p-adic methods for rational points on curves

MA841 at BU Fall 2019

Jennifer Balakrishnan

September 25, 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 **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 **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 $\#X(\mathbf{Q}) \le 10$. But we find points

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

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 $r \ge 28$.

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 $D \in \operatorname{Div}_X(k)$. 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 $W \in \operatorname{Div}_X(k)$ s.t. for every $D \in \operatorname{Div}_X(k)$ 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 [30], 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 [32]. (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*

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

[31].

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

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

[85]. 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 $\mathbf{Z}_p$. [56].

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*

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

[86].

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

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

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. □

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 $\lambda_i < 1$. ◊

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 ∞. □

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.

[57], [35], 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: [36] [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
$$\left\{ \sum_{-\infty}^{\infty} s_n(x)y^n : s_n \in \mathbf{Z}_q[x],\ \deg s_n \le 2g,\ \mathrm{ord}_p(s_n) > c^n \text{ for some } c > 0 \right\}.$$

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

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

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

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

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

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

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

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

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

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

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

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

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

□

References

References

[1] Conrad, Brian David. *Arithmetic algebraic geometry*. Vol. 9. American Mathematical Soc., 2001.

[2] Apostol, Tom M. *Introduction to analytic number theory*. Springer Science & Business Media, 2013.

[3] 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.

[4] 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.

[5] Balakrishnan, Jennifer S. *Coleman integration for even-degree models of hyperelliptic curves*. LMS Journal of Computation and Mathematics 18.1 (2015): 258-265.

[6] Balakrishnan, Jennifer S. *Iterated Coleman integration for hyperelliptic curves*. The Open Book Series 1.1 (2013): 41-61.

[7] Balakrishnan JS, Dogra N. *Quadratic Chabauty and rational points I: p-adic heights*. arXiv preprint arXiv:1601.00388. 2016 Jan 4.

[8] 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.

[9] Balakrishnan JS, Tuitman J. *Explicit Coleman integration for curves*. arXiv preprint arXiv:1710.01673. 2017 Oct 4.

[10] 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.

[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] Chen, Kuo-Tsai. *Algebras of iterated path integrals and fundamental groups.* Transactions of the American Mathematical Society 156 (1971): 359-379.

[30] Coleman, Robert F. *Torsion points on curves and p-adic abelian integrals.* Annals of Mathematics 121.1 (1985): 111-168.

[31] Coleman, Robert F. *Effective Chabauty* Duke Math. J 52.3 (1985): 765-770.

[32] 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.

[33] Coleman, Robert F. *Dilogarithms, regulators and p-adic L-functions*. Inventiones mathematicae 69, no. 2 (1982): 171-208.

[34] Coleman, Robert F., and B. Gross. *p-adic Heights on Curves* Math. Sciences Research Inst., Berkeley, Calif. (1987).

[35] Edixhoven, Bas. *Point Counting after Kedlaya, EIDMA-Stieltjes Graduate Course, Leiden, September 22–26, 2003*, n.d., 23.

[36] Fresnel, Jean, and Marius Van der Put *Rigid analytic geometry and its applications* Vol. 218. Springer Science & Business Media, 2012.

[37] Gabber O, Ramero L. *Almost ring theory*. Springer; 2003 Dec 15.

[38] 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.

[39] Gerritzen, L. and Van der Put, M., 2006. *Schottky groups and Mumford curves* (Vol. 817). Springer.

[40] Gonçalves, Cécile. *A point counting algorithm for cyclic covers of the projective line*. Contemporary mathematics 637 (2015): 145.

[41] Goncharov, Alexander. *Mixed elliptic motives*. London Mathematical Society Lecture Note Series (1998): 147-222.

[42] Goncharov, Alexander B., and Andrey M. Levin. *Zagier's conjecture on L (E, 2)*. Inventiones mathematicae 132, no. 2 (1998): 393-432.

[43] González, Josep, Jordi Guardia, and Victor Rotger. *Abelian surfaces of GL2-type as Jacobians of curves*. arXiv preprint math/0409352 (2004).

[44] Harrison, Michael C. *An extension of Kedlaya's algorithm for hyperelliptic curves*. Journal of Symbolic Computation 47.1 (2012): 89-101.

[45] Hartshorne, Robin. *Algebraic geometry*. Vol. 52. Springer Science & Business Media, 2013.

[46] Harvey, David. *Counting points on hyperelliptic curves in average polynomial time*. Annals of Mathematics 179, no. 2 (2014): 783-803.

[47] Harvey, David. *Kedlaya's Algorithm in Larger Characteristic*. IMRN: International Mathematics Research Notices 2007 (2007).

[48] 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.

[49] 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.

[50] 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.

[51] Hida, Haruzo. *Geometric modular forms and elliptic curves*. World Scientific, 2012.

[52] Hulsbergen, Wilfred WJ. *Conjectures in arithmetic algebraic geometry*. Braunschweig: Vieweg, 1992.

[53] Jannsen, Uwe. *Continuous Étale Cohomology*. Mathematische Annalen 280.2 (1988): 207-246.

[54] 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.

[55] Katz, Nicholas. *Serre-Tate local moduli*. In Surfaces algébriques, pp. 138-202. Springer, Berlin, Heidelberg, 1981.

[56] 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.

[57] 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.

[58] Lang, Serge, *Algebra*, Graduate Texts in Mathematics 1.211 (2002): ALL-ALL.

[59] Lang, Serge. *Algebraic number theory*. Vol. 110. Springer Science & Business Media, 2013.

[60] Lee, John M. *Smooth manifolds*. Springer, New York, NY, 2003. 9780387954486.

[61] 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.

[62] Qing Liu. *Algebraic geometry and arithmetic curves*. Vol. 6. Oxford University Press, 2002.

[63] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput., 24 (1997), 235–265.

[64] Matsumura, Hideyuki. *Commutative ring theory*. Vol. 8. Cambridge university press, 1989.

[65] Matsumura, Hideyuki. *Commutative algebra*. Vol. 120. New York: WA Benjamin, 1970.

[66] Mazur, Barry, William Stein, and John Tate. *Computation of p-adic heights and log convergence.* Doc. Math (2006): 577-614.

[67] 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.

[68] Milne, James S. *Etale cohomology* (PMS-33). Vol. 33. Princeton university press, 2016.

[69] Minzlaff, Moritz. *Computing zeta functions of superelliptic curves in larger characteristic*. Mathematics in Computer Science 3.2 (2010): 209-224.

[70] Mumford, David. *Abelian varieties*. Vol. 5. Oxford University Press, USA, 1974.

[71] Narkiewicz, Wladyslaw *Elementary and Analytic Theory of Algebraic Numbers*. Springer, 2004.

[72] 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.

[73] Polishchuk, Alexander. *Abelian varieties, theta functions and the Fourier transform*. Vol. 153. Cambridge University Press, 2003.

[74] 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.

[75] *SageMath, the Sage Mathematics Software System (Version 8.1.0)*, The Sage Developers, 2017, http://www.sagemath.org.

[76] Serre, Jean-Pierre. *A course in arithmetic*. Vol. 7. Springer Science & Business Media, 2012.

[77] Serre, Jean-Pierre. *Galois cohomology*. Springer Science & Business Media, 2013.

[78] Serre, Jean-Pierre. *Linear representations of finite groups*. Springer Science & Business Media, 1977.

[79] Serre, Jean-Pierre. *Local algebra*. Springer Science & Business Media, 2000.

[80] Serre, Jean-Pierre, Martin Brown, and Michel Waldschmidt. *Lectures on the Mordell-Weil theorem*. Vol. 2. Braunschweig: Vieweg, 1990.

[81] Shafarevich, Igor R., and Alexey O. Remizov. *Linear algebra and geometry*. Springer Science & Business Media, 2012.

[82] Silverman, Joseph H. *The arithmetic of elliptic curves*. Vol. 106. Springer Science & Business Media, 2009.

[83] Silverman, Joseph H. *Advanced topics in the arithmetic of elliptic curves*. Vol. 151. Springer Science & Business Media, 2013.

[84] Stacks Project Authors, *The Stacks Project*, https://stacks.math.columbia.edu.

[85] 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.

[86] 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.

[87] 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.

[88] Tamme, Günter. *Introduction to étale cohomology*. Springer Science & Business Media, 2012.

[89] Towse, Christopher. *Weierstrass Points on Cyclic Covers of the Projective Line*. Transactions of the American Mathematical Society 348, no. 8 (1996): 3355–3378.

[90] Tuitman, Jan. *Counting points on curves using a map to* $\mathbf{P}^1$. Mathematics of Computation 85.298 (2016): 961-981.

[91] Tuitman, Jan. *Counting points on curves using a map to* $\mathbf{P}^1$*, II*. Finite Fields and Their Applications 45 (2017): 301-322.

[92] van der Geer, G., Moonen, B. *Abelian Varieties*, from https://www.math.ru.nl/~bmoonen/research.html#bookabvar.

[93] Vélu, Jacques. *Isogénies entre courbes elliptiques*. CR Acad. Sci. Paris, Séries A 273 (1971): 305-347.

[94] Voight, John. *Quaternion Algebras*. http://quatalg.org

[95] Washington, Lawrence C. *Introduction to cyclotomic fields*. Vol. 83. Springer Science & Business Media, 1997.

[96] Waterhouse, William C. *Profinite groups are Galois groups*. Proceedings of the American Mathematical Society 42.2 (1974): 639-640.

[97] Weng, L., and Nakamura, I. *Arithmetic geometry and number theory*, World Scientific, 2006.

[98] Zagier, Don. *The Bloch-Wigner-Ramakrishnan polylogarithm function*. Mathematische Annalen 286, no. 1 (1990): 613-624.

[99] 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.

[100] *Pug Template Engine* see pug-lang.com.