V'$ is a rigid analytic map then*
$$\int_P^Q \phi^*\eta = \int_{\phi P}^{\phi Q} \eta.$$

4. *Fundamental theorem of calculus*
$$\int_P^Q \mathrm{d}f = f(Q) - f(P)$$
for f a rigid analytic function on V.

Goal: want to integrate
$$\int_P^Q \omega$$
for a 1-form of the second kind, $P, Q \in V(\mathbf{Q}_p)$. Idea

1. Take ϕ to be a lift of frobenius from the special fibre.
2. Write a basis $\{\omega_i\}$ of 1-forms of the second kind.
3. Compute $\phi^*\omega_i$ and use properties of Coleman integral to relate $\int_P^Q \phi^*\omega_i$ to $\int_P^Q \omega_i$ and other terms we can compute.

[59], [37], also Stephanie Chan MMath thesis (is this online?)
Setup $p \neq 2$ prime
$$\overline{X}/\mathbf{F}_q,\ q = p^n$$
hyperelliptic of genus g with affine equation
$$y^2 = P(x)$$
with $P(x)$ monic degree $2g + 1$, with no repeated roots.
$$X\colon \overline{X} \smallsetminus \{\infty, y = 0\}.$$
W ring of Witt vectors over $\mathbf{F}_q$, (the unique unramified extension of $\mathbf{Z}_p$ with residue field $\mathbf{F}_q$.

Choose a lift $\tilde{P}$ of P, to a monic polynomial of degree $2g + 1$. Over W this gives a lift $\widetilde{X}$ of X. Let $A = W[x, y, y^{-1}]/(y^2 - \tilde{P}(x))$ Let $A^\dagger$ be the weak completion of A, explicitly let v_p denote the p-adic valuation on W extend it to polynomials. If $g(x) = \sum a_i x^i$, define $v_p(g) = \min\{v_p(a_i)\}$. The elements of $A^\dagger$ are series

$$\sum_{-\infty}^{\infty}(S_n(x) + T_n(x)y)y^{2n}$$

where S_n and T_n are polynomials of degree at most $2g$ s.t. limits are positive.

Lecture 5 19/9/2019

References for Rigid Geometry: [38] [21].

$\overline{X}/\mathbf{F}_q$ a hyperelliptic curve of genus g, with odd degree model and monic, no repeated roots.

$$X\colon \overline{X} \setminus \{\infty, y = 0\}$$

$$\widetilde{X}$$

is a lift of X to $\mathbf{Z}_q$ the ring of Witt vectors over $\mathbf{F}_q$.

$$y^2 = \tilde{P}(x).$$

$$A\colon \mathbf{Z}_q[x, y, y^{-1}]/(\tilde{y}^2 - \tilde{P}(x))$$

$A^\dagger$ the weak completion of A, this is

$$\left\{\sum_{-\infty}^{\infty} s_n(x)y^n : s_n \in \mathbf{Z}_q[x],\ \deg s_n \leq 2g,\ \mathrm{ord}_p(s_n) > c^n \text{ for some } c > 0\right\}.$$

Monsky-Washnitzer cohomology is a p-adic cohomology theory for smooth affine varieties, over fields of characteristic p.

Theorem 2.25 Special case, Berthelot, (1974, 1997). *The algebraic de Rham cohomology of $\widetilde{X}$ coincides with the Monsky-Washnitzer cohomology of X.*

Monsky-Washnitzer cohomology is finite dimensional and is equipped with an action of Frobenius. So the theorem tells us that we can compute via a description of de Rham cohomology.

Proposition 2.26 *The de Rham cohomology of A splits into eigenspaces under the hyperelliptic involution: a positive eigenspace generated by*

$$\frac{x^i\,\mathrm{d}x}{y^2},\ i = 0, \ldots, 2g$$

and a negative eigenspace generated by

$$\frac{x^i\,\mathrm{d}x}{y},\ i = 0, \ldots, 2g - 1.$$

We lift p-power frobenius to an endomorphism of $A^\dagger$ by defining it as the canonical Witt vector frobenius on $\mathbf{Z}_q$.

$$(a_0, a_1, \ldots) \mapsto (a_0^p, a_1^p, \ldots)$$

for $a_i \in \mathbf{F}_q$, then extend it to $\mathbf{Z}_q[x]$ by mapping $x \mapsto x^p$. Then since $y^2 = \tilde{P}(x)$, we have

$$(y^\sigma)^2 = (y^2)^\sigma = (\tilde{P}(x))^\sigma$$

$$= (\tilde{P}(x))^\sigma \left(\frac{y^2}{\tilde{P}(x)}\right)^p = \frac{y^{2p}\tilde{P}(x)^\sigma}{\tilde{P}(x)^p}$$

$$\begin{aligned} y &\mapsto y^p \left(\frac{\tilde{P}(x)^\sigma}{\tilde{P}(x)^p}\right)^{\frac{1}{2}} \\ &= y^p \left(1 + \frac{\tilde{P}(x)^\sigma - \tilde{P}(x)^p}{\tilde{P}(x)^p}\right)^{\frac{1}{2}} \\ &= y^p \sum_{i=0}^{\infty} \binom{1/2}{i} \left(\frac{\tilde{P}(x)^\sigma - \tilde{P}(x)^p}{y^{2p}}\right)^i \end{aligned}$$

Remark 2.27 Here is why we removed the Weierstrass points (we don't want to divide by y and have things diverge). Its possible to compute a Frobenius lift without deleting Weierstrass points, but then we need to solve for images of x, y using a 2 variable newton iteration.

Further extend to differentials by sending

$$\mathrm{d}x \mapsto \mathrm{d}(x^p) = px^{p-1}\,\mathrm{d}x$$

define $F_* = \sigma^{\log_p q}$ this is a lift of q-power frobenius.

Key reduction lemmas, (to prove prop on eigenspaces).

Lemma 2.28 *If $A(x) = \tilde{P}(x)B(x) + \tilde{P}'C(x)$ then*

$$\frac{A(x)\,\mathrm{d}x}{y^2} = \left(B(x) + \frac{2C'(x)}{s-2}\right)\frac{\mathrm{d}x}{y^{s-2}}$$

as elements of $H^1_{MW}(X)$.

We also have

$$\mathrm{d}(x^i y^j) = ix^{i-1}\,\mathrm{d}x\, y^j + x^i j y^{j-1}\,\mathrm{d}y,$$

use $y^2 = \tilde{P}(x)$ which implies

$$\mathrm{d}(y^2 = \tilde{P}(x)) = 2y\,\mathrm{d}y = \tilde{P}'(x)\,\mathrm{d}x$$

$$\implies \mathrm{d}y = \frac{\tilde{P}'(x)\,\mathrm{d}x}{2y}$$

giving

$$\mathrm{d}(x^i y^j) = ix^{i-1}y^j\,\mathrm{d}x + x^i j y^{j-1}\frac{\tilde{P}'(x)\,\mathrm{d}x}{2y}.$$

A special case of this: let $Q(x) = x^{m-2g}$ then

$$\mathrm{d}(Q(x)y) = (Q(x)\tilde{P}'(x) + 2Q'(x)\tilde{P}(x))\frac{\mathrm{d}x}{y} \equiv 0 \text{ in } H^1_{MW}(X).$$

Goal for Coleman integration: We compute

$$\left(\frac{x^i\,\mathrm{d}x}{y}\right)^\sigma$$

reduce using the above reductions to get a cohomologous differential that's a linear combination of the basis

$$\left\{\frac{x^i\,\mathrm{d}x}{y}\right\}_{i=0,\dots,2g-1}.$$

What does this look like?

1. The reduction process is essentially subtracting the right linear combinations of $\mathrm{d}(x^i y^j)$ and using $y^2 = \tilde{P}(x)$.

2. Precision is lost when we divide by p in the reduction algorithm, so we'll need to measure the loss of precision at each step to know how many provably correct p-adic digits we have.

We compute

$$\left(\frac{x^i\,\mathrm{d}x}{y}\right)^\sigma = \frac{px^{pi+p-1}\,\mathrm{d}x}{y^p}\sum_{i=0}^{L}\binom{-1/2}{i}\frac{(\tilde{P}(x)^\sigma - \tilde{P}(x)^p)^i}{y^{2pi}}$$

we need to know how large L must be to get provably correct expansions.

If the result of this is

$$\sum_{j=-M}^{N}\frac{A_j(x)\,\mathrm{d}x}{y^{2j+1}}$$

using the reduction formulas to eliminate the $j = N$ term then the $N-1$ term until no terms with $j > 0$ remain. Do likewise with the $j = -M, -M+1, \ldots$ terms.

At the end of the reduction algorithm we are left with

$$\left(\frac{x^i\,\mathrm{d}x}{y}\right)^\sigma = \mathrm{d}f_i + \sum_{j=0}^{2g-1} M_{ji}\frac{x^j\,\mathrm{d}x}{y}$$

the $\mathrm{d}f_i$ is whats eliminated by the reduction algorithm, we sum the d's at each step.

Do this for each $i = 0, \ldots, 2g-1$. Then $M = (M_{ij})$ gives the matrix of Frobenius. Its characteristic polynomial gives you the numerator of the zeta function of X.

Lemmas on precision:

Lemma 2.29 *Let $A(x) \in \mathbf{Z}_q[x]$ be a polynomial of degree $\leq 2g$. For some $m > 0$ consider the reduction of*

$$\omega = \frac{A(x)\,\mathrm{d}x}{y^{2m+1}}$$

by Reduction 1

$$\omega = \frac{A(x)\,\mathrm{d}x}{y^{2m+1}} = \frac{B(x)\,\mathrm{d}x}{y} + \mathrm{d}f$$

with $B(x) \in \mathbf{Q}_q[x]$ with $\deg B(x) \leq 2g-1$. We have

$$p^{\lfloor \log_p(2m-1)\rfloor}B(x) \in \mathbf{Z}_q[x].$$

$$f = \sum_{k=-1}^{m-1}\frac{F_k(x)}{y^{2k+1}},\ \deg F_k \leq 2g.$$

Lemma 2.30 *Let $A(x) \in \mathbf{Z}_q[x]$ be a polynomial of degree $\leq 2g$. For some $m > 0$ consider the reduction of*

$$\omega = \frac{A(x)y^{2m}\,\mathrm{d}x}{y}$$

by Reduction 2

$$\omega = \frac{A(x)y^{2m}\,\mathrm{d}x}{y} = \frac{B(x)\,\mathrm{d}x}{y} + \mathrm{d}f$$

with $B(x) \in \mathbf{Q}_q[x]$ *with* $\deg B(x) \leq 2g-1$,

$$f = cy^{2m+1} + \sum_{k=0}^{m-1} F_k(x)y^{2k+1}$$

$c \in \mathbf{Q}_q$, $\deg F_k \leq 2g$, $p^{\lfloor \log_p(2g+1)(2m+1) \rfloor} B(x) \in \mathbf{Z}_q[x]$.

Proposition 2.31 *To get N correct digits in the expansion after reduction we need to start with precision*

$$N_1 = N + \max\left\{\left\lfloor \log_p(2M-3)\right\rfloor, \left\lfloor \log_p(2g+1)\right\rfloor\right\} + 1 + \left\lfloor \log_p(2g-1)\right\rfloor,$$

where M is the smallest integer s.t.

$$M - \max\left\{\left\lfloor \log_p(2M+1)\right\rfloor, \left\lfloor \log_p(2g+1\right\rfloor)\right\}.$$

Example 2.32 Let

$$y^2 = \tilde{P}(x) = x^3 + x + 1/\mathbf{Q}$$

let $p = 5$ (or take this over $\mathbf{F}_5$ and lift to $\mathbf{Z}_5$). Let $N = 2$ be the number of correct 5-adic digits, so $M = 3$, so $N_1 = 3$, use the differentials $\frac{\mathrm{d}x}{y}$, $\frac{x\,\mathrm{d}x}{y}$

$$\left(\frac{\mathrm{d}x}{y}\right)^{\sigma} = \left(\frac{25x+50}{y^{15}} + \frac{75x^2+100x+25}{y^{13}} + \frac{50x^2+50x+100}{y^{11}} + \frac{75x+50}{y^{9}} + \frac{50x^2+50x}{y^{7}} + \frac{70x^2+70x+25}{y^{5}} + \frac{5x}{y^3}\right.$$

similar for

$$\left(\frac{x\,\mathrm{d}x}{y}\right)^{\sigma} = \left(\frac{100x^2+100x+75}{y^{15}} + \cdots\right)\mathrm{d}x \pmod{5^3}$$

let F_k be the polynomial in the term

$$\frac{F_k\,\mathrm{d}x}{y^{2k+1}}$$

starting from $k = 7$, set $s_k(x) = F_k(x)$, compute a series of polynomials inductively for $k-1, k-2, \ldots, 0$. Given S_{k+1} find polynomials A_{k+1}, B_{k+1} s.t.

$$A_{k+1}\tilde{P} + B_{k+1}\tilde{P}' = s_{k+1}$$

then set $s_k(x) = F_k(x) + A_{k+1}(x) + \frac{2B'_{k+1}(x)}{2k+1}$

$$\left(\frac{\mathrm{d}x}{y}\right)^{\sigma} = 15x\frac{\mathrm{d}x}{y} \pmod{5^2}$$

$$\left(\frac{x\,\mathrm{d}x}{y}\right)^{\sigma} = (22x+18)\frac{\mathrm{d}x}{y} \pmod{5^2}$$

$$M = \begin{pmatrix} 0 & 18 \\ 15 & 22 \end{pmatrix} \pmod{5^2}.$$

□

I missed a day heere!

Lecture 7 1/10/2019

Set-up for Tuitman's algorithm:
X: Smooth projective curve $\mathbf{F}_q$, birational to

$$Q(x, y) = y^{d_x - 1} + Q_{d_x - 1} y^{d_x - 1} + \cdots + Q_0 = 0$$

is irreducible, where $Q_i \in \mathbf{F}_q[x]$ for $i = 0, \ldots, d_x - 1$. This is part II of Tuitman [93] as we have a not necessarily smooth model.

Tuitman's idea:

1. Use the (low degree) map $x \colon X \to \mathbf{P}^1$.
2. remove the ramification locus of x, call this $r(x) = 0$, c.f. Kedlaya's algorithm where we deleted the Weierstrass points.
3. Choose a lift of Frobenius that sends x to x^p. Compute y via Hensel lifting.
4. Compute the action of Frobenius on differentials, reduce in cohomology, using Lauders fibration algorithm.

Then for a basis $\{\omega_i\}$ of $H^1_{\mathrm{dR}}(X)$ Tuitman's algorithm computes:

$$\phi^* \omega_i = \mathrm{d} f_i + \sum_j M_{ji} \omega_j$$

and as before this can be used to give an algorithm for Coleman integration [8].

Let

$$S = \mathbf{Z}_q[x, 1/r],\ R = \mathbf{Z}_q[x, 1/r, y]/Q$$

where Q is a lift of Q to $\#\mathbf{Z}_q$ that is monic with same monomials in support. This is possibly an issue for $g \geq 5$, see Tuitmans paper. See also [29] for heuristics, possible solutions in higher genus.

Let $V = \operatorname{Spec} S$, $U = \operatorname{Spec} R$. The ring of overconvergent functions on U is

$$R^\dagger = \mathbf{Z}_q \langle x, 1/r, y \rangle^\dagger / Q$$

Goal: compute a lift of Frobenius on $R^\dagger$ in an explicit and fast way.

Let $\mathbf{F}_q(x, y)$ denote the field of fractions of $R \otimes_{\mathbf{Z}_q} \mathbf{F}_q$ and $\mathbf{Q}_q(x, y)$ the field of fractions of $R \otimes_{\mathbf{Z}_q} \mathbf{Q}_q$.

Assumption 0 : The polynomial $r(x)$ is separable over $\mathbf{F}_q$, recall that

$$\Omega^1_{R^\dagger} = \frac{R^\dagger \, \mathrm{d}x \oplus R^\dagger \, \mathrm{d}y}{\mathrm{d}Q}$$

and if we write $\mathrm{d} \colon R^\dagger \to \Omega^1_{R^\dagger}$ we have

$$H^1_{rig}(U) = \operatorname{coker}(\mathrm{d}) \otimes \mathbf{Q}_q.$$

[10]

We will compute $H^(X) \subseteq H^1(U)$???????????????

Proposition 2.33 *$R^\dagger$ is a free module of rank d_x over $S^\dagger = \mathbf{Z}_q\langle x, 1/r \rangle^\dagger$. A basis is*

$$[1, y, \ldots, y^{d_x - 1}].$$

Theorem 2.34 *There is a lift of Frobeius ϕ on $R^\dagger$ that sends x to x^p.*

idea compute $\phi(y)$ by Hensel lifting, using equation

$$Q^\sigma(x^p, \phi(y))$$

note that this is possible since we've removed zeroes of $\frac{\partial Q}{\partial y}$ from the curve by deleting $r(x)$.

After precomputing $\phi(y), \phi(y^2), \dots, \phi(y^{d_x-1})$ and $\phi(1/r)$ it is easy to compute ϕ on $R^\dagger, \Omega^1_{R^\dagger}$.

Proposition 2.35 *Let $G \in M_{d_x \times d_x}(\mathbf{Z}_q[x, 1/r])$ denote the matrix s.t.*

$$\mathrm{d}(y^j) = \sum_{i=0}^{d_x-1} G_{i+1,j+1} y^i \,\mathrm{d}x$$

for $j = 0, \dots, d_x - 1$. then $G = M/r$ where $M \in \mathrm{Mat}_{d_x \times d_x}(\mathbf{Z}_q[x])$.

Assumption 1: Let $W^0 \in \mathrm{GL}_{d_x}(\mathbf{Z}_q[x, 1/r])$, $W^\infty \in \mathrm{GL}_{d_x}(\mathbf{Z}_q[x, 1/x, 1/r])$ be matrices such that if we denote

$$b^0_j = \sum_{i=0}^{d_x-1} W^0_{i+1,j+1} y^i$$

$$b^\infty_j = \sum_{i=0}^{d_x-1} W^\infty_{i+1,j+1} y^i$$

for all $0 \le j \le d_x - 1$. Then $\{b^0_j\}_{j=0}^{d_x-1}$ is an integral basis for $\mathbf{Q}(x, y)$ over $\mathbf{Q}[x]$. $\{b^\infty_j\}_{j=0}^{d_x-1}$ is an integral basis for $\mathbf{Q}(x, y)$ over $\mathbf{Q}[1/x]$.

Remark 2.36 Magma can compute these integral bases.

Once we compute the action of Frobenius on 1-forms we need to reduce, Tuitman uses Lauder's fibration algorithm.

1. Reduce pole order of points not lying over ∞.
2. Reduce pole order of points lying over ∞.

Let r' denote $\mathrm{d}r/\mathrm{d}x$ for points not over ∞.

Proposition 2.37 *For all $l \in \mathbf{N}$ and every $w \in \mathbf{Q}_q[x]^{\oplus d_x}$ there exist vectors $u, v \in \mathbf{Q}_q[x]^{\oplus d_x}$ such that*

$$\deg(v) < \deg(r)$$

and

$$\frac{\sum_{i=0}^{d_x-1} w_i b^0_i}{r^l} \frac{\mathrm{d}x}{r} = \mathrm{d}\left(\frac{\sum_{i=0}^{d_x-1} v_i b^0_i}{r^l}\right) + \left(\frac{\sum_{i=0}^{d_x-1} u_i b^0_i}{r^{l-1}}\right) \frac{\mathrm{d}x}{r}$$

Proof. Since r is separable, r' is invertible in $\mathbf{Q}_q[x]/r$ Check that there exists a unique solution v to the $d_x \times d_x$ linear system.

$$\left(\frac{M}{r'} - lI\right) v \equiv \frac{w}{r'} \pmod{r}$$

over $\mathbf{Q}_q[x]/(r)$. Then take

$$u = \frac{w - (M - lr'I)v}{r} - \frac{\mathrm{d}v}{\mathrm{d}x}.$$

■

For points over infinity, similar proposition. ?????????

Theorem 2.38 *Define the $\mathbf{Q}_q$-vector spaces*

$$E_0 = \left\{ \left(\sum_{i=0}^{d_x - 1} u_i(x) b_i^0 \right) \frac{\mathrm{d}x}{r} : u \in \mathbf{Q}_q[x]^{\oplus d_x} \right\}$$

$$E_\infty = \left\{ \left(\sum_{i=0}^{d_x - 1} u_i(x, 1/x) b_i^\infty \right) \frac{\mathrm{d}x}{r} : u \in \mathbf{Q}_q[x, 1/x]^{\oplus d_x} \right\}$$

$$B_0 = \left\{ \sum_{i=0}^{d_x - 1} v_i(x) b_i^0 : v \in \mathbf{Q}_q[x]^{\oplus d_x} \right\}$$

$$B_\infty = \left\{ \sum_{i=0}^{d_x - 1} v_i(x, 1/x) b_i^\infty : v \in \mathbf{Q}_q[x, 1/x]^{\oplus d_x} \right\}$$

then $E_0 \cap E_\infty$ and $\mathrm{d}(B_0 \cap B_\infty)$ are finite dimensional $\mathbf{Q}_q$-vector spaces and

$$H^1_{rig}(U) \simeq (E_0 \cap E_\infty)/\mathrm{d}(B_0 \cap B_\infty).$$

Theorem 2.39 *There is an exact sequence*

$$0 \to H^1(X) \to H^1_{rig}(U) \xrightarrow{)(\mathrm{res}_0 \oplus \mathrm{res}_\infty) \otimes \mathbf{Q}_q}$$

Lecture 8 3/10/2019

I lovingly stole this from Angus' notes, ty Angus.

1. Determine a basis for cohomology. We want to find $\omega_0, \dots, \omega_{k-1} \in (E_0 \cap E_\infty) \cap \Omega^1(U)$ such that
   (a) $\{\omega_0, \dots, \omega_{k-1}\}$ is a basis of
   $$H^1_{\mathrm{rig}} \cong (E_0 \cap E_\infty)/d(B_0 \cap B_\infty)$$
   (b) The class of every element of $(E_0 \cap E_\infty) \cap \Omega^1(U)$ in $H^1_{\mathrm{rig}}(U)$ has p-adically integral coefficients with respect to $\{\omega_0, \dots, \omega_{k-1}\}$.
   (c) $\{\omega_0, \dots, \omega_{k-1}\}$ is a basis for the kernel of $\mathrm{res}_0 \oplus \mathrm{res}_\infty$ and hence for the subspace $H^1_{\mathrm{rig}}(X)$ of $H^1_{\mathrm{rig}}(U)$.
2. Compute lift of Frob ϕ, and compute the action of Frob on $\{\omega_0, \dots, \omega_{k-1}\}$.
3. Reduce pole orders so that we have
   $$\phi^* \omega_i = df_i + \sum_j M_{ji} \omega_j$$
   where
   $$df_i = \underbrace{df_{i,0}}_{\text{finite pole reduction}} + \underbrace{df_{i,\infty}}_{\text{infinite pole reduction}} + df_{i,\mathrm{end}}$$

Remark 2.40

1. Let X be a genus 3 smooth plane quartic, say $X = X_s(13)$, the split Cartan curve of level 13. Then $\dim H^1_{\mathrm{rig}}(X) = 6$, but $\dim H^1_{\mathrm{rig}}(U) = 45 = 6 + 39$,

where $39 = 3 \deg r(x)$.

2. For applications to Coleman integrals between "good points", proceed as before
$$\int_{\phi(P)}^{\phi(Q)} \omega_i = \int_P^Q \phi^* \omega_i$$
and correct endpoints.

3. For Coleman integration from a *very bad point* (a point above ∞ or a point with x-coordinate such that $r(x) = 0$) B, split up the integral
$$\int_B^Q \omega_i = \int_B^{B'} \omega_i + \int_{B'}^Q \omega_i$$
for B' a point near the boundary of the residue disk of B.

Finite pole order reduction:. For $i = 0, \dots, 2g-1$, find $f_{i,0} \in \mathcal{R}^\dagger \otimes \mathbf{Q}_p$ such that
$$\phi^* \omega_i = df_{i,0} + G_i \frac{dx}{r}$$
where $G_i \in \mathcal{R} \otimes \mathbf{Q}_p$ only has poles above ∞.

Infinite pole order reduction:. For $i = 0, \dots, 2g-1$, find $f_{i,\infty} \in \mathcal{R} \otimes \mathbf{Q}_p$ such that
$$\phi^* \omega_i = df_{i,0} + df_{i,\infty} + H_i$$
where H_i only has poles at point P above ∞, and $\operatorname{ord}_P(H_i) \geq (\operatorname{ord}_0(W) - \deg r + 2)e_p$ where $W = (W^0)^{-1} W^\infty$ and e_p is the index of ramification of x-map at P.

Final reduction:. For $i = 0, \dots, 2g-1$, find $f_{i,\mathrm{end}} \in \mathcal{R} \otimes \mathbf{Q}_p$ such that
$$\phi^* \omega_i = \underbrace{df_{i,0} + df_{i,\infty} + df_{i,\mathrm{end}}}_{=df_i} + \sum_j M_{ji} \omega_j.$$

2.4 Iterated Coleman Integrals

Let $X/\mathbf{Q}$ be a smooth, projective curve, p a prime of good reduction.

Goal:. Describe an iterated Coleman integral on $X_{\mathbf{Q}_p}$ and applications to rational points.

Roughly speaking, an iterated Coleman integral is an iterated path integral
$$\int_P^Q \eta_n \dots \eta_1 = \int_0^1 \int_0^{t_1} \cdots \int_0^{t_{n-1}} f_n(t_n) \dots f_1(t_1) dt_n \dots dt_1.$$

Idea:. Want to apply Kedlaya/Tuitman as before, by computing action of Frob and reducing to simpler integrals. Earlier we had
$$\int_P^Q df = f(Q) - f(P)$$
and now reduce n-fold integral to $(n-1)$-fold integral.

Notation:. $P, Q \in X(\mathbf{Q}_p)$, $\eta_1, \ldots, \eta_n$ are 1-forms of the 2nd kind, without poles at P, Q.

$$\eta_P^Q \eta_1 \ldots \eta_n = \int_P^Q \eta_1(R_1) \int_P^{R_1} \eta_2(R_2) \ldots \int_P^{R_{n-2}} \eta_{n-1}(R_{n-1}) \int_P^{R_{n-1}} \eta_n$$

for dummy variables R_i.

2.5 Algorithm for tiny iterated integral

Input:. Points $P, Q \in X(\mathbf{Q}_p)$ in same residue disk.

Output:. $\int_P^Q \eta_1 \ldots \eta_n$

1. Compute a local coordinate at P, $(x(t), y(t))$
2. For each k, write $\eta_k(x, y)$ as $\eta_k(t)dt$.
3. Let $I_{n+1} = 1$. Compute for $k = n, n-1, \ldots, 2$

   $$I_k = \int_P^{R_{k-1}} \eta_k I_{k+1} = \int_P^{t(R_{k-1})} \eta_k(t) I_{k+1} dt$$

   where $t(R_{k-1})$ is parameterising points in the residue disk of P.
4. $\int_P^Q \eta_1 \ldots \eta_n = \int_P^{t(Q)} \eta_1(t) I_2(t) dt$.

To compute more general iterated Coleman integrals, we'll use the following properties.

Proposition 2.41 *Let $\omega_{i_1}, \ldots \omega_{i_n}$ be forms of the second kind, regular at $P, Q \in X(\mathbf{Q}_p)$.*

1. $$\int_P^P \omega_{i_1} \ldots \omega_{i_n} = 0$$
2. $$\sum_{\text{all permutations } \sigma} \int_P^Q \omega_{\sigma(i_1)} \ldots \omega_{\sigma(i_n)} = \prod_{j=1}^n \int_P^Q \omega_{i_j}$$
3. $$\int_P^Q \omega_{i_1} \ldots \omega_{i_n} = (-1)^n \int_Q^P \omega_{i_n} \ldots \omega_{i_1}$$

Corollary 2.42 $\int_P^Q \omega_i \ldots \omega_i = \frac{1}{n!} \left(\int_P^Q \omega_i \right)^n$

References. For classical theory of iterated integrals

- K-T. Chen, Algebras of iterated path integrals and fundamental groups, Trans. of AMS 156 (1971) [30]

For p-adic theory

- Coleman, Dilogarithms, regulators and p-adic L-functions, Invent. Math 1982 [34].
- Coleman, de Shalit, p-adic regulators on curves and special values of p-adic L-functions, Invent. Math. 1988 [33]
- Besser, Coleman integration using the Tannakian formalism, Math. Ann. 2002 [15]

Remark 2.43 Still have linearity in the integrand, change of variables under rigid analytic maps. Be careful about additivity in endpoints.

Lemma 2.44 *Let $P, P', Q \in X(\mathbf{Q}_p)$. Then*

$$\int_P^Q \omega_{i_1} \dots \omega_{i_n} = \sum_{j=0}^{n} \int_{P'}^Q \omega_{i_1} \dots \omega_{i_j} \int_P^{P'} \omega_{i_{j+1}} \dots \omega_{i_n}$$

For all algorithms, we'll restrict to the case $n = 2$ (double Coleman integrals).

Example 2.45 Let $\phi(P), \phi(Q)$ be images of $P, Q \in X(\mathbf{Q}_p)$ under Frobenius ϕ, then

$$\int_P^Q \omega_i \omega_k = \int_P^{\phi(P)} \omega_i \omega_k + \int_{\phi(P)}^{\phi(Q)} \omega_i \omega_k + \int_{\phi(Q)}^{Q} \omega_i \omega_k + \int_P^{\phi(P)} \omega_k \int_{\phi(P)}^{Q} \omega_i + \int_{\phi(P)}^{\phi(Q)} \omega_k \int_{\phi(Q)}^{Q} \omega_i \tag{2.1}$$

□

2.6 Strategy for computing double Coleman integrals of words in $H^1_{\mathbf{dR}}(X)$

Input:. $\int_P^Q \omega_i \omega_j$

1. Compute $\phi(P)$, $\phi(Q)$
2. Compute action of Frob and do some linear algebra to simplify

$$\int_{\phi(P)}^{\phi(Q)} \omega_i \omega_j = \int_P^Q \phi^*(\omega_i)\phi^*(\omega_j)$$

3. Correct endpoints using equation (2.1).

$$\begin{aligned}
\int_{\phi(P)}^{\phi(Q)} \omega_i \omega_k &= \int_P^Q \phi^*(\omega_i \omega_k) \\
&= \int_P^Q (\phi^* \omega_i)(\phi^* \omega_k) \\
&= \int_P^Q \left(df_i + \sum_j M_{ji} \omega_j \right)\left(df_k + \sum_j M_{jk} \omega_j \right) \\
&= \int_P^Q \left(df_i df_k + df_i \sum_j M_{jk} \omega_j + \sum_j M_{ji} \omega_j df_K + \sum_j M_{ji} \omega_j \sum_j M_{jk} \omega_j \right)
\end{aligned}$$

Lecture 9 8/10/2019

Last time: we were computing Coleman integrals

$$\int_{\phi(P)}^{\phi(Q)} \omega_i \omega_j = \int_P^Q \phi^*(\omega_i \omega_j)$$

$$= \int_P^Q \mathrm{d} f_i \, \mathrm{d} f_k + \int_P^Q \sum_j M_{ji} \omega_j \, \mathrm{d} f_k + \int_P^Q \mathrm{d} f_i \sum_j M_{jk} \omega_j + \int_P^Q \sum_j M_{ji} \omega_j \sum_j M_{jk} \omega_j$$

expand each of the first three terms into expressions involving single Coleman integrals

$$\int_P^Q \mathrm{d}f_i \, \mathrm{d}f_k = \int_P^Q \mathrm{d}f_i(R) \int_P^R \mathrm{d}f_k = \int_P^Q \mathrm{d}f_i(R)(f_k(R) - f_k(P)) = \int_P^Q f_k \, \mathrm{d}f_i - f_k(P)(f_i(Q) - f_i(P))$$

$$\int_P^Q \sum M_{ji}\omega_j \, \mathrm{d}f_k = \int_P^Q \sum M_{ji}\omega_j(R) \int_P^R \mathrm{d}f_k = \int_P^Q \sum M_{ji}\omega_j(R)(f_k(R) - f_k(P)) = \int_P^Q \sum_j f_k M_{ji}\omega_j - f_k(P) \int_P$$

$$\int_P^Q \mathrm{d}f_i \sum_j M_{jk}\omega_j = \int_P^Q \mathrm{d}f_i(R) \int_P^R \sum M_{jk}\omega_j$$

$$= f_i(R) \int_P^R \sum_j M_{jk}\omega_j| - \int_P^Q f_i(R) \left(\sum M_{jk}\omega_j(R)\right))$$

$$= f_i(Q) \int_P^Q \sum_j M_{jk}\omega_j - \int_P^Q f_i \sum M_{jk}\omega_j$$

then collect terms If c_{ik} is the sum of the expanded above, then the vector of double coleman integrals is a solution of a linear system involving all of the above.

Application (preview). Let $\mathcal{E}/\mathbf{Z}$ be the minimal regular model of an elliptic curve, and let $\mathcal{X} = \mathcal{E} - 0$. Let

$$\omega_0 = \frac{\mathrm{d}x}{2y + a_1 x + a_3}, \; \omega_1 = x\omega_1$$

in Weierstrass coordinates, let b be 0 (really a tangential base-point at 0). Or an integral 2-torsion point. Let p be an odd prime of good reduction, suppose $\mathcal{E}$ has analytic rank 1, and Tamagawa product 1.

Consider

$$\log(z) = \int_b^z \omega_0, \; D_2(z) = \int_b^z \omega_0\omega_1,$$

can think of log as extending the log in the formal group.

Theorem 2.46 Kim '10, B.-Kedlaya-Kim '11. *Suppose P is a point of infinite order in $\mathcal{E}(\mathbf{Z})$ then $\mathcal{X}(\mathbf{Z}) \subseteq \mathcal{E}(\mathbf{Z})$ is in the zero set of*

$$f(z) = (\log(P))^2 D_2(z) - (\log(z))^2 D_2(P).$$

Chabauty-Coleman wrap up. What if Coleman's bound

$$\#X(\mathbf{Q}) \leq \#X(\mathbf{F}_p) + 2g - 2$$

is larger than $\#X(\mathbf{Q})_{\text{known}}$. If we carry out Chabauty-Coleman, what can we do if we seem to find "extra" p-adic points that don't look like they live if $X(\mathbf{Q})$?

Try using the Mordell-Weil sieve (developed by Scharashkin in his thesis 99, adapted by Flynn ('04), Poonen-Schaefer-Stoll 07, Bruin-Stoll. See (((Unresolved xref, reference "bib-bruin-stoll-mw"; check spelling or use "provisional" attribute))) (((Unresolved xref, reference "bib-siksek-mw"; check spelling or use "provisional" attribute))) .

Set-up

$$X/\mathbf{Q}$$

a curve of genus $g \geq 2$, $M > 0$ an integer

$$i \colon X \hookrightarrow J$$

suppose $c_M \subseteq J(\mathbf{Q})/MJ(\mathbf{Q})$ is a set of residue classes for which we want to show that no rational point $P \in X(\mathbf{Q})$ maps to c_M under $\pi \circ i$.

Simplest case: pick a good prime v

$$\begin{tikzcd} X(\mathbf{Q}) \arrow[r] \arrow[d] & J(\mathbf{Q})/MJ(\mathbf{Q}) \arrow[d] \\ X(\mathbf{F}_v) \arrow[r] & J(\mathbf{F}_v)/MJ(\mathbf{F}_v) \end{tikzcd}$$

if $\alpha_v(c_M) \cap \beta_v(X(\mathbf{F}_v)) = \emptyset$ then done. Typically this is not enough: More generally consider set S of good primes and the commutative diagram

$$\begin{tikzcd} X(\mathbf{Q}) \arrow[r] \arrow[d] & J(\mathbf{Q})/MJ(\mathbf{Q}) \arrow[d] \\ \prod_v X(\mathbf{F}_v) \arrow[r] & \prod_v J(\mathbf{F}_v)/MJ(\mathbf{F}_v) \end{tikzcd}$$

then it suffices to show that $\alpha_s(c_M) \cap \beta_s(\prod_v X(\mathbf{F}_v)) = \emptyset$.

The goal is then to find a good set of S s.t.

$$A(S, c_M) = \left\{ c \in c_M : \alpha_S(c) \in \beta_s(\prod_v X(\mathbf{F}_v)) \right\}$$

is empty.

Heuristically the size of $A(S, c_M)$ is as follows: For a good prime

$$X_{M,v} = \beta_v(X(\mathbf{F}_v))$$

$$\gamma(v, M) = \frac{\# X_{M,v}}{\# J(\mathbf{F}_v)/M(J(\mathbf{F}_v))}$$

Note : v is only useful if $\gamma(v, M) < 1$.

Expected size of $A(S, M)$ is

$$\# c_M \prod_c \gamma(v, M)$$

want this to be small.

Difficulties in using the sieve, the set, $A(S, c_M)$ can be large. The computation of images of $X(\mathbf{F}_v)$ in $J(\mathbf{F}_v)$ can become infeasible (the computation requires v discrete logs in $J(\mathbf{F}_v)$). Can be mitigated by using primes for which $\# J(\mathbf{F}_v)$ is sufficiently smooth.

Two variations on Chabauty-Coleman: Pass to a collection of covering curves, (difficulty: constructing covers) Elliptic Chabauty method: (difficulty computing $E(K)$ for $K/\mathbf{Q}$ a larger degree number field.

These methods can potentially compute $X(\mathbf{Q})$ when $\operatorname{rk} J(\mathbf{Q}) \geq g$.

Theorem 2.47 Chevalley-Weil. *Let $f \colon Y \to X$ be an unramified morphism of curves $/\mathbf{Q}$ then there is a computable finite extension $K/\mathbf{Q}$ such that*

$$f^{-1}(X(\mathbf{Q})) \subseteq Y(K).$$

Theorem 2.48 Wetherell '97. *There is a finite set of unramified covering curves $Y_i \to X$ over $\mathbf{Q}$ (all isomorphic over $\overline{\mathbf{Q}}$), such that*

$$X(\mathbf{Q}) \subseteq \bigcup_{i=1}^{n} f_i(Y_i(\mathbf{Q})).$$

Remark 2.49 When X is an elliptic curve this is descent in the proof of the Mordell-Weil theorem.

2.7 Introduction to p-adic heights

Lecture 11 17/10/2019

The theory of p-adic heights has developed over 20 years, with work due to Bernardi, Neron, Schneider, Perrin-Riou, Mazur, Tate, Zarhin, Iovita, Werner, Coleman, Gross, Nekovar.

We will begin with p-adic heights on elliptic curves. Let $E/\mathbf{Q}$ be an elliptic curve, then a p-adic height h is a function

$$h\colon E(\overline{\mathbf{Q}}) \to \mathbf{Q}_p$$

that plays a similar role to the canonical height

$$\hat{h}E(\overline{\mathbf{Q}}) \to \mathbf{R}.$$

Let $p \geq 5$ be a prime of good ordinary reduction for E. Let $0 \neq P \in E(\mathbf{Q})$, then write

$$P = (x(P), y(P)) = \left(\frac{a(P)}{d(P)^2}, \frac{b(P)}{d(P)^2}\right)$$

and assume $(a(P), d(P)) = (b(P), d(P)) = 1$ and $d \geq 1$. $d(P)$ is the denominator of P.

Suppose P satisfies two conditions

1. P reduces to 0 in $E(\mathbf{F}_p)$.
2. P reduces to a non-singular point of $E(\mathbf{F}_l)$ for all bad primes l.

1. Implies $E(P) = -x(P)/y(P)$ is divisible by P.

Definition 2.50 Let $E/\mathbf{Q}$ and $p \geq 5$ be good ordinary, the cyclotomic p-adic height h on such points P in $E(\mathbf{Q})$ is

$$h(P) = \frac{1}{p}\log_p\left(\frac{\sigma(P)}{d(P)}\right).$$

$\sigma(P)$ is the p-adic sigma function associated to $E/\mathbf{Z}_p$. ◊

What is $\sigma(P)$?

Mazur-Stein-Tate "Computation of p-adic heights and log convergence", Doc. Math 2006. Mazur-Tate "The p-adic sigma function", Duke 1991. Mazur-Tate gave 11 different characterizations of the p-adic sigma function. We'll describe one characterization, let

$$x(t) = t^{-2} + \cdots \in \mathbf{Z}_p((t))$$

be x in the formal group of $E/\mathbf{Z}_p$, then

$$y(t) = t^{-3} + \cdots \in \mathbf{Z}_p((t))$$

(Silverman AEC, Ch IV).

Theorem 2.51 Mazur-Tate. *There is exactly on odd function*

$$\sigma(t) = t + \cdots \in t\mathbf{Z}_p[[t]]$$

and constant $c \in \mathbf{Z}_p$ that together satisfy the p-adic differential equation

$$x(t) + c = \frac{-\mathrm{d}}{\omega}\left(\frac{1}{\sigma}\frac{\mathrm{d}\sigma}{\omega}\right)$$

ω is the invariant differential associated to a chosen Weierstrass model for E

$$\omega = \frac{\mathrm{d}x}{2y + a_1 x + a_3}$$

and

$$c = \frac{a_1^2 + 4a_2 - E_2(E, \omega)}{12}$$

we'll say more about $E_2(E, \omega)$ in a bit!

Lemma 2.52 *The height function h extends uniquely to the full Mordell-Weil group $E(\mathbf{Q})$ and satisfies $h(nQ) = n^2 h(Q)$ for all $n \in \mathbf{Z}$, and $Q \in E(\mathbf{Q})$ for $P, Q \in E(\mathbf{Q})$ setting*

$$(P, Q) = h(P) + h(Q) - h(P + Q)$$

we get a pairing on $E(\mathbf{Q})$.

To compute $h(Q)$ for arbitrary $Q \in E(\mathbf{Q})$. Let $n_1 = \#E(\mathbf{F}_p)$, $n_2 = \mathrm{lcm}_v(\{c_v\})$, let $n = \mathrm{lcm}(n_1, n_2)$ then $P = nQ$ satisfies 1) and 2) from earlier. So compute $h(P) = h(nQ)$ and then

$$h(Q) = \frac{1}{n^2} h(nQ) = \frac{1}{n^2} h(P).$$

Remark 2.53 The p-adic regulator Reg_p of $E/\mathbf{Q}$ is the determinant of the matrix of pairings on $E(\mathbf{Q})/E(\mathbf{Q})_{\mathrm{tors}}$.

Conjecture 2.54 Schneider '82. *The (cyclotomic) height pairing is non-degenerate, equivalently Reg_p is non-zero.*

Contrast with canonical height $\hat{h}(P) = 0 \iff P$ is torsion

Remark 2.55 This p-adic regulator fits into a p-adic BSD conjecture.

Conjecture 2.56 Special case of Mazur-Tate-Teitelbaum, '86, Inventionnes. *Suppose E has good ordinary reduction at p, let $\mathcal{L}_p(E, T)$ be the p-adic L-function attached to $E/\mathbf{Q}$.*

1. $$\mathrm{ord}_{T=0}\,\mathcal{L}_p(E, T) = \mathrm{rk}\,E(\mathbf{Q})$$

2. $$\mathcal{L}_p^*(E, 0) = \frac{\epsilon_p \prod c_v |\text{Ш}(E/\mathbf{Q})| \,\mathrm{Reg}_p}{\#E(\mathbf{Q})_{tors}^2}$$

   the leading coefficient.

$\epsilon_p = (1 - \alpha^{-1})^2$ where α is the unit root of $x^2 - a_p x + p = 0$.

Remark 2.57 See also Stein-Wuthrich, "Algorithms for the arithmetic of elliptic curves using Iwasawa theory", Math. Comp. 2013.

Back to $E_2(E,\omega)$, Katz '73, gave an interpretation of $E_2(E,\omega)$ as a direction of the unit-root eigenspace of frobenius acting on Monsky-Washnitzer cohomology. Suppose $E\colon y^2 = f(x)$, then the basis for

$$H^1_{\mathrm{dR}}(E) = H^1_{MW}(E')^- = \left\{\frac{\mathrm{d}x}{y}, \frac{x\,\mathrm{d}x}{y}\right\}$$

moreover $H^1_{\mathrm{dR}}(E) = H^0(E,\Omega^1) \oplus U$ with U the unit root subspace. Compute the matrix of p-power frobenius F, want to find a basis for U. We know that

$$F\left(\frac{\mathrm{d}x}{y}\right) \in pH^1_{\mathrm{dR}}(E)$$

so that $\mod p^n$, U is the span of $F^n\left(\frac{x\,\mathrm{d}x}{y}\right)$ so for each n write

$$F^n\left(\frac{x\,\mathrm{d}x}{y}\right) = a_n\frac{\mathrm{d}x}{y} + b_n\frac{x\,\mathrm{d}x}{y}$$

then $E_2(E,\omega) = -12\frac{a_n}{b_n} \pmod{p^n}$.

What does this have to do with rational/integral points on E?

$$E\colon y^2 = f(x)$$

Recall

$$x + c = \frac{-\,\mathrm{d}}{\omega}$$

in formal group

$$\implies \omega(x+c) = -\,\mathrm{d}\left(\frac{1}{\sigma}\frac{\mathrm{d}\sigma}{\omega}\right)$$

$$\implies \int\left(\frac{x\,\mathrm{d}x}{y} + \frac{c\,\mathrm{d}x}{y}\right) = -\frac{\mathrm{d}\sigma}{\sigma\omega} = \frac{\mathrm{d}}{-}.$$

Lecture 1? 22/10/2019

p-adic heights after Coleman-Gross, "p-adic heights on curves" 1989.

Let $X/\mathbf{Q}$ be a smooth projective curve of genus $g \geq 1$ and p a prime of good reduction for X and ordinary reduction for J. We'll be thinking of $X/\mathbf{Q}_p = K$.

Important: fix a subspace of $H^1_{\mathrm{dR}}(Y_{/K})$ complementary to $H^0(X,\Omega^1_{X/K})$ call this W. $H^1_{\mathrm{dR}}(X_{/K}) = H^0(X,\Omega^1_X) \oplus W$.

We'd like to understand the p-adic height of two degree 0 divisors D_1, D_2. Assume $D_1, D_2 \in \mathrm{Div}^0(X)$ have disjoint support.

Definition 2.58 The cyclotomic p-adic height is a symmetric bilinear pairing

$$h\colon \mathrm{Div}^0(X) \times \mathrm{Div}^0(X) \to \mathbf{Q}_p$$

$$(D_1, D_2) \mapsto h(D_1, D_2)$$

disjoint support.

where

1. $$h(D_1,D_2) = \sum_v h_v(D_1,D_2) = h_p(D_1,D_2) + \sum_{v\neq p} h_v(D_1,D_2)$$

$$= \int_{D_2}\omega_{D_1} + \sum_{v\neq p} m_v \log_p(v)$$

with the left term a coleman integral of the third kind and m_v some intersection multiplicities.

2.
$$h(D, \div(\beta)) = 0$$
for $\beta \in \mathbf{Q}(X)^\times$, so h is well defined on $J \times J$.

$\Diamond$

Remark 2.59 The local heights can be extended non-uniquely to give the self-pairing
$$h(D, D) = \sum h_v(D, D)$$
this needs a choice of tangent vector at each point in the support of D.

Remark 2.60 The local height at p is a Coleman integral of a normalized differential w.r.t. W of the third kind.

e.g. if
$$X\colon y^2 = f(x)$$
is a hyperelliptic curve
$$D_1 = (P) - (Q),\ P, Q \in X(\mathbf{Q}),\ y(P), y(Q) \neq 0$$
can we construct ω with $\mathrm{Res}(\omega) = D_1$? We want residue 1 at P and -1 at Q. So ω has simple poles at P, Q. e.g.
$$\omega = \frac{\mathrm{d}x}{2y}\left(\frac{y + y(P)}{x - x(P)} - \frac{y + y(Q)}{x - x(Q)}\right)$$
has $\mathrm{Res}(\omega) = D_1$. But there are lots more!

Recall: $H^1_{\mathrm{dR}}(X)$ has a canonical non-degenerate form given by cup-product pairing
$$H^1_{\mathrm{dR}}(X/K) \times H^1_{\mathrm{dR}}(X/K) \to K$$
$$([\mu_1], [\mu_2]) \mapsto [\mu_1] \cup [\mu_2]$$
where
$$[\mu_1] \cup [\mu_2] = \sum_Q \mathrm{Res}_Q \left(\mu_2 \int \mu_1\right)$$
note that μ_1, μ_2 are differentials of the second kind (residue 0). So the residue does not depend on the choice of local integral for μ_1 since μ_2 has no residue at any point.

Let $T(K)$ be the space of differentials of the third kind on X, at most simple poles, integer residues. We have a residue divisor hom
$$\mathrm{Res}\colon T(K) \to \mathrm{Div}^0(X)$$
$$\omega \mapsto \mathrm{Res}(\omega) = \sum_p \mathrm{Res}_p\, \omega$$
we have the short exact sequence
$$0 \to H^0(X, \Omega^1_X) \to T(K) \xrightarrow{\mathrm{Res}} \mathrm{Div}^0(X) \to 0.$$
We're interested in $T_l(K)$ these are log differentials
$$\frac{\mathrm{d}f}{f},\ f \in K(X)^\times.$$

Since
$$T_l(K) \cap H^0(X, \Omega^1_{X/K}) = \{0\}$$
and $\mathrm{Res}(\mathrm{d}f/f) = \mathrm{div}(f)$ we get from the above sequence
$$0 \to H^0(X, \Omega^1_X) \to T(K)/T_l(K) \to J(K) \to 0$$
Proposition 2.61 *There is a canonical homomorphism*
$$\Psi \colon T(K)/T_l(K) \to H^1_{\mathrm{dR}}(X).$$
Note: Ψ is the identity on differentials of the first kind. Ψ sends third kind differentials to second kind or exact differentials. Ψ sends log differentials to 0.

Definition 2.62 Let $D \in \mathrm{Div}^0(X)$ then ω_D is the unique form of the third kind with
$$\mathrm{Res}(\omega_D) = D$$
and
$$\Psi(\omega_D) \in W$$
recall we fixed
$$H^1_{\mathrm{dR}}(X) = H^0(X, \Omega^1_X) \oplus W.$$
◊

Definition 2.63 The local height at p of D_1, D_2 is
$$h_p(D_1, D_2) = \int_{D_2} \omega_{D_1}.$$
◊

Remark 2.64 When X has good reduction and J has ordinary reduction then there is a canonical choice for W, the unit root subspace for the action of frobenius.

Proposition 2.65 *If $\{\omega_0, \ldots, \omega_{2g-1}\}$ is a basis for $H^1_{\mathrm{dR}}(X)$ with $\{\omega_0, \ldots, \omega_{g-1}\} \subseteq H^0(X, \Omega^1)$. Then*
$$\{(\phi^*)^n \omega_g, \ldots, (\phi^*)^n \omega_{2g-1}\}$$
is a basis for W mod p^n where ϕ is a lift of frobenius.

Algorithm 2.66 Coleman integral of differential of the third kind, with poles in non-weierstrass disks. *Input: ω with $\mathrm{Res}(\omega) = (P) - (Q)$. $P, Q \in X(\mathbf{Q})$ non-weierstrass. $R, S \in X(\mathbf{Q}_p)$, $R, S \notin \mathrm{disk}(P), \mathrm{disk}(Q)$. Output:*
$$\int_S^R \omega$$

1. *Compute $\Psi(\omega) \in H^1_{\mathrm{dR}}(X)$. Let ϕ be a lift of Frobenius. Let $\alpha = \phi^*\omega - p\omega$. Use $\Psi(\omega)$ and frobenius equivariance. We have*
$$\begin{aligned}\Psi(\alpha) &= \Psi(\phi^*\omega - p\omega)\\ &= \Psi(\phi^*\omega) - \Psi(p\omega)\\ &= \phi^*\Psi(\omega) - p\Psi(\omega)\end{aligned}$$
2. *Let β be a 1-form with $\mathrm{Res}(\beta) = (R) - (S)$. Compute $\Psi(\beta)$.*
3. *Compute $\Psi(\alpha) \cup \Psi(\beta)$, easy since both are elements in H^1_{dR} that we just computed.*

4. *Compute*

$$\int_{\phi(S)}^{S} \omega$$

and

$$\int_{R}^{\phi(R)} \omega$$

tiny

5. *Compute*

$$\sum_A \mathrm{Res}_A(\alpha \int \beta).$$

6.

$$\int_S^R \omega = \frac{1}{1-p}\left(\Psi(\alpha) \cup \Psi(\beta) + \sum_A \mathrm{Res}_A(\alpha \int \beta) - \int_{\phi(S)}^{S} \omega - \int_{R}^{\phi(R)} \omega\right)$$

Remark 2.67 Idea behind this algorithm is that α is almost of the second kind, in that the sum of the residues of α in each annulus is 0.

Algorithm 2.68 Local height at p. *Output: $h_p(D_1, D_2)$.*

1. *Let ω be a differential in $T(K)$ with $\mathrm{Res}(\omega) = D_1$.*
2. *Compute $\Psi(\omega) = \sum_{i=0}^{2g-1} a_i\omega_i \in H^1_{\mathrm{dR}}(X)$. Then*

$$\Psi(\omega) - \sum_{i=0}^{g-1} a_i\omega_i \in W$$

let $\omega_{D_1} = \omega - \sum_{i=0}^{g-1} a_i\omega_i$.

3. *Compute using the previous algorithm*

$$h_p(D_1, D_2) = \int_{D_2} \omega_{D_1}.$$

More details in Balakrishnan-Besser "computing local p-adic heights on hyperelliptic curves". IMRN 2012.

What if D_1 and D_2 have common support? e.g. $h_p(D, D)$.

The local height at P would be

$$h_p(D, D) = \int_D \omega_D$$

idea of Gross "local heights on curves" Arithmetic Geometry '86.

At each point x in the common support of your divisors, choose a basis t, t_x for the tangent space.

Let $z = z_\infty$ be a uniformizer at x

$$\partial_t z = 1$$

any function

$$f \in K(X)^\times$$

then has a well-defined "value" at x

$$f[x] = \frac{f}{z^m}(x)$$

where $m = \mathrm{ord}_x(f)$. This depends only on t and not z. To do this for local p-adic heights use Besser's p-adic Arakelov theory, JNT 2005.

Balakrishnan-Besser Coleman-Gross height pairings and p-adic sigma function, Crelle, 2015.

Proposition 2.69 *Let $X/\mathbf{Q}$ be a hyperelliptic curve with odd degree model monic.*

$$D = (P) - (\infty)$$

$$h(D, D) = \text{“} \cancel{\int_D \omega_D''}$$

$$= \int_{i=0}^{g-1} \int_{\infty}^{P} \omega_i \overline{\omega}_i$$

ω_i self dual basis for cup.

Lecture 1? 29/10/2019

How do we use local heights on Jacobians of curves to study integral points.

Theorem 2.70 Quadratic Chabauty for integral points on hyperelliptic curves B.-Besser-Muller. *Let $f(x) \in \mathbf{Z}[x]$ be monic separable polynomial of degree $2g + 1 \geq 3$, that does not reduce to a square modulo q for any prime q. (in the paper monic is not used, this condition then restricts the reduction type) Let $U = \mathrm{Spec}(\mathbf{Z}[x, y]/(y^2 - f(x)))$ and let X be the normalization of the proj closure of the generic fiber of U. Let J be the Jacobian on X and assume $\mathrm{rk}\, J(\mathbf{Q}) = g$, choose a prime p of good ordinary reduction. Suppose that the p-adic Coleman integrals*

$$f_i(z) = \int_{\infty}^{z} \omega_i = \int_{\infty}^{z} \frac{x^i \,\mathrm{d}x}{2y}$$

then there exists explicitly computable constants $\alpha_{ij} \in \mathbf{Q}_p$ s.t. the locally analytic function

$$\rho(z) = \theta(z) - \sum_{0 \leq i \leq j \leq g-1} \alpha_{ij} f_i(z) f_j(z),$$

where $\theta(z) = h_p((z) - (\infty), (z) - (\infty))$ is an extension of the Coleman-Gross local height at p which takes values in

$$\mathcal{U}(\mathbf{Z}[1/p])$$

in an effectively computable finite set $S \subseteq \mathbf{Q}_p$.

Refs, Balakrishnan, Jennifer S., Amnon Besser, and J. Steffen Müller. "Quadratic Chabauty: P-Adic Heights and Integral Points on Hyperelliptic Curves." Journal Für Die Reine Und Angewandte Mathematik (Crelles Journal) 2016, no. 720 (January 1, 2016). https://doi.org/10.1515/crelle-2014-0048. Balakrishnan, Jennifer S., Amnon Besser, and J. Steffen Müller. "Computing Integral Points on Hyperelliptic Curves Using Quadratic Chabauty." Mathematics of Computation 86, no. 305 (October 12, 2016): 1403–34. https://doi.org/10.1090/mcom/3130. Müller, Jan Steffen. "Computing Canonical Heights Using Arithmetic Intersection Theory." Mathematics of Computation 83, no. 285 (2014): 311–336. https://doi.org/10.1090/S0025-5718-2013-02719-6.

Proof. Sketch: Recall the Coleman-Gross p-adic height for $X/\mathbf{Q}$ is a symmetric bilinear pairing

$$h \colon J(\mathbf{Q}) \times J(\mathbf{Q}) \to \mathbf{Q}_p$$

the global height decomposes as a sum of local heights

$$h(D_1, D_2) = \sum_v h_v(D_1, D_2)$$

in particular we have

$$h(D_1, D_2) = h_p(D_1, D_2) + \sum_{v \neq p} h_v(D_1, D_2)$$

$$= \int_{D_2} \omega_{D_1} + \sum_{v \neq p} h_v(D_1, D_2)$$

where ω_{D_1} is a normalized differential of the 3rd kind (depends on a splitting of the Hodge filtration on $H^1_{\mathrm{dR}}(X/\mathbf{Q}_p)$) and for $v \neq p$

$$h_v(D_1, D_2) = m_v \log_p v,\ m_v \in \mathbf{Q}$$

computed using arithmetic intersection theory. See Muller and: Bommel, Raymond van, David Holmes, and J. Steffen Müller. "Explicit Arithmetic Intersection Theory and Computation of Néron-Tate Heights." Mathematics of Computation, 2019. https://arxiv.org/abs/1809.06791v1.

Then look at $h = h_p + \sum_{v \neq p} h_v$ note

1. h is a quadratic form, so can be written in terms of a basis of space of quadratic forms for $J(\mathbf{Q})$ and this can be done using Coleman integrals.

$$h(z - \infty, z - \infty) = \sum \alpha_{ij} f_i(z) f_j(z),$$

2. h_p is a locally analytic function and in the extension to self-pairing:

$$h_p(z - \infty, z - \infty) = -2 \sum_{i=0}^{g-1} \int_\infty^z \omega_i \bar{\omega}_i,\ \omega_i = \frac{x^i\,\mathrm{d}x}{2y},\ \bar{\omega}_i \text{ cup product duals.}$$

3. The sum

$$\sum_{v \neq p} h_v(z - \infty, z - \infty)$$

takes on finitely many values in S when restricted to p-integral points. The set S can be computed by knowing the reduction of X at bad primes.

4. Then rewrite

$$h - h_p \in \{\sum_{v \neq p} h_v\} = S$$

5. this ρ can be computed as a convergent power series in each residue disk. So now pretend we are working in classical Chabauty Coleman. Expand ρ in each disk, set equal to each value in S solve for all $t \in U(\mathbf{Z}_p)$ s.t. $\rho(z) \in Z$. Take all such points call that $X(\mathbf{Z}_p)_2$.

6. It's possible that $X(\mathbf{Z}_p)_2$ is strictly larger than the known points in $U(\mathbf{Z})$. In this case run 1-4 on a collection of good ordinary p and run Mordell-Weil sieve.

More details on each step

1. Let $D_1, \dots, D_g \in \mathrm{Div}^0(X)$ representing basis elements of $J(\mathbf{Q}) \otimes \mathbf{Q}$ then compute global height pairings. $h(D_i, D_j)$ using B.-Besser-Muller. A basis for spaces of bilinear forms on $J(\mathbf{Q})$ is
$$\frac{1}{2}(f_k f_l + f_l f_k)$$
so compute
$$\frac{1}{2}(f_k(D_i)f_l(D_j) + f_l(D_i)f_k(D_j))$$
do linear algebra to compute
$$\alpha_{k,l}$$
$$h(D_i, D_j) = \sum \alpha_{k,l}(\frac{1}{2}(f_k(D_i)f_l(D_j) + f_l(D_i)f_k(D_j)))$$

2. Want to compute
$$\{\bar{\omega}_i\}$$
for $0 \le 1 \le g-1$ such that $[\bar{\pi}_i] \cup [\omega_j] = \delta_{ij}$
   (a) Compute splitting of
   $$H^1_{\mathrm{dR}}(X/\mathbf{Q}_p) = H^0(X, \Omega^1_{\mathrm{X}}) \oplus W,$$
   where W is the unit root eigenspace of frob, recall that modulo p^n a basis for W is
   $$\{(\phi^*)^n \omega_g, \dots, (\phi^*)^n \omega_{2g-1}\}$$
   (b) Let $\tilde{\omega}_j$ be a projection of ω_j onto W along $H^0(X, \Omega^1)$. i.e.
   $$\tilde{\omega}_j = \omega_j - \sum_{i=0}^{g-1} a_i \omega_i.$$
   (c) use cup product matrix to compute
   $$\bar{\omega}_0 = \sum_{i=g}^{2g-1} b_{0i}\tilde{\omega}_i$$
   $$\vdots$$
   $$\bar{\omega}_{g-1} = \sum_{i=g}^{2g-1} b_{g-1,i}\tilde{\omega}_i$$
   then let
   $$\theta(z) = -2\sum_{i=0}^{g-1}\int \omega_i\bar{\omega}_i$$
   to compute this as a power series in each residue disk for each residue disk compute a $\mathbf{Z}_p$ point P, the value $\theta(P)$ local coordinate z_P at P.
   $$\theta(z) = -2\sum_{i=0}^{g-1}\int_\infty^z \omega_i\bar{\omega}_i$$
   $$= -2\left(\sum_{i=0}^{g-1}\int_\infty^P \omega_i\bar{\omega}_i + \sum_{i=0}^{g-1}\int_P^{z_P} \omega_i\bar{\omega}_i + \sum_{i=0}^{g-1}\int_P^{z_P} \omega_i \int_\infty^P \bar{\omega}_i\right)$$
   $$= \theta(P) - 2\left(\sum_{i=0}^{g-1}\int_P^{z_P} \omega_i\bar{\omega}_i + \sum_{i=0}^{g-1}\int_P^{z_P} \omega_i \int_\infty^P \bar{\omega}_i\right)$$

3. Prop. There is a proper regular model $\mathcal{X}$ of $X \otimes \mathbf{Q}_q$ over $\mathbf{Z}_q$ $(q \neq p)$ such that if $\mathcal{X}$ is p-integral then

$$h_q((x) - (\infty), (x) - (\infty))$$

depends solely on the component of the special fibre $\mathcal{X}_q$ that the section in $\mathcal{X}(\mathbf{Z}_z)$ corresponding to x intersects. e.g. in $g = 2$ special fibres have been classified by Namikawa-Ueno and if $\mathcal{X}$ is semistable then the types are

$$[I_{n_1} - I_{n_2} - m] \text{ or } [I_{n_1 n_2 - n_3}]$$

pos integers n_i, m. Need to compute regular models (implementation in Magma by Donnelly) and grobner bases of ideals of divisors to compute intersection multiplicities.

■

Remark 2.71 Roughly speaking intersections are computing denominators which is why its not obvious how to go beyond integral points using this construction. e.g. for elliptic curves have Mazur-Stein-Tate p-adic height.

$$h(P) = \frac{1}{p}\log_p(\sigma(P)) - \frac{1}{p}\log_p(D(P))$$

Coleman-Gross

$$h(P - \infty) = h_p(P - \infty) + \sum_{v \neq p} h_v(P - \infty)$$

extended appropriately.

Example 2.72 Let

$$X\colon y^2 = (x^3 + x + 1)(x^4 + 2x^3 - 3x^2 + 4x + 4)$$

$$C_{496}^J$$

new modular curve studied by Baker Gonzalez-Jimenez Gonzalez, Poonen

$$J(\mathbf{Q}) = \mathbf{Z}^3 \oplus \mathbf{Z}/2$$

let $P = (-1, 2), Q = (0, 2), R = (-2, 12), S = (3, 62)$ want to show that up to hyperelliptic involution these are the only integral points. Gens for $J(\mathbf{Q}) \otimes \mathbf{Q}$.

$$\{P_1 = [(P) - (\infty)], P_2 = [(S) - (w(Q))], P_3 = [(w(S)) - (R)]\}.$$

□

Lecture 1? 31/10/2019

Goal today: Give more context for quadratic chabauty, discuss Kim's non-abelian Chabauty program.

References

1. "p-adic approaches to rational and integral points on curves" - Poonen

2. From chabauty's method to kim's non-abelian chabauty method - Corwin

Let X be a smooth projective curve over K a number field and let Z be a 0-dimensional subscheme. Let $U = X - Z$, $d = \#Z(\overline{K})$. The topological Euler characteristic of U is $\chi(U) = \chi(X) - d = 2g - 2 - d$. If $\chi(U) < 0$ we say that U is hyperbolic (we want to consider hyperbolic curves because they have nonabelian π_1.)

Example 2.73 $g = 0$, $d \geq 3$ e.g. $\mathbf{P}^1 \smallsetminus \{0, 1, \infty\}$. □

Example 2.74 $g = 1$, $d \geq 1$ e.g. punctured elliptic curve $E \smallsetminus \{0\}$. □

Example 2.75 $g = 2$, $d \geq 0$ e.g. smooth projective curves of genus $g \geq 2$ or punctured versions, integral points. □

Fix a prime p of good reduction for X.

Recall the classical Chabauty-Coleman diagram

$$\begin{tikzcd} X(K) \arrow[r] \arrow[d] & X(K_p) \arrow[d] & \\ J(K) \arrow[r] & J(K_p) \arrow[r] & \operatorname{Lie} J_{K_p} \end{tikzcd}$$

in the classical chabauty-coleman method, the image of $J(K)$ in the g-dimensional space Lie J_{K_p} spans a K_p subspace of dimension at most $r = \operatorname{rk} J(K)$. So if $r < g$ there exists a non-zero K_p valued functional on Lie J_{K_p} vanishing on $J(K)$. This pulls back to d non-zero locally analytic functions on $X(K_p)$ that vanish on $X(K)$.

Problem: By using the geometry of J impose too much structure, can't extend this to $r \geq g$. Kim's idea: Replace J with references to X and various homology groups, then generalize the diagram by replacing homology with various deeper quotients of (nonabelian) π_1.

Gives construction of Selmer varieties.

References for Kims work: Kim, Minhyong. "The Motivic Fundamental Group of $P^1 \smallsetminus \{0, 1, \infty\}$ and the Theorem of Siegel." Inventiones Mathematicae 161, no. 3 (September 2005): 629–56. https://doi.org/10.1007/s00222-004-0433-9. Kim, Minhyong. "The Unipotent Albanese Map and Selmer Varieties for Curves." Publications of the Research Institute for Mathematical Sciences 45, no. 1 (2009): 89–133. https://doi.org/10.2977/prims/1234361156. Kim, Minhyong. "Massey Products for Elliptic Curves of Rank 1." Journal of the American Mathematical Society 23, no. 3 (2010): 725–47. https://doi.org/10.1090/S0894-0347-10-00665-X.

$$\begin{tikzcd} X(K) \arrow[r] \arrow[d] & X(K_p) \arrow[d] & \\ J(K) \arrow[r] \arrow[d] & J(K_p) \arrow[r] \arrow[d] & \operatorname{Lie} J_{K_p} \\ \widehat{J(K)}[1/p] \arrow[r] \arrow[d] & \widehat{J(K_p)}[1/p] \arrow[ur] & \\ \operatorname{Sel}_{\mathbf{Q}_p}(J) = H^1_f(G_K, V) \arrow[r] \arrow[d] & H^1_f(G_{K_v}, V) \arrow[r] \arrow[d] & H_1^{\mathrm{dR}}(X_{K_p})/F^0 \\ H^1(G_K, V) & H^1(G_K, V) & \end{tikzcd}$$

We want to start by removing $J(K)$ from the diagram. Recall: Let M be an abelian group. The p-adic completion

$$\widehat{M} = \varprojlim_n M/p^n M$$

is a $\mathbf{Z}_p$-module. We can get a $\mathbf{Q}_p$-vector space by inverting p.

$$\widehat{M}[1/p] \simeq \widehat{M} \otimes_{\mathbf{Z}_p} \mathbf{Q}_p.$$

The group $J(K_p)$ is compact so that the images of $p^n J(K_p)$ in $\operatorname{Lie} J(K_p) \to 0$, p-adically as $n \to \infty$. So the homomorphism

$$J(K_p) \to \operatorname{Lie} J_{K_p}$$

factors through $\widehat{J(K_p)}$ and hence also through $\widehat{J(K_p)}[1/p]$. Since log is a local diffeomorphism with finite kernel get a $\mathbf{Q}_p$-linear map

$$\widehat{J(K_p)}[1/p] \to \operatorname{Lie} J_{K_p}$$

is an isomorphism.

Recall the Kummer exact sequence

$$0 \to J[m] \to J \xrightarrow{\cdot m} J \to 0$$

take $G_K = \operatorname{Gal}(\overline{K}/K)$-cohomology to get a long exact sequence which leads to a short exact sequence

$$0 \to J(K)/mJ(K) \xrightarrow{\kappa_m} H^1(G_K, J[m]) \to H^1(G_K, J)[m] \to 0$$

where κ is the Kummer map. There is a canonical G_K-equivariant isomorphism

$$J[m] \simeq H_1^{\text{et}}(J_{\overline{K}}, \mathbf{Z}/m) \simeq H_1^{\text{et}}(X_{\overline{K}}, \mathbf{Z}/m).$$

The Kummer map gives an embedding

$$J(K)/mJ(K) \hookrightarrow H^1(G_k, H_1^{\text{et}}(X_{\overline{K}}, \mathbf{Z}/m))$$

to get an embedding of $J(K)$ rather than just $J(K)/mJ(K)$ take $m = p^n$ and inverse limit.

Get a $\mathbf{Z}_p$-Tate module.

$$T = \varprojlim_n J[p^n] \simeq H_1^{\text{et}}(X_{\overline{K}}, \mathbf{Z}_p)$$

let $V = T[1/p] = T \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$. Let $J(K)_{\mathbf{Z}_p} = J(K) \otimes_{\mathbf{Z}} \mathbf{Z}_p$, $J(K)_{\mathbf{Q}_p} = J(K) \otimes_{\mathbf{Z}} \mathbf{Q}_p$.

This gives us embeddings

$$J(K)_{\mathbf{Z}_p} \hookrightarrow H^1(G_K, T)$$

$$J(K)_{\mathbf{Q}_p} \hookrightarrow H^1(G_K, V)$$

this is almost our replacement for J.

We still need to identify $\mathbf{Q}_p$-span of $J(K)$ inside $H^1(G_K, V)$ using V and without reference to J.

The vector space V has the structure of a G_K-rep so we want a Galois theoretic way of identifying the image of $J(K)_{\mathbf{Q}_p}$ in $H^1(G_K, V)$. This is where the Bloch-Kato Selmer groups come in. Back to the fundamental short exact sequence from the Kummer sequence let $m = p^n$ and we have the local diagram as well.

$$\begin{tikzcd}
0 \arrow[r] & J(K)/mJ(K) \arrow[r, "\kappa"] \arrow[d] & H^1(G_K, J[m]) \arrow[r] \arrow[d, "\alpha"] & H^1(G_K, J)[m] \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \prod_v J(K_v)/mJ(K_v) \arrow[r, "\beta"'] & \prod H^1(G_{K_v}, J[m]) \arrow[r] & \prod H^1(G_{K_v}, J)[m] \arrow[r] & 0
\end{tikzcd}$$

the selmer group is a finite dimensional subspace of $H^1(G_K, J[p^n])$.

$$\mathrm{Sel}_{p^n}(J) = \alpha^{-1}(\operatorname{im}\beta)$$

we have

$$J(K)/p^nJ(K) \hookrightarrow \mathrm{Sel}_{p^n}(J)$$

now taking inverse limits gives

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

and inverting p gives

$$\widehat{J(K)}[1/p] \hookrightarrow \mathrm{Sel}_{\mathbf{Q}_p} J \subseteq H^1(G_K, V)$$

let Ш be the Shafarevich-Tate group of J. we have

$$0 \to J(K)/p^nJ(K) \to \mathrm{Sel}_{p^n}(J) \to Ш[p^n] \to 0$$

take inverse limits and invert p

$$0 \to \widehat{J(K)}[1/p] \to \mathrm{Sel}_{\mathbf{Q}_p}(J) \to (\varprojlim_n Ш[p^n])[1/p] \to 0$$

if Ш$[p^\infty]$ is finite, then

$$\varprojlim_n Ш[p^n] = 0$$

so

$$\widehat{J(K)}[1/p] \simeq \mathrm{Sel}_{\mathbf{Q}_p}(J)$$

we want to determine the image of $J(K)_{\mathbf{Q}_p}$ in $H^1(G_K, V)$ in terms of V using V as a Galois rep. We're almost there, we've replaced $J(K)_{\mathbf{Q}_p}$ with $\mathrm{Sel}_{\mathbf{Q}_p}(J)$. Remaining problem is that the local conditions giving us

$$\mathrm{Sel}_{\mathbf{Q}_p}(J) \subseteq H^1(G_K, V)$$

we use information from the geometry of J. (certain subgroups of $\prod H^1(G_{K_v}, V)$). This problem was solved by Bloch and Kato using Bloch-Kato Selmer groups. use p-adic Hodge theory to re-interpret $\operatorname{im}\beta$.

Lecture 1? 5/11/2019

Recall the big chabauty-kim diagram.
Last time we had this

$$\begin{tikzcd}
J(K)/p^nJ(K) \arrow[r] \arrow[d] & H^1(G_K, J[p^n]) \arrow[d, "\alpha"] \\
\prod_v J(K_v)/p^nJ(K_v) \arrow[r, "\beta"'] & H^1(G_K, J[p^n])
\end{tikzcd}$$

$$\mathrm{Sel}_{p^n}(J) = \alpha^{-1}(\mathrm{im}(\beta))$$
$$\varprojlim_n \mathrm{Sel}_{p^n}(J) = \mathrm{Sel}_{\mathbf{Z}_p} J,$$

then we get
$$\widehat{J}(K)[1/p] \hookrightarrow \mathrm{Sel}_{\mathbf{Q}_p}(J) \subseteq H^1(G_K, V).$$

Goal is to determine the image of $J(K)_{\mathbf{Q}_p}$ in $H^1(G_K, V)$ in terms of the Galois representation V. We replaced $J(K)_{\mathbf{Q}_p}$ by $\mathrm{Sel}_{\mathbf{Q}_p}$, defined by local conditions. But the local conditions (subgroup of $\prod_v H^1(G_{K_v}, V)$ are defined via geometry of J rather than via galois reps.

Bloch and Kato defined $\mathrm{im}\,\beta$ using p-adic Hodge theory and defined $\mathrm{Sel}_{\mathbf{Q}_p}(J)$ in terms of data from V.

1. They wanted to extend Selmer and Shafarevich-Tate groups to motives beyond H^1 of abelian varieties.

2. this construction will let us extend the idea of Selmer group from

$$T = H_1^{\mathrm{et}}(X_{\overline{K}}, \mathbf{Z}_p) \simeq \pi_1^{\mathrm{et}}(X_{\overline{K}})^{\mathrm{ab}} \otimes \mathbf{Z}_p$$

   to certain (non-abelian) quotients of π_1^{et}.

Crash course in Bloch-Kato Selmer groups. Let V be a finite dimensional $\mathbf{Q}_q$-vector space with a continuous action of G_{K_v}. Let, $K_v = \mathbf{Q}_p$. Fontaine defined $D_{\mathrm{cris}}(V) = (B_{\mathrm{cris}} \otimes_{\mathbf{Q}_p} V)^{G_{K_v}}$ for a ring of p-adic periods B_{cris} we have

$$\dim_{K_v} D_{\mathrm{cris}}(V) \leq \dim_{\mathbf{Q}_p} V$$

and if equality holds we say that V is crystalline. See Berger, or Caruso, or Andre.

An element $\xi \in H^1(G_{K_v}, V)$ corresponds to an isomorphism class of extensions of $\mathbf{Q}_p$ by V
$$0 \to V \to E \to \mathbf{Q}_p \to 0$$

and ξ is said to be crystalline if the galois representation is. Let $H^1_f(G_{K_v}, V)$ be the set of crystalline classes in $H^1(G_{K_v}, V)$. The "local Bloch-Kato Selmer group" at v.

Definition 2.76 The Bloch-Kato Selmer group $H^1_f(G_{K_v}, V)$ is the set of $\xi \in H^1(G_K, V)$ whose image in $H^1(G_{K_v}, V)$ is crystalline for each $v|p$. ◊

Theorem 2.77 Bloch-Kato. *The image of the Kummer map*

$$\kappa_v \colon J(K_v)_{\mathbf{Q}} \to H^1(G_{K_v}, V)$$

is $H^1_f(G_{K_v}, V)$.

Corollary 2.78 *The Selmer group*

$$\mathrm{Sel}_{\mathbf{Q}_p} J$$

coincides with $H^1_f(G_K, V)$ in $H^1(G_K, V)$.

Need to also define log intrinsically, also needs a new target space in place of Lie $J(K_{K_p})$.

Definition 2.79 A filtered module over a commutative ring #][m R] is an R-module M with a collection
$$\{G^i M\}$$
of submodules that is decreasing
$$F^{i+1} M \subseteq F^i M, \forall i.$$
If $\bigcup F^i M = M$ the filtration is exhaustive. For any filtered R-module M the associated graded module
$$\mathrm{gr}(M) = \bigoplus_i \mathrm{gr}^i(M),\ \mathrm{gr}^i(M) = F^i M/Fi + 1M.$$
$\lozenge$

Recall the Hodge filtration on de Rham cohomology, this is a decreasing filtration F^i on $H^1_{\mathrm{dR}}(J_{K_p})$ with
$$0 = F^2 \subseteq F^1 = H^0(J_{K_p}, \Omega^1) \subseteq F^0 = H^1_{\mathrm{dR}}.$$

The de Rham cohomology $H^1_{\mathrm{dR}}(J_{K_p})$ is the dual of $H_1^{\mathrm{dR}}(J_{K_p})$ and has a decreasing hodge filtration dual to that of $H^1_{\mathrm{dR}}(J_{K_p})$, defined as
$$H^i H_1^{\mathrm{dR}}(J_{K_p}) = \mathrm{Ann}(F^{-i+1} H^1_{\mathrm{dR}}(J_{K_p}))].$$

$$H^0(X, \Omega^1)^\vee \simeq H^0(J, \Omega^1)^\vee = (\mathrm{gr}^1 H^1_{\mathrm{dR}}(J_{K_p}))^\vee = \mathrm{gr}^{-1} H_1^{\mathrm{dR}}(J_{K_p})$$
$$\mathrm{gr}^{-1} H_1^{\mathrm{dR}}(J_{K_p}) = H_1^{\mathrm{dR}}(J_{K_p})/F^0 H_1^{\mathrm{dR}}(J_{K_p}) \simeq H_1^{\mathrm{dR}}(X_{K_p})/F^0 H_1^{\mathrm{dR}}(X_{K_p})$$
this is our intrinsic definition of $H^0(X, \Omega^1)^\vee$.

More of our crash course on p-adic hodge theory. To define $\log_{BK}$.

We assume $K_p \simeq \mathbf{Q}_p$, Fontaine's theory defines a series of $\mathbf{Q}_p$-algebras with $G_{\mathbf{Q}_p}$-action and additional structure compatible with this, (i.e. frob, differential operators, hodge) we have
$$B_{crys} \subseteq B_{\mathrm{dR}}???$$

Facts, theres a descending filtration F^1 on B_{dR}, for which $B^+_{\mathrm{dR}} = F^0 B_{dR}$ is a DVR with fraction field B_{dR} and residue field $\mathbf{C}_p$. There is an action of frobenius on B_{crys} whose fixed subring is denoted
$$B^{\phi=1}_{crys}.$$

We have $B^{G_{K_p}}_{crys} = B^{G_{K_p}}_{\mathrm{dR}} = K_p$.

For a continuous p-adic representation V of $G_{\mathbf{Q}_p}$. We define
$$D_{\mathrm{dR}}(V) = (B_{\mathrm{dR}} \otimes V)^{G_{K_p}}$$
$$D^+_{\mathrm{dR}}(V) = (B^+_{\mathrm{dR}} \otimes V)^{G_{K_p}}$$
the filtration on B_{dR} induces one on $D_{\mathrm{dR}}(V)$.

If Y is a smooth variety over $\mathbf{Q}_p$ then p-adic height gives for
$$V = H^i_{\mathrm{et}}(Y_{\overline{\mathbf{Q}}_p}, \mathbf{Q}_p)$$
that
$$D_{\mathrm{dR}}(V) \xrightarrow{\sim} H^i_{\mathrm{dR}}(Y).$$

Respecting the Hodge filtration on either side. Also $D^+_{\mathrm{dR}}(V)$ is naturally identified with $F^0 D_{\mathrm{dR}}(V)$.

$$F^m D_{\mathrm{dR}}(V) = (F^m B_{\mathrm{dR}} \otimes V)^{G_{K_v}}$$

Frobenius on B_{crys} induces a Frobenius map on $D_{\mathrm{crys}}(V)$ and $V = H^i_{\mathrm{et}}(Y_{\overline{\mathbf{Q}}_p}, \mathbf{Q}_p)$ and Y good reduction with special fibre $Y_{\mathbf{F}_p}$. Then there's a natural isomorphism

$$D_{\mathrm{crys}}(V) \xrightarrow{\sim} H^1_{\mathrm{crys}}(Y_{\mathbf{F}_p}, \mathbf{Q}_p)$$

respects frob on each side.

D_{dR} and D_{crys} commute with taking $^\vee$ so have corresponding results for homology.

Example 2.80 Let $V = H^{\mathrm{et}}_1(X_{\overline{K}}, \mathbf{Q}_p)$ then

$$H^{\mathrm{dR}}_1(X_{K_p}) \simeq D_{\mathrm{dR}}(V) \simeq D_{\mathrm{crys}}(V)]$$

compat with hodge □

Lecture 1? 7/11/2019

$$T = H^{\mathrm{et}}_1(X_{\overline{K}}, \mathbf{Z}_p)$$
$$V = H^{\mathrm{et}}_1(X_{\overline{K}}, \mathbf{Q}_p)$$

want to define the Bloch-Kato logarithm.

$$\log_{BK} \colon H^1_f(G_{K_p}, V) \to H^{\mathrm{dR}}_1(X_{K_p})/F^0.$$

Bloch-Kato 1990 give a short exact sequence

$$0 \to \mathbf{Q}_p \xrightarrow{\alpha} B^{\phi=1}_{cris} \oplus B^+_{\mathrm{dR}} \xrightarrow{\beta} B_{\mathrm{dR}} \to 0,$$

where $\alpha(x) = (x, x), \beta(x, y) = x - y$. Tensor with V and take Galois cohomology to get

$$0 \to V^{G_{K_p}} \to D_{cris}(V)^{\phi=1} \oplus D^+_{\mathrm{dR}}(V) \to D_{\mathrm{dR}}(V) \to H^1(G_{K_p}, V) \to H^1(G_{K_p}, V \otimes B^{\phi=1}_{cris}) \to \cdots$$

Bloch-Kato show that

$$H^1_e(G_{K_p}, V) = \ker(H^1(G_{K_p}, V) \to H^1(G_{K_p}, V \otimes B^{\phi=1}_{cris}))$$

is equal to

$$H^1_f(G_{K_p}, V).$$

This gives a surjection

$$D_{\mathrm{dR}}(V)/D^+_{\mathrm{dR}}(V) \to H^1_f(G_{K_p}, V)$$

this is the Bloch-Kato exponential map. (coincides with usual exp in the case of a p-adic formal lie group). The kernel of this map is

$$D_{cris}(V)^{\phi=1}/V^{G_{K_p}}$$

this is trivial since V is the Tate module of an abelian variety (true because of the Weil conjecture, and what we know about eigenvalues of frobenius).

So in this case the Bloch-Kato exponential map has an inverse, our Bloch-Kato logarithm.

$$\log_{BK} \colon H^1_f(G_{K_p}, V) \xrightarrow{\sim} D_{\mathrm{dR}}(V)/D^+_{\mathrm{dR}}(V) \simeq H_1^{\mathrm{dR}}(X)/F^0$$

Kim's generalization. Let G be a group (resp. topological group). For subgroups

$$A, B \subseteq G$$

let $[A, B]$ denote the (the closure of) the commutator of the subgroups.

Definition 2.81 Let

$$G^{[1]} = G$$

$$G^{[2]} = [G^{[1]}, G]$$

$$\dots$$

$$G^{[i+1]} = [G^{[i]}, G]$$

then

$$G^{[1]} \trianglerighteq G^{[2]} \trianglerighteq \cdots$$

is a descending chain of normal subgroups of G called the lower central series of G. Let $G_n = G/G^{[n+1]}$. ◊

Example 2.82

$$G_1 = G/G^{[1]} = G/[G, G]$$

is the abelianization G^{ab} of G. For $n \geq 2$ the group G_n is an n-step nilpotent group, typically nonabelian. □

Now for various flavours of $\pi_1(X)$ we have

$$\pi_1(X)_1 = \pi_1(X)^{ab} = H_1(X)$$

so above we should think of H_1 as the abelianization of π_1. We can therefore try to replace it by $\pi_1(X)_n$ for $n > 1$. We'll do this for the two homology groups associated to X

1. p-adic étale homology
2. de Rham homology

we can define the geometric étale fundamental group $\pi_1^{\mathrm{et}}(X_{\overline{K}})$ such that

$$\pi_1^{\mathrm{et}}(X_{\overline{K}})^{ab} \simeq H_1^{\mathrm{et}}(X_{\overline{K}}, \widehat{\mathbf{Z}})$$

$$\pi_1^{\mathrm{et}}(X_{\overline{K}})^{ab} \simeq H_1^{\mathrm{et}}(X_{\overline{K}}, \widehat{\mathbf{Z}}) \twoheadrightarrow H_1^{\mathrm{et}}(X_{\overline{K}}, \mathbf{Z}_p) \subseteq H_1^{\mathrm{et}}(X_{\overline{K}}, \mathbf{Q}_p) = V = \mathbf{G}_a^{2g}(\mathbf{Q}_p)$$

with action of G_K in particular G_K acts via $\mathbf{Q}_p$-linear automorphisms on $\mathbf{G}_a^{2g}$.

For $n \geq 2$ there's an analogous construction that transforms $\pi_1^{\mathrm{et}}(X_{\overline{K}})_n$ into a topological group V_n that is the group of $\mathbf{Q}_p$-points of a unipotent algebraic group $\mathcal{V}_n/\mathbf{Q}_p$, equipped with a G_K-action.

Definition 2.83 A pro-unipotent group over $\mathbf{Q}_p$ is a group scheme of $\mathbf{Q}_p$ that is a projective limit of unipotent algebraic groups over $\mathbf{Q}_p$. ◊

Then there is a notion of $\mathbf{Q}_p$-pro-unipotent completion

$$\pi_1^{\mathrm{et}}(X_{\overline{K}})_{\mathbf{Q}_p}$$

of
$$\pi_1^{\text{et}}(X_{\overline{K}})$$
there is a continuous homomorphism
$$\pi_1^{\text{et}}(X_{\overline{K}}) \to \pi_1^{\text{et}}(X_{\overline{K}})_{\mathbf{Q}_p}(\mathbf{Q}_p)$$
is universal among such maps.

There are lower central series quotients
$$U_n^{\text{et}} = \pi_1^{\text{et}}(X_{\overline{K}})_{\mathbf{Q}_p,n} = \pi_1^{\text{et}}(X_{\overline{K}})_{\mathbf{Q}_p}/\pi_1^{\text{et}}(X_{\overline{K}})_{\mathbf{Q}_p}^{[n+1]}.$$

In the cases we consider, these are finite dimensional varieties. The coordinate ring
$$\mathcal{O}(\pi_1^{\text{et}}(X_{\overline{K}})_{\mathbf{Q}_p})$$
is a $\mathbf{Q}_p$-vector space. Recall that for a smooth curve X we had
$$H_1^{\text{dR}}(X_{K_p}) \simeq D_{\text{dR}}(H_1^{\text{et}}(X_{\overline{K}}, \mathbf{Q}_p))$$
we may define the de Rham fundamental group
$$\pi_1^{\text{dR}}(X_{K_p})$$
as
$$\text{Spec}(D_{\text{dR}}(\mathcal{O}(\pi_1^{\text{et}}(X_{\overline{K}})_{\mathbf{Q}_p}))).$$

π_1^{dR} is equipped with a Hodge filtration. Just like we took the lower central series filtration on $\pi_1^{\text{et}}(X_{\overline{K}})_{\mathbf{Q}_p}$. do the same thing for quotients by
$$\pi_1^{\text{dR}}(X_{K_p})_n$$
We'll denote these as U_n^{dR}. We have
$$U_n^{\text{dR}} = D_{cris}(U_n^{\text{et}})$$
so it is equipped with a frobenius action.

Now we have a non-abelian version of the Chabauty-Coleman diagram
$$\begin{tikzcd}
X(K) \arrow[r] \arrow[d] & X(K_p) \arrow[d] \arrow[dr] & \\
H^1_f(G_K, \pi_1^{\text{et}}(X_{\overline{K}})_{\mathbf{Q}_p,n}) \arrow[r] & H^1_f(G_{K_p}, U_n^{\text{et}}) \arrow[r] & U_n^{\text{dR}}/F^0
\end{tikzcd}$$

An element of
$$H^1_f(G_K, U_n^{\text{et}})$$
is a scheme over $\mathbf{Q}_p$ with continuous G_K-action and G_K-equivariant action of U_n^{et} making it into a U_n^{et}-torsor.

Kim shows that
$$H^1_f(G_K, U_n^{\text{et}}) \subseteq H^1(G_K, U_n^{\text{et}})$$
has the structure of an algebraic variety the Selmer variety $\text{Sel}(U_n)$.

We refer to $H^1_f(G_{K_p}, U_n^{\text{et}})$ as the local Selmer variety.

Theorem 2.84 Kim. *For some $n > 1$ if*

$$\dim \mathrm{Sel}(U_n) < \dim H^1_f(G_{K_p}, U_n^{\mathrm{et}})$$

then $X(K)$ is contained in the zero locus of non-trivial locally analytic function on $X(K_p)$ so $X(K)$ is finite.

Lecture 1? 12/11/2019

Lemma 2.85 *Let X be a smooth projective curve over an algebraically closed field $k = \overline{k}$ and $n \geq 1$ be invertible in k then*

$$H^0_{\mathrm{et}}(X_{\overline{k}}, \mu_n) = \mu_n$$

$$H^1_{\mathrm{et}}(X_{\overline{k}}, \mu_n) = \mathrm{Pic}^0(X_{\overline{k}})[n].$$

Proof. Sketch: Recall the Kummer sequence

$$0 \to \mu_n \to \mathbf{G}_m \to \mathbf{G}_m \to 0$$

we also have

$$H^0_{\mathrm{et}}(X, \mathbf{G}_m) = k^\times$$

$$H^1_{\mathrm{et}}(X, \mathbf{G}_m) = \mathrm{Pic}(X)$$

$$H^q_{\mathrm{et}}(X, \mathbf{G}_m) = 0 \text{ for } q \geq 2$$

take cohomology of the Kummer sequence to get

$$0 \to H^0_{\mathrm{et}}(X_{\overline{k}}, \mu_n) \to k^\times \to k^\times \to 0$$

$$0 \to H^1_{\mathrm{et}}(X_{\overline{k}}, \mu_n) \to \mathrm{Pic}(X) \to H^2_{\mathrm{et}}(x, \mu_n) \to 0$$

We also have

$$0 \to \mathrm{Pic}^0(X) \to \mathrm{Pic}(X) \to \mathbf{Z} \to 0$$

and we can identify $\mathrm{Pic}^0(X)$ with the group of k-rational points of J of X. Note that multiplication by n is surjective and the kernel is $\mathrm{Pic}^0[n]$. ■

More generally, for any galois stable quotient U of U_n^{et} we have a similar diagram $U^{\mathrm{dR}} = D_{\mathrm{cris}}(U)$ and corresponding maps

$$j_U^{\mathrm{et}}, j_U^{\mathrm{dR}}, \mathrm{loc}_{U,p}, j_U^{\mathrm{et}} \colon X(\mathbf{Q}) \to \mathrm{Sel}(U).$$

We have that $X(\mathbf{Q})$ is contained in

$$X(\mathbf{Q}_p)_U = j_{U,p}^{\mathrm{et},-1}(\mathrm{loc}_{U,p}(\mathrm{Sel}(U))) \subseteq X(\mathbf{Q}_p)$$

when

$$U = U_n$$

we get

$$X(\mathbf{Q}_p)_n = X(\mathbf{Q}_p)_{U_n}$$

we have

$$X(\mathbf{Q}) \subseteq \cdots \subseteq X(\mathbf{Q}_p)_n \subseteq \cdots \subseteq X(\mathbf{Q}_p)_1 \subseteq X(\mathbf{Q}_p).$$

Conjecture 2.86 Kim. *For $n \gg 0$ $X(\mathbf{Q}_p)_n$ is finite.*

Remark 2.87 This is implied by Beilinson-Bloch-Kato and other standard conjectures on motives.

Conjecture 2.88 Kim. *For $n \gg 0$ $X(\mathbf{Q}_p)_n = X(\mathbf{Q})$.*

The analogue of analytic properties of AJ_b (there is a non-zero functional we can construct that vanishes on $\overline{J(\mathbf{Q})}$ with Zariski dense image, and given by a convergent p-adic power series), so there are finitely many zeroes on each residue disk of $X(\mathbf{Q}_p)$) is the following

Theorem 2.89 Kim 09. *The map j_n^{dR} has Zariski dense image and is given by convergent p-adic power series on every residue disk.*

The analogue of Chabauty-Coleman $r < g$ hypothesis is non-density of $\mathrm{loc}_{U,p}$.

Theorem 2.90 Kim 09. *Suppose $\mathrm{loc}_{U,p}$ is non-dominant, yhen $X(\mathbf{Q}_p)_U$ is finite.*

Remark 2.91 All finiteness results come from bounding the dimension of $\mathrm{Sel}(U)$.

Coates and Kim did this:

Theorem 2.92 Coates, Kim '10. *Let $X/\mathbf{Q}$ be a smooth projective curve of genus $g \geq 2$ and suppose J is isogenous over $\overline{\mathbf{Q}}$ to*

$$J \sim \prod A_i$$

of abelian varieties with A_i having CM by K_i of degree $2 \dim A_i$. Then for $n \gg 0$ have $X(\mathbf{Q}_p)_n$ is finite.

Examples:

- Fermat curves
$$x^m + y^m + z^m = 0.$$
- Twisted fermat curves
$$ax^m + by^m + cz^m = 0.$$
- Van Wamelen's list of genus 2 curves whose jacobians have CM and are simple.

Coates, John, and Minhyong Kim. "Selmer Varieties for Curves with CM Jacobians." Kyoto Journal of Mathematics 50, no. 4 (2010): 827-52. https://doi.org/10.1215/0023608X-2010-015.

Key idea is to use multivariable Iwasawa theory to bound the dimension of the Selmer variety.

Recall $\pi_1^{\mathrm{et}}(X_{\overline{\mathbf{Q}}})_{\mathbf{Q}_p}$ is the $\mathbf{Q}_p$-pro-unipotent completion of $\pi_1^{\mathrm{et}}(X_{\overline{\mathbf{Q}}})$. Let

$$W = \pi_1^{\mathrm{et}}(X_{\overline{\mathbf{Q}}})_{\mathbf{Q}_p} / [\pi_1^{\mathrm{et}}(X_{\overline{\mathbf{Q}}})^{(2)}_{\mathbf{Q}_p}, \pi_1^{\mathrm{et}}(X_{\overline{\mathbf{Q}}})^{(2)}_{\mathbf{Q}_p}]$$

be the quotient by the derived series

$$G^{(0)} = G$$

$$G^{(n)} = [G^{(n-1)}, G^{(n-1)}]$$

W itself has a lower central series filtration

$$W = W^1 \supseteq W^2 \supseteq \cdots W^{n-1} = [W, W^n] \supseteq \cdots$$

and associated quotients $W_n = W/W^{n+1}$.

Theorem 2.93 Coates-Kim. *There is a bound B depends on X and T s.t.*

$$\dim \sum_{i=1}^{n} H^2(G_T, W^i/W^{i+1}) \le Bn^{2g-1}.$$

This is done by controlling the zeroes of an algebraic p-adic L-function (really an annihilator of an ideal class group).

A corollary of this gives a dimension bound on Selmer varieties.

Corollary 2.94 *For $n \gg 0$ have* $\dim H^1_f(G, W_n) < \dim W_n^{\mathrm{dR}}/F^0$.

Remark 2.95 Structure of Selmer variety as an algebraic variety is a consequence of $\mathbf{Q}_p$-pro-unipotent completion of $\pi_1^{\mathrm{et}}(X_{\overline{\mathbf{Q}}})$.

$\mathbf{Q}_p$-pro-unipotent completion:

Given a finitely presented discrete group E, take the group algebra

$$\mathbf{Q}[E]$$

complete it with respect to the augmentation ideal K

$$\mathbf{Q}[[E]] = \varprojlim_{n} \mathbf{Q}[E]/K^n$$

the coproduct

$$\Delta\colon \mathbf{Q}[E] \to \mathbf{Q}[E] \otimes \mathbf{Q}[E]$$

defined by $g \mapsto g \otimes g$ takes K to the ideal

$$K \otimes \mathbf{Q}[E] + \mathbf{Q}[E] \otimes K$$

then there's an induced coproduct on

$$\Delta\colon \mathbf{Q}[[E]] \to \mathbf{Q}[[E]]\hat{\otimes}\mathbf{Q}[[E]].$$

The unipotent completion

$$U(E)$$

can be realized as the grouplike elements in $\mathbf{Q}[[E]]$.

$$U(E) = \{g \in \mathbf{Q}[[E]] : \Delta(g) = g \otimes g\}$$

This defines the $\mathbf{Q}$-points of a pro-algebraic group over $\mathbf{Q}$.

When E is topologically finitely presented profinite group the $\mathbf{Q}_p$-pro-unipotent completion is defined analogously.

Lecture 1? 15/11/2019

Missed a lecture

Lecture 1? 19/11/2019

Definition 2.96 Filtered ϕ modules. A **filtered ϕ-module** is a finite dimensional $\mathbf{Q}_p$-vector space W, equipped with an exhaustive and separated decreasing filtration Fil^i and an automorphism ϕ. ◊

Remark 2.97 We have seen instances of this already, V_{dR} is a filtered ϕ-module.

Definition 2.98 Mixed extensions. We define $M_{\mathrm{Fil},\phi}(\mathbf{Q}_p, V_{\mathrm{dR}}, \mathbf{Q}_p(1))$ to be the category of **mixed extensions** of filtered ϕ-modules, the objects are triples $(M, M_\bullet, \psi_\bullet)$ where

1. M is a filtered ϕ-module.

2. $M_\bullet$ is a filtration by sub-filtered ϕ-modules

$$M = M_0 \supseteq M_1 \supseteq M_2 \supseteq M_3 = 0.$$

3. $\psi_\bullet$ are isomorphisms of filtered ϕ-modules

$$\phi_0 \colon M_0/M_1 \xrightarrow{\sim} \mathbf{Q}_p$$
$$\phi_1 \colon M_1/M_2 \xrightarrow{\sim} V_{\mathrm{dR}}$$
$$\phi_2 \colon M_2/M_3 \xrightarrow{\sim} \mathbf{Q}_p(1)$$

and the morphisms of this category are morphisms of filtered ϕ-modules which also respect the filtrations $M_\bullet$ and commute with the isomorphisms ψ_i and ψ_i'.

Let
$$M_{\mathrm{Fil},\phi}(\mathbf{Q}_p, V_{\mathrm{dR}}, \mathbf{Q}_p(1))$$
denote the set of isomorphism classes of objects in this category. ◊

Lemma 2.99 *For any filtered ϕ-module W for which*

$$W^{\phi=1} = 0$$

we have an isomorphism
$$\mathrm{Ext}^1(\mathbf{Q}_p, W) \simeq W/\mathrm{Fil}^0 .$$

Idea. Given an extension of $\mathbf{Q}_p$ by W

$$0 \to W \to E \to \mathbf{Q}_p \to 0$$

choose a splitting $s^\phi \colon \mathbf{Q}_p \to E$ which is ϕ-invariant. Choose a splitting $s^{\mathrm{Fil}} \colon \mathbf{Q}_p \to E$ which respects the filtration. s chosen earlier. s^ϕ is unique by s^{Fil} is determined up to an element of

$$\mathrm{Fil}^0 W.$$

So
$$s^\phi - s^{\mathrm{Fil}} \in W \pmod{\mathrm{Fil}^0 W}$$
is independent of choices.

Recall
$$M_{\mathrm{dR}} = D_{\mathrm{cris}}(M_{\mathrm{et}}).$$
Then the structure of a mixed extension of filtered ϕ-modules on M_{dR} allows us to define extensions

$$E_1 = E_1(M) = M_{\mathrm{dR}}/\mathbf{Q}_p(1)$$
$$E_2 = E_2(M) = \ker(M_{\mathrm{dR}} \to \mathbf{Q}_p).$$

We have
$$0 \to \mathbf{Q}_p(1) \to E_2/\mathrm{Fil}^0 \to V_{\mathrm{dR}}/\mathrm{Fil}^0 \to 0. \tag{2.2}$$

The image of the extension class

$$[M] \in H^1_f(G_{\mathbf{Q}_p}, E_2) \simeq E_2/\mathrm{Fil}^0$$

inside
$$V_{\mathrm{dR}}/\mathrm{Fil}^0 \simeq H^1_f(G_{\mathbf{Q}_p}, V_{\mathrm{dR}})$$

is $[E_1]$.

We define δ to be

$$\delta\colon V_{\mathrm{dR}}/\mathrm{Fil}^0 \xrightarrow{s} V_{\mathrm{dR}} \to E_2 \to E_2/\mathrm{Fil}^0$$

where s is our fixed splitting of the Hodge filtration on V_{dR} and

$$V_{\mathrm{dR}} \to E_2$$

is the unique frobenius equivariant splitting of

$$0 \to \mathbf{Q}_p(1) \to E_2 \to V_{\mathrm{dR}} \to 0$$

by construction $[M]$ and $[\delta(E_1)]$ have the same image in $V_{\mathrm{dR}}/\mathrm{Fil}^0$ so by (2.2) their difference defines an element of $\mathbf{Q}_p(1)$.

Since the filtered ϕ-module

$$\mathbf{Q}_p(1) \cong H^1_f(G_{\mathbf{Q}_p}, \mathbf{Q}_p(1))$$

by Lemma 2.99 we can think of

$$[M] - [\delta(E_1)] \in H^1_f(G_{\mathbf{Q}_p}, \mathbf{Q}_p(1)).$$

Finally, taking the local component

$$\chi_p\colon \mathbf{Q}_p^\times \to \mathbf{Q}_p$$

of idèle class character fixed at the beginning of the discussion of Nekovář heights. This gives a map

$$\chi_p\colon H^1_f(G_{\mathbf{Q}_p}, \mathbf{Q}_p(1)) \to \mathbf{Q}_p$$

and

$$h_p(M) = \chi_p([M] - [\delta(E_1)]).$$

For applications to rational points we need to make this more explicit.

The splitting s of the Hodge filtration we fixed earlier defines idempotents

$$s_1, s_2\colon V_{\mathrm{dR}} \to V_{\mathrm{dR}}$$

projecting onto

$$s(V_{\mathrm{dR}}/\mathrm{Fil}^0) \text{ and } \mathrm{Fil}^0$$

components, respectively.

Suppose that we are given a vector space splitting of

$$s_0\colon \mathbf{Q}_p \oplus V_{\mathrm{dR}} \oplus \mathbf{Q}_p(1) \xrightarrow{\sim} M.$$

The split mixed extension

$$\mathbf{Q}_p \oplus V_{\mathrm{dR}} \oplus \mathbf{Q}_p(1)$$

has the structure of a filtered ϕ-module as a direct sum. So we choose two further splittings

$$s^\phi\colon \mathbf{Q}_p \oplus V_{\mathrm{dR}} \oplus \mathbf{Q}_p(1) \xrightarrow{\sim} M$$

$$s^{\mathrm{Fil}}\colon \mathbf{Q}_p \oplus V_{\mathrm{dR}} \oplus \mathbf{Q}_p(1) \xrightarrow{\sim} M$$

s^ϕ is frobenius-equivariant and s^{Fil} respects the filtrations, s^ϕ is unique and s^{Fil} is not.

Now choose bases for $\mathbf{Q}_p, V_{\mathrm{dR}}, \mathbf{Q}_p(1)$ such that with respect to these bases we have

$$s_0^{-1} \circ s^\phi = \begin{pmatrix} 1 & 0 & 0 \\ \alpha_\phi & 1 & 0 \\ \gamma_\phi & \beta_\phi^{\mathrm{T}} & 1 \end{pmatrix}$$

$$s_0^{-1} \circ s^{\mathrm{Fil}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \gamma_{\mathrm{Fil}} & \beta_{\mathrm{Fil}}^{\mathrm{T}} & 1 \end{pmatrix}$$

then with respect to these choices

$$\begin{aligned} h_p(M) &= \chi_p([M] - [\delta(E_1)]) \\ &= \chi_p(\gamma_\phi - \gamma_{\mathrm{Fil}} - \beta_\phi^{\mathrm{T}} s_1(\alpha_\phi) - \beta_{\mathrm{Fil}}^{\mathrm{T}} s_2(\alpha_\phi)). \end{aligned}$$

Goal: Compute these components explicitly and construct M as

$$\text{“}A_Z(b,x)\text{”}$$

where Z is a choice of endomorphism. Then

$$E_1(x) = E_1(M) = E_1(A_Z(b,x)) = \mathrm{AJ}_b(x).$$

Remark 2.100 By work of Olsson

$$D_{\mathrm{cris}}(A_Z(b,x)) = A_Z^{\mathrm{dR}}(b,x).$$

$$E_{2,Z}(x) = E_2(A_Z(b,x)) = E(\mathrm{AJ}_b(x)) + c.$$

this is done by a twisting construction and some input from a quadratic Chabauty pair.

Definition 2.101 Quadratic Chabauty pairs. Let $X/\mathbf{Q}$ be a smooth projective curve of genus g. Suppose $\operatorname{rk} J(\mathbf{Q}) = g$ and that

$$\overline{J(\mathbf{Q})} \subseteq J(\mathbf{Q}_p)$$

has finite index. A **quadratic Chabauty pair** (θ, S) is a function

$$\theta \colon X(\mathbf{Q}_p) \to \mathbf{Q}_p$$

and a finite set S such that

1. On each residue disk of $X(\mathbf{Q}_p)$ the map
$$(\mathrm{AJ}_b, \theta) \colon X(\mathbf{Q}_p) \to H^0(X, \Omega^1)^* \times \mathbf{Q}_p$$
has Zariski dense image and is given by a convergent p-adic power series.
2. There exists an endomorphism E of
$$H^0(X_{\mathbf{Q}_p}, \Omega^1)^*,$$
a functional $c \in H^0(X_{\mathbf{Q}_p}, \Omega^1)^*$ and a bilinear form B
$$B \colon H^0(X_{\mathbf{Q}_p}, \Omega^1)^* \otimes H^0(X_{\mathbf{Q}_p}, \Omega^1)^* \to \mathbf{Q}_p$$
such that for all $x \in X(\mathbf{Q})$, we have
$$\theta(x) - B(\mathrm{AJ}_b(x), E(\mathrm{AJ}_b(x)) + c) \in S. \tag{2.3}$$

◊

This gives us a finite set of points containing $X(\mathbf{Q})$, since Item 1 implies that only finitely many points satisfy (2.3) and Item 2 implies that all rational points satisfy (2.3).

Remark 2.102 We will use the Nekovář height to do this, the function θ will be the local height at p and B will be the global p-adic height.

If we further add the hypothesis that X has everywhere potentially good reduction then $S = \{0\}$.

Now we describe how knowing θ and S gives us a method for determining a finite subset of $X(\mathbf{Q}_p)$ containing $X(\mathbf{Q})$.

For $\alpha \in S$ define

$$X(\mathbf{Q}_p)_\alpha = \{x \in X(\mathbf{Q}_p) : \theta(z) - B(\mathrm{AJ}_b(x), E(\mathrm{AJ}_b(x)) + c) = \alpha\}.$$

By definition

$$X(\mathbf{Q}) \subseteq \bigsqcup_{\alpha \in S} X(\mathbf{Q}_p)_\alpha$$

so it suffices to describe

$$X(\mathbf{Q}_p)_\alpha.$$

Let

$$\mathcal{E}\colon H^0(X_{\mathbf{Q}_p}, \Omega^1)^* \otimes H^0(X_{\mathbf{Q}_p}, \Omega^1)^*.$$

Lemma 2.103 *Suppose we have $P_1, \ldots, P_m \in X(\mathbf{Q})$ s.t.*

$$\{\mathrm{AJ}_b(P_i) \otimes E(\mathrm{AJ}_b(P_i)) + c\}$$

forms a basis for $\mathcal{E}$. Suppose

$$\{\psi_1, \ldots, \psi_m\}$$

forms a basis for $\mathcal{E}^*$.

Assume that $P_i \in X(\mathbf{Q}_p)_{\alpha_i}$ where $\alpha_i \in S$.

For $x \in X(\mathbf{Q}_p)$ define the matrix $T(x) = T_{(\theta,S)}(x)$ via

$$T(x) = \begin{pmatrix} \theta(z) - \alpha & \Psi_1(x) & \cdots & \Psi_m(x) \\ \theta(P_1) - \alpha_1 & \Psi_1(P_1) & \cdots & \Psi_m(P_1) \\ \vdots & \vdots & \ddots & \vdots \\ \theta(P_m) - \alpha_m & \Psi_1(P_m) & \cdots & \Psi_m(P_m) \end{pmatrix}.$$

Where

$$\Psi_i(x) = \psi_i(\mathrm{AJ}_b(P_i) \otimes E(\mathrm{AJ}_b(P_i)) + c)$$

if $x \in X(\mathbf{Q}_p)_\alpha$ then

$$\det(T(x)) = 0.$$

Remark 2.104 Computing $\det T(x) = 0$ and finding its zeroes is what gives us our finite set of points containing $X(\mathbf{Q})$.

We need enough rational points so that the ψ_i forms a basis for $\mathcal{E}$ and we need a base point so which means we need $g^2 + 1$ points with this approach, It can be possible to make do with only $g + 1$ if height is taken to be equivalent with respect to some other structure.

Lecture 1? 21/11/2019

Theorem 2.105 B.-Dogra. *Let $X/\mathbf{Q}$ be a smooth projective curve of genus $g \geq 2$. Let $r = \operatorname{rk} J(\mathbf{Q})$ and*

$$\rho = \rho(J_{\mathbf{Q}}) = \operatorname{rk} \mathrm{NS}(J_{\mathbf{Q}})$$

suppose $r < g + \rho - 1$. Then

$$X(\mathbf{Q}_p)_2$$

is finite.

Remark 2.106 This is also true for X/K, with K an imaginary quadratic field.

To prove this, look at Kim's diagram

$$\begin{tikzcd} X(\mathbf{Q}) \arrow[r] \arrow[d] & X(\mathbf{Q}_p) \arrow[d] \arrow[dr] & \\ \mathrm{Sel}(U_n) \arrow[r] & H^1_f(G_{\mathbf{Q}_p}, U_n^{\mathrm{et}}) \arrow[r] & U_n^{\mathrm{dR}}/F^0 \end{tikzcd}$$

In this case take $n = 2$. One interpretation of U_2 is

$$1 \to \operatorname{coker}(\mathbf{Q}_p(1) \to \bigwedge^2 V) \to U_2 \to V \to 1.$$

The main idea is not to work with the full U_2, which is hard, but instead to use a suitable Galois stable quotient U for which

$$\dim \underbrace{H^1_f(G_T, U)}_{=\mathrm{Sel}(U)} < \dim H^1_f(G_{\mathbf{Q}_p}, U).$$

Then the result follows since

$$X(\mathbf{Q}_p)_2 \subseteq X(\mathbf{Q}_p)_U.$$

We'll take U to be a quotient of U_2 surjecting onto V, in particular,

$$[U, U] \cong \mathbf{Q}_p(1)^m, \text{ for } m \geq 1.$$

The reason for considering such quotients (extensions of V by $\mathbf{Q}_p(1)^m$) is to more easily prove the necessary dimension hypotheses for Selmer varieties.

Let $K = \mathbf{Q}$ or quadratic imaginary, p split prime in K

$$H^1_f(G_{K_p}, \mathbf{Q}_p(1)) \cong \mathcal{O}_p^\times \otimes \mathbf{Q}_p \cong \mathbf{Q}_p$$

(Bloch-Kato)

$$H^1_f(G_T, \mathbf{Q}_p(1)) \cong \mathcal{O}_K^\times \otimes \mathbf{Q}_p \cong 0$$

then

$$\dim H^1_f(G_T, \ldots) < \dim H^1_f(G_{K_p}, \ldots).$$

Lemma 2.107 *Let U be a quotient of U_2 that is an extension of V by $\mathbf{Q}_p(1)^m$, let p be a prime of good reduction for X.*

1. $$\dim \mathrm{Sel}(U) \leq \operatorname{rk} J(\mathbf{Q})$$

2. $$\dim H^1_f(G_{\mathbf{Q}_p}, U) = g + m$$

Then apply lemma when $m = \rho - 1$ to get the finiteness result.

We want to construct this quotient U of U_2, that's nonabelian but small enough to make computations practical.

Let

$$\tau \colon X \times X \to X \times X$$
$$(x_1, x_2) \mapsto (x_2, x_1)$$

be the canonical involution.

Definition 2.108 Correspondences. A **correspondence** $Z \in \mathrm{Pic}(X \times X)$ is symmetric if there are $Z_1, Z_2 \in \mathrm{Pic}(X)$ such that

$$\tau_* Z = Z + \pi_1^* Z_1 + \pi_2^* Z_2$$

where π_1, π_2 are the canonical projections

$$X \times X \to X.$$

◊

Definition 2.109 Nice correspondences. A **nice correspondence** Z is one that is non-trivial symmetric and for which the cycle class

$$\xi_Z \in H^1(X) \otimes H^1(X)(1) \simeq \mathrm{End}\, H^1(X)$$

has trace zero. ◊

Lemma 2.110 *Suppose J is absolutely simple, and let $Z \in \mathrm{Pic}(X \times X)$ a symmetric correspondence. Then the class associated to Z lies in the subspace*

$$\bigwedge^2 H^1(X)(1) \subseteq H^1(X) \otimes H^1(X)(1).$$

Moreover Z is nice iff the image of this class in $H^2(X)(1)$ under the cup product is zero.

By the lemma, if Z is a nice correspondence we get a homomorphism

$$c_Z \colon \mathbf{Q}_p(-1) \to \ker(\bigwedge^2 H^1_{\mathrm{et}}(X_{\mathbf{Q}_p}, \mathbf{Q}_p) \xrightarrow{\cup} H^2(X_{\overline{\mathbf{Q}}}, \mathbf{Q}_p))$$

and using that U_2 was a central extension

$$1 \to \mathrm{coker}(\mathbf{Q}_p(1) \xrightarrow{\cup^*} \bigwedge^2 V) \to U_2 \to V \to 1$$

take the quotient $U_Z = U_2/\ker(c_Z^*)$ and we have a short exact sequence

$$1 \to \mathbf{Q}_p(1) \to U_Z \to V \to 1.$$

Twisting and p-adic heights. On 11/12 we defined the $\mathbf{Q}$-pro-unipotent completion. Now say a little more about the $\mathbf{Q}_p$-pro-unipotent completion.

$$\mathbf{Z}_p[[\pi_1^{\mathrm{et}}(X_{\overline{\mathbf{Q}}}, b)_{\mathbf{Q}_p}]] = \varprojlim \mathbf{Z}_p[\pi_1^{\mathrm{et}}(X_{\overline{\mathbf{Q}}}, b)]/N$$

where the limit is over all finite quotients of p-power order.

Let I denote the augmentation ideal of

$$\mathbf{Q}_p \otimes \mathbf{Z}_p[[\pi_1^{\mathrm{et}}(X_{\overline{\mathbf{Q}}}, b)_{\mathbf{Q}_p}]].$$

Define the algebra

$$A_n^{\mathrm{et}}(b) = \mathbf{Q}_p \otimes \mathbf{Z}_p[[\pi_1^{\mathrm{et}}(X_{\overline{\mathbf{Q}}}, b)_{\mathbf{Q}_p}]]/I^{n+1}.$$

Fix a correspondence $Z \in \mathrm{Pic}(X \times X)$ and let U_Z denote the corresponding quotient of U_2^{et}.

Definition 2.111 The mixed extension $A_Z(b)$ is the pushout of $A_2^{\text{et}}(b)$ by

$$\mathrm{cl}_Z^*:\ \mathrm{coker}(\mathbf{Q}_p(1) \xrightarrow{\cup^*} V^{\otimes 2}) \to \mathbf{Q}_p(1).$$

◊

Remark 2.112
$$A_Z(b) \in M_f(G_T, \mathbf{Q}_p, V, \mathbf{Q}_p(1))$$
with respect the I-adic filtration.

Recall: $\mathrm{Sel}(U)$ is defined using nonabelian cohomology, satisfying certain conditions. Our goal is to get an equation for

$$X(\mathbf{Q}_p)_U$$

and use Nekovář's construction to define a map

$$\mathrm{Sel}(U) \to \mathbf{Q}_p.$$

A natural analogue of Nekovář's construction is to start with the input of a cohomology class ξ in $H^1(G_T, \mathbf{Q}_p)$ and define at all bad primes v an algebraic function
$$H^1(G_{\mathbf{Q}_v}, U) \to \mathbf{Q}_p$$
which when restricted to
$$H^1(G_{\mathbf{Q}_v}, \mathbf{Q}_p(1))$$
is the cup product with ξ. Given a splitting of the Hodge filtration can do this. But to get equality for Selmer varieties better to have a construction with linearity properties analogous to the global height pairing. So here we describe how to embed $\mathrm{Sel}(U)$ into

$$H^1_{st}(G_T, \ldots) \subseteq H^1(G_T, \ldots)$$

via twisting. Then apply Nekovář's construction giving local functions from

$$\mathrm{Sel}(U) \to \mathbf{Q}_p.$$

For more on twisting see Serre, Galois Cohomology [79].

Let G be a profinite group U a G-group. Let V be a continuous representation of G with an equivariant action of U. Then for any G-equivariant U-torsor P and also U acts on V on the left. We form the twist of V by P as follows, let $\sim$ denote the equivalence.

$$(p, v) \sim (p \cdot u, u^{-1} v)$$

on $P \times V$ for all $u \in U$. Then the twist of V by P

$$V^{(P)} = P \times_U V/\sim$$

has a continuous G-representation structure.

Remark 2.113 For all $p \in P$ the map

$$v \mapsto pv$$

is a bijection of V onto $V^{(P)}$ for this reason we say that this is the twist of V by P.

Now define maps

$$\tau\colon H^1_f(G_T, U_Z) \to M_f(G_T, \mathbf{Q}_p, V, \mathbf{Q}_p(1))$$
$$P \mapsto P \times_{U_Z} A_Z(b)$$
$$\tau_p\colon H^1_f(G_T, U_Z) \to M_f(G_{\mathbf{Q}_p}, \mathbf{Q}_p, V, \mathbf{Q}_p(1))$$
$$P \mapsto P \times_{U_Z} A_Z(b)$$

Remark 2.114 Can show that τ is injective.

Definition 2.115 Let $x \in X(\mathbf{Q})$ and $P \in \pi_1^{\mathrm{et}}(X_{\overline{\mathbf{Q}}}, b, x)$ then

$$A_Z(b, x) = \tau([P]) = P \times_{U_Z} A_Z(b).$$

◊

Remark 2.116 For $x \in X(\mathbf{Q}_p)$, similarly.

$$A_Z(b, x) = \tau_p([P])$$

is the mixed extension of $G_{\mathbf{Q}_p}$-modules obtained by twisting $A_Z(b)$. Can also define $A_1(b, x), IA_Z(b, x)$ by twisting $A_1^{\mathrm{et}}(b)$ and $IA_Z(b)$ respectively.

Now we can define our quadratic Chabauty pair. We have

$$\theta\colon X(\mathbf{Q}_p) \to \mathbf{Q}_p$$
$$x \mapsto h_p(A_Z(b, x))$$

and using local heights at all bad $v \in T_0$ we define

$$S = \left\{ \sum_{v \in T_0} h_v(A_Z(b, x_v)) : (x_v) \in \prod_{v \in T_0} X(\mathbf{Q}_v) \right\}$$

Theorem 2.117 Kim-Tamagawa '08. *The set S is finite.*

Lemma 2.118 *Let X be as before, then (θ, S) is a quadratic Chabauty pair. The endomorphism is that induced by the correspondence Z. The constant is*

$$[IA_Z(b)]$$

and the bilinear pairing B is the global Nekovář height.

Corollary 2.119 *If further X has everywhere potentially good reduction, then*

$$(\theta, S) = (h_p(A_Z(b, \cdot), \{0\})$$

is a quadratic Chabauty pair.

Lecture 1? 26/11/2019

Recall: if $X/\mathbf{Q}$ is a smooth projective curve of genus $g \geq 2$ then we assume

$$r = \operatorname{rk} J(\mathbf{Q}) = g$$
$$\rho = \operatorname{rk} \mathrm{NS}(J_{\mathbf{Q}}) \geq 2$$

and

$$\overline{J(\mathbf{Q})} \subseteq J(\mathbf{Q}_p)$$

is finite index with p good for X. X has everywhere potential good reduction.

Then

$$(h_p(A_Z(b, \cdot)), \{0\})$$

is a quadratic Chabauty pair.

Remark 2.120 Hypotheses may seem rather restrictive. Nevertheless there are some interesting examples

1. $X = X_s(13)$ the "split Cartan" modular curve of level 13.
2. $X = X_0(p)^+ = X_0(p)/w_p$ the Atkin-Lehner quotient. For p prime.

To compute $X(\mathbf{Q}_p)_U$ we need to compute $h_p(A_Z(b,x))$ so we need to choose a nice correspondence Z and write the locally analytic function

$$\begin{aligned}\theta\colon X(\mathbf{Q}_p) &\to \mathbf{Q}_p\\ x &\mapsto h_p(A_Z(b,x))\end{aligned}$$

as a power series on every residue disk of $X(\mathbf{Q}_p)$.

By our formula

$$h_p(A_Z(b,x)) = \chi_p(\gamma_\phi - \gamma_{\mathrm{Fil}} - \beta_\phi^{\mathrm{T}} \cdot s_1(\alpha_\phi) - \beta_{\mathrm{Fil}}^{\mathrm{T}} s_2(\alpha_\phi)),$$

we see that we want to compute an explicit description of $A_Z(b,x)$ as a filtered ϕ-module. This we do in two parts: The Hodge filtration (today) and Frobenius structure (via solving a p-adic differential equation using Tuitman's algorithm, see later), of certain universal objects A_Z^{dR}.

Remark 2.121 Unlike the Frobenius structure which is p-adic, the Hodge filtration has a global meaning and can be computed over $\mathbf{Q}$.

Let $X/\mathbf{Q}$ be a smooth projective curve of genus $g \geq 2$. And $Y \subseteq X$ an affine open, let $b \in Y(\mathbf{Q}_p)$ be integral at p. Suppose

$$\#(X \smallsetminus Y)(\overline{\mathbf{Q}}) = d$$

and let $L/\mathbf{Q}$ be a finite extension over which all points of $D = X \smallsetminus Y$ are defined.

Choose a set $\omega_0, \ldots, \omega_{2g+d-2} \in H^0(Y_{\mathbf{Q}}, \Omega^1)$ s.t.

1. The differentials $\omega_0, \ldots, \omega_{2g-1}$ are of the second kind on X and form a symplectic basis for $H^1_{\mathrm{dR}}(X_{\mathbf{Q}})$ s.t. the cup product is the standard symplectic form with respect to this basis.
2. The differentials
$$\omega_{2g}, \ldots, \omega_{2g+d-2}$$
are of the third kind on X (i.e. all poles are of order 1).

Let $V_{\mathrm{dR}}(Y) = H^1_{\mathrm{dR}}(Y)^*$ and

$$T_0, \ldots, T_{2g+d-2}$$

be the dual basis. Let

$$A_n^{\mathrm{dR}} = A_n^{\mathrm{dR}}(b)$$

be the universal n-step unipotent object associated to $\pi_1^{\mathrm{dR}}(X,b)$-representation $A_n^{\mathrm{dR}}(b)$ this vector bundle carries a Hodge filtration. For our applications to computing p-adic heights, take $n = 2$ and let $A_Z = A_Z(b)$ be a certain quotient of A_2^{dR}. We will compute the Hodge filtration on A_Z via characterization of the Hodge filtration universal property by Hadian.

Definition 2.122 Filtered connections. A **filtered connection** (V, ∇) is a connection on X together with an exhaustive, descending filtration

$$\cdots \supseteq \mathrm{Fil}^i V \supseteq \mathrm{Fil}^{i+1} V \supseteq \cdots$$

satisfying Griffiths transversality

$$\nabla(\mathrm{Fil}^i V) \subseteq \mathrm{Fil}^{i-1} V \otimes \Omega^1.$$

◊

Theorem 2.123 Hadian '11. *For all $n > 0$ the Hodge filtration on A_n^{dR} is the* unique *filtration s.t.*

1. $\mathrm{Fil}^\bullet$ *makes $(A_n^{\mathrm{dR}}, \nabla)$ into a filtered connection.*

2. *The natural maps induce a sequence of filtered connections*

$$V_{\mathrm{dR}}^{\otimes n} \otimes \mathcal{O}_X \to A_n^{\mathrm{dR}} \to A_{n-1} \to 0.$$

3. *the identity element of $A_n^{\mathrm{dR}}(b)$ lies in $\mathrm{Fil}^0 A_n^{\mathrm{dR}}(b)$.*

Remark 2.124 The important part of this theorem is the uniqueness of the Hodge filtration satisfying the above properties, in what we do the sub-bundle Fil^0 of A_Z is determined in an explicit trivialization on Y, by writing down a general form for a basis, solving for the coefficients using the fact that it extends uniquely to X and satisfies the 3 conditions.

We choose a trivialization

$$s_0(b, \cdot)\colon (\mathbf{Q} \oplus V_{\mathrm{dR}} \oplus \mathbf{Q}(1)) \otimes \mathcal{O}_Y \xrightarrow{\sim} A_Z(b)|_Y$$

s.t. the connection ∇ on A_Z via this trivialization is given by

$$s_0^{-1} \nabla s_0 = \mathrm{d} + \Lambda$$

where

$$\Lambda = -\begin{pmatrix} 0 & 0 & 0 \\ \omega & 0 & 0 \\ \eta & \omega^{\mathrm{T}} Z & 0 \end{pmatrix}$$

for some η of the third kind on X in space spanned by

$$\{\omega_{2g}, \ldots, \omega_{2g+d-2}\}$$

$$\omega = \{\omega_0, \ldots, \omega_{2g-1}\}.$$

Z is the matrix of the Tate class with respect to

$$H^1_{\mathrm{dR}}(X) \otimes H^1_{\mathrm{dR}}(X)$$

(associated to the correspondence Z). Fix a basis

$$\{1, T_0, \ldots, T_{2g-1}, S\}$$

to write down s_0.

The trivialization allows us to describe the connection on Y; to keep track of the fact that it extends to X, introduce the gauge transformation at all

$$x \in D.$$

Recall. all points x are defined over $L/\mathbf{Q}$ finite. In a formal neighborhood of such a point x with local coordinate t_x we can find a trivialization of A_Z

$$s_x\colon ((\mathbf{Q} \oplus V_{\mathrm{dR}} \oplus \mathbf{Q}(1)) \otimes L[[t_x]], \mathrm{d}) \xrightarrow{\sim} (A_Z|_{L[[t_x]]}, \nabla)$$

since A_Z is unipotent and any unipotent connection on a formal disk is trivial.

We have a gauge transformation

$$C_x = s_x^{-1} s_0$$

this is unipotent and satisfies

$$C_x^{-1}\, \mathrm{d}C_x = \Lambda.$$

Expanding out this equation we get that C_x is of the following form:

$$C_x = \begin{pmatrix} 1 & 0 & 0 \\ \Omega_x & 1 & 0 \\ g_x & \Omega_x^{\mathrm{T}} Z & 1 \end{pmatrix}.$$

Where

$$\mathrm{d}\Omega_x = -\omega$$

$$\mathrm{d}g_x = \Omega_x^{\mathrm{T}} Z\, \mathrm{d}\Omega_x - \eta.$$

Lemma 2.125 BDMTV 4.10. *The differential η in Λ is the unique differential satisfying*

1. *η is in the space spanned by*

$$\{\omega_{2g}, \ldots, \omega_{2g+d-2}\}.$$

2. *The connection ∇ extends to a holomorphic connection on the whole of X.*

Proof. The defining equations of the gauge transformation C_x imply that

$$\mathrm{Res}(\Omega_x^{\mathrm{T}} Z\, \mathrm{d}\Omega_x - \eta) = 0$$

for all $x \in D$. Since the kernel of

$$H^1_{\mathrm{dR}}(Y_{\mathbf{Q}}) \longrightarrow L^d$$

given by the residues at all d points $x \in D$ is precisely $H^1_{\mathrm{dR}}(X)$, so the first condition implies that η is unique. ∎

Now we can describe the Hodge filtration on A_Z with respect to our chosen trivialization, s_0 i.e. an explicit isomorphism

$$s^{\mathrm{Fil}} \colon ((\mathbf{Q} \oplus V_{\mathrm{dR}} \oplus \mathbf{Q}(1)) \otimes \mathcal{O}_Y) \xrightarrow{\sim} A_Z$$

that respects the Hodge filtration on both sides, where the LHS is given by

$$\begin{aligned} \mathrm{Fil}^{-1} &= (\mathbf{Q} \oplus V_{\mathrm{dR}} \oplus \mathbf{Q}(1)) \otimes \mathcal{O}_Y \\ \mathrm{Fil}^{0} &= (\mathbf{Q} \oplus \mathrm{Fil}^0 V_{\mathrm{dR}}) \otimes \mathcal{O}_Y \\ \mathrm{Fil}^{1} &= 0. \end{aligned}$$

So we just need to describe Fil^0, define

$$\gamma_{\mathrm{Fil}} \in \mathcal{O}_Y$$

$$b_{\mathrm{Fil}} = (b_g, \ldots, b_{2g-1})^{\mathrm{T}} \in \mathbf{Q}^g$$

by the requirement that

$$\gamma_{\mathrm{Fil}}(b) = 0$$

and for all $x \in D$:

$$g_x + \gamma_{\mathrm{Fil}} - b_{\mathrm{Fil}}^{\mathrm{T}} N^{\mathrm{T}} \Omega_x - \Omega_x^{\mathrm{T}} Z N N^{\mathrm{T}} \Omega_x \in L[[t_x]]$$

where

$$N = (0_g, 1_g)^{\mathrm{T}} M_{2g \times g}(\mathbf{Q}).$$

Then a basis for $\mathrm{Fil}^0 A_Z$ w.r.t. s_0 is given by

$$\{1 + \gamma_{\mathrm{Fil}} S, T_g + b_g S, \ldots, T_{2g-1} + b_{2g-1} S\}.$$

That is we may choose s^{Fil} s.t. the restriction of

$$s_0^{-1} s^{\mathrm{Fil}}$$

$(\mathbf{Q} \oplus \mathrm{Fil}^0 V_{\mathrm{dR}}) \otimes \mathcal{O}_Y$ given by the $(2g+2) \times (g+1)$ matrix

$$\begin{pmatrix} 1 & 0 \\ 0 & N \\ \gamma_{\mathrm{Fil}} & b_{\mathrm{Fil}}^{\mathrm{T}} \end{pmatrix}.$$

Algorithm for Hodge filtration

1. Compute local coordinates at each $x \in D$
2. For each $x \in D$ compute Laurent series expansions ω at x to large precision,
3. Compute Ω_x defined by
$$\mathrm{d}\Omega_x = -\omega_x$$
4. solve for η as the unique
$$\omega_{2g}, \ldots, \omega_{2g+d-2}$$
s.t.
$$\mathrm{d}\Omega$$
has residue zero at all $x \in D$.
5. Solve the system of equations for g_x.

Remark 2.126 For hyperelliptic curves β_{Fil} and γ_{Fil} are both zero.

Lecture 1? 3/12/2019

Recall:

Goal is to compute $h_p(A_Z(b, x))$:

Consider certain rank $2g + 2$ vector bundle

$$\mathcal{A}_Z$$

our working quotient of

$$\mathcal{A}_2.$$

$$\mathcal{A}_Z$$

has the structure of a filtered connection which we computed last time.

The importance of $\mathcal{A}_Z$ having filtered connection is that the base change of $\mathcal{A}_Z$ to $\mathbf{Q}_p$ has a Frobenius structure and then we have an isomorphism of filtered ϕ-modules

$$x^*\mathcal{A}_Z = D_{\mathrm{cris}}(\mathcal{A}_Z(b,x)) \text{ for all } x \in X(\mathbf{Q}_p).$$

Today: describe frobenius structure on isocrystal

$$A_Z^{rig}(\bar{b})$$

and compute this using universal properties.

What is an isocrystal?

(for now affine story, for more details on the rigid picture, see Appendix to B.-Dogra-Müller-Tuitman-Vonk)

Let A be an affinoid algebra and $A^\dagger$ its weak completion. Let $\bar{A} = A^\dagger/\pi$. The idea behind isocrystals and its relation to iterated Coleman integrals is that the iterated Coleman integral can be thought of as a solution to a certain p-adic differential equation (with certain additional structure).

The iterated Coleman integral

$$\int \omega_n \omega_{n-1} \omega_1$$

is the y_n coordinate of a solution to the following system of differential equations:

$$\mathrm{d}y = \Omega y,\ \Omega = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ \omega_1 & 0 & \cdots & 0 \\ 0 & \omega_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots \omega_n & 0 \end{pmatrix}.$$

With $y_0 = 1$. This is a unipotent differential equation

$$y = \begin{pmatrix} y_0 \\ \vdots \\ y_n \end{pmatrix}.$$

Definition 2.127 A **unipotent isocrystal** on $\bar{A}$ is a $A^\dagger$-module M together with an (integrable) connection.

$$\nabla\colon \ \longrightarrow M \otimes_{A^\dagger} \Omega^1(\otimes K)$$

that is an iterated extension of trivial connections where a trivial connection is

$$\mathbf{1} = (A^\dagger, \mathrm{d}).$$

A morphism of unipotent isocrystals is a map of $A^\dagger$-modules, that is horizontal, i.e. commutes with connection. We denote the category of unipotent isocrystals as $Un(\bar{A})$. By Berthelot it only depends on $\bar{A}$ as the notation suggests (in particular it doesn't depend on $A^\dagger$. ◊

Example 2.128 Let $M \in Un(\bar{A})$ be rank 2 then it sits in

$$0 \longrightarrow \mathbf{1} \longrightarrow M \longrightarrow \mathbf{1} \longrightarrow 0$$

which is non-canonically split. Its isomorphic to the object having underlying

module
$$(A^{\dagger})^2$$
and connection
$$\nabla = \mathrm{d} - \begin{pmatrix} 0 & 0 \\ \omega & 0 \end{pmatrix}$$
we have
$$\mathrm{Ext}^1(\mathbf{1}, \mathbf{1}) \simeq H^1_{MW}(\bar{A}).$$

□

For more see Besser's Heidelberg lectures on Coleman integration.

There is an analogous category of unipotent isocrystals via rigid triples (see Appendix of BDMTV). Let $C^{rig}(\mathcal{X}_{\mathbf{F}_p})$ be the category of (rigid) unipotent isocrystals on the special fibre of X.

There is an action of frobenius on path torsors
$$\pi_1^{rig}(\mathcal{X}_{\mathbf{F}_p}, \bar{b}, x)$$
of π_1^{rig}, and n-step unipotent quotients of π_1^{rig}.
$$\phi_n \colon A_n(\bar{b}, \bar{x}) \to A_n(\bar{b}, \bar{x})$$
there is a frobenius structure on $\mathcal{A}_n^{\mathrm{rig}}(\bar{b})$ the universal n-step object. The frobenius structure is an isomorphism
$$\Phi_n \colon \phi^* \mathcal{A}_n^{\mathrm{rig}}(\bar{b}) \xrightarrow{\sim} \mathcal{A}_n^{\mathrm{rig}}(b)$$
of overconvergent unipotent isocrystals. There is a corresponding de Rham realization, the pull back of frobenius to $\mathcal{X}_{\mathbf{F}_p}$ gives frobenius on
$$\pi_1^{\mathrm{dR}}(X_{\mathbf{Q}_p}, b, x)$$
and a frobenius operator on the n-step unipotent quotients
$$\phi_n(b, x) \colon A_n^{\mathrm{dR}}(b, x) \to A_n^{\mathrm{dR}}(b, x).$$

Chiarellotto, B., & Le Stum, B. (1999). F-isocristaux unipotents. Compositio Mathematica, 116(1), 81-110. doi:10.1023/A:1000602824628

Theorem 2.129 Chiarellotto-Le Stum 99. *There is an equivalence of categories*
$$C^{\mathrm{dR}}(X_{\mathbf{Q}_p}) \xrightarrow{\sim} C^{\mathrm{rig}}(\mathcal{X}_{\mathbf{F}_p})$$
given by the analytification functor $(\cdot)^{\mathrm{an}}$. For any $x \in X(\mathbf{Q}_p)$ with reduction $\bar{x}$ we have a canonical isomorphism of fibre functors
$$i_x \colon \bar{x}^* \circ (\cdot)^{\mathrm{an}} \simeq x^*$$
such that if x, y belong to the same residue disks the canonical isomorphism $\tau_{x,y} = i_x \circ i_y^{-1}$ is given by parallel transport along the connection.

Now let b_0 and x_0 be Teichmuller representatives of b, x respectively.

This is how we relate our frobenius operator $\phi_n(b, x)$ to the isocrystal $A_n^{\mathrm{rig}}(\bar{b})$ we have
$$\phi_n(b, x) = \tau_{b,x} \circ \phi_n(b_0, x_0) \circ \tau_{b,x}^{-1}$$
where $\tau_{b,x}$ is from Chiarellotto-Le Stum.

We can describe $\tau_{b,x}$ on $A_n^{\mathrm{dR}}(b,x)$ is a quotient of $A_n^{\mathrm{dR}}(Y)(b,x)$ so suffices to describe parallel transport here.

Recall we've fixed s_0

$$s_0(b,x)\colon \bigoplus_{i=0}^{n} V_{\mathrm{dR}}(Y)^{\otimes i} \xrightarrow{\sim} A_n^{\mathrm{dR}}(b,x)$$

for any $x_1, x_2 \in X(\mathbf{Q}_p)$ that lie in the same residue disk. Define

$$I(x_1,x_2) = 1 + \sum_{x} \int_{x_1}^{x_2} w(\omega_0, \dots, \omega_{2g+d-2}$$

in

$$\bigoplus_{i=0}^{n} V_{\mathrm{dR}}(Y)^{\otimes i}$$

where the sum is over all words in $\{T_0, \dots, T_{2g+d-2}\}$ of length at most n make the substitution with ω_i for T_i.

Here the integrals are given by formally integrating power series (since x_1, x_2 are in the same residue disk). Then $\tau_{b,x}$ when considered on $\mathcal{A}_n^{\mathrm{dR}}(Y)$ via s_0.

$$\begin{aligned} \tau_{b,x}\colon \bigoplus_{i=0}^{n} V_{\mathrm{dR}}(Y)^{\otimes i} &\xrightarrow{\sim} \bigoplus_{i=0}^{n} V_{\mathrm{dR}}(Y)^{\otimes i} \\ v &\mapsto I(x_0,x) \vee I(b,b_0) \end{aligned}$$

then by Besser's theory of Coleman integration on unipotent connections, we have that for any

$$b, b_0, x, x_0 \in Y(\mathbf{Q}_p)$$

the same formula describes the unique frobenius equivariant isomorphism

$$A_n^{\mathrm{dR}}(b,b_0) \xrightarrow{\sim} A_n^{\mathrm{dR}}(x,x_0)$$

if the above is interpreted via Coleman integration.

Finally by taking quotient of the various A_2^* by our nice correspondence Z we get frobenius operators

$$\phi_Z(b,x)\colon A_Z^{\mathrm{dR}}(b,x) \longrightarrow A_Z^{\mathrm{dR}}(b,x)$$

and a quotient $A_Z^{\mathrm{rig}}(\bar{b})$ of the universal 2-step object.

Chiarellotto-Le Stum give us an isomorphism

$$\Phi_Z\colon \phi^* A_Z^{\mathrm{rig}}(\bar{b}) \longrightarrow A_Z^{\mathrm{rig}}(\bar{b})$$

we have the following equalities.

$$\phi_Z(b_0,x_0) = x_0^* \Phi_Z$$

$$\phi_Z(b,x) = \tau_{b,x} \circ \phi_Z(b_0,x_0) \circ \tau_{b,x}^{-1}.$$

The connections on

$$A_Z^{\mathrm{dR}}(b)^{\mathrm{an}}|_Y$$

and

$$\phi^* A_Z^{\mathrm{dR}}(b)^{\mathrm{an}}|_Y$$

are described with respect to s_0 and are equal to $\mathrm{d}+\Lambda$ (as before) and $\mathrm{d}+\Lambda_\phi$, where

$$\Lambda_\phi = -\begin{pmatrix} 0 & 0 & 0 \\ \phi^*\omega & 0 & 0 \\ \phi^*\eta & \phi^*\omega^* Z & 0 \end{pmatrix}$$

so to make the frobenius structure explicit we must compute G s.t.

$$\Lambda_\phi G + \mathrm{d}G = G\Lambda$$

where $G = \Phi_Z^{-1}$ (inverse of frobenius structure).

Proposition 2.130 *Can take G as follows*

$$G = \begin{pmatrix} 1 & 0 & 0 \\ f & F & 0 \\ h & g^{\mathrm{T}} & p \end{pmatrix}$$

where

$$\begin{cases} \phi^*\omega = F\omega + \mathrm{d}f \\ f(b_0) = 0 \\ \mathrm{d}g^{\mathrm{T}} = \mathrm{d}f\mathrm{T}ZF \\ \mathrm{d}h = \omega FZf + \mathrm{d}f^{\mathrm{T}}Zf - g\omega + \phi^8\eta - p\eta \\ h(b_0) = 0 \end{cases}$$

Here is the algorithm for frobenius structure on A_Z

1. Use Tuitman's algorithm to compute matrix of frobenius F and overconvergent functions f s.t.
$$\phi^*\omega = F\omega + \mathrm{d}f.$$

2. Compute the matrix
$$A = I(x, x_0)^+ I(b_0, b)^-$$
where we define for any pair $x_1, x_2 \in X(\mathbf{Q}_p)$ parallel transport matrices
$$I^\pm(x_1, x_2) = \begin{pmatrix} 1 & 0 & 0 \\ \int_{x_1}^{x_2}\omega & 1 & 0 \\ \int_{x_1}^{x_2}\eta + \int_{x_1}^{x_2}\omega^{\mathrm{T}}\omega Z\omega & 1 & \end{pmatrix}$$
solve p-adic differential equation.

References

References

[1] Apostol, Tom M. *Introduction to analytic number theory*. Springer Science & Business Media, 2013.

[2] Arul, V., Best, A. J., Costa, E., Magner, R., & Triantafillou, N. *Computing zeta functions of cyclic covers in large characteristic*.Proceedings of the Thirteenth Algorithmic Number Theory Symposium, The Open Book Series, 2(1), 37-53, 2019.

[3] Balakrishnan, Jennifer S., Robert W. Bradshaw, and Kiran S. Kedlaya. *Explicit Coleman Integration for Hyperelliptic Curves*. In ANTS-IX 2010, LNCS 6197, pp. 16-31, 2010.

[4] Balakrishnan, Jennifer S. *Coleman integration for even-degree models of hyperelliptic curves*. LMS Journal of Computation and Mathematics 18.1 (2015): 258-265.

[5] Balakrishnan, Jennifer S. *Iterated Coleman integration for hyperelliptic curves*. The Open Book Series 1.1 (2013): 41-61.

[6] Balakrishnan JS, Dogra N. *Quadratic Chabauty and rational points I: p-adic heights*. arXiv preprint arXiv:1601.00388. 2016 Jan 4.

[7] Balakrishnan JS, Dogra N, Müller JS, Tuitman J, Vonk J. *Explicit Chabauty-Kim for the Split Cartan Modular Curve of Level 13*. arXiv preprint arXiv:1711.05846. 2017 Nov 15.

[8] Balakrishnan JS, Tuitman J. *Explicit Coleman integration for curves*. arXiv preprint arXiv:1710.01673. 2017 Oct 4.

[9] Balakrishnan, J., Dan-Cohen, I., Kim, M., and Wewers, S. (2012). *A non-abelian conjecture of Birch and Swinnerton-Dyer type for hyperbolic curves*. arXiv preprint arXiv:1209.0640.

[10] Baldassarri, Francesco, and Bruno Chiarellotto. *Algebraic Versis Rigid Cohomology with Logarithmic Coefficients*. In Barsotti Symposium in Algebraic Geometry, edited by Valentino Cristante and William Messing, 15:11–50. Perspectives in Mathematics. Academic Press, 1994. https://doi.org/10.1016/B978-0-12-197270-7.50007-3.

[11] Banagl, Markus. *Topological invariants of stratified spaces*. Springer Science & Business Media, 2007.

[12] Berkovich, Vladimir G. *Integration of One-forms on P-adic Analytic Spaces*. (AM-162). No. 162. Princeton University Press, 2007.

[13] Berthelot, Pierre.*Cohomologie Cristalline des Schémas de Caractéristique* $p > 0$ LNM 407, Springer, 1974.

[14] Berthelot, Pierre. *Finitude et pureté cohomologique en cohomologie rigide* https://perso.univ-rennes1.fr/pierre.berthelot/publis/Finitude.pdf

[15] Besser, Amnon. *Coleman integration using the Tannakian formalism*. Mathematische Annalen 322, no. 1 (2002): 19-48.

[16] Besser, Amnon. *Heidelberg lectures on Coleman integration*. In The Arithmetic of Fundamental Groups, pp. 3-52. Springer, Berlin, Heidelberg, 2012.

[17] Besser, Amnon, and Rob De Jeu. *$Li^{(p)}$-Service? An Algorithm for Computing p-Adic Polylogarithms*. Mathematics of Computation 77, no. 262 (2008): 1105–34.

[18] Besser, Amnon. *Syntomic regulators and p-adic integration I: Rigid syntomic regulators*. Israel Journal of Mathematics 120, no. 2 (2000): 291-334.

[19] Besser, Amnon. *Syntomic regulators and p-adic integration II: K 2 of curves*. Israel Journal of Mathematics 120, no. 2 (2000): 335-359.

[20] Best, A. *Explicit Coleman integration in larger characteristic*. Proceedings of the Thirteenth Algorithmic Number Theory Symposium, The Open Book Series, 2(1), 85-102, 2019.

[21] S. Bosch, U. Güntzer, R. Remmert, *Non-Archimedean Analysis*, Grundlehren der mathematischen Wissenschaften 261, Springer, 1984. MR 86b:32031

[22] Bloch, Spencer. *Higher regulators, algebraic K-theory, and zeta functions of elliptic curves.* Vol. 11. American Mathematical Soc., 2000.

[23] Bochner, S. *Formal Lie Groups*. Annals of Mathematics, vol. 47, no. 2, 1946, pp. 192–201. JSTOR, JSTOR, www.jstor.org/stable/1969242.

[24] Borel, Armand. *Sur La Cohomologie Des Espaces Fibres Principaux Et Des Espaces Homogenes De Groupes De Lie Compacts*. Annals of Mathematics, Second Series, 57, no. 1 (1953): 115-207. doi:10.2307/1969728.

[25] Bostan, Alin, Gaudry, Pierrick, and Schost, Éric. *Linear recurrences with polynomial coefficients and application to integer factorization and Cartier-Manin operator*. SIAM Journal on Computing 36, no. 6 (2007): 1777-1806.

[26] Boston, Nigel. *Explicit deformation of Galois representations*. Inventiones mathematicae 103.1 (1991): 181-196.

[27] Boston, Nigel, and Barry Mazur. *Explicit universal deformations of Galois representations*. Algebraic Number Theory—in honor of K. Iwasawa. Mathematical Society of Japan, 1989.

[28] Booker, Andrew R., Jeroen Sijsling, Andrew V. Sutherland, John Voight, and Dan Yasaki. *A Database of Genus 2 Curves over the Rational Numbers*. LMS Journal of Computation and Mathematics 19, no. A (2016): 235–54. https://doi.org/10.1112/S146115701600019X.

[29] Castryck, Wouter, and Jan Tuitman. *Point Counting on Curves Using a Gonality Preserving Lift*. ArXiv:1605.02162 [Math], May 7, 2016. http://arxiv.org/abs/1605.02162.

[30] Chen, Kuo-Tsai. *Algebras of iterated path integrals and fundamental groups.* Transactions of the American Mathematical Society 156 (1971): 359-379.

[31] Coleman, Robert F. *Torsion points on curves and p-adic abelian integrals.* Annals of Mathematics 121.1 (1985): 111-168.

[32] Coleman, Robert F. *Effective Chabauty* Duke Math. J 52.3 (1985): 765-770.

[33] Coleman, Robert, and Ehud De Shalit. *p-adic regulators on curves and special values of p-adic L-functions*. Inventiones mathematicae 93, no. 2 (1988): 239-266.

[34] Coleman, Robert F. *Dilogarithms, regulators and p-adic L-functions*. Inventiones mathematicae 69, no. 2 (1982): 171-208.

[35] Coleman, Robert F., and B. Gross. *p-adic Heights on Curves* Math. Sciences Research Inst., Berkeley, Calif. (1987).

[36] Conrad, Brian David. *Arithmetic algebraic geometry*. Vol. 9. American Mathematical Soc., 2001.

[37] Edixhoven, Bas. *Point Counting after Kedlaya, EIDMA-Stieltjes Graduate Course, Leiden, September 22–26, 2003*, n.d., 23.

[38] Fresnel, Jean, and Marius Van der Put *Rigid analytic geometry and its applications* Vol. 218. Springer Science & Business Media, 2012.

[39] Gabber O, Ramero L. *Almost ring theory*. Springer; 2003 Dec 15.

[40] Gaudry, Pierrick, and Nicolas Gürel. *An extension of Kedlaya's point-counting algorithm to superelliptic curves*. Advances in Cryptology - ASIACRYPT 2001, Springer, Berlin, Heidelberg, 2001.

[41] Gerritzen, L. and Van der Put, M., 2006. *Schottky groups and Mumford curves* (Vol. 817). Springer.

[42] Gonçalves, Cécile. *A point counting algorithm for cyclic covers of the projective line*. Contemporary mathematics 637 (2015): 145.

[43] Goncharov, Alexander. *Mixed elliptic motives*. London Mathematical Society Lecture Note Series (1998): 147-222.

[44] Goncharov, Alexander B., and Andrey M. Levin. *Zagier's conjecture on L (E, 2)*. Inventiones mathematicae 132, no. 2 (1998): 393-432.

[45] González, Josep, Jordi Guardia, and Victor Rotger. *Abelian surfaces of GL2-type as Jacobians of curves*. arXiv preprint math/0409352 (2004).

[46] Harrison, Michael C. *An extension of Kedlaya's algorithm for hyperelliptic curves*. Journal of Symbolic Computation 47.1 (2012): 89-101.

[47] Hartshorne, Robin. *Algebraic geometry*. Vol. 52. Springer Science & Business Media, 2013.

[48] Harvey, David. *Counting points on hyperelliptic curves in average polynomial time*. Annals of Mathematics 179, no. 2 (2014): 783-803.

[49] Harvey, David. *Kedlaya's Algorithm in Larger Characteristic*. IMRN: International Mathematics Research Notices 2007 (2007).

[50] Harvey, David, and Andrew V. Sutherland. *Computing Hasse–Witt matrices of hyperelliptic curves in average polynomial time*. LMS Journal of Computation and Mathematics 17, no. A (2014): 257-273.

[51] Harvey, David, and Andrew V. Sutherland. *Computing Hasse-Witt matrices of hyperelliptic curves in average polynomial time II*. Frobenius distributions: Lang–Trotter and Sato–Tate conjectures, Contemporary Mathematics 663 (2016): 127-148.

[52] Hasegawa, Yuji, and Mahoro Shimura. *Trigonal Modular Curves*. Acta Arithmetica 88, no. 2 (1999): 129–40. https://doi.org/10.4064/aa-88-2-129-140.

[53] Hida, Haruzo. *Geometric modular forms and elliptic curves*. World Scientific, 2012.

[54] Hulsbergen, Wilfred WJ. *Conjectures in arithmetic algebraic geometry*. Braunschweig: Vieweg, 1992.

[55] Jannsen, Uwe. *Continuous Étale Cohomology*. Mathematische Annalen 280.2 (1988): 207-246.

[56] Jeff Bezanson, Alan Edelman, Stefan Karpinski and Viral B. Shah, *Julia: A Fresh Approach to Numerical Computing*. (2017) SIAM Review, 59: 65–98. doi: 10.1137/141000671. https://julialang.org/research/julia-fresh-approach-BEKS.pdf.

[57] Katz, Nicholas. *Serre-Tate local moduli*. In Surfaces algébriques, pp. 138-202. Springer, Berlin, Heidelberg, 1981.

[58] Katz, Eric, and David Zureick-Brown. *The Chabauty–Coleman Bound at a Prime of Bad Reduction and Clifford Bounds for Geometric Rank Functions*. Compositio Mathematica 149, no. 11 (November 2013): 1818–38. https://doi.org/10.1112/S0010437X13007410.

[59] Kedlaya, Kiran S. *Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology*, J. Ramanujan Math. Soc. 16 (2001), no. 4, 323-338; errata, ibid. 18 (2003), 417--418.

[60] Lang, Serge, *Algebra*, Graduate Texts in Mathematics 1.211 (2002): ALL-ALL.

[61] Lang, Serge. *Algebraic number theory*. Vol. 110. Springer Science & Business Media, 2013.

[62] Lee, John M. *Smooth manifolds*. Springer, New York, NY, 2003. 9780387954486.

[63] Le Gall, François. *Faster algorithms for rectangular matrix multiplication*. In Foundations of Computer Science (FOCS), 2012 IEEE 53rd Annual Symposium on, pp. 514-523. IEEE, 2012.

[64] Qing Liu. *Algebraic geometry and arithmetic curves*. Vol. 6. Oxford University Press, 2002.

[65] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput., 24 (1997), 235–265.

[66] Matsumura, Hideyuki. *Commutative ring theory*. Vol. 8. Cambridge university press, 1989.

[67] Matsumura, Hideyuki. *Commutative algebra*. Vol. 120. New York: WA Benjamin, 1970.

[68] Mazur, Barry, William Stein, and John Tate. *Computation of p-adic heights and log convergence.* Doc. Math (2006): 577-614.

[69] Mazur, Barry, John Tate, and Jeremy Teitelbaum. *On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer*. Inventiones mathematicae 84, no. 1 (1986): 1-48.

[70] Milne, James S. *Etale cohomology* (PMS-33). Vol. 33. Princeton university press, 2016.

[71] Minzlaff, Moritz. *Computing zeta functions of superelliptic curves in larger characteristic*. Mathematics in Computer Science 3.2 (2010): 209-224.

[72] Mumford, David. *Abelian varieties*. Vol. 5. Oxford University Press, USA, 1974.

[73] Narkiewicz, Wladyslaw *Elementary and Analytic Theory of Algebraic Numbers*. Springer, 2004.

[74] Claus Fieker, William Hart, Tommy Hofmann and Fredrik Johansson, *Nemo/Hecke: Computer Algebra and Number Theory Packages for the Julia Programming Language*. In: Proceedings of ISSAC '17, pages 157–164, New York, NY, USA, 2017. ACM.

[75] Polishchuk, Alexander. *Abelian varieties, theta functions and the Fourier transform*. Vol. 153. Cambridge University Press, 2003.

[76] Rolshausen, Klaus, and Norbert Schappacher. *On the second K-group of an elliptic curve.* Journal für die reine und angewandte Mathematik 495 (1998): 61-77.

[77] *SageMath, the Sage Mathematics Software System (Version 8.1.0)*, The Sage Developers, 2017, http://www.sagemath.org.

[78] Serre, Jean-Pierre. *A course in arithmetic*. Vol. 7. Springer Science & Business Media, 2012.

[79] Serre, Jean-Pierre. *Galois cohomology*. Springer Science & Business Media, 2013.

[80] Serre, Jean-Pierre. *Linear representations of finite groups*. Springer Science & Business Media, 1977.

[81] Serre, Jean-Pierre. *Local algebra*. Springer Science & Business Media, 2000.

[82] Serre, Jean-Pierre, Martin Brown, and Michel Waldschmidt. *Lectures on the Mordell-Weil theorem*. Vol. 2. Braunschweig: Vieweg, 1990.

[83] Shafarevich, Igor R., and Alexey O. Remizov. *Linear algebra and geometry*. Springer Science & Business Media, 2012.

[84] Silverman, Joseph H. *The arithmetic of elliptic curves*. Vol. 106. Springer Science & Business Media, 2009.

[85] Silverman, Joseph H. *Advanced topics in the arithmetic of elliptic curves*. Vol. 151. Springer Science & Business Media, 2013.

[86] Stacks Project Authors, *The Stacks Project*, https://stacks.math.columbia.edu.

[87] Stoll, Michael. *Independence of Rational Points on Twists of a given Curve*. Compositio Mathematica 142, no. 5 (September 2006): 1201–14. https://doi.org/10.1112/S0010437X06002168.

[88] Stoll, Michael. *Uniform Bounds for the Number of Rational Points on Hyperelliptic Curves of Small Mordell–Weil Rank*. Journal of the European Mathematical Society 21, no. 3 (December 12, 2018): 923–56. https://doi.org/10.4171/JEMS/857.

[89] Sutherland, Andrew. *Isogeny volcanoes*. The Open Book Series 1, no. 1 (2013): 507-530. https://msp.org/obs/2013/1-1/obs-v1-n1-p25-s.pdf.

[90] Tamme, Günter. *Introduction to étale cohomology*. Springer Science & Business Media, 2012.

[91] Towse, Christopher. *Weierstrass Points on Cyclic Covers of the Projective Line*. Transactions of the American Mathematical Society 348, no. 8 (1996): 3355–3378.

[92] Tuitman, Jan. *Counting points on curves using a map to* $\mathbf{P}^1$. Mathematics of Computation 85.298 (2016): 961-981.

[93] Tuitman, Jan. *Counting points on curves using a map to* $\mathbf{P}^1$*, II*. Finite Fields and Their Applications 45 (2017): 301-322.

[94] van der Geer, G., Moonen, B. *Abelian Varieties*, from `https://www.math.ru.nl/~bmoonen/research.html#bookabvar`.

[95] Vélu, Jacques. *Isogénies entre courbes elliptiques*. CR Acad. Sci. Paris, Séries A 273 (1971): 305-347.

[96] Voight, John. *Quaternion Algebras*. `http://quatalg.org`

[97] Washington, Lawrence C. *Introduction to cyclotomic fields*. Vol. 83. Springer Science & Business Media, 1997.

[98] Waterhouse, William C. *Profinite groups are Galois groups*. Proceedings of the American Mathematical Society 42.2 (1974): 639-640.

[99] Weng, L., and Nakamura, I. *Arithmetic geometry and number theory*, World Scientific, 2006.

[100] Zagier, Don. *The Bloch-Wigner-Ramakrishnan polylogarithm function*. Mathematische Annalen 286, no. 1 (1990): 613-624.

[101] Zagier, D. *Modular Points, Modular Curves, Modular Surfaces and Modular Forms*. In Arbeitstagung Bonn 1984, edited by Friedrich Hirzebruch, Joachim Schwermer, and Silke Suter, 225–48. Lecture Notes in Mathematics. Springer Berlin Heidelberg, 1985.

[102] *Pug Template Engine* see pug-lang.com.