p-adic Methods in Number Theory: A Conference Inspired by the Mathematics of Robert Coleman May 26-30, 2015

Notes by Tony Feng

Conference Program

Disclaimer

These are *very rough* and informal notes that I live-TEXed at the conference. I emphasize that they are my personal notes and *may not accurately reflect the actual contents* of the talks. (In particular, I was unable to scribe for any of the talks on the second day.) Their faithfulness to the originals has suffered from my insufficiently fast typing, lack of understanding, mental exhaustion, and in some cases shortage of computer battery. Of course, I take full responsibility and apologize for all omissions and inaccuracies.

My intention in writing these notes was for private use, but I have made them public in case they turn out to be useful to anybody.

INTEGRATION ON CURVES, FROM ABEL TO COLEMAN

DICK GROSS

♠♠♠ TONY: [I missed the first 15 minutes due to traffice :(]

1. Coleman Integration

X is a curve of genus g.

1.1. **Differentials of the second kind.**

Definition 1.1. The *differentials of the second kind* on a curve are those which are locally exact at every point P of X, which is equivalent to having vanishing residue at all points.

Example 1.2. Exact differentials $\eta = dG$ are differentials of the second kind.

The quotient space of the differentials of the second kind by the exact ones has dimension $2g$, and is isomorphic to the first de Rham cohomology group $H^1(X, \mathbb{C})$.

1.2. **Rigid analytic spaces.**

Suppose we have an affine variety $Y_0 = \operatorname{Spec} A_0$ over a finite field $\mathbb{F}_p$. Lift A_0 to a smooth, finitely generated $\mathbb{Z}_p$-algebra A and then form

$$\widehat{A} = \varprojlim (A/p^n A).$$

Example 1.3. If $Y_0 = \mathbb{A}^1_{\mathbb{F}_p}$ then $A_0 = \mathbb{F}_p[t]$. One lift is $A = \mathbb{Z}_p[t]$, and then the completion is $\widehat{A} = \mathbb{Z}_p[[t]]$. We can think of this as the ring of power series converging on the closed unit disk.

Let Y be the rigid analytic space with the algebra of functions $\widehat{A} \otimes \mathbb{Q}_p$. The quotient of the space of locally exact analytic differentials by the subspace of exact differentials on Y is the finite dimensional vector space $H^1(Y_0, \mathbb{Q}_p)$. The definition depended on a choice of lift, but it turns out that this cohomology group is in some sense "independent" of the lift (for instance, its dimension is independent).

Strictly speaking, this isn't quite right. It turns out that there are some things that you expect to be exact but aren't. Technically, one needs to consider instead a "weaker completions" and "wide open spaces," but we'll ignore these technicalities.

The cohomology group $H^1(Y_0, \mathbb{Q}_p)$ is equipped with a linear endomorphism T induced from an analytic lifting $F\colon Y \to Y$ of the Frobenius morphism $F_0\colon Y_0 \to Y_0$ to Y. This depends of the lift of course, but the characteristic polynomial of Frobenius turns out to depend only on Y_0. Miraculously, it has integer coefficients, and is the same as the characteristic polynomial of Frobenius on ℓ-adic cohomology group $H^1(\overline{Y_0}, \mathbb{Q}_\ell)$ for all ℓ. This can be used to do point counts, via the formula

$$\#Y_0(\mathbb{F}_p) = p - \mathrm{tr}(pT^{-1}|_{H^1}).$$

(T is invertible because we know from the theory of weights that the eigenvalues of Frobenius have absolute value $p^?$, and in particular are non-zero.)

1.3. **Coleman integration.** Robert had the following beautiful observation. If M is the characteristic polynomial of T, then by the Cayley-Hamilton theorem, $M(T) = 0$ on $H^1(Y_0, \mathbb{Q}_p)$ so $M(F^*)(\eta) = dG$ is exact (since it vanishes in cohomology). This gives a rigid analytic integral for $M(F^*)(\eta)$. What about locally analytic integrals for η?

The problem is that there are too many. Indeed, notice that on the open residue disc of points with the same reduction as a given point P, we have a convergent expansion

$$\eta = \sum a_n z^n\, dz, \text{ where } a_{-1} = 0 \text{ (since } \eta \text{ is of the second kind).}$$

Then a locally analytic integral of η is given by the convergent series

$$\sum \frac{a_n}{(n+1)} z^{n+1} + C_P,$$

which converges since we're on the open disc. However, we can choose the constants C_P in each disc arbitrarily. This lack of uniqueness makes it hard to turn this into a functorial theory.

Robert solved this as follows. Start with complete curve X over $\mathbb{Q}_p$ with good reduction X_0. Let $Y_0 = X_0 - S$ be the affine curve obtained by removing a finite set S of points of X. Let Y be the rigid analytic space obtained by lifting and removing the open residue discs reducing to points in S. Let ω be an algebraic differential on X whose poles all lie in the removed residue discs (and thus is analytic on Y), and let y be a point in Y.

Theorem 1.4. *There is a unique locally analytic function $G(x) = \int_y^x \omega$ on Y satisfying*

(1) $dG = \omega$,
(2) $G(y) = 0$, and
(3) $M(F^*)(G)$ is rigid analytic.

This turns the theory of p-adic cohomology on its head! We started out discussing cohomology by starting with a variety over $\mathbb{F}_p$ and constructing a rigid analytic space; Robert instead considered integration on rigid analytic spaces by looking to the special fiber.

Example 1.5. I'll show you one of Robert's favorite examples. Let $X = \mathbb{P}^1$ and $\omega = \frac{dx}{x}$ (which is not of the second kind)

Remove $D(0) = \{x\colon |x| > 1\}$ and $D(\infty) = \{x\colon |x| < 1\}$ and you get $Y = \{x\colon |x| = 1\}$. In the complex analytic world this is a very small set, the unit circle, but in the p-adic world it is actually quite large. Robert named the "unit tire." You can imagine it as a union of $p-1$ discs, each centered at a distinct $p-1$st root of unity.

Then $F(x) = x^p$ and $\omega = \frac{dx}{x}$ is a basis of $H^1(Y_0, \mathbb{Q}_p)$. So $F^*(\omega) = p\omega$, and the characteristic polynomial is $M(x) = x - p$.

For $y = 1$, the Coleman integral $G(x) = \int_1^x \omega$ satisfies:

(1) G is locally analytic,
(2) $dG = \omega$,
(3) $G(1) = 0$,
(4) $G(x^p) - pG(x)$ is a rigid analytic with derivative zero ♠♠♠ TONY: [why?], there must be a constant C. (This is the importance of analyticity - there are many locally constant functions, which all have derivative 0.)

But since $G(1) = 0$, $C = 0$. So $G(x^p) = pG(x)$, and by iteration $G(x^{p^n}) = p^n G(x)$. Now, in a residue disk around 1,

$$G(1+z) = \int \frac{d(1+z)}{1+z} = z - z^2/2 + z^3/3 - z^4/4 + \dots$$

What about the other disks? Since $\zeta^{p^n} = 1$, the relation $G(x^p) = pG(x)$ implies that $p^n G(\zeta) = 0$, so $G(\zeta) = 0$, and all the values at the other disks are determined by this relation.

So the Coleman integral $G = \log_p$ is Iwasawa's logarithm.

In this computation the key point was that $p^n \neq 1$: there are no Frobenius eigenvalues that are roots of unity.

1.4. **Effective Chabauty.** If ω is of the first kind, then its integral G is locally analytic everywhere. For a divisor $D = \sum m_x[x]$ of degree 0, let

$$\int_D \omega = G(D) := \sum m_x G(x).$$

In the complex case, Abel's theorem implies that the value $G(D) = \int_D \omega$ depends only on the image of D in the Jacobian J. Robert recognized that you should be able to describe this purely in the arithmetic of the abelian variety.

He found that the integral of ω is the composition

$$\mathrm{Div}^0(X)(\mathbb{Q}_p) \to J(\mathbb{Q}_p) \xrightarrow{\log} \mathrm{Lie}(J(\mathbb{Q}_p)) \cong H^1(X, \mathcal{O}_X) \xrightarrow{\langle \omega, - \rangle} \mathbb{Q}_p$$

(We have used the Serre duality pairing at the end.)

An important consequence of this was that $D \equiv (x) - (y)$ is torsion in J if and only if $\int_y^x \omega = 0$ for all regular ω. Why? If the integrals are 0 for all the regular differentials, and Serre duality is perfect, then the image of the divisor in $H^1(X, \mathcal{O}_X)$ is 0, so the logarithm is 0. But it was known classically that the kernel of the logarithm precisely consists of torsion.

You can attempt to explicitly calculate the integrals as a power series in order to find an explicit description of the torsion. This led to Robert's *effective* Chabauty method: if the Mordell-Weil rank of X is less than g, then the closure of the rational points has codimension at least 1 in the Jacobian, so there is a regular differential vanishing on them, and pulling back to the curve cuts out an algebraic condition on the rational points.

2. Differentials and Height Pairings

2.1. **Differentials of the Third Kind.** Abel also defined "integrals of the third kind."

Definition 2.1. A differential ν is said to be of the *third kind* if its only poles on X are simple, and if all of its residues are integers. (In particular, they include the differentials of the first kind, which are regular.)

Remark 2.2. This is not a vector space, because of the integrality condition.

Example 2.3. Logarithmic differentials $\nu = df/f$ are of the third kind.

The quotient of differentials of the third kind by logarithmic derivatives is a commutative, connected algebraic group G of dimension $2g$, whose tangent space is $H^1(X)$. In the complex case there is a homomorphism $H^1(X, \mathbb{C}) \xrightarrow{\exp} G(\mathbb{C})$ and in the p-adic case there is a logarithm $G(\mathbb{Q}_p) \to H^1(X, \mathbb{Q}_p)$.

Associated to the differential of the third kind, we have the residual divisor of degree zero:

$$\mathrm{Resdiv}(\nu) := \sum_P \mathrm{Res}_P(\nu)[P].$$

Every divisor D of degree zero occurs as a residual divisor of a differential of the third kind. This follows from an easy argument using Riemann-Roch. Indeed, it is evidently sufficiently to construct divisors of the form $P - Q$ as residual divisors. By Riemann-Roch, there is a divisor of high degree with simple poles at $P + Q$ and no simple poles anywhere else (compare $H^0(K)$

with $H^0(K+P+Q)$. The residues at P and Q are negatives, since their sum is 0, and rescaling gives a residual divisor $P-Q$.

Given a differential of the third kind ν with a given residual divisor, any other such is unique up to the addition of a differential of the first kind: $\nu^* = \nu + \omega$.

When $D = (f)$ is principal, we can take $\nu_D = df/f$. Can we normalize the lifting $D \mapsto \nu_D$ to generalize this? We don't know. ♠♠♠ TONY: [don't know what this means]

2.2. **Periods.** How did Riemann do this? For a closed path γ on a R surface X and a differential ω of the first kind, the period $\int_\gamma \omega$ depends only on the class of γ.

The period integrals determine ω, so there is an injection

$$W = H^0(X, \Omega^1) \hookrightarrow V = \mathrm{Hom}(H_1(X, \mathbb{Z}), \mathbb{C}) = H^1(X, \mathbb{C}).$$

The space V is symplectic of dimension $2g$, the subspace W is of dimension g and isotropic, satisfying $W \cap \overline{W} = 0$. The map taking $\omega \mapsto \mathrm{Rep} \int_\gamma \omega$ gives an isomorphism $W \cong \mathrm{Hom}(H_1(X, \mathbb{Z}), \mathbb{R})$, because the dimensions are the same and this is an injection. Indeed, suppose you had form whose real parts of periods were 0. Then the complex conjugate form would have real periods, which would be something in $W \cap \overline{W}$.

2.3. **Local Height Pairing.** Let D be a degree 0 divisor and ν be a differential of the third kind with residual divisor D. Let ω be the unique differential of the first kind withs $\mathrm{Rep} \int_\gamma \omega = \mathrm{Rep} \int_\gamma \nu$. Then $\nu_D := \nu - \omega$ is the unique differential of the third kind with

(1) $\mathrm{Resdiv}(\nu_D) = D$ and
(2) $\mathrm{Rep} \int (\nu_D) = 0$ for all cycles $\gamma \in H_1(X - |D|, \mathbb{Z})$.

Then you can define a Neron local height pairing on relatively prime divisors D and E, given by

$$\langle D, E \rangle = \mathrm{Rep} \int_E \nu_D = \mathrm{Rep} \int_D \nu_E,$$

with equality following from a form of Stokes. A nice property of this is that if $\nu = df/f$, then

$$\langle (f), E \rangle = \log |f(E)|.$$

The important thing about these pairings is that if you sum up them up, then you get one on the Jacobian.

Robert recognized that this could be done p-adically. Nomalize the choice of differential ν_D with residual divisor D. When the reduced curve X_0 is ordinary, we can normalize ν_D using the unit root eigenspace. To elaborate,

we have $H^1(X, \mathbb{Q}_p) = W \oplus U$. There is a part of W where the eigenvalues of Frobenius are p-adic units. Normalize as follows: there's an exact sequence

$$W = H^0(X, \Omega^1) \to G(\mathbb{Q}_p) \to J(\mathbb{Q}_p)$$

where G is differential of third kind modulo logarithmic derivatives (see Example 2.3). By the logarithm, $G(\mathbb{Q}_p)$ maps to $H^1(X, \mathbb{Q}_p)$. This has two coordinates, in W and U: normalize so that the W-coordinate is in the unit root eigenspace.

The local height pairing is then given by the Coleman integral

$$\langle D, E \rangle_p = \int_E \nu_D = \int_D \nu_E$$

satisfying $\langle (f), E) \rangle_p = \log_p(f(E))$. For relatively prime divisors, the poles lie in disjoint residue disks. See Colmez book - Integration sur les varieties p-adiques, Asterisque 248 (1998).

QUADRATIC TWISTS OF ELLIPTIC CURVES

JOHN COATES

1. Introduction

Let me begin by reviewing what we know about elliptic curves concerning the Birch and Swinnerton-Dyer conjecture. Let $E/\mathbb{Q}$ be an elliptic curve. We denote, as usual,

- $E(\mathbb{Q})$ for the rational points of E,
- $Ш(E)$ for its Tate-Shafarevich group,
- $L(E, s)$ for its L-function, and
- $r_E = \mathrm{ord}_{s=1} L(E, s)$, the *analytic rank*.

Theorem 1.1 (Gross-Zagier, Kolyvagin)**.** *If $r_E \leq 1$, then $E(\mathbb{Q})$ has rank r_E and $Ш(E)$ is finite.*

Remark 1.2. Even with these hypotheses, we do not know the precise formula for the order of $Ш(E)$ which is predicted by Birch and Swinnerton-Dyer.

Theoretically, very little is known in the way of how to show that $r_E \leq 1$ (of course, it is can be checked numerically in examples).

Throughout, let M be the discriminant of a quadratic extension of $\mathbb{Q}$. Let $k = k(M)$ be the number of prime factors of M, and $E^{(M)}$ the quadratic twist of E by $\mathbb{Q}(\sqrt{M})/\mathbb{Q}$. Associated to $L(E^{(M)}, s)$ there is a *root* number $w_E(M) = \pm 1$.

Conjecture 1.3 (Goldfeld)**.**

(1) Among all twists with $w_E(M) = +1$, we have $r_E(M) = 0$ outside a set of density 0.

(2) Among all twists with $w_E(M) = -1$, we have $r_E(M) = 1$ outside a set of density 0.

The best previous results toward this were proved by Bump, Hoffstein, etc. which say that there are *infinitely many* twists with these properties.

2. Statement of results

Together with Y. Li, Y. Tian, and S. Zhai we have investigated this for particular curves. In particular, we consider quadratic twists of $X_0(49)$. A

model is

$$A = X_0(49)\colon\ y^2 + xy = x^3 - x^2 - x - 1.$$

This has CM by O_K, where $K = \mathbb{Q}(\sqrt{-7})$. This elliptic curve, and its twists, are the only curves over $\mathbb{Q}$ for which 2 is ordinary or potentially ordinary. One can show by 2-descent that $A(\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z}$, with the cusps ∞ and $[0] = (2, -1)$.

We know that $w_A(M) = +1$ when $M > 0$ and $(M, 7) = 1$ and $w_A(M) = -1$ when $M < 0$ and $(M, 7) = 1$.

We now restrict our attention to twists by:

$$\mathcal{R} = \{R = p_1 \dots p_k \mid p_i \equiv 1 \pmod 4,\ \text{inert in } K\}.$$

If $R \in \mathcal{R}$, then $\mathrm{Sel}_2(A^{(R)})$ has $\mathbb{F}_2$-dimension 1 (it's obviously at least 1, because there's a 2-torsion point). So the rank is 0, as you can verify by 2-descent. According to Birch and Swinnerton-Dyer, you would expect the L-function to be non-vanishing.

Theorem 2.1 (CLTZ)**.** *If $R \in \mathcal{R}$, then $L(A^{(R)}, 1) \neq 0$.*

Theorem 2.2 (Rubin-Gonzalez-Aviles)**.** *If $L(A^{(M)}, 1) \neq 0$, then $\#Ш(A^{(M)})$ is as predicted by BSD.*

The fundamental (least positive real) period of A is

$$\Omega_\infty = \frac{\Gamma(1/7)\Gamma(2/7)\Gamma(4/7)}{2\pi\sqrt{7}}.$$

The theorem then says that if $R \in \mathcal{R}$, then

$$\#Ш(A^{(R)}) = \frac{L(A^{(R)}, 1) \cdot \sqrt{R}}{\Omega_\infty 2^{k(R)=1}}.$$

We know that this is an odd positive integer (odd because the 2-descent shows that the 2-part of Ш is zero).

Numerical data. Dabroski, Jedrzejak, Szymaszkriewicz computed for $\#Ш(A^{(R)})$ for $R \in \mathcal{R}(32 \times 10^9)$, where $\mathcal{R}(X) := \{R \in \mathcal{R}\colon\ R \leq X\}$. Based on this, they guessed:

(1) For every odd positive t, there exists $R \in \mathcal{R}$ with $\#Ш(A^{(R)}) = t^2$. This is verified for $t \leq 2357$. The large p such that $Ш(A^{(R)})(p) \neq 0$ is $p = 2851$.

(2) The "cumulative" Shafarevich group size

$$\sum_{R \in \mathcal{R}(X)} \#(Ш(A^{(R)}))$$

is either (a) $cX^{3/2}$ for $c = 0.00434$, or (b) based on heuristics of Heath-Brown $c'X^{3/2}/(\log X)^{1/8}$ with $c' = 0.0124$. Since $(\log X)^{1/8}$

is basically constant in the range, we can't really tell which one is correct from the data.

Now, we turn to a case where the twists have rank 1.

Definition 2.3. Let

$$\mathcal{P} = \left\{ M = -\ell R \mid \begin{smallmatrix} \ell \text{ prime }, \ell \equiv 3 \pmod 4, \ell > 3, \ell \text{ inert in } K \\ R = p_1 \dots p_k \in \mathcal{R}, p_i \text{ inert in } \mathbb{Q}(\sqrt{-\ell}) \end{smallmatrix} \right\}.$$

The last condition is unnecessary for 2-descent, but it is needed for our method, which uses the theory of Heegner points.

If $M \in \mathcal{P}$ then $\mathrm{Sel}_2(A^{(M)})$ has $\mathbb{F}_2$-dimension 2. BSD predicts that $L(A^{(M)}, s)$ has a simple 0 at $s = 1$, and we confirm this.

Theorem 2.4 (CLTZ)**.** *If $M \in \mathcal{P}$, then $r_A(M) = 1$.*

In this case predicts that $\frac{L'(A^{(M)},1)\sqrt{-M}}{\Omega_\infty 2^{k(R)}}$ is supposed to be $\#Ш(A^{(M)})$ times the height of the canonical generator.

Numerical data. Again we have some numerical results. Let

$$V_\ell(X) = \{M = -\ell R \in \mathcal{P}, |M| \le X\}$$

and

$$T_\ell(X) = \sum_{M \in V_\ell(X)} \frac{L'(A^{(M)}, 1)\sqrt{-M}}{\Omega_\infty 2^{k(R)}} \asymp c_\ell X^{3/2} \log X$$

for some c_ℓ.

Let $E/\mathbb{Q}$ be an elliptic curve and C the conductor of E. We have by modularity a map $f\colon X_0(C) \to E$ sending $f([\infty])$ to 0 and $f([0])$ to some torsion point of $E(\mathbb{Q})$.

Lemma 2.5 (Birch-Heegner)**.** *Assume that $f([0]) \notin 2E(\mathbb{Q})$ (so the 2-primary part of $E(\mathbb{Q})$ is non-trivial). Let ℓ be any prime with $\ell > 3$ and $\ell \equiv 3 \pmod 4$ such that C splits in $\mathbb{Q}(\sqrt{-\ell})$. Then $L(E^{(-\ell)}, s)$ has a simple zero at $s = 1$.*

Their argument, as it stands, only works when you twist by a *prime*.

Theorem 2.6 (CLTZ)**.** *Assume that (i) $f([0]) \notin 2E(\mathbb{Q})$ and (ii) E has a good supersingular prime q with $q \equiv 1 \pmod 4$. Then, for each $k \ge 1$, there exist infinitely many odd squarefree M with $k(M) = k$ and $r_{E^{(M)}} = 1$. Also, for each $k \ge 2$ there exist infinitely many odd squarefree M with $r_{E^{(M)}} = 0$.*

Example 2.7. Let $E = X_0(14)$. Then we can take $q = 5$ and $E(\mathbb{Q})(2) = \mathbb{Z}/2\mathbb{Z}$. The theorem tells us that $L(E^{(M)}, 1) \neq 0$ for infinitely many $M = q_1 \dots q_k$ if $k \ge 1$.

You can do a 2-descent on E to find that $\mathrm{Sel}_2(E^{(M)})$ has $\mathbb{F}_2$-dimension 1 for $q_i \equiv 3, 5, 6 \pmod 7$ and $5 \pmod 8$. So we should have non-vanishing in all of these cases, but we can't prove it.

Example 2.8. If E is given by $y^2 = x^3 - x^2 - x - 2$, then $C = 84$ and we can take $q = 41$ or 89. Looking through the tables, there are many elliptic curves satisfying the necessary properties. There are probably infinitely many curves to which this applies.

The proof is via analysis of what happens at the humble prime 2. Somehow, this is more powerful than any analytic methods (so far) - they can't prove infinitude while control the *number* of prime factors, which we do.

P-ADIC VECTOR BUNDLES AND PARALLEL TRANSPORT

ANNETTE WERNER

1. Setup

Let $X/\overline{\mathbb{Q}_p}$ be a proper, smooth, connected scheme. We may sometimes base change to $X_{\mathbb{C}_p}$. We denote $\overline{\mathbb{Z}_p} \subset \overline{\mathbb{Q}_p}$ and $\mathcal{O}_p \subset \mathbb{C}_p$ the respective valuation subrings, which both have residue field $k \cong \overline{\mathbb{F}_p}$.

Goal. Define a category of vector bundles on $X_{\mathbb{C}_p}$ admitting "p-adic parallel transport."

By "parallel transport" we mean a representation of the étale fundamental groupoid $\pi_1(X)$ in parallel transports of vector spaces. More precisely, $\pi_1(X)$ is a category whose objects are $x \in X(\mathbb{C}_p)$ and whose morphisms between $x, x' \in X(\mathbb{C}_p)$ are isomorphisms of fiber functors:

$$\mathrm{Hom}_{\pi_1(X)}(x, x') = \mathrm{Iso}(\mathcal{F}_x, \mathcal{F}_{x'})$$

where $\mathcal{F}_x$ is the functor from the category of finite étale covers $Y \to X$ to the category of finite sets taking $\alpha\colon Y \to X$ to the fiber $\{y \in Y(\mathbb{C}_p) \mid \alpha(y) = x\}$. So an isomorphism of fiber functors is a recipe for taking a point of the fiber over x under any finite étale cover to a point over x'. This is a profinite set.

Definition 1.1. A *p-adic parallel transport* on a vector bundle E is a functor

$$\rho_E\colon \pi_1(X) \to \underbrace{\mathrm{Vec}_{\mathbb{C}_p}}_{\text{fin. dim.}}$$

which is continuous, meaning that it is continuous on each set of morphisms.

In particular, for all $x \in \mathbb{C}_p$ we get a finite-dimensional continuous representation of $\pi_1^{\text{ét}}(X, x)$ over $\mathbb{C}_p$.

2. Statement of Results

2.1. **Dimension one.** There are several results known when $\dim X = 1$.

Theorem 2.1 (Deninger-Werner)**.** *Vector bundles E of degree 0 with potentially strongly semistable reduction admit parallel transport.*

Let us explain the condition here.

- "Potentially" means "after replacing X by a finite cover $Y \xrightarrow{\alpha} X$ and E by $\alpha^* E$.
- "Semistable" means that the *slope* $\frac{\deg}{\operatorname{rank}}$ of a subbundle is no larger than that of E.
- "Strongly semistable" means that pullbacks via all (non-negative) powers of absolute Frobenius are semistable.
- The technical condition we require is that there is a relative curve $\mathcal{X}/\overline{\mathbb{Z}_p}$ with generic fiber X, and a vector bundle $\mathcal{E}$ on $\mathcal{X} \otimes \mathcal{O}_p$ with generic fiber E, such that the special fiber $\mathcal{E} \otimes_{\mathcal{O}_p} k$ is strongly semistable of degree 0 on each irreducible component of $\mathcal{X}_k$.

Semistability is a difficult notion on reducible varieties, and we remove difficulties by imposing this condition on each component.

2.2. **Motivation.** This is a p-adic analog of results on the topological fundamenetal group in complex geometry. Harder-Narasimhan showed that from *unitary* representations one gets stable vector bundles. There is also a correspondence discovered by Simpson.

Faltings showed a p-adic version of the Simpson correspondence: there is an equivalence of categories

$$\left\{\begin{matrix} p\text{-adic Higgs bundles} \\ \text{on } X_{\mathbb{C}_p} \end{matrix}\right\} \leftrightarrow \left\{\begin{matrix} \text{generalized representations} \\ \text{of } \pi_1^{\text{ét}}(X, x) \end{matrix}\right\}.$$

A big open question is to determine the subcategory of p-adic Higgs bundles corresponding to (honest) representations of $\pi_1^{\text{ét}}(X, x)$. One can show that the degree 0 line bundles are there, but we don't know what else is.

2.3. **Higher dimension.** There is a work in progress in higher dimensions. Let $X/\overline{\mathbb{Q}_p}$ be a smooth, proper connected scheme and $U \subset X$ a Zariski open subset.

Definition 2.2. Let $B_{X,U}$ be the (full) category of vector bundles on $X_{\mathbb{C}_p}$ such that there exists a (flat, proper, finite presented) $\mathcal{X}/\overline{\mathbb{Z}_p}$ with generic fiber X, and

- there exists a vector bundle $\mathcal{E}$ on $X \otimes \mathcal{O}_p$ with generic fiber E,
- There exists a proper, finitely presented map $\pi\colon \mathcal{Y} \to \mathcal{X}$ such that $\pi|_{\pi^{-1}(U)}$ is finite étale and the special fiber $(\pi^*\mathcal{E}) \otimes_{\mathcal{O}_p} k$ is trivial on Y_k.

Definition 2.3. Let $\mathcal{B}_X$ be the category of vector bundles in $\mathcal{B}_{X,U_i}$ for all members U_i of a Zariski covering (U_i) for X.

Theorem 2.4 (Deninger-Werner)**.** *Every E in $\mathcal{B}_X$ admits p-adic parallel transport $\rho_E\colon \pi_1(X) \to Vec_{\mathbb{C}_p}$. Moreover, the association $E \mapsto \rho_E$ is functorial in E, exact, and compatible with $\oplus, \otimes, \underline{\mathrm{Hom}}$, and $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$-conjugation.*

3. Sketch of Proof

Let $E \in \mathcal{B}_{X,U}$. Take $x, x' \in U(\mathbb{C}_p) \subset \mathcal{X}(\mathcal{O}_p)$. Let γ be an étale path in U from x to x'. We want to construct an isomorphism $\rho_E \colon E_x \to E_{x'}$.

We're going to define for all n a morphism $\rho_{\mathcal{E},n} \colon \mathcal{E}_x \otimes \mathcal{O}_p/p^n \to \mathcal{E}_{x'} \otimes \mathcal{O}_p/p^n$ ($\mathcal{E}_x$ is an $\mathcal{O}_p$-lattice) and set

$$\rho_E(\gamma) := (\varinjlim_n \rho_{\mathcal{E},n}(\gamma)) \otimes \mathbb{C}_p$$

Assume that there exists $\pi \colon \mathcal{Y} \to \mathcal{X}$ proper and finitely presented such that

(1) $(\pi^*\mathcal{E}) \otimes \mathcal{O}_p/p^n$ is trivial on $\mathcal{Y} \otimes \mathcal{O}_p/p^n$ (the nth tickening of the special fiber), and
(2) $\pi|_{\pi^{-1}(U)}$ is finite étale.

This looks like a p-adic thickening of the condition imposed on the category $\mathcal{B}_{X,U}$.

If this is given, then replacing $\mathcal{Y}$ by a "nice" covering we have a canonical parallel transport on the trivial bundle $\pi^*\mathcal{E} \otimes \mathcal{O}_p/p^n$, by using the trivialization.

To elaborate, choose $y \in Y(\mathbb{C}_p) = \mathcal{Y}(\mathcal{O}_p)$ over x. Then $\gamma(y) = y'$ where $\pi(y') = x'$, as γ is by definition an isomorphism of the fiber functor. This gives

$$\begin{array}{ccc} (\pi^*\mathcal{E})_y \otimes \mathcal{O}_p/p^n & \xrightarrow{\cong} & (\pi^*\mathcal{E})_{y'} \otimes \mathcal{O}_p/p^n \\ \downarrow \cong & & \downarrow \cong \\ \mathcal{E}_x \otimes \mathcal{O}_p/p^n & \xrightarrow{\rho_{\mathcal{E},n}(\gamma)} & \mathcal{E}_{x'} \otimes \mathcal{O}_p/p^n. \end{array}$$

That defines a representation modulo p^n. Of course, there are many things to check in order to ensure that this is well-defined.

The induction step uses de Jong's theory of alterations and generalizations of ideas of Bhatt. You see, Y depends on n. The obstruction to it working for $n+1$ is some obstruction in a cohomology group. Then you have to kill this obstruction class by passing to some bigger cover. The obstruction lives in a world modulo p^n, and you want to lift all the way to characteristic 0, so there is quite some work to be done.

Now, to get a representation on all of X, you use an analogue of the Seifert van Kampen theorem.

4. Abelian varieties

Let $X = A/\overline{\mathbb{Q}_p}$ be an abelian variety with good reduction. Then it can be shown that every homogeneous bundle on A lies in $\mathcal{B}_A$. (Homogeneous means that $t_x^* E \cong E$ for all $x \in A(\mathbb{C}_p)$.) Over $\mathbb{C}$, the homogeneous bundles are precisely the ones admitting an integrable connection.

Theorem 4.1 (Deninger-Werner)**.** *The following diagram commutes:*

$$\begin{array}{ccc}
\mathrm{Ext}^1(\mathcal{O}_A, \mathcal{O}_A) & \xrightarrow{E \mapsto \rho_E} & \mathrm{Ext}^1_{\mathrm{Rep}\,\pi_1(A,0)}(\mathbb{C}_p, \mathbb{C}_p) \\
 & & \cong \big\downarrow \begin{pmatrix} 1 & * \\ & 1 \end{pmatrix} \mapsto * \\
\cong \big\downarrow & & \mathrm{Hom}(\pi_1(A,0), \mathbb{C}_p) \\
 & & \cong \big\downarrow \\
H^1(A, \mathcal{O}_A) \otimes_{\overline{\mathbb{Q}_p}} \mathbb{C}_p & \xrightarrow[\text{Hodge-Tate}]{} & H^1_{\acute{e}t}(A, \overline{\mathbb{Q}_p}) \otimes \mathbb{C}_p)
\end{array}$$

The proof relies crucially on Coleman's description of the Hodge-Tate periods in terms of Coleman integrals, which goes as follows. Let $\mathcal{A}$ be the Néron model of A, and let

$$0 \to \omega_{\widehat{A}} \to \mathcal{V} \to \mathcal{A} \to 0$$

be the *universal vectorial extension* (i.e. any other vectorial extension is a pushout of $\mathcal{V}$), which has $\omega_{\widehat{\mathcal{A}}}(S) = H^0(S, e^* \Omega^1_{\mathcal{A}/S})$. If $(a_{p^n})_{p^n} \in A_p(\mathbb{C}_p) = \mathcal{A}_{p^n}(\mathcal{O}_p)$, choose pre-images $b_n \in \mathcal{V}(\mathcal{O}_p)$ (which are well-defined up to $\omega_{\widehat{A}}(\mathcal{O}_p)$. Then $p^n b_n$ is a well-defined class in $\omega_{\mathcal{A}}(\mathcal{O}_p)/p^n \omega_{\widehat{\mathcal{A}}}(\mathcal{O}_p)$. We have a map

$$\theta_A : T_p A \to \omega_{\mathcal{A}}(\mathcal{O}_p)$$

sending $(a_{p^n}) \mapsto \varprojlim_n p^n b_n$. Dualizing and tensoring with $\mathbb{C}_p$ gives the Hodge-Tate map.

MOST ODD DEGREE HYPERELLIPTIC CURVES HAVE ONLY ONE RATIONAL POINT

BJORN POONEN

1. Introduction

Let me begin by recalling a theorem which you probably al know.

Theorem 1.1 (Faltings)**.** *Let C be a curve of genus $g > 1$ over $\mathbb{Q}$. Then $C(\mathbb{Q})$ is finite.*

Consider C a smooth, projective curve with model $y^2 = f(x)$, a monic separable polynomial of degree $2g + 1$. It is most convenient to view this as the *weighted projective space* $\operatorname{Proj} \mathbb{Q}[x, y, z]/(y^2 = z^{2g+2} f(x/z))$, where y has weight $g + 1$ and x, z have weight 1.

There is an obvious rational point on C, namely the point at ∞: $(1 : 0 : 0) \in C(\mathbb{Q})$.

Theorem 1.2 (Poonen-Stoll)**.** *For each $g \geq 3$,*

(1) the fraction of such C satisfying $C(\mathbb{Q}) = \{\infty\}$ is positive,
(2) this fraction tends to 1 as $g \to \infty$,
(3) in fact, it is $\geq 1 - (12g + 20)2^{-g}$.

Remark 1.3. The "fraction" is meant in an asymptotic sense, by choosing models with integer coefficients and studying the asymptotics of the fraction as the coefficients vary in a growing box. Conjecturally, the fraction should be 1 for all g.

The proof is by Chabauty's method at the prime 2. The proof uses results of Bhargava-Gross on sizes of Selmer groups of the Jacobians, and also on equidistribution of Selmer elements. It strengthens earlier work of Bhargava-Gross bounding the average number of rational points by 3 (this is actually a bound on the Selmer group).

2. Chabauty's method

Chabauty's idea was to consider the embedding $C \hookrightarrow J_C$ sending $x \mapsto [x] - [\infty]$ and study it p-adically, for some fixed prime p. Let $r = \operatorname{rank} J(\mathbb{Q})$. Envision the Jacobian as a box and C as a curve in it.

The nice thing about working p-adically is that $J(\mathbb{Q})$-points must lie in a small analytic subgroup - unlike $\mathbb{Q}$, where they can (and probably will) spiral around in a Zariski-dense way if they have irrational coefficients (the point is somehow that $\mathbb{Z}$ is bounded in $\mathbb{Z}_p$, but unbounded in $\mathbb{R}$.) You can show that $J(\mathbb{Q}_p)$ has a finite index open subgroup isomorphic to $\mathbb{Z}_p^g$. Therefore, $\overline{J(\mathbb{Q})}$ is of at most g. More generally, if $J(\mathbb{Q})$ is of rank r then $\overline{J(\mathbb{Q})}$ is of dimension at most r. Now, $\overline{C(\mathbb{Q}_p)}$ has dimension 1, and $C(\mathbb{Q}) \subset C(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}$. Chabauty's idea was that if $r < g$, then the intersection should be finite for these dimension reasons.

Theorem 2.1 (Chabauty)**.** *If $r < g$, then $C(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}$ is finite, so in particular $C(\mathbb{Q})$ is finite.*

Our method proceeds by studying the commutative diagram

$$\begin{array}{ccccc} C(\mathbb{Q}) & \hookrightarrow & & & C(\mathbb{Q}_p) \\ \downarrow & & & & \downarrow \\ J(\mathbb{Q}) & \hookrightarrow & \overline{J(\mathbb{Q})} & \hookrightarrow & J(\mathbb{Q}_p) \end{array}$$

To analyze this, you don't actually look at equations for J (which can't be found or used effectively in practice). Instead, you examine the logarithm map: there exists a homomorphism/local diffeomorphism

$$J(\mathbb{Q}_p) \xrightarrow{\log} \mathbb{Q}_p^g$$

sending

$$P \mapsto \left(\int_0^P \omega_1, \dots, \int_0^P \omega_g \right).$$

Choose the basis $\omega_1, \dots, \omega_g \in H^0(J_{\mathbb{Q}_p}, \Omega^1)$ so that the image of the logarithm is $\mathbb{Z}_p^g$. (This is technically non-trivial.)

$$\begin{array}{ccccccc} C(\mathbb{Q}) & \hookrightarrow & & & C(\mathbb{Q}_p) & & \\ \downarrow & & & & \downarrow & & \\ J(\mathbb{Q}) & \hookrightarrow & \overline{J(\mathbb{Q})} & \hookrightarrow & J(\mathbb{Q}_p) & \xrightarrow{\log} & \mathbb{Z}_p^g \end{array}$$

Now, to make this work one has to have some control of the "direction" of the Mordell-Weil group inside $J(\mathbb{Q}_p)$, to make sure that it doesn't intersect $C(\mathbb{Q}_p)$ too much. The idea is that you can get a little bit of information of the Mordell-Weil group by knowing about the p-Selmer group.

3. The Selmer Group

Let me remind you of the construction of the Selmer group. From the Kummer sequence

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

one gets an inclusion

$$J(\mathbb{Q})/pJ(\mathbb{Q}) \hookrightarrow H^1(\mathbb{Q}, J[p]).$$

The global image is hard to control. However, you can do this for each place, and take the product

$$\begin{array}{ccc} J(\mathbb{Q})/pJ(\mathbb{Q}) & \xrightarrow{\delta} & H^1(\mathbb{Q}, J[p]) \\ \downarrow & & \downarrow \text{res} \\ \prod_v J(\mathbb{Q}_v)/pJ(\mathbb{Q}_v) & \xrightarrow{\delta'} & \prod_v H^1(\mathbb{Q}_v, J[p]) \end{array}$$

Any class in the image of $J(\mathbb{Q})/pJ(\mathbb{Q}) \hookrightarrow H^1(\mathbb{Q}, J[p])$ certainly comes from δ', and the p-Selmer group measures this first-order condition.

Definition 3.1. We define the $\mathrm{Sel}_p J := \mathrm{res}^{-1}(\mathrm{Im}\ \delta')$.

So we have an obvious map $\mathrm{Sel}_p J \to J(\mathbb{Q}_v)/pJ(\mathbb{Q}_v)$ for each v.

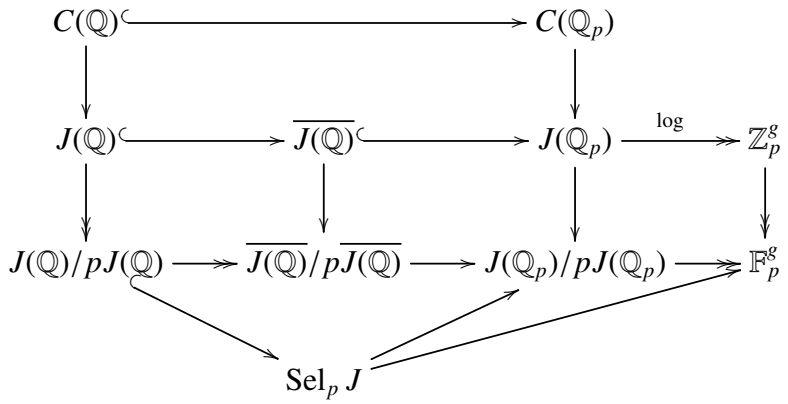
Theorem 3.2 (Bhargava-Gross)**.** *Consider a family $\mathcal{F}$ of hyperelliptic curves C defined by finitely many congruence conditions on the coefficients.*

(1) The average size of $\mathrm{Sel}_2 J = 3$*,*
(2) $J(\mathbb{Q}_v)/2J(\mathbb{Q}_v)$ is locally constant as the C varies v-adically, and if we shrink $\mathcal{F}$ to trivialize this bundle of finite groups so that we may pick a uniform isomorphism $J(\mathbb{Q}_v)/2J(\mathbb{Q}_v) \cong G$ for all $C \in \mathcal{F}$, then

$$\left\{\textit{image of } s \textit{ under } \mathrm{Sel}_2 J \to J(\mathbb{Q}_v)/2J(\mathbb{Q}_v) \cong G : \begin{smallmatrix} C \in \mathcal{F}\ \textit{height}(C) < X \\ s \in \mathrm{Sel}_2 J \setminus \{0\} \end{smallmatrix}\right\}$$

becomes equidistributed in G as $X \to \infty$.

Remark 3.3. Obviously one has to remove $s = 0$ from consideration, as 0 always maps to the identity of G. The map $\mathrm{Sel}_2 J \to J(\mathbb{Q}_v)/2J(\mathbb{Q}_v)$ isn't an injection, so you do also hit the identity of G.



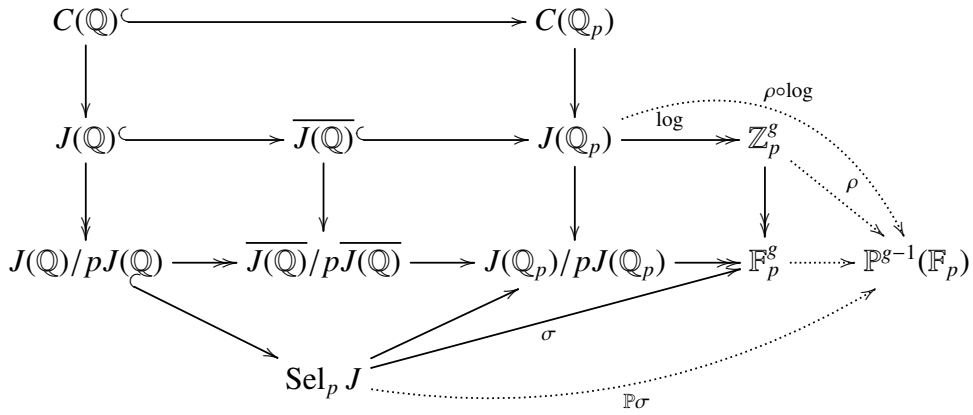
(Why is$J(\mathbb{Q})/pJ(\mathbb{Q}) \to \overline{J(\mathbb{Q})}/p\overline{J(\mathbb{Q})}$ surjective? For (not very deep) topological reasons: $p\overline{J(\mathbb{Q})}$ is open.)

We'd like to control the image of the Mordell-Weil group. That's too hard, but if we reduce modulo p, then we know whatever goes through the Mordell-Weil group goes through the Selmer group. That's like knowing "one p-adic digit" about the image of the Mordell-Weil group.

The surjectivity of $J(\mathbb{Q})/pJ(\mathbb{Q}) \to \overline{J(\mathbb{Q})}/p\overline{J(\mathbb{Q})}$ follows from topological facts.

Now we have to take $p = 2$ in order to use Bhargava-Gross, and $v = p$ to get the right Selmer group.

Let's add a little more into the diagram. We define $\rho\colon \mathbb{Z}_p^g \dashrightarrow \mathbb{P}^{g-1}(\mathbb{F}_p)$ to be the "scale and reduce" map if it's defined.



Lemma 3.4. *If*

- σ *is injective and*
- $\rho \circ \log C(\mathbb{Q}_2)$ *and* $\mathbb{P}\sigma(\mathrm{Sel}_2 J)$ *are disjoint,*

then $C(\mathbb{Q}_2) \cap \overline{J(\mathbb{Q})} \subset J(\mathbb{Q}_2)[odd]$.

The proof of this is basically by chasing through the diagram. You would like to force something to be just $\{\infty\}$, but the logarithm kills all torsion so you can't get that from the diagram.

Lemma 3.5. *For 100% of C, $C(\mathbb{Q}_2) \cap \overline{J(\mathbb{Q})} \subset J(\mathbb{Q}_2)[2]$.*

The Bhargava-Gross equidistribution theorem implies that σ is usually injective, and $\mathbb{P}\sigma(\mathrm{Sel}_2)$ is usually small.

I think of it in this way. You're sitting at the origin, and looking up into the sky - however, you have bad vision so you can only see with "one digit" of precision. You see two types of things. One is the curve winding around in the sky. The second is the Selmer group elements, which appear randomly like shooting stars. You hope that the shooting stars don't intersect the curve often.

This will be the case if both are pretty sparse. We just indicated why the Selmer elements are sparse, so what remains is to show that the image of the curve is *also* small.

4. The image of $C(\mathbb{Q}_2)$

We need to show that the average $\#\rho(\log C(\mathbb{Q}_2)) = o(2^g)$.

Proposition 4.1. *On average we have*

$$\#\rho(\log C(\mathbb{Q}_2)) \leq 6g + 9.$$

First suppose that C has good reduction at 2. Obviously this isn't okay for the proof, because not 100% of curves have good reduction at 2, but let's think about what happens in this case. Think of $C(\mathbb{Q}_2) \to C(\mathbb{F}_2)$ as a fibration with fibers being p-adic disks. We need to show:

(1) the number of disks is small, and
(2) the size of $\rho \circ \log$(each disk) is small.

The first is easy because $\#C(\mathbb{F}_2) \leq 5$, because C is a ramified double cover of $\mathbb{P}^1_{\mathbb{F}_2}$ ramified at ∞.

What about the second part? The restriction of log to a disk takes the form

$$\log|_{\text{disk}} = \left(\int w_1(t)\,dt, \ldots, \int w_g(t)\,dt\right), \quad w_i(t) \in \mathbb{Z}_2[[t]].$$

Up to 1-units, this is the same as $(f_1(t), \ldots, f_g(t))$ with $f_i \in \mathbb{Q}_2[t]$.

Lemma 4.2. *If ϕ is the map $\mathbb{P}^1_{\mathbb{Q}_p} \xrightarrow{f_1,\ldots,f_g} \mathbb{P}^{g-1}_{\mathbb{Q}_p}$ with $\deg f_i \leq n$ for each i, then*

$$\#\rho \circ \phi(\mathbb{P}^1(\mathbb{Q}_p)) \leq np + 1.$$

This is done by resolving the birational map of arithmetic surfaces over $\mathbb{Z}_p$, and counting the number of components in the special fiber.

There is a similar, but much worse, picture in the case of bad reduction. You have to work with a proper regular model $\mathcal{C}$ of C, which could now have hundreds of components. The final ingredient is that the average size of $\#\mathcal{C}^{\text{smooth}}(\mathbb{F}_2)$. If you just compute this over all possibilities, you can show that it is < 3. Remarkably, this is even smaller than in the good reduction case! The point is that the most common type of bad reduction is quite mild, involvng two points coming together, and this *reduces* the number of rational points.

♠♠♠ TONY: [is this really only over $\mathbb{Q}$?]

DIOPHANTINE STABILITY

KARL RUBIN

1. Introduction

1.1. **Notation.** Throughout this talk, K is a number field, V is a variety over K, and L is an extension field of K. We'll think of K and V as fixed, and L as varying.

Definition 1.1. We say that V is *diophantine stable* for the extension L/K if $V(L) = V(K)$, i.e. V acquires no new rational points over L.

We say that a finite, non-trivial extension L *belongs to* V if there exists $x \in V(\overline{K})$ such that $L = K(x)$, or equivalently if $V(L) \supsetneq \bigcup_{K \subset F \subsetneq L} V(F)$.

Let $\mathcal{L}(V)$ be the set of finite extensions L/K such that L belongs to V.

Example 1.2. $\mathcal{L}(\mathbb{P}^1) = \{\text{all finite non-trivial } L/K\}$, since $\mathbb{P}^1$ acquires new points over every non-trivial extension. The same is obviously true for any variety containing $\mathbb{P}^1$.

More generally, suppose X is smooth, projective, irreducible curve of genus 0. Let $\Sigma = \{v \colon X(K_v) = \emptyset\}$. Then by the Hasse principle,

$$\mathcal{L}(X) = \{L/K \colon 2 \mid [L_w : K_v] \text{ for all } v \in \Sigma, w \mid v \text{ of } L\}.$$

Note that Σ determines X up to isomorphism. ♠♠♠ TONY: [by "split primes philosophy"?]

Example 1.3. Let $E/(K = \mathbb{Q})$ be an elliptic curve. Then conjecturally $\mathcal{L}(E)$ contains "half" of the quadratic extensions of K.

Philosophy. The general belief is that apart from "special" families of examples, $\mathcal{L}(V)$ should be sparse. So we expect that most extensions are diophantine stable.

We denote $X \sim Y$ if X and Y are birational, and $\mathcal{L}(X) \sim \mathcal{L}(Y)$ if these two sets are "equal up to a finite number of fields." It's easy to show that if $X \sim Y$ (birational), then $\mathcal{L}(X) \sim \mathcal{L}(Y)$.

What about the converse? That turns out to be **false**. A counterexample was produced by Golstein and Klagsbrum.

Example 1.4. Suppose C, C' are curves of genus 1 such that $\mathrm{Jac}(C) \cong \mathrm{Jac}(C') =: E$. Then we can think of C, C' are elements of the Weil-Chatelet

group $H^1(K, E)$, i.e. as principal homogeneous spaces for E. If these generate the same subgroup, then $\mathcal{L}(C) = \mathcal{L}(C')$. ♠♠♠ TONY: [don't quite see why]

These are the only examples that we know of where the converse fails.

1.2. **Statement of Results.**

Theorem 1.5. *Suppose that X and Y are irreducible curves, with $g(X) = 0$. If $\mathcal{L}(X) \sim \mathcal{L}(Y)$ then $X \sim Y$.*

The point is that if Y doesn't have genus g, then $\mathcal{L}(Y)$ is not "big enough" to match $\mathcal{L}(X)$.

Theorem 1.6. *Suppose X is a smooth, irreducible, projective curve of genus $g(X) > 0$ and $\mathrm{End}_K(\mathrm{Jac}(X)) = \mathrm{End}_{\overline{K}}(\mathrm{Jac}(X))$. Then there exists a set S of rational primes with positive density such that for all $\ell \in S$ and all $n \geq 1$, there exist infinitely many cyclic extensions L/K of degree ℓ^n such that $X(L) = X(K)$.*

Contrast this with the genus 0 case. In the genus 0 case, once the curve has a point, then it has new points in every extension. In the positive genus case, we can always finitely many cyclic extensions for which there are no new rational points.

Our actual work is on abelian varieties, from which we deduce the preceding result.

Theorem 1.7. *Suppose A is a simple abelian variety and $\mathrm{End}_K(A) = \mathrm{End}_{\overline{K}}(A)$. Then there exists a set S of rational primes with positive density (in the set of all rational primes) such that for all $\ell \in S$ and all $n \geq 1$, there exist infinitely many cyclic extensions L/K of degree ℓ^n such that $A(L) = A(K)$.*

The deduction works by picking a map $X \to J(X)$ (not necessarily an embedding - to define this map we just need a rational divisor of sufficiently high degree) and then compose with projection to a simple quotient A of $J(X)$. There is some work here, since the map is not necessarily an embedding, but it is not too serious.

Remark 1.8.

(1) Sometimes, e.g. if E is a non-CM elliptic curve, we have
$$S = \{\ell : \ell \gg_E 0\}.$$
In particular, the density of S is 1.

(2) We can require L/K to be completely split at a given finite set of places. (For instance, if K is totally real then we can find infinitely many diophantine stable L which are totally real; if $K \subset \mathbb{Q}_p$ then we can find infintely many diophantine stable L which are in $\mathbb{Q}_p$.)

This follows from general theorems in mathematical logic.

1.3. **Applications.** By applying the theorem iteratively, you can find many infinite extensions furnishing no new rational points.

Corollary 1.9. *Given X as in Theorem 1.6, there are uncountably many L/K with $X(L) = X(K)$.*

Most of these have to be infinite, since there are only countably many finite extensions.

Example 1.10. If $X = X_0(p)$ and $p \geq 23$ is not $37, 43, 67, 163$ then the only rational points on $X_0(p)$ over $\mathbb{Q}$ are the cusps. This gives uncountably many fields $L/\mathbb{Q}$ such that no elliptic curve over L has an L-rational subgroup of order p.

Example 1.11. If we apply this to X an elliptic curve over $\mathbb{Q}$ with positive rank, it follows by work of Shlapentokh, building on work of Poonen, etc. that there exist uncountably many L with

(1) Hilbert's 10th problem has a negative answer over $\mathcal{O}_L$,
(2) The first-order theory of L is undecidable.

1.4. **Sharpness of the results.** How close is our theorem to being sharp? It turns out that the answer is: not close at all.

Definition 1.12. For an extension L/K, let $D_{L/K}$ be the relative discriminant. Set

$$N_\ell(X) = \#\{L/K \text{ cyclic of degree } \ell \mid V(L) = V(K), \mathrm{Nm}(D_{L/K}) < X\}.$$

and

$$N_{E,\ell}(X) = \#\{L/K \text{ cyclic of degree } \ell \mid V(L) = V(K), \mathrm{Nm}(D_{L/K}) < X.$$

Theorem 1.13 (Wright)**.** *We have*

$$N_\ell(X) \sim X^{1/(\ell-1)}(\log X)^{\textit{explicit power}}.$$

Example 1.14. If $\ell = 2$ and $K = \mathbb{Q}$, then (as mentioned earlier) we expect $N_{E,2}(X) \sim \frac{1}{2}N_2(X)$. For general K, we expect $N_{E,2}(X) \sim cN_2(X)$ for some $0 \leq c \leq 1$.

For general ℓ, we expect $N_{E,\ell}(X) \sim N_\ell(X)$ certainly for $\ell \gg 0$, and one might even expect this for $\ell \geq 3$. (There are some precise conjectures that predict that when $K = \mathbb{Q}$, this should be true for $\ell \geq 3$, and that the difference is *finite* if $\ell \geq 7$.)

Theorem 1.15. *If L is large enough so that $G_K \to \mathrm{Aut}(E[\ell]) \cong \mathrm{GL}_2(\mathbb{F}_\ell)$ is surjective, then*

$$N_{E,\ell}(X) \gg N_\ell(X)/(\log X)^{\ell/(\ell^2-1)}.$$

Remark 1.16. By work of Serre, we know that the hypothesis holds for all sufficiently large ℓ.

2. Ideas of Proof

Let A be a simple abelian variety. We want to find many L/K of degree ℓ such that the rank doesn't grow - the torsion is not a problem to control. We consider the Weil restriction of A from L to K, which fit into a short exact sequence

$$0 \to \underbrace{A_{L/K}}_{\text{def}} \to \operatorname{Res}_K^L A \to A \to 0.$$

♠♠♠ TONY: [what is this, actually?] Taking K-points gives the exact sequence

$$0 \to A_{L/K}(K) \to A(L) \to A(K)$$

so if we want to know if rank $A(L)$ = rank $A(K)$, then it suffices to study if $A_{L/K}(K)$ has rank 0.

We have an inclusion $\mathbb{Z}[\mathrm{Gal}(L/K)] \hookrightarrow \mathrm{End}(\operatorname{Res}_K^L(A))$. That induces $\mathbb{Z}[\mu_\ell] \hookrightarrow \mathrm{End}(A_{L/K})$. If $\lambda = \zeta_\ell - 1 \in \mathbb{Z}[\mu_\ell]$ then we have $A_{L/K}[\lambda] \cong A[\ell]$ ♠♠♠ TONY: [why?]. Therefore,

$$\mathrm{Sel}_\lambda(A_{L/K}) \subset H^1(K, A_{L/K}[\lambda]) \cong H^1(K, A[\ell]).$$

Now, the Selmer group is cut out by local conditions depending on L. By controlling the local behavior of L/K, we can control $\mathrm{Sel}_\lambda(A_{L/K})$ and hence choose L/K so that $\mathrm{Sel}_\lambda(A_{L/K}) = 0$.

Let me just finish by saying the new input needed for this. The idea is to carefully choose a set of primes at which the image of Frobenius acts in a certain special way. For this, we need the image of Galois to be pretty large at those primes.

Theorem 2.1 (Larsen)**.** *Let $\mathcal{O}$ be the ring of integers of the center of* $\mathrm{End}(A)\otimes\mathbb{Q}$*. There exists a set S of rational primes of positive density such that for all $\ell \in S$ and $\lambda \in \mathcal{O}$ above ℓ,*

(1) there exists $\gamma \in G_{K(\mu_\ell)}$ such that $A[\lambda]/(\gamma - 1)A[\lambda]$ is a non-zero simple $\mathrm{End}(A)/\lambda$*-modules and*

(2) there exists $\gamma \in G_{K(\mu_\ell)}$ such that $A[\lambda]/(\gamma - 1)A[\lambda] = 0$.

RANKIN-SELBERG EULER SYSTEMS IN COLEMAN FAMILIES

SARAH ZERBES

1. Euler systems

Let V be a p-adic representation of $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, unramified outside a finite set of primes Σ.

Definition 1.1 (Rubin). An *Euler System* for V is a collection $\{z_m\}_{m\geq 1}$, with $z_m \in H^1(\mathbb{Q}(\mu_m), V^*(1))$ such that

(1) the z_m take values in a lattice independent of m,
(2) The Euler system norm relations:

$$\mathrm{cores}_m^{m\ell}\, z_{m\ell} = \begin{cases} z_m & l \mid m \text{ or } \ell \in \Sigma, \\ P_\ell(\sigma_\ell^{-1}) z_m & \text{otherwise. } = \end{cases}$$

where $P_\ell(X) = \det(1 - X\sigma_\ell^{-1}|_V)$.

Theorem 1.2 (Rubin)**.** *If $z_1 \neq 0$, then the strict Selmer group* $\mathrm{Sel}(V/\mathbb{Q})$ *is finite.*

If one knows some stronger hypothesis, then one gets that the Bloch-Kato Selmer group is finite.

Example 1.3. There are two classical examples of Euler systems.

(1) Cyclotomic units: $V = \mathbb{Q}_p$ is the trivial representation.
(2) Kato's Euler system: $V = V_p(E)$ for E an elliptic curve, or $V = M(f)$, where f is a modular form of weight ≥ 2.

2. The Euler System of Beilinson-Flach classes

Let f, g be modular forms, more precisely eigenforms of level N such that $p \mid N$, of weights $k+2, k'+2 \geq 2$.

Theorem 2.1 (Lei-L-Z, Kings-L-Z)**.** *Let $0 \leq j \leq \min(k, k')$. Then there exist (Beilinson-Flach) classes $(BF_m^{(f,g,j)})_{m\geq 1}$, with $BF_m^{(f,g,j)} \in H^1(\mathbb{Q}(\mu_m), M(f)^* \otimes M(g)^*(-j))$, satisfying "Euler System style" norm relations, which are related to $L_p(f, g, 1+j)$.*

2.1. **Idea of construction.** Start with a Siegel unit

$$g_{1/m^2N} \in \mathcal{O}(Y_1(m^2N))^\times \xrightarrow{Kummer} H^1_{\text{ét}}(Y_1(m^2N), \mathbb{Z}_p(1)).$$

Then construct an embedding $\iota_{m,N}\colon Y_1(m^2N) \to Y_1(N^2) \times \mu_m$ sending $z \mapsto (z, z + 1/m)$. Now consider the pushforward

$$H^1_{\text{ét}}(Y_1(m^2N), \mathbb{Z}_p(1)) \xrightarrow{(\iota_{m,N})_*} H^3_{\text{ét}}(Y_1(N)^2 \times \mu_m, \mathbb{Z}_p(2))$$

♠♠♠ TONY: [what is this?] This maps by the Hoschild-Serre spectral sequence to $H^1(\mathbb{Q}(\mu_m), H^2_{\text{ét}}(\overline{Y_1(N)}, \mathbb{Z}_p(2))$, and then to $H^1(\mathbb{Q}(\mu_m), M(f)^* \otimes M(g)^*(-j))$. The image is the class $BF_m^{(f,g,j)}$ that we wanted.

This only construct classes in a very limited range of j. To get higher weights, one uses interpolation.

3. Interpolation in cyclotomic families

Let $\Gamma = \text{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \cong \mathbb{Z}_p^\times$. Write $\Lambda(\Gamma)$ for the $\mathbb{Q}_p$-valued measures on Γ. (This is the Iwasawa algebra.)

We would like to have classes $(BF^{(f,g,\text{cyc})})_{m\geq 1, p\nmid m}$ (here cyc is the cyclotomic character) which interpolate the geometric classes that we have constructed. That is, we would like

$$(BF)_m^{(f,g,\text{cyc})} \in H^1(\mathbb{Q}(\mu_m), M(f)^* \otimes M(g)^* \otimes \Lambda(\Gamma))$$

such that integrating against the measures recovers the "geometric" classes that we already constructed:

$$(BF)_{mp^r}^{(f,g,j)} = \int_{1+p^r\mathbb{Z}_p} \chi^j \alpha (BF)_m^{(f,g,\text{cyc})} \text{ for all } r \geq 0, 0 \leq j \leq \min k, k'. \quad (1)$$

What we would need is that

$$\text{cores}_{mp^r}^{mp^{r+1}} BF_{mp^r}^{(f,g,j)} = BF_{mp^r}^{(f,g,j)}.$$

But our classes didn't *quite* satisfy the Euler system norm relations. They satisfied

$$\text{cores}_{mp^r}^{mp^{r+1}} (BF)_{mp^{r+1}}^{(f,g,j)} = \alpha_f \alpha_g \cdot BF_{mp^r}^{(f,g,j)}$$

where α_f, α_g are U_p-eigenvalues of f, g. If $\lambda = V_p(\alpha_f \alpha_g) > 0$, then renormalizing gives denominators.

Definition 3.1. We denote by $D_\lambda(\Gamma)$ the $\mathbb{Q}_p$-valued distributions on Γ of weight λ.

Theorem 3.2 (KLZ, LZ)**.** *Assuming that $\lambda < 1 + \min(k, k')$. Then there exist $(BF_m^{(f,g,cyc)}$ such that $BF_m^{(f,g,cyc)} \in H^1(\mathbb{Q}(\mu_m), M(f)^* \otimes M(g)^* \otimes D_\lambda(\Gamma))$ satisfying* (1)*.*

Ths gives an Euler system for j in the critical range. However, this is a little unsatisfying for a couple reasons: we had to assume a small slope condition, and it only works for modular forms of weight at least 2, whereas we would really like the result for modular forms of weight 1. The solution to these problems is to consider variation in Coleman families.

4. Variation in Coleman families

Let W be a weight space and $U \subset W$ an open disc such that $\mathbb{Z}_{\geq 0} \cap U$ is dense in U. Let Λ_U be the ring of functions on U.

Definition 4.1. A *Coleman family* $\mathcal{F}$ over U (of tame level N) is a power series

$$f = \sum_{n \geq 1} a_n(\mathcal{F}) q^n \in \Lambda_U[[q]]$$

such that

(1) $a_1(\mathcal{F}) = 1$,
(2) the specialization $\mathcal{F}_k$ for almost all $k \in \mathbb{Z}_{\geq 0} \cap U$ is a classical modular form of weight $k+2$ and level $\Gamma_1(N) \cap \Gamma_0(p)$.

Theorem 4.2 (Coleman-Mazur, Buzzard)**.** *Let f be an eigenform of weight at least 2 and level N suh that $p \mid N$. Assume that f is of finite slope and not critical slope. Then there exists a Coleman family through f.*

4.1. **Λ_U-adic representation attached to $\mathcal{F}$.** Let $Y_1(N(p))$ be the modular curve attached to $\Gamma_1(N) \cap \Gamma_0(p)$. Let $\mathcal{H}$ be the relative homology sheaf of the universal elliptic curve above $Y_1(N(p))$. Audreatta-Iovita-Stevens construct a sheaf of distributions $\mathcal{D}_U(\mathcal{H})$ on $Y_1(N(p))$ (a sheaf of Λ_U-modules). This is closely related to overconvergent modular symbols.

Definition 4.3. We define the *étale overconvergent cohomology*

$$M_U = H^1_{\text{ét}}(\overline{Y_1(N(p))}, \mathcal{D}_U(\mathcal{H})).$$

This has an action of $G_{\mathbb{Q}}$ and the Hecke algebra.

Definition 4.4. Let $\mathcal{F}$ be a Coleman family of tame level N. Define

$$M_U(\mathcal{F}) = M_U[\gamma_n = a_n(\mathcal{F}) \text{ for all } n]$$

i.e. the part with Hecke eigenvalues $a_n(\mathcal{F})$.

Theorem 4.5 (Ash-Stevens, Bellendre)**.** *$M_U(\mathcal{F})$ is a direct summand of M_U, and recovers $M(\mathcal{F}_k)^*$ for almost all $k \in \mathbb{Z}_{\geq 0} \cap U$.*

Theorem 4.6 (LZ)**.** *Let $\mathcal{F}, \mathcal{G}$ be Coleman families of tame level N over M, M' of slopes $\lambda_{\mathcal{F}}, \lambda_{\mathcal{G}}$. Then there exists $(BF_m^{(\mathcal{F},\mathcal{G},cyc)})_{m \geq 1, p \nmid m}$, with $BF_m^{(\mathcal{F},\mathcal{G},cyc)} \in H^1(\mathbb{Q}(\mu_m), M(\mathcal{F}) \widehat{\otimes} M(\mathcal{G}) \widehat{\otimes} D_{\lambda_{\mathcal{F}} + \lambda_{\mathcal{G}}}(\Gamma))$ interpolating geometric classes.*

Relation to L-values. It turns out that these classes are related to special values of Urban's p-adic L-function. We call this the "explicit reciprocity law." Let $k \in \mathbb{Z}_{\geq 0} \cap U, k' \in \mathbb{Z}_{\geq 0} \cap U'$ and $j \gg 0$. Then

$$\exp^*(BF_1^{(\mathcal{F}_k, \mathcal{G}_k, j)}) = (*)L_p(\mathcal{F}_k, \mathcal{G}_k, 1+j)$$

This is deduced by using knowledge of the relation between the *geometric* classes and the L-function, and then analytic continuation to get the general case.

4.2. **Idea of proof of construction.** The first step is to construct a 2-variable family $(BF_m^{(\mathcal{F}, \mathcal{G}, j)})$ for fixed j. The second step is to show interpolation in the cyclotomic direction.

To elaborate on the first step: we need to introduce "étale nearly overconvergent cohomology," whose relation to étale overconvergent cohomology is analogous to that between Urban's theory of "nearly overconvergent modular forms" and overconvergent modular forms.

Remark 4.7.

- If you special the 2-parameter family, you can get a 1-parameter (cyclotomic) family for any pair of forms which are not of critical slope. This gets rid of the no small slope assumption.
- If f, g have level prime to p, then we get an Euler system for each pair of non-critical slope p-stabilizations.
- This is a generalization of earlier results about variation in Hida families.

5. Applications

Theorem 5.1 (K-L-Z,L-Z)**.** *Let f, g be modular forms such that $wt(f) > wt(g) \geq 1$ such that $L(f, g, 1+j)$ is critical. If $L(f, g, 1+j) \neq 0$ and some technical hypotheses are satisfied, then the Bloch-Kato Selmer group of $M(f) \otimes M(g)(1+j)$ is finite.*

The sketch of proof: put f and g into Hida families. Specialize, and use Rubin's Euler system machine.

We emphasize that f, g may be non-ordinary.

5.1. **Special case.** Let's assume that f corresponds to an elliptic curve over $\mathbb{Q}$ and g has weight 1, hence corresponds to a 2-dimensional Artin representation ρ, trivialized by K.

Definition 5.2. We say that g is *p-regular* if $\rho(\mathrm{Frob}_p)$ is not a scalar.

Theorem 5.3 (KLZ, LZ)**.** *If $L(E, \rho, 1) \neq 0$ then for all but fintely many p such that g is p-regular, $\mathrm{Sel}_{p^\infty}(E/K)[p]$ is finite.*

In particular, this implies finiteness of the p-primary part of $Ш(E/K)[p]$. This was first proved by Bertolini, Darmon, and Rogers.

THE WITT VECTOR AFFINE GRASSMANNIAN

PETER SCHOLZE

1. The classical case

Let k be a field. We want to parametrize $k[[t]]$-lattices in $k((t))^n$, for some fixed $n \geq 1$. We want to do this not just for points but also families. So consider the functor

$$\mathrm{Gr}^{\mathrm{aff}} : k - \textbf{algebras} \to \textbf{Sets}$$

sending R to the set of finite projective $R[[t]]$-modules M, equipped with an isomorphism $M[1/t] \cong R((t))^n$. This is the functor of points of a scheme, the classical affine Grassmannian.

There are several reasons to be interested in this. Historically, it comes up in studying the moduli stack of G-bundles on a curve. It also comes up in the geometric Langlands program, again in the context of studying the moduli stack of $G = \mathrm{GL}_n$-bundles on a curve.

However, today we're going to consider this as an object of interest for its own sake.

The affine Grassmannian is huge (not finite type). To get something of finite type, one needs to cut it down by finite bounds. Let $a \leq b$ for $a, b \in \mathbb{Z}$. Let $\mathrm{Gr}^{\mathrm{aff},[a,b]} \subset \mathrm{Gr}^{\mathrm{aff}}$ parametrize lattices between $t^a k[[t]]^n$ and $t^b k[[t]]^n$. Then

$$\mathrm{Gr}^{\mathrm{aff}} = \varinjlim_{a,b} \mathrm{Gr}^{\mathrm{aff},[a,b]}$$

where all the transition maps are closed embeddings.

Theorem 1.1 (Beauville-Laszlo)**.** *All the* $\mathrm{Gr}^{\mathrm{aff},[a,b]}$ *are projective schemes over* k*.*

Example 1.2. $\mathrm{Gr}^{\mathrm{aff},[0,1]} = \{\text{lattices between } k[[t]]^n \text{ and } tk[[t]]^n\}$. This is just the same as sub k-vector spaces of $k^n = k[[t]]^n/tk[[t]]^n$, which is $\coprod_{d=0}^n \mathrm{Gr}(d, n)$.

2. The Witt vector case

Let k be a perfect field of characteristic p. Let $W(k)$ be the ring of Witt vectors. We want to parametrize "$W(k)$-lattices in $W(k)[1/p]^n$."

Why might one be interested in such structures? One source of examples comes from Dieudonné theory. If M is a Diudonné module over k, i.e. a finite free $W(k)$-module M equipped with $\varphi_M : (\varphi^* M)[1/p] \cong M[1/p]$, then

M and $\varphi(M)$ are two lattices in the same vector space $M[1/p]$ (here φ is the lift of Frobenius). If you have a family of such and you trivialize one, then you can view the other as varying in a fixed vector space, which gives rise to period maps. Thus one obtains period maps from "moduli spaces of p-adic Hodge structures" (e.g. from Rapoport-Zink spaces) to spaces of such lattices.

The problem is that $W(R)$ for a general k-algebra R are not well-behaved. For example, they may have p-torsion (if R is not reduced), and $W(R)/p \to R$ is not an isomorphism in general (if R is not perfect) - so $W(R)$ can't be viewed as a "flat" lift of R.

Definition 2.1. Recall that R is *perfect* if $\Phi\colon R \to R$ sending $x \mapsto x^p$ is an isomorphism. Any R has a (functorial) perfection: $\varinjlim_{\Phi} R =: R_{\mathrm{perf}}$.

Example 2.2. The perfection of $R = \mathbb{F}_p[t]$ is $\mathbb{F}_p[t^{1/p^\infty}]$.

The perfection doesn't change the étale site, so "R_{perf} knows étale cohomology."

Fact. If R is perfect, then

$$W(R) = \left\{ \sum_{n=0}^{\infty} [a_n] p^n \mid a_n \in R \right\}$$

and evidently $W(R)/p \cong R$.

Because of the problems with non-perfect rings, it is useful to focus on representing *only* perfect things.

Definition 2.3. Define the functor

$$\mathrm{Gr}^{W\,\mathrm{aff}}\colon \{\text{perfect } k\text{-algebras}\} \to \mathbf{Set}$$

sending R to the set of finite projective $W(R)$-modules M equipped with an isomorphism $M[1/p] \cong W(R)[1/p]^n$, up to equivalence.

Theorem 2.4 (Bhatt-Scholze)**.** $\mathrm{Gr}^{W\,\mathrm{aff},[a,b]}$ *is represented by the perfection of a projective scheme over* k.

Previously, X. Zhu had proved that it is a perfection of a proper algebraic space. However, the method of proof is completely different.

Once you know this, you can talk about the étale cohomology of this space. Zhu proved a geometric Satake equivalence in this setting.

The strategy is to construct a natural line bundle $\mathcal{L}$ on $\mathrm{Gr}^{W\,\mathrm{aff}}$ and prove that it is ample. We can't construct enough sections directly; the method is indirect.

Example 2.5. We have $\mathrm{Gr}^{W\,\mathrm{aff},[0,1]} = \coprod_d \mathrm{Gr}(d,n)_{\mathrm{perf}}$.

Classically, on $\mathrm{Gr}^{\mathrm{aff},[a,b]}$ we have the line bundle $\mathcal{L} := \det_R(t^a R[[t]]^n/M)$, which makes sense because $t^a R[[t]]^n/M$ is a finite projective R-module. This gives an embedding

$$\mathrm{Gr}^{\mathrm{aff},[a,b]} \hookrightarrow \coprod_d \mathrm{Gr}(d, t^a k[[t]]^n/t^b k[[t]]^n).$$

What happens if you try to do this in mixed characteristic? Well, you run into the problem that $p^a W(R)^n/M$ is no longer an R-module (e.g. consider $W(R)/p^3$).

The idea is to *filter* $p^a W(R)^n/M$ such that all the gradeds Q_i are finite projective R-modules. For example, if R is a field then one can filter by powers of p. Then one would like to "define"

$$\mathcal{L} := \det{}_R(p^a W(R)^n/M) = \bigotimes_i \det{}_R(Q_i).$$

The intuition is that if you have a short exact sequence of R-modules, then the determinant of the middle module is the tensor product of the outer determinants.

There are some problems:

(1) Such a filtration may not exist; it exists only after non-flat covers of Spec R ♠♠♠ TONY: [mmm?]. So we need a strong *non-flat* descent.
(2) Even if such a filtration exists, it may not be unique. There are two solutions to this problem; the more conceptual one is to use K-theory (which we shall explain).

Example 2.6. What's an example where the naïve filtration (by powers of p) doesn't work?

You can have a family of modules which looks like a family of $W(R)/p^2$ degenerating $(W(R)/p)^{\oplus 2}$ (think a Schubert cell limiting to something in its closure). Modulo p, the family has generically rank 1, but the special fiber has rank 2, so this can't be finite projective.

3. Non-flat descent

We want to consider a bigger topology (than fpqc) where all the necessary descent works.

Definition 3.1. A map $f\colon X \to Y$ of (qcqs) schemes is a v-cover (v stands for valuation) (=universally subtrusive) if for all maps Spec $V \to Y$, with V a valuation ring, there exists an extension of valuation rings $V \hookrightarrow W$ and a

diagram

$$\begin{array}{ccc} \operatorname{Spec} W & \overset{\exists}{\dashrightarrow} & X \\ \downarrow & & \downarrow \\ \operatorname{Spec} V & \longrightarrow & Y \end{array}$$

Said differently, to any scheme X there is a set of (equivalence classes of) valuations on X, denoted $|X^{\mathrm{ad}}|$, and we are asking that $|X^{\mathrm{ad}}| \twoheadrightarrow |Y^{\mathrm{ad}}|$.

Example 3.2. (1) If f is faithfully flat, then f is a v-cover. First lift the most special point, then use the going up theorem to extend.

(2) If f is proper surjective, then f is a v-cover. First lift the most generic point, then use the valuative criterion to extend. (e.g. $Y^{\mathrm{red}} \hookrightarrow Y$ is a v-cover.)

(3) a finitely presented v-cover is an h-cover in the sense of Voevodsky. The h covers apply to most geometric situations, but it turns out that you can do it more generally and this is sometimes useful.

Example 3.3. If $Y = \mathbb{A}^2_k$ and $X = \mathrm{Bl}_{(0,0)} \mathbb{A}^2 \setminus \{x\}$ for x in the exceptional fiber, but there's a valuation on Y corresponding to the "direction of x" which doesn't extend to the blowup. ♠♠♠ TONY: [eh?]

Recall that a Grothendieck topology is said to be *subcanonical* if all repesentable presheaves are schemes.

Theorem 3.4 (Gabber, Bhatt-Scholze)**.** *The v-topology on qcqs perfect schemes is subcanonical and*

$$H^i_v(\operatorname{Spec} A, \mathcal{O}) = \begin{cases} A & i = 0, \\ 0 & i > 0 \end{cases}$$

for perfect A, and vector bundles form a stack for the v-topology.

Remark 3.5. We've restricted to the category of perfect schemes. This can't work for the category of *all* schemes because the fact that the inclusion of reduction is v-cover would imply that a scheme and its reduced structure both represent the same functor.

Remark 3.6. If $B \leftarrow A \rightarrow C$ is a diagram of perfect rings, then $\mathrm{Tor}^A_i(B, C) = 0$ for $i > 0$. So coherent base change always holds for perfect schemes.

Remark 3.7. This is a more elementary analogue of the "faithful topology" on perfectoid spaces, developed in Peter's Berkeley course.

We want to define

$$\mathcal{L} := \text{“}\det{}_R\text{”}(p^n W(R)^n / M) = \text{“}\det{}_R\text{”}(M \rightarrow p^a W(R)^n)$$

where $M \rightarrow p^a W(R)^n$ is a perfect complex of $W(R)$-modules supported on $\operatorname{Spec} R$.

Definition 3.8. We define the K-theory spectra $K(R)$ to be the group built from perfect complexes of R-modules, and modding out by the usual relations of short exact sequences.

We define the spectra $K(W(R)$ on $R)$ to be the same construction for complexes of perfect $W(R)$-modules supported on Spec R.

Then $M \to p^a W(R)^n$ can be interpreted as a point of $K(W(R)$ on $R)$.

Corollary 3.9. *The functor* $\det_R \colon K(R) \to \mathrm{Pic}(R)$ *extends uniquely to a functor* $\widetilde{\det}_R \colon K(W(R)$ *on* $R) \to \mathrm{Pic}(R)$.

There's always a $K(R) \to K(W(R)$ on $R)$ because any perfect complex of R-modules can be regarded as a perfect complex of $W(R)$-modules.

Proof. If R is a perfection of a *regular* ring, then a theorem of Quillen says that $K(R) \xrightarrow{\sim} K(W(R)$ on $R)$. Concretely this means that when you have a complex of perfect $W(R)$ modules on R, then there exists a filtration whose gradeds are R-modules.

In general, you use this plus de Jong's alterations and v-descent. □

Remark 3.10. Since everything here commutes with filtered colimits, we can immediately reduce to the finitely generated case.

4. The central extension of LG

Let $G = \mathrm{SL}_n$. The *algebraic loop group* $LG(R) = G(W(R)[1/p])$, for R perfect. Then LG acts on $\mathrm{Gr}^{W\,\mathrm{aff}}$ by translating the lattice. However, $\mathcal{L}$ is not equivariant for this action.

Proposition 4.1 (Bhatt-Scholze)**.** *There is a simple extension (as in the classical case)*

$$1 \to \mathbb{G}_m \to \widetilde{LG} \to LG \to 1$$

such that $\mathcal{L}$ *is* $\widetilde{LG}$*-equivariant.*

Definition 4.2. $\widetilde{LG}$ is defined by the functor of points

$$R \mapsto \{g \in LG(R) + \text{ isom. } \widetilde{\det}_R(W(R)^n \xrightarrow{g} p^{-N}W(R)^n) \cong R, N \gg 0\}.$$

Question. What is this extension for $R = \mathbb{F}_p$?

$$1 \to \mathbb{F}_p^\times \to \widetilde{LG}(\mathbb{F}_p) \to \mathrm{SL}_n(\mathbb{Q}_p) \to 1. \tag{1}$$

This turns out to be related to a construction of Steinberg. For any field L $(= \mathbb{Q}_p)$, there is an extension

$$1 \to K_2(L) \to \widetilde{\mathrm{SL}_n(L)} \to \mathrm{SL}_n(L) \to 0. \tag{2}$$

One way to understand this is the following. There is a map of classifying spaces $B\,\mathrm{SL}_n(L) \to B\,\mathrm{GL}_\infty(L)$, which in turn maps to $B\,\mathrm{GL}_\infty(L)^+ \cong K(L)$.

We have $\pi_0(B\,\mathrm{SL}_n(L)) = *$ and $\pi_1(B\,\mathrm{SL}_n) = \mathrm{SL}_n(L)$, and $\pi_0(K(L)) = 2$ and $\pi_1(K(L)) = L^*$. It turns out that the composition $K_2(L) \to \widetilde{\mathrm{SL}_n(L)} \to \mathrm{SL}_n(L)$ induces the determinant on π_1. So one gets

$$BS\,L_n(L) \to \tau_{\geq 2}K(L) \to \tau_{\geq 2}^{\leq 2}K(L) = B^2(K_2(L),$$

and unlooping this is exactly equivalent to giving such an extension. ♠♠♠ TONY: [learn more homotopy theory]

So we have two natural extension of $\mathrm{SL}_n(\mathbb{Q}_p)$, by $\mathbb{F}_p^\times$ and $K_2(\mathbb{Q}_p)$.

Proposition 4.3. *The extension* (1) *is the pushout of the extension* (2) *along the Hilbert symbol:* $K_2(\mathbb{Q}_p) \to K_1(\mathbb{F}_p) = \mathbb{F}_p^\times$.

THE P-ADIC GEOMETRY OF MODULAR CURVES AND OTHER MODULI SPACES

JARED WEINSTEIN

1. Semistable reduction

1.1. **Semistable models.** Let $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ be a congruence subgroup.

Motivation Question. Describe the semistable reduction of $X(\Gamma)_{\mathbb{C}_p}$.

Let's recall the meaning of "semistable reduction." Given a curve $X/\mathbb{C}_p$, there exists a semistable model $\mathcal{X}/\mathcal{O}_{\mathbb{C}_p}$, i.e. a model whose special fiber whose only singularities are nodes. The special fiber $\mathcal{X}_s$ is well-defined up to $\mathbb{P}^1$ (obtained as the exceptional fibers of blowing up).

Remark 1.1. If X started out over $\mathbb{Q}_p$, then you might need to pass to an extension field to see the semistable reduction. This is the original problem that Coleman was considering when I got involved.

Let p be odd, $p \nmid N \geq 5$. We confuse $X_0(p^n)$ with $X(\Gamma_0(p^n) \cap \Gamma_1(N))$. (This N is an auxiliary "tame inertia" level.)

Example 1.2.

- $X(1)$ has good reduction.
- $X_0(p)$ has semistable reduction over $\mathbb{Q}_p$. The special fiber has two copies of $X_0(1)$ (which is $X_0(N)$), meeting over the supersingular locus.

  ♠♠♠ TONY: [Deligne-Rapoport picture of $X_0(p)$ as "DNA strand".]
- $X_0(p^2)$ was done by Edixhoven in '90.
- $X(p)$ was done by Bouw-Wewers in '04.
- $X_0(p^3)$ was done by Coleman-McMurdy in '10.
- $X_0(p^4)$ was done by Tsushina in '11.
- $X_1(p^3)$ was done by Imai-Tshushima in '11.

The latter three use rigid geometry. To give a semistable model of the curve is equivalent to give a covering of the associated rigid analytic space.

1.2. **Semistable coverings.**

Definition 1.3. A *semistable covering* of a rigid-analytic curve X is a covering by wide open spaces U_v such that

(1) for all v, w distinct, $U_v \cap U_w$ is a finite disjoint union of annuli,
(2) for all v, w, x distinct, we have $U_v \cap U_w \cap U_x = \emptyset$,
(3) $Z_v := U_v \setminus \bigcup_{w \neq v} U_w$ is affinoid with $\overline{Z}_i$ irreducible smooth.

We won't define the meaning of "wide open." See Coleman's original paper, or the paper of Coleman-McMurdy.

♠♠♠ TONY: [picture - widen opens are open 2-manifolds]

The affinoid Z_v is necessary to talk about good reduction. (You can't "reduce" an arbitrary rigid analytic space.) Let $Z = \operatorname{Spm} A$ and $\overline{Z} = \operatorname{Spec} A^+/\mathfrak{m}_{\mathbb{C}_p} A^+$.

Theorem 1.4 (Coleman '93)**.** *If $X/\mathbb{C}_p$ is a smooth proper algebraic curve, then*

$$\{\textit{semistable models of } X\} \leftrightarrow \{\textit{semistable covering of } X\}.$$

How does this work? If you have a semistable model $\mathcal{X}$, then its special fiber is a union of components Y_v. On the other side, there is a reduction map $X^{\mathrm{an}} \to \mathcal{X}_s$. Then $U_v = \mathrm{red}^{-1}(Y_v)$, Z_v is the pre-image of a smooth point, and the annuli are the pre-images of nodes.

2. Modular curves

Let's think about applying this to the semistable reduction of modular curves.

We can reduce the main question to the following. Let $E_0/\overline{\mathbb{F}_p}$ be a supsersingular elliptic curve. Let M_m be the region in $(X(p^m)^{\mathrm{an}}_{\mathbb{C}_p})$ where $\overline{E} = E_0$. This is like a residue neighborhood of E_0. Then by Coleman's Theorem, it suffices to find a semistable covering of M_m.

Why does it suffice to treat the supersingular case? We understand the ordinary regions much better. Katz-Mazur have a description of the semistable model in terms of Igusa curves, which intersect horribly over the supsersingular locus.

This is what Coleman and McMurdy did for $X_0(p^3)$. There actual work was quite technical, so I'll just try to distill the important principles.

2.1. Observations of Coleman-McMurdy.

- The importance of the elliptic curves $E \in X_0(p^3)$ such that their formal group $\widehat{E}$ has extra endomorphisms: $\widehat{E} \supsetneq \mathbb{Z}_p$. They called such E "fake CM." Elliptic curves with CM have this property, but some without CM do too. The wide opens are *centered around* points with fake CM.
- The importance of the Gross-Hopkins map.

2.2. **Challenges.**

- It is difficult to find coordinates on $X(p^m)$.
- The question is related to the representations of $\mathrm{GL}_2(\mathbb{Q}_p)$. After all, modular curves are where modular forms live, and modular forms are automorphic forms for $\mathrm{GL}_2(\mathbb{Q}_p)$. But $X(p^n)$ only has a $\mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$ action - in particular the full symmetry group isn't present - plus Hecke operators.

The solution to both of these challenges is to work at "infinite level." That means "set $m = \infty$." Since we have a tower of modular curves, we might seek to find a *tower* of semistable reductions.

3. Infinite level

Notation: M_m is the rigid space, and $\mathcal{M}_m$ is the corresponding formal scheme. Can we make a tower

$$\ldots \to \mathcal{M}_2 \to \mathcal{M}_1 \to \mathcal{M}_0$$

of semistable models for

$$\ldots \to M_2 \to M_1 \to M_0?$$

Furthermore, we demand that $\mathcal{M}_i \to \mathcal{M}_{i-1}$ be finite.

This seemed promising because Coleman actually proved that given a morphism of two rigid curves, you can find semistable models and a map between them. This might seem like it already solves the problem, but doing it for the tower is tricky. You can produce $\mathcal{M}_1 \to \mathcal{M}_0$, but to produce $\mathcal{M}_2 \to \mathcal{M}_1$ you might have to refine the wide opens involved in defning $\mathcal{M}_1$. But that destroys the original semistable covering, so you have to refine that. Anyway, if you try to do this for the whole tower, you don't end up with a semistable covering because you had to shrink the wide opens so much that they were no longer wide opens. In fact, they shrink infinitely much precisely *around the points of fake CM*. So you have to remove those.

Let $M_m^{sp} \subset M_m$ (sp for "special") be the subset of fake CM points and $M_m^{nsp} = M_m \setminus M_m^{sp}$. This is still a rigid space, but it's complicated because we have removed infinitely many points. It's like the Drinfeld upper half-plane, $\mathbb{P}^1 \setminus \mathbb{P}^1(\mathbb{Q}_p)$ ♠♠♠ TONY: [???]

Theorem 3.1 (Weinstein)**.** *There exists a $GL_2(\mathbb{Q}_p)$-compatible family of semistable models $\mathcal{M}_m^{nsp}$:*

$$\ldots \to \mathcal{M}_2^{nsp} \to \mathcal{M}_1^{nsp} \to \mathcal{M}_0^{nsp}$$

such that all components of the special fibers fit into a tower

$$\ldots \to C_2 \to C_1 \to C_0$$

with $C_i \subset \mathcal{M}_{i,s}^{nsp}$ an irreducible component. Moreover, $C := \varprojlim C_i$ is the perfection of one of three isomorphism classes of curves:

(1) $\mathbb{P}^1$,
(2) $y^2 = x^p - x$,
(3) $y^{p+1} = x^p + x$.

Remark 3.2. The second curve appears already in Coleman-McMurdy, and the third appears in Tsushima's paper.

Let A_m be the deformation ring of $\widehat{E_0}$ with level p^m structure. Then we have a sequence

$$A_0 \to A_1 \to A_2 \to \dots$$

with $A_0 \cong \mathbb{Z}_p[[u]]$. The space M_m is the rigid generic fiber of Spf A_m.

Theorem 3.3 (Weinstein)**.** *Let $A_\infty = (\varinjlim A_m)^\wedge$ (completed with respect to the topology generated by p and u). Then*

$$A_{\infty,\mathcal{O}_{\mathbb{C}_p}} \cong \frac{\mathcal{O}_{\mathbb{C}_p}[[x^{1/p^\infty}, y^{1/p^\infty}]]}{(\Delta(x,y)^{1/p^m} - \zeta_{p^m})_{m\geq 1}}.$$

Remark 3.4. The $\Delta(x,y)$ is explicit, and the $\mathrm{SL}_2(\mathbb{Q}_p)$ action on $A_{\infty,\mathcal{O}_{\mathbb{C}_p}}$ is explicit. It's miraculous that this group symmetry, which is absent at any finite level, appears at infinite level, and we can explicitly describe it.

In terms of this, the wide opens forming a semistable cover are defined in terms of linear inequalities in x, y.

Let Γ be the set of systems $\dots \to C_2 \to C_1 \to C_0$, where $C_i \subset \mathcal{M}_{i,s}^{nsp}$. This is the dual graph of the semistable model. There are two kinds of "ends" of Γ. One kind comes from fake CM points, and the other ones come from the fact that M_m was not compact, so it has ends to begin with. So there are two kinds of ends.

There's a picture of the dual graph. From the Bruhat-Tits building of $\mathrm{GL}_2(\mathbb{Q}_p)$, you have ends parametrized by $\mathbb{P}^1(\mathbb{Q}_p)$, with branching by $\mathbb{P}^1(\mathbb{Z}/p^m\mathbb{Z})$ at each juncture. However, there are other ends branching out, which reach towards the fake CM curves. These don't have degree $p+1$, for example - their degrees are related to *supercuspidal* representations of $\mathrm{GL}_2(\mathbb{Q}_p)$.

Corollary 3.5. *$M_\infty = \varprojlim M_m$ is a perfectoid space.*

The story of this is that Peter Scholze and I gave consecutive talks at the IAS, his introducing perfectoid spaces and my introducing this theorem. We both realized immediately that what I was talking about was a perfectoid space. Since then, Peter has realized that other things become perfectoid at "infinite level," such as Rapoport-Zink spaces and Shimura varieties.

EIGENVARIETIES AND THE P-ADIC LANGLANDS PROGRAM

MATT EMERTON

1. Introduction

1.1. **Eigenvarieties.** There is a correspondence

$$\left\{\begin{array}{c}\text{certain } p\text{-adic families of}\\ \text{automorphic eigenforms}\end{array}\right\} \leftrightarrow \left\{\begin{array}{c}\text{certain } p\text{-adic families of}\\ \text{Galois representations}\end{array}\right\}.$$

When one talks about eigenforms, one should be more precise: eigenforms for what? For the Hecke operators. Which Hecke operators? In particular, there are two "cases:" the part prime to p, and the Hecke operators at p. Here we mean to consider eigenforms for *all* Hecke operators. Now, by Cebotarev's theorem a Galois representation is already determined by what happens away from p, so it "loses" information at p. One should include some extra data at p to make up for it.

$$\left\{\begin{array}{c}\text{certain } p\text{-adic families of}\\ \text{automorphic eigenforms}\\ \text{for } \textit{all} \text{ Hecke operators}\end{array}\right\} \leftrightarrow \left\{\begin{array}{c}\text{certain families of}\\ \text{Galois representations}\\ \text{plus extra data at } p\end{array}\right\}.$$

1.2. **p-adic Langlands.** The p-adic Langlands program describes a correspondence between the p-adic representation theory of $\mathrm{GL}(\mathbb{A})$, or $\mathrm{GL}_n(\mathbb{Q}_\ell)$, or $\mathrm{GL}_n(\mathbb{Q}_p)$) and global or local p-adic Galois representations.

The basic thing about p-adic Galois representations is that *away* from p the data is relatively simple because a local Galois group at ℓ is almost pro-ℓ: there is a filtration

$$G_{\mathbb{Q}_\ell} \supset I_\ell \supset \underbrace{I_\ell^{\mathrm{wild}}}_{\text{pro-}\ell}.$$

So in a p-adic representation I_ℓ^{wild} doesn't play much of a role. On the other hand, the data at p is much more complicated.

This global recipe is via a local recipe, describing a local correspondence between p-adic representations of $\mathrm{GL}_n(\mathbb{Q}_\ell)$, $\mathrm{GL}_n(\mathbb{Q}_p)$ and local p-adic Galois representations.

The point of the Langlands program is to exploit representation theory. Langlands emphasized that automorphic forms have many symmetries, and the data of an automorphic form looks confusely redundant if you don't take the symmetries into account.

In Hida or Coleman's theory, group representations don't appear at all. So it's at least interesting to ask if we can understand the theory of eigenvarities from the point of view of representation theory.

2. Relating Eigenvarieties to Representation Theory

2.1. **Completed cohomology.** To fix ideas, we start with GL_2. We recall the construction of *completed cohomology*. $Y(p^m)$ is the modular curve of full level p^m. (There should be an auxiliary tame level floating around, as in Jared's talk, which we'll just ignore.) Then we can consider $H_1(Y(p^m), \mathbb{Z}_p)$. Since the modular curves form a tower, the homologies form a projective system, so we can take

$$\widetilde{H}_1 := \varprojlim_m H_1(Y(p^m), \mathbb{Z}_p).$$

This is a representation of $\mathrm{GL}_2(\mathbb{Q}_p)$, and admits an action of the "prime-to-p" Hecke algebra $\mathbb{T}$.

Theorem 2.1. *$\widetilde{H}_1$ is finitely generated over $\mathbb{Z}_p[[\mathrm{GL}_2(\mathbb{Z}_p)]]$.*

A more traditional thing to do in the Langlands program would be to take the *cohomology*. Then we would have an inductive limit, which basically amounts to taking the union of all cohomology classes. This would be an admissible smooth representation - smooth because any class lives at finite level, and admissible because taking invariants of a compact open takes you back to finite level. On the other hand, the representation $\widetilde{H}_1$ is far from smooth - it is much bigger than the representations that appear in the traditional p-adic Langlands program.

2.2. **Galois deformations.** Fix $\overline{\rho}\colon G_{\mathbb{Q}} \to \mathrm{GL}_n(\overline{\mathbb{F}_p})$ an irreducible modular representation, corresponding to a maximal ideal $\mathfrak{m} \subset \mathbb{T}$. Then you would have an action of $\mathbb{T}_{\mathfrak{m}}$ on $\widetilde{H}_{1,\mathfrak{m}}$. Then there is a "universal Galois representation" obtained from gluing together all the stuff ♠♠♠ TONY: [eh???]; this is packaged in the ring $\mathbb{T}_{\overline{\rho}}$. There is a also a universal deformation ring $R_{\overline{\rho}}$, and a map between them:

$$\mathrm{Spec}\ \mathbb{T}_{\overline{\rho}} \to \mathrm{Spec}\ R_{\overline{\rho}}.$$

Under some assumptions on $\overline{\rho}$, this is an isomorphism.

If we had considered something else (cohomology), we would have seen all weight 2 modular forms of level p^*, which is only countably much data. Taking completed homology smashes together the Galois representations, etc. making this an isomorphism.

$\mathrm{Spec}\ R_{\overline{\rho}}$ is 2-dimensional over $\mathbb{Z}_p$. The third dimension (coming from $\mathbb{Z}_p$) can be viewed as the determinant; we will often fix a determinant, eliminating this determinatn. Now, $\widetilde{H}_1$ is four-dimensional, but it has an action of

the three-dimensional symmetries $\mathbb{T}_{\overline{\rho}}$, so you might naïvely guess that the result is one-dimensional, i.e. a module of one-dimensional support over the Iwasawa eigencurve.

The main thing to take away is that p-adic homology knows about all the p-adic modular forms and all the p-adic Galois representations. But it contains a lot more than the eigenvariety. In particular, it contains all sorts of bad things: modular forms of infinite slope, Galois representations which are not crystalline, etc.

What is an intuitive description of the dimensions of $R_{\overline{\rho}}$? One is twisting (this is the dimension of the determinant, which we've already mentioned). Another is the weight (Hida). What about the other? It's a little confusing; there's no canonical label that we know. So two dimensions of deformations over Spec $\mathbb{Z}_p$ are a little mysterious.

2.3. **Cutting out the eigenvariety.** What I'd like to describe is how to cut this picture down to an eigenvariety. We have to somehow remove $\mathrm{GL}_2(\mathbb{Q}_p)$ and introduce U_p into the game. $\widetilde{H}_1$ is a p-adically completed object, living on a space Spec $\mathbb{T}_{\overline{\rho}}$, or perhaps more naturally considered as the formal scheme Spf $\mathbb{T}_{\overline{\rho}}$. So $\widetilde{H}_1$ is a kind of formal scheme-y type of object, whereas the eigenvariety is a rigid analytic object. To go from formal to rigid, we pass to analytic vectors:

$$\widetilde{H}_{1,\mathrm{an}} = \widetilde{H}_1 \otimes_{\mathbb{Z}_p[\mathrm{GL}_2(\mathbb{Z}_p)]} D(\mathrm{GL}_2(\mathbb{Z}_p)).$$

Here $D(\mathrm{GL}_2(\mathbb{Z}_p))$ are distributions on $\mathrm{GL}_2(\mathbb{Z}_p)$. When you have a formal scheme and invert p, you can pass to the rigid analytic generic fiber. That's a quasi-stein (wide-open), and it has its own ring of functions $\mathbb{T}^{\mathrm{rig}}_{\overline{\rho}}$, and also an action of $\mathrm{GL}_2(\mathbb{Q}_p)$. It's maybe not obvious because $\mathrm{GL}_2(\mathbb{Q}_p)$ doesn't stabilize $\mathrm{GL}_2(\mathbb{Z}_p)$, but actually you could have taken any compact open subgroup instead of $\mathrm{GL}_2(\mathbb{Z}_p)$ and it would give you something canonically isomorphic, and $\mathrm{GL}_2(\mathbb{Q}_p)$ *does* stabilize the system of compact opens.

On the space of coinvariants $(\widetilde{H}_{1,\mathrm{an}})_{\left(\begin{smallmatrix}1 & \mathbb{Z}_p\\ 0 & 1\end{smallmatrix}\right)}$ you have an action of Hecke operators h_t, for

$$t \in T^+ = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \mid t \begin{pmatrix} 1 & \mathbb{Z}_p \\ 0 & 1 \end{pmatrix} t^{-1} \subset \begin{pmatrix} 1 & \mathbb{Z}_p \\ 0 & 1 \end{pmatrix} \right\}.$$

Then the action of h_t on $(\widetilde{H}_{1,\mathrm{an}})_{\left(\begin{smallmatrix}1 & \mathbb{Z}_p\\ 0 & 1\end{smallmatrix}\right)}$ is defined by

$$v \mapsto \sum_{n \in \left(\begin{smallmatrix}1 & \mathbb{Z}_p\\ 0 & 1\end{smallmatrix}\right) / t \left(\begin{smallmatrix}1 & \mathbb{Z}_p\\ 0 & 1\end{smallmatrix}\right) t^{-1}} ntv.$$

The fact that we are averaging over $\begin{pmatrix} 1 & \mathbb{Z}_p \\ 0 & 1 \end{pmatrix}$ ensure that this sum lies in the space of coinvarants. So now we have an action of the monoid T^+.

Now we want to cut down to things of finite slope. There's a good way to do that! We have an inclusion $T^+ \subset T$ (diagonal matrices). To make T^+ act invertibly is to make T act. We want a group algebra to act, but what group algebra? If you just tensor, you get something algebraic which is insensitive to the topological structure. This is bad, so we instead define $\widehat{T}$ to be the ring of continuous characters $T \to \overline{\mathbb{Q}_p}^\times$. As $T \cong \mathbb{Z} \times Z \times \mathbb{Z}_p^\times \times \mathbb{Z}_p^\times$, a character of T corresponds to two characters of $\mathbb{Z}_p^\times$ and two characters of $\mathbb{Z}$. A character $\mathbb{Z}_p^\times$ is parametrized by the "weight space" $\mathcal{W}$, and a character of $\mathbb{Z}$ is any choice of element of $\overline{\mathbb{Q}_p}^\times$, so this is $\mathcal{W} \times \mathcal{W} \times \mathbb{G}_m \times \mathbb{G}_m$.

Definition 2.2. We define the *completed group ring*

$$\mathcal{M} := O(\widehat{T}) \widehat{\otimes}_{\mathbb{Q}_p[T^+]} (\widetilde{H}_{1,\mathrm{an}})_{\begin{pmatrix} 1 & \mathbb{Z}_p \\ 0 & 1 \end{pmatrix}}.$$

This is an $O(\widehat{T}) \times \mathbb{T}_{\overline{\rho}}$-module.

Theorem 2.3. *$\mathcal{M}$ is the global sections of a coherent sheaf on $\widehat{T}$.*

Imagine drawing $\widehat{G}_m \times W$. The support of $\mathcal{M}$ is a curve, and it has discrete (but infinite) fibers over $\mathcal{W}$. This is the "spectral curve" of Coleman and Mazur, cut out by Fredholm power series of U_p. To see that, you could localize $\widetilde{H}_1$ at $\overline{\rho}$, which is irreducible; then we get a projective module over the group ring and you can show that the coinvariants are an orthonormalizable Frechet module over the group ring of $\mathbb{Z}_p^\times$, namely $\mathcal{W}$.

You can look at the $O(\widehat{T})$-subalgebra $\mathcal{A}$ of $\mathrm{End}(\mathcal{M})$ given by the image of $\mathbb{T}$, which is a coherent commutative algebra acting faithfully on $\mathcal{M}$ by construction, and so we can consider the relative spec, $\mathrm{Spec}\ \mathcal{A}$. The claim is that this is an eigenvariety. If we fix a $\mathbb{G}_m$ (i.e. determinant) and weight space then it's a curve, and we are claiming that it is the eigencurve.

Remark 2.4. This is quite similar to Stevens' theory of modular symbols for overconvergent modular forms.

3. Applications

What can you do with this? Several different things, including applications to p-adic L-functions.

I'll instead talk about how to use more representation-theoretic methods. For instance, it's nice to know that when you have a sheaf over an eigenvariety that you have a multiplicity one statement. For instance, is $\mathcal{M}$ locally free? I don't know. It's obviously locally free on an open set, but we'll give

a meaninful locally free description at many points. (If you had something like smoothness of the base plus Cohen-Macaulayness of $\mathcal{M}$ then we would get freeness ♠♠♠ TONY: [?!], but you don't have that.)

One of the subtle ways was discovered by Fred Diamond, using the Taylor-Wiles patching method. I want to explain how to apply that to the setup here. The key thing that drives Fred's argument: globally you know almost nothing about Spec $\mathbb{T}_{\bar{\rho}}$. Even if you had Cohen-Macaulay on $\mathcal{M}$ (which we don't), we don't have smoothness on the base. The patching thing is that you compute the deformation rings locally, where you can see that they are smooth. This is analogous to what you dow ith perverse sheaves in Geometric Langlands.

So here's how the argument goes. You have a *local* deformation space of $\bar{\rho}_{K/\mathbb{Q}_p}$, which is honestly smooth. There's a fact that has been proved in some generality: the map from global to local is actually finite. So it's not far from the truth to assume that it's a closed immersion. (That would be the statement that some strict Selmer group vanishes).

[Picture of a slice including into a box. The boxiness corresponds to unobstructedness]

Choose an auxiliary prime $q \equiv 1 \pmod{p^n}$ for some large n. Now we consider a deformation ring relaxing the conditons at q [picture is slightly thicker slice], but the choice of q makes this still an embedding. It's surprising that you can do this: you allow ramification at q, but arranging so that the decomposition group at p remembers it. This is like having a character whose conductor is divisible by q, but is captured by the decomposition group at p - the condition that you need is that Frob_p generates $(\mathbb{Z}/q)^\times$.

Okay, so we've chosen a prime q. The amount of extra stuff you see is the p-Sylow of $(\mathbb{Z}/q)^\times$. As far as modular forms are concerned, you get genuinely more modular forms by adding this q into the level. You get free of rank one over the group ring adjoint the p-sylow. You're doing infinitesimal thickening in the p-sylow direction. As n gets large, you fill out the local deformation space.

We're going to describ a local version of $\widetilde{H}_1$, namely $\mathcal{M}_\infty$ - it is a patched version of $\widetilde{H}_1$. This gives another construction of p-adic local Langlands of Breuil. You can show that at ∞, the coinvariants of the augmentation ideal is supported on the locus of Barsotti-Tate representations. (You don't know that it's supported on the whole locus - that would be the content of modularity.) One can form $(M_{\infty,\mathrm{an}})_{\begin{pmatrix}1 & \mathbb{Z}_p \\ 0 & 1\end{pmatrix}}$ (coinvariants) and tensor with $O(\widehat{T})$ to get $\mathcal{M}_\infty$.

Theorem 3.1 (Breuil-Mellman-Schraen)**.** *The support of* $\mathcal{M}_\infty$ *(in* $(\mathrm{Spf}\, R_{loc})^{rig}\times$

$\widehat{T}$) is a union of components of the trianguline locus.

The optimal result is that the support is the *entire* trianguline locus: the Zariski closure of trianguline representations. Also implicit in their arguments is that $\mathcal{M}_\infty$ is Cohen-Macaulay, hence free over the smooth locus. Then you can recover $\mathcal{M}$ over the eigenvariety by pulling back along the map from global to local.

THE SPECTRAL HALO

ADRIAN IOVITA

1. Introduction

[This is joint work with F. Andreatta and V. Pillowi on a conjecture of R. Coleman.]

We begin by basically transcribing some private notes of Robert concerning the eigencurve. Let $p > 0$ be a prime integer and $N > 0$ an integer prime to p. Then

- (1998) Coleman-Mazur defined a rigid analytic object called the *eigencurve* when $p > 2$ and $N = 1$.
- (2003) Kevin Buzzard extended the construction to all p and all N. Denote this object $\mathcal{E}_p(N)$.

There is a simple description of the eigencurve in terms of moduli properties. It is a rigid analytic curve which parametrizes finite slope, overconvergent, normalized, p-adic eigenforms of tame level N.

The geometry of $\mathcal{E}_p(N)$ is still poorly understood. Let W^{rig} denote the rigid analytic space associated to the formal scheme $\mathrm{Spf}(\mathbf{\Lambda})$ where

$$\mathbf{\Lambda} := \mathbb{Z}_p[[\mathbb{Z}_p^\times]] \cong \mathbb{Z}_p[(\mathbb{Z}/p\mathbb{Z})^\times][[T]]$$
$$1 + p \mapsto 1 + T.$$

There is a morphism $\kappa\colon \mathcal{E}_p(N) \to W^{\mathrm{rig}}$ sending $f \mapsto \kappa(f)$ (its weight).

Definition 1.1. If f is a p-adic overconvergent eigenform, then $U_p(f) = a_p f$ and we say that the *slope* of f is $v_p(a_p)$.

Let $k\colon \mathbb{Z}_2^\times \to \mathbb{C}_2^\times$ be a character (viewed as an element of weight space). In 2005, Buzzard-Kilford proved that if $p = 2$ and $N = 1$, $k \in W^{\mathrm{rig}}$, such that $|k(5) - 1|_2 > 1/8$ then the slopes of overconvergent 2-adic modular forms of weight k are $0, t, 2t, 3t, \ldots$, where $t = v_2(k(5) - 1)$, and each slope occurs with multiplicity 1. A similar result for $p = 3, N = 1$ was proved by Roe in 2008. Robert was interested in generalizing this.

1.1. **Robert's conjecture.** From now on assume $p \geq 5, N \geq 3$. Fix a character $\epsilon\colon (\mathbb{Z}/p\mathbb{Z})^\times \to \overline{\mathbb{Q}_p}^\times$. Let $\Lambda = \mathbf{\Lambda}_\epsilon$ be the ϵ-component of $\mathbf{\Lambda}$, so $\Lambda \cong \mathbb{Z}_p[[T]]$. Let $Q_\epsilon(X) \in \Lambda[[X]]$ be the characteristic series of the operator U_p on p-adic families of overconvergent eigenforms.

Conjecture 1.2 (Coleman, 2012?)**.** *There exists a Banach space over $\mathbb{F}_p((T))$, denoted $\overline{M}_\epsilon$ of "overconvergent modular forms over $\mathbb{F}_p((T))$" with a compact action of U_p such that the characteristic series*

$$P_\epsilon(X) := \det(I - XU_p \mid \overline{M}_\epsilon) = Q_\epsilon(X) \mod p\Lambda[[x]].$$

This conjecture expresses something very deep. The p-adic modular forms live in $\mathbb{Q}_p$-vector spaces, which are very rigid. But the characteristic polynomial of U_p - the most important Hecke operator - has a very simple integral shape. So Robert's guess was that there should exist an *integral* theory of families of p-adic modular forms.

Remark 1.3.

(1) Robert gives a precise recipe for the construction of $\overline{M}_\epsilon$ using reduction modulo p of p-adic families in characteristic 0 close to the boundary of the weight space $W_\epsilon^{\mathrm{rig}}$.
(2) Coleman claimed that his conjecture is related to generalizing the result of Buzzard-Kilford for all p and all N.
(3) A recent result of R. Liu, D. Wan, and L. Xiao proved the Buzzard-Kilford result for all p for modular forms associated to definite quaternion algebras.

2. Geometric definition of $\overline{M}_\epsilon$

Let $\overline{k} := \overline{k}_\epsilon \colon \mathbb{Z}_p^\times \to \mathbb{F}_p[[T]]^\times$ be the character sending $1 + p \mapsto 1 + T$ and $(\mathbb{Z}/p\mathbb{Z})^\times \xrightarrow{\epsilon} \mathbb{F}_p^\times$.

2.1. **The construction.** Let $\overline{X} = X_1(N)_{\mathbb{F}_p}$. We have the ordinary locus $\overline{X}^{\mathrm{ord}}$. In the moduli-theoretic interpretation of $X_1(N)_{\mathbb{F}_p}$ parametrizing elliptic curves plus a point of order N, the ordinary locus describes the subset of elliptic curves of ordinary reduction. Equivalently, $\overline{X}^{\mathrm{ord}} = \{x \in \overline{X} \mid Ha(x) \neq 0\}$ where $Ha \in H^0(X, \overline{\omega}^{p-1})$ is the Hasse invariant.

(1) Let $E \to \overline{X}^{\mathrm{ord}}$ be the universal semi-abelian scheme and $\mathrm{Frob}^n \colon E \to E^{(p^n)}$. Then $H_n := \ker(\mathrm{Frob}^n) \subset E[p^n]$ is the canonical subgroup of E.
(2) The Cartier dual H_n^D is étale. For all $n \geq 1$, we can consider $IG_n := \mathrm{Isom}_{\overline{X}^{\mathrm{ord}}}(H_n^D, \underline{\mathbb{Z}/p^n\mathbb{Z}})$ - here $\underline{\mathbb{Z}/p^n\mathbb{Z}}$ is the constant scheme. This admits a map to $\overline{X}^{\mathrm{ord}}$ which is finite étale, Galois with group $G_n = (\mathbb{Z}/p^n\mathbb{Z})^\times$.
(3) We have a tower

$$\ldots \to IG_{n+1} \to IG_n \xrightarrow{(\mathbb{Z}/p^n\mathbb{Z})^\times} \overline{X}^{\mathrm{ord}}.$$

This gives a monodromy representation $\pi_1(\overline{X}^{\mathrm{ord}}, *) \to \mathbb{Z}_p^\times \xrightarrow{\bar{k}} \mathbb{F}_p[[T]]^\times$, which can be interpeted as an action of $\pi_1(\overline{X}^{\mathrm{ord}}, *)$ on $\mathbb{F}_p[[T]]$. By work of Katz, one can canonically attach a pair $(\overline{\omega}^{\mathrm{ord},\bar{k}}, \phi^{\mathrm{ord}})$ where $\overline{\omega}^{\mathrm{ord},\bar{k}}$ is a locally free rank 1 sheaf on $\overline{X}^{\mathrm{ord}} \times_{\mathbb{F}_p} \mathbb{F}_p[[T]]$ and ϕ^{ord} is a Frobenius endomorphism on $\overline{\omega}^{\mathrm{ord},\bar{k}}$.

(4) Let $\overline{M}_\epsilon^{\mathrm{ord}} := H^0(\overline{X}^{\mathrm{ord}} \times_{\mathbb{F}_p} \mathbb{F}_p[[T]], \overline{\omega}^{\mathrm{ord},\bar{k}})$, the space of T-adic modular forms over $\mathbb{F}_p[[T]]$.

Question. Does $(\overline{\omega}^{\mathrm{ord},\bar{k}}, \phi^{\mathrm{ord}})$ overconverge? (i.e. does it extend to a neighborhood of this formal scheme?)

(5) Let $r \geq 1$. Set $\overline{\mathcal{X}}^{\mathrm{ord}} = \overline{X}^{\mathrm{ord}} \times_{\mathbb{F}_p} \mathbb{F}_p[[T]]$ and $\overline{\mathcal{X}} = \overline{X} \times_{\mathbb{F}_p} \mathbb{F}_p[[T]]$. Then we construct some open formal subscheme $\mathcal{X}_r$ in the blowup (in the category of formal schemes) of $\overline{\mathcal{X}}$ along $I = (Ha^{p^r}, T)$. We have a map

$$\begin{array}{ccc} \overline{\mathcal{X}_r} & & \\ \downarrow & & \\ \overline{\mathcal{X}} & \longleftarrow & \overline{\mathcal{X}}^{\mathrm{ord}} \end{array}$$

(6) For all $n \geq 1$, we have an Igusa tower $IG_n \times_{\mathbb{F}_p} \mathbb{F}_p[[T]]$ over $\overline{\mathcal{X}}^{\mathrm{ord}}$, and denote by $\mathcal{IG}_{r,n}$ the normalization of $\overline{\mathcal{X}}_r$ in $IG_n \times_{\mathbb{F}_p} \mathbb{F}_p[[T]]$. So we get a tower of formal schemes.

$$\begin{array}{c} \mathcal{IG}_{r,n+1} \\ \downarrow \\ \mathcal{IG}_{r,n} \\ \downarrow{\scriptstyle (\mathbb{Z}/p^n\mathbb{Z})^\times} \\ \mathcal{X}_r \end{array}$$

We now define

$$\begin{array}{c} \mathcal{IG}_{r,\infty} := \varprojlim_n \mathcal{IG}_{r,n} \\ \downarrow{\scriptstyle \pi} \\ \mathcal{X}_r \end{array}$$

This admits a $\mathbb{Z}_p^\times$ action.

Definition 2.1. We define the sheaf $\underline{\omega}_r^{\bar{k}} := \pi_*(\mathcal{O}_{\mathcal{IG}_{r,\infty}})[\overline{k}^{-1}]$.

A priori, this seems like it could be a terrible thing, or completely trivial. However, we prove:

Theorem 2.2. *$\underline{\omega}^{\bar{k}}$ is locally free of rank 1 over $\mathcal{X}_r$ for $r \geq 2$, and*

$$\underline{\omega}^{\bar{k}}_r|_{\overline{\mathcal{X}}^{\mathrm{ord}}} = \underline{\omega}^{\mathrm{ord},\bar{k}}.$$

Define

$$\overline{M}^{\bar{k}}_{\epsilon} := H^0(\mathcal{X}_r, \underline{\omega}^{\bar{k}}_r).$$

This is a space of overconvergent modular forms over $\mathbb{F}_p[[T]]$ of weight $\bar{k}$, r. It admits a Hecke action. One should invert T to get a Banach space, such that U_p is compact for the T-adic topology (but we think it is important that this came from an integral construction.)

3. Connections with modular forms in characteristic 0

Oops, we're out of time. Let me just say that we can work near the boundary of the weight space (an adic space) in the T-adic topology and we can produce *integral* locally free modular sheaves of rank 1, whose reduction mod p is $\underline{\omega}^{\bar{k}}_r$.

THE EIGENCURVE: A VIEW FROM THE BOUNDARY

KEVIN BUZZARD

1. The eigencurve

Coleman and Mazur raise several questions about eigencurves at the beginning of their paper. The eigencurve seems very abstract, but I eventually realized that they are actually not so hard to write down. For instance, the "simplest" example is for $p = 2$ and $N = 1$, there is a "level $1, 2$" eigencurve, and Emerton and I figured out how to answer many of their questions for this special case.

Let p be a prime number. We'll work in tame level 1 throughout. Then we have the familiar isomorphism

$$j\colon X_0(1)_{/\mathbb{Z}_p} \xrightarrow{\sim} \mathbb{P}^1$$

Thinking of $X_0(1)_{\mathbb{F}_p}$ as parametrizing elliptic curves, you have the cusp at ∞, some "random" supersingular points, and the rest of the points are nice ordinary curves.

The pre-image of each point is a disk. In $X_0(1)(\mathbb{C}_p)$, there is a disk lying over ∞ which parametrizes curves of bad reduction, and 3 open disks parametrizing elliptic curves with supersingular reduction.

Nick Katz emphasized that congruences between modular forms reflects something about the modular forms being p-adically close, which comes down to being close away from the supersingular discs. Let $X_0(1)^{\mathrm{ord}}$ be $X_0(1)$ minus the supersingular discs.

You can do something slightly more subtle: throw away smaller disks. This requires a choice of center (in non-archimedean geometry, all points are the center). Choose a center x of a supersingular disc with x defined over $W(\overline{\mathbb{F}}_p)$ (there's a canonical disc of radius $1/p$ parametrizing curves defined over an unramified extension). Then $X_0(1)_{\geq r}$ is obtained by throwing away the open discs of radius r centered at these x's.

Set M_0^{ord} to be the holomorphic (i.e. rigid analytic) functions on $X_0(1)^{\mathrm{ord}}$. Define $M_0(r)$ to be holomorphic functions on $X_0(1)_{\geq r}$. These are (big!) p-adic Banach spaces, admitting continuous Hecke action. This work goes back to Katz. Katz also knew that the special Hecke operator U_p was continuous on $M_0(1)^{\mathrm{ord}}$ and compact on $M_0(r)$.

2. A toy model

Let me give a toy example of how I think about these things. Let q be a p-adic variable. A toy model for $X_0(1)^{\mathrm{ord}}$ is a closed disc $|q| \leq 1$, and a toy model for $X_0(1)_{\geq r}$ is a closed disc $|q| \leq 1 + \epsilon$. Then

$$M_0^{\mathrm{ord}} = \left\{ \sum a_n q^n : |a_n| \to 0 \right\}$$

and

$$M_0(r) = \left\{ \sum a_n q^n : |a_n|(1+\epsilon)^n \to 0 \right\}.$$

Now we think of

$$U_p\left(\sum a_n q^n\right) = \sum a_{n/p} q^n.$$

With respect to the obvious basis $\{1, q, q^2, q^3, \ldots\}$ of M_0^{ord}, U_p has the matrix (for $p = 2$)

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & \ldots \\ 0 & 0 & 1 & 0 & 0 & \ldots \\ 0 & 0 & 0 & 0 & 1 & \ddots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

since $U_p(1) = 1, U_p(q) = 0, U_p(q^2) = q$, etc.

You can easily see that this is continuous. First, well-definedness is that each column has entries tending to 0 p-adically, and continuity is that property that there is a global bound on the entries of the matrix.

We can also see that this is not compact. Indeed, a compact operator is a limit of finite rank operators. Concretely, for any $\epsilon > 0$ there is a horizontal line such that everything below has size at most ϵ. That obviously fails here, as there are always 1's in the matrix below any horizontal line.

On the disc $|q| \leq 2$, a basis is $1, 2q, 4q^2, \ldots$. So now the matrix for U_2 is

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & \ldots \\ 0 & 0 & 2 & 0 & 0 & \ldots \\ 0 & 0 & 0 & 0 & 4 & \ddots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

Now we see that this *is* compact.

Compact operators are really good, because they're well-approximated by ones of finite rank. If $M = (m_{ij})_{i,j \geq 0}$ is a compact endomorphism, we can define

$$\det(1 - XM) = \lim_{N \to \infty} \det(1 - XM_N)$$

where M_N is the truncation of M to $i, j \leq N$.

3. Back to the real world

The operator U_p acting on overconvergent functions *is* compact (as we said, this was already known to Katz), so

$$\det(1 - XU_p) \in \mathbb{Q}_p[[X]]$$

is defined, and even better this converges for all $X \in \mathbb{C}_p$.

Katz studied this for integer weights.

Question. Can we make this work for a *general* p-adic weight $\kappa \in \mathcal{W} := \mathrm{Hom}_{\mathrm{cts}}(\mathbb{Z}_p^\times, \mathbb{C}_p^\times)$?

In other words, can we give a definition of overconvergent modular forms of weight κ? This was a problem that Robert solved brililantly.

Example 3.1. For $k \geq 2$ even,

$$E_k = 1 + \frac{2}{\zeta_p(1-k)} \sum \sigma_{k-1}^*(n) q^n.$$

This is a level p Eisenstein series, with $U_p E_k = E_k$.

This sits in a nice family. For $\kappa \in W$, we can define E_κ by a *formal* q-expansion in $\mathbb{C}_p[[q]]$ (specializing to the usual one when k is an integer).

Robert recognized that it would be hard to say anything about these, but he somehow found interesting things to say nonetheless. A *crucial result* is that $E_\kappa(q)/E_\kappa(q^p)$ is the q-expansion of an overconvergent function (this is expected, if you expect both the numerator and the denominator to be overconvergent modular forms of weight k). This is *hard*! It uses the construction of the eigencurve, for instance.

One can ask interesting questions like: how far does this overconverge? $\mathcal{W}$ is a finite union of discs, and as $\kappa \to$ boundary, $E_\kappa(q)/E_\kappa(q^p)$ overconverges less and less.

Why is this important? It allows us to give a definnition of overcongergent modular forms of weight κ. This was Robert's definition (there are better ones now):

Definition 3.2. An *overconvergent modular form* of weight κ is a formal q-expansion $F = \sum a_n q^n$ such that F/E_κ the q-expansion of an overconvergent function (weight 0).

Now the big question is: do we have a theory of Hecke operators?

Question. Is $U_p(F)$ overconvergent of weight κ if F is?

The answer (due to Coleman) is yes! The reason is that one can fill in a diagram

$$\begin{array}{ccc} M_0(r) & \xrightarrow{E_\kappa} & M_\kappa(r) \\ \vdots\, U_p^* & & \downarrow U_p \\ M_0(r) & \longrightarrow & M_\kappa(r) \end{array}$$

where

$$U_p^*(F) = U_p(FE_\kappa(q)/E_\kappa(q^p)).$$

This definition makes sense because everything is an overconvergent function. So the operator

$$U_p\colon \sum a_n q^n \mapsto \sum a_{np} q^n$$

is compact (because the diagram commutes, it factors through a compact map). Then it makes sense to define

$$P_\kappa(X) = \det(1 - U_p X|_{M_\kappa(r)}).$$

For all $\kappa \in \mathcal{W}$, we have $P_\kappa(X) \in \mathbb{C}_p[[X]]$ converging for all $x \in \mathbb{C}_p$. Now, since this all varies analytically, the P_κ glue to give $P(X) = \sum a_n X^n \in \mathcal{O}(W)[[X]]$. In fact, Robert proved that $P(X) \in \mathbb{Z}_p[\mathbb{Z}_p^\times][[X]]$.

Remark 3.3. Here is a question of Bergdall-Pollack. Each a_n is a function on $\mathcal{W}$. Does there exist a closed disc $D \subset \mathcal{W}$ such that the zeroes of a_n all lie in D? Or are there zeros arbitrarily close to the boundary?

The reason that we went through it is to emphasize that this is really concrete mathematics, which you can compute.

4. Eisenstein series

If $p = 2$ and $N = 1$ then $X_0(1)^{\mathrm{ord}}$ is isomorphic to a closed disc. You can compute $E_\kappa(q)/E_\kappa(q^p)$ using a formula in Washington's book.

If $\mathbb{E}$ is the Eisenstein family, you can compute $\mathbb{E}(q)/\mathbb{E}(q^p) \in \mathbb{Z}_2[[w]][[x]]$.

If $f = \Delta(q^2)/\Delta(q)$, then f induces an isomorphism between $X_0(1)^{\mathrm{ord}}$ and a closed disc. We can use this to express:

$$\frac{\mathbb{E}(q)}{\mathbb{E}(q^2)} = \sum b_n f^n, \quad b_n \in \mathbb{Z}_2[[w]].$$

Now, $\mathbb{E}$ *doesn't* overconverge, so the b_n don't tend to 0 p-adically.

However, on the closed disc $|w| \le 1/8$, the function $\frac{\mathbb{E}(q)}{\mathbb{E}(q^2)}$ *does* overconverge (only at the boundary does it fail to overconverge). Therefore,

$$\frac{\mathbb{E}(q)}{\mathbb{E}(q^2)} \in \mathbb{Z}_2[[w/8]][[8f]].$$

This is saying that on a small closed disc (parametrized by the first variable), the family overconverges a lot.

We also have $\frac{\mathbb{E}(q)}{\mathbb{E}(q^2)} \in \mathbb{Z}_2[[w, f]]$. Therefore, $\frac{\mathbb{E}(q)}{\mathbb{E}(q^2)} \in \mathbb{Z}_2[[w, wf, 8f]]$. This tells us something about the coefficients b_n, namely that $b_n \in (8, w)^n$.

Upshot: we can compute the matrix of U_2 on ordinary 2-adic modular forms. Using basis $1, f, f^2, \ldots$ the matrix of U_2 is (the matrix of U_2 in weight 0) times (the matrix representing multiplication multiplication by $\frac{\mathbb{E}(q)}{\mathbb{E}(q^2)}$), but we know that the latter can be described is in terms of the explicit calculable b_n.

If $f = \frac{\Delta(q^2)}{\Delta(q)}$, we want to compute $U_2(f^n)$. That is $f(\frac{\tau}{2})^n + f(\frac{1+\tau}{2})^n$. You can explicitly solve this to get an explicit formulae for the matrix entries. That implies that U_2 on ordinary forms looks like

$$\begin{pmatrix} 1 & & & & & \\ 8^2 & 8 & 1 & & & \\ 8^4 & 8^3 & 8^2 & 8 & 1 & \ldots \\ \vdots & \vdots & & & & \ddots \end{pmatrix} \times \begin{pmatrix} b_0 & & & & \\ b_1 & b_0 & & & \\ b_2 & b_1 & b_0 & \ldots & \\ \vdots & \vdots & & \ddots & \end{pmatrix}$$

This implies that the matrix for U_2 looks like

$$\begin{pmatrix} 1 & & & & & \\ (8,w)^2 & (8,w) & 1 & & & \\ (8,w)^4 & (8,w)3 & (8,w)^2 & (8,w) & 1 & \ldots \\ \vdots & & & & & \ddots \end{pmatrix}$$

Even though this matrix is not compact, we can still define the characteristic power series $\det(1 - X(m_{ij})_{0 \le i,j \le N})$ and it is a miraculous fact that this converges as $N \to \infty$. That gives bounds for $P(X)$, and implies that the slopes of U_2 near the boundary are bounded below by $0, v(w), 2v(w), \ldots$.

What I actually did with Kilford was some hideous combinatorics concerning when you get p-adic units, and the result was that these lower bounds exact.

Later, work of Liu, Wan, and Xiao showed that these lower bounds must be tight for formal reasons: near the boundary, if you have a form of weight α then you also have a form of weight $k - 1 - \alpha$ by an Atkin-Lehner involution. They then pushed through the theory for automorphic forms on a definite quaternion algebra, and used the Atkin-Lehner trick to get precise formulae for the slopes.

♠♠♠ TONY: [picture of christmas tree]

I told this to Robert and he instantly said that is great because you can glue in $\mathbb{P}^1$ to get something compact. I still haven't figured out if this is sueful for anything.

A SURVEY OF 15 YEARS OF P-ADIC POINT COUNTING

KIRAN KEDLAYA

1. Zeta functions of algebraic varieties

Let $\mathbb{F}_q$ be a finite field of characteristic p. We defined the *zeta function* of a variety X over $\mathbb{F}_q$ as

$$\zeta(X, s) = \prod_x (1 - \#\kappa(x)^{-s})^{-1}$$

as x runs over closed points of X and $\kappa(x)$ denotes the residue field.

Example 1.1. If $X = \operatorname{Spec} \mathbb{Z}$, then the analogous definition gives the Riemann zeta function.

Equivalently (and probably closer to the language Weil would have originally expressed it in), x runs over Galois orbits of $\overline{\mathbb{F}_q}$-rational points and $\kappa(x)$ denotes the minimal field of definition.

Let $T = q^{-s}$. Then one can show that

$$\zeta(X, T) = \exp\left(\sum_{n=1}^{\infty} \frac{T^n}{n} \#(\mathbb{F}_{q^n})\right).$$

This form is much easier to use in practice.

Example 1.2. $\zeta(\mathbb{P}^d_{\mathbb{F}_q}, T) = \frac{1}{(1-T)(1-qT)\dots(1-q^dT)}$ and if X is an elliptic curve of $\mathbb{F}_q$, then

$$\zeta(X, T) = \frac{1 - aT + qT^2}{(1 - T)(1 - qT)}$$

where $a = q + 1 - \#X(\mathbb{F}_q)$. Hasse proved a bound $|a| \leq 2\sqrt{q}$.

Based on these and more examples, Weil famous conjectured analogues of the properties of the Riemann zeta function. The first was:

Conjecture 1.3. *The power series $\zeta(X, T)$ represents a rational function of T.*

Theorem 1.4 (Dwork, 1960)**.** *The power series $\zeta(X, T)$ is p-adic meromorphic: it is the ratio of two power series over $\mathbb{Q}_p$ with infinite radii of convergence.*

This $\zeta(X, T)$ converges for small $T \in \mathbb{C}$ (by a trivial estimate on the number points in terms of the dimension), an argument of Borel (1894) then shows that it is rational.

2. The computational problem

Problem. Can one produce an algorithm that, given an explicit definition of X (i.e. defining equations), returns the rational function $\zeta(X, T)$?

The answer is *yes*: you can compute a bound on the degree of the numerator and denominator of $\zeta(X, T)$, and then enumerate by brute force $X(\mathbb{F}_{q^n})$ for enough values of n.

However, this is clearly at least an "exponential-time" algorithm. Unless q and the degree bound are quite small, it is impractical.

What if we demand a "polynomial-time" algorithm?

A careless version of the question is probably no: even the length of the *answer* can be exponential in the length of the input. Also, $X(\mathbb{F}_q)$ is dicey because some NP-complete problems can be reduced to it. For instance if $q = 2$ then this is asking for solutions to boolean equations.

That just means you should ask this question in a more modest way. In 2000, interest grew due to applications to hyperelliptic curve cryptography. Other interest comes from computing motivic L-functions, to test special values conjectures such as BSD. So versions of this question are of interest both within number theory and in more applied areas.

2.1. First attempt.

Let's try to formulate a more precise version of the question.

Problem. Fix a positive integer n. Is there an algorithm that, given an algebraic variety X of postive dimension n, returns the rational function $\zeta(X, T)$ in "polynomial time?"

To quantify "polynomial time" (in the length of the input) we must specify an input mechanism for X. If $Z \subset X$ is a closed subscheme, then the set-theoretic disjoint union $X = Z \coprod (X \setminus Z)$ induces a factorization

$$\zeta(X, T) = \zeta(Z, T)\zeta(X - Z, T)$$

This reduces computing the zeta function in general to computing it for affine hypersurfaces.

Example 2.1. You can write $\mathbb{P}^n$ as a union of affine spaces in the standard way.

Remark 2.2. This is similar to how Dwork originally attacked the rationality problem, except that Dwork originally reduced to a hypersurface of a torus.

Question. Fix a positive integer n. Is there an algorithm that, given $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ of degree d returns the rational function $\zeta(X, T)$ for $X = \operatorname{Spec} \mathbb{F}_q[x_1, \ldots, x_n]/(f)$ in time $\operatorname{poly}(d, \log q)$?

This is open. Some special cases are known. The earliest methods are based on étale cohomology. In principle, one can compute $\zeta(X, T)$ by computing the action of Frobenius on mod ℓ cohomology for a few small primes ℓ.

Theorem 2.3 (Schoof 1985; Pila 1990)**.** *Fix a positive integer d. There is an algorithm which, for $f \in \mathbb{F}_q[x_1, x_2]$ of degree d, returns the rational function $\zeta(X, T)$ for $X = \operatorname{Spec} \mathbb{F}_q[x_1, x_2]/(f)$ in time poly$(\log q)$.*

Schoof's original work is practical for cryptographers, e.g. $q = 2^{100}$. Pila's is worse, but maybe works for genus 2. At lower scales, such as used by number theorists, other methods are competitive.

The dependence on d is horrible: it's worse than exponential.

Theorem 2.4 (Lauder-Wan, 2000-2008)**.** *Fix a positive integer n. There is an algorithm which, for $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ of degree d, returns the rational function $\zeta(X, T)$ for $X = \operatorname{Spec} \mathbb{F}_q[x_1, \ldots, x_n]/(f)$ in time poly$(d, p, \log_p q)$.*

Remark 2.5. This is bad if p is huge (it's exponential in that input argument).

The approach is by transcribing Dwork's proof of rationality. However, the resulting algorithm has not been made practical.

However, Dwork's approach was later adapted in a p-adic Weil cohomology theory bearing a more formal resemblance to étale cohomology, and also yielding more effective computation methods. This is work of Kedlaya, Lauder, Denef, ...

We will restrict our discussion to the case where X is a curve. In this case, there are important links to Coleman's theory of p-adic abelian integrals, Chabauty-Coleman, and non-abelian Chabauty.

3. p-adic cohomology for curves

Let X be a curve of genus g over $\mathbb{F}_q$. Lift X to a smooth proper curve $\widetilde{X}$ over $\mathbb{Z}_q$ (this is possible e.g. because the moduli stack of curves is smooth). The p-adic cohomology of X "is" the algebraic de Rham cohomology of the generic fiber $\widetilde{X}_{\mathbb{Q}}$. The important part is H^1, which sits in an exact sequence

$$0 \to H^0(\widetilde{X}_{\mathbb{Q}}, \Omega) \to H^1_{\mathrm{dR}}(\widetilde{X}_{\mathbb{Q}}, \mathbb{Q}_q) \to H^1(\widetilde{X}_{\mathbb{Q}}, \mathcal{O}) \to 0.$$

As in the classical theory of Rieman surfaces, elements of H^1_{dR} can be represented by certain meromorphic differential forms. There is a canonical endomorphism Frob_q of H^1_{dR} such that

$$\zeta(X,T) = \frac{\det(1 - T\,\mathrm{Frob}_q, H^1_{\mathrm{dR}})}{(1-T)(1-qT)}.$$

One way to produce Frob_q is using *crystalline cohomology* (Grothendieck's preferred approach). This is by Grothendieck's typical abstract approach - he defines a "crystalline site," etc. However, from this interpretation it is not straightforward to cmotue the matrix action of Frob_q on a basis.

3.1. **Rigid analytic space.** By rigid GAGA, $H^1_{\mathrm{dR}}(\widetilde{X}_{\mathbb{Q}}, \mathbb{Q}_q)$ is also the de Rham cohomology of the rigid analytification Y of $\widetilde{X}_{\mathbb{Q}}$. There is a reduction map $\mathrm{red}\colon Y \to X$ whose inverse images are open residue discs.

Definition 3.1. A *wide open* subset of Y is an open subset consisting of the complement of a (non-empty) finite union of closed discs, each contained in a residue disc.

3.2. **Monsky-Washnitzer Frobenius action.** In general, there does not exist an automorphism of $\widetilde{X}_{\mathbb{Q}}$ (or Y) lifting the q-power Frobenius automorphism of X.

However, for any open affine subspace U of X, there exist wide open subset V_1, V_2 of Y with $f(Y - V_i) = X - U$ and an isomorphism $\varphi\colon V_1 \to V_2$ lifting Frobenius.

Theorem 3.2 (Monsky-Washnitzer, 1971)**.** *Via the canonical isomprhism $H^1_{\mathrm{dR}}(V_1) \cong H^1_{\mathrm{dR}}(V_2)$, we have*

$$\zeta(U,T) = \frac{\det(1 - q\varphi^{-1}T, H^1_{\mathrm{dR}}(V_1))}{1-qT}.$$

Computing the zeta function of U is basically equivalent to computing the zeta function of X, up to a finite number of Euler factors.

3.3. **A p-adic framework for computing ζ.**

(1) Choose $\widetilde{X}$ lifting X.
(2) Choose the open subset U, wide open V, and isomorphism φ. (If $q \neq p$, one can lift p-power Frobnenius and iterate. This is how you get the $\log_p q$ runtime. Henceforth we ignore this issue.)
(3) Apply φ to 1-forms representing a basis of $H^1_{\mathrm{dR}}(V)$.
(4) Use known relations in $H^1_{\mathrm{dR}}(V)$ to write result of Frobenius pullback as exact 1-forms plus $\mathbb{Q}_q$-linear combinations of basis vectors.
(5) Since we know essentially have the matrix of φ, we may recover $\zeta(U,T)$ from the characteristic polynomial of φ on $H^1_{\mathrm{dR}}(V)$.

Note that the characteristic polynomial has coefficients in $\mathbb{Z}$, but we compute it over $\mathbb{Q}_q$. This involves inexact (truncated) arithmetic, analogous to floating-point arithmetic for $\mathbb{R}$. Similarly, since V is a wide open its holomorphic functions are infinite power series, so you truncate here as well.

3.4. **Example.** (Kedlaya, 2001) Suppose $p \neq 2$ and X is a hyperelliptic curve of the form $y^2 = P(x)$ where $\deg P(x) = 2g+1$, lifted to $y^2 = \widetilde{P}(x)$ where $\widetilde{P}(x) = 2g+1$ (it's espcially easy to lift since the curve is hyperelliptic). Let $U \subset X$ be the set where y is invertible - so we're throwing out the point at infinity as well as the finite Weierstrass points. Then $H^1_{\mathrm{dR}}(V)$ admits a basis consisting of $x^i dx/y$ for $0 \leq i \leq 2g-1$ and $x^j dx/y^2$ for $0 \leq j \leq 2g$. These span the -1 and $+1$ (respectively) eigenspaces $H^1_{\mathrm{dR}}(V)^{mp}$ for $y \mapsto -y$, and it turns out that the -1 eigenspace spans $H^1_{\mathrm{dR}}(Y)$ so we focus on that.

We may take φ to sends $x \mapsto x^q$ and $y \mapsto y^q(\widetilde{P}(x^q)/\widetilde{P}(x)^q)^{-1/2}$ (computed by e.g. a binomial series). You can perform calculations in $H^1_{\mathrm{dR}}(V)$ systematically, e.g. there are explicit relations convering $Q(x)dx/y^{2n+1}$ into $R(x)dx/y^{2n-1}$ (we omit technicalities, but remark that this is easy using the fact that P, P' have resultant 1).

Remark 3.3. The infinite series expansion for $\varphi(y)$ requires careful truncation both p-adically and x-adically.

4. Coleman integration

Coleman defined path integrals $\int_P^Q \omega$ for any meromorphic differential ω on a wide open subset $V \subset Y$ and any P, Q which are not poles of ω. This is easy if P, Q lie in a single residue disc, because ω admits an analytic antiderivative F on the disc, so we can simply define

$$\int_P^Q \omega = F(Q) - F(P).$$

Coleman figured out how to make this work if F is only locally analytic on U. The problem is that there is a different"constant of integration" for each disc - how do you make coherent choices for all of them?

The key was the idea of "analytic continuation along Frobenius," pioneered by Dwork. This was done by Coleman in 1981. In 2007 at Banff, Robert and I resolved it in a different way. We were discussing how to develop an algorithm to effectively compute Coleman integrals. It turns out that you can do it easily with a slight modification of his original construction!

The key property of Coleman integrals is that they satisfy a change of variables formula for lift of Frobenius:

$$\int_P^Q \varphi^*(\omega) = \int_{\varphi(P)}^{\varphi(Q)} \omega.$$

Coleman used this originally by applying $R(\varphi)$ where R is the characteristic polynomial of φ on $H^1_{\mathrm{dR}}(U)$. By Cayley-Hamilton, $R(\varphi^*)(\omega)$ is exact, hence has an analytic primitive. If you take a basis $\omega_1, \dots, \omega_n$ of $H^1_{\mathrm{dR}}(U)$, then the Monsky-Washnitzer computation gave us

$$\varphi^*(\omega_j) = \sum_i A_{ij}\omega_i + df_j$$

in which we previously we discarded f_j and retained A_{ij}. Then

$$\int_P^Q \varphi^*(\omega_j) = \int_{\varphi(P)}^{\varphi(Q)} \omega_j = \sum_i A_{ij} \int_P^Q \omega_i + f_j(Q) - f_j(P).$$

But writing $\int_{\varphi(P)}^{\varphi(Q)} = \int_{\varphi(P)}^{P} + \int_P^Q + \int_Q^{\varphi(Q)}$ (recalling the integration within residue disc is easy!) we end up with

$$(A - 1)^{-1}(\text{vector of } \int_P^Q \omega_i) = (\text{computable vector})$$

Since A has no eigenvalues equal to 1 by Weil (we've assumed good reduction!), this pins down all the constants of integration.

For hyperelliptic curves, this strategy was implemented by Jennifer Balakrishnan in her PhD thesis (based on work of Robert Bradshaw at the 2007 Arizona Winter School). Balakrishnan and Tuitman are currently extending this to more general curves (even arbitrary curves of good reduction). This should make it routine to compute the integrals arising in Chabauty-Coleman method. Previously indirect methods were used - using additivity and the arithmetic of the Jacobian to reduce to a single disc. Moreover, you can used *iterated Coleman integrals* arising in Kim's non-abelian Chabauty method.

P-ADIC METHODS AND CLASS FIELDS OF REAL QUADRATIC FIELDS

HENRI DARMON

The theme is the explicit construction of class fields of real quadratic fields. This is a joint work with Alan Lauder and Victor Rotger, and but also of earlier work with Samit Dasgputa.

1. Introduction

1.1. **Explicit class field theory.** The story starts with the theorem of Kronecker-Weber that all abelian extensions of $\mathbb{Q}$ can be generated by roots of unity:

Over quadratic imaginary fields, there is a similar story by which abelian extension can be explicitly constructed using ellilptic curves with complex multiplication, and specifically their j-value and torsion points.

Hilbert's 12th problem asks about explicit class field theory in general: is it possible to generate class fields of other number fields from values of concrete transcendental functions at explicit arguments?

So there is a satisfying answer for $K = \mathbb{Q}$ or a quadratic imaginary extension. The "first" case where this is open is that of real quadratic fields.

1.2. **Stark's conjecture.** Let K be a real quadratic field and

$$\psi\colon\ \mathrm{Gal}(H/K) \to L^\times \subset \mathbb{C}^\times$$

a character of mixed signature (i.e. -1 on one real embedding and $+1$ on the other).

Conjecture 1.1 (Stark)**.** *The L-function $L(K, \psi, s)$ has a simple zero at $s = 0$ and*

$$L'(K, \psi, 0) = \log |u_\psi|$$

where $u_\psi \in (\mathcal{O}_H^\times \otimes L)^\psi$.

Thus one can construct explicit units in H by exponentiating values of $L'(K, \psi, 0)$. This leads to many concrete computations of explicit class fields. In fact, this approach is used by many computer packages. The drawbacks:

(1) Stark's conjecture is open, and
(2) (more subjectively) there is not a very strong analogy with the theory of singular moduli.

1.3. **Fourier coefficients of modular forms.** The idea of Bill Duke and Yingkun Li was that the Fourier coefficients of "mock modular forms" of weight one involve logarithms of algebraic numbers belonging to interesting class fields.

The goals of this lecture:

(1) describe this idea, and
(2) propose a p-adic variant which is better suited than archimedean counterpart for explicit class field theory for real quadratic fields.

2. Weak harmonic Maass forms

Definition 2.1. A *weak harmonic Maass form* of weight k, level N, and character $\chi\colon (\mathbb{Z}/N)^\times \to \mathbb{C}^\times$ is a real analytic function $f\colon \mathbb{H} \to \mathbb{C}$ satisfying

(1) the usual modular transformation property,
(2) linear exponential growth at cusps,
(3) $\Delta_k F = 0$ where Δ_k is the weight k hyperbolic Laplacian.

The hyperbolic Laplacian Δ_k factors as $\delta_k = \xi_{2-k} \circ \xi_k$ where ξ_k is some "lowering operator." This sends weak harmonic Maass forms of weight k to holomrphic cusp form of weight $2-k$. So we get an exact sequence:

$$0 \to M_k^! \to H_k \xrightarrow{\xi_k} S_{2-k} \to 0.$$

The kernel is the space of "weakly holomorphic modular form of weight k," poles at cusps (and in particular is infinite dimensional). This is usually applied with k being small or negative. In our application, $k = 1$.

2.1. **Fourier expansion.** A wakly harmonic Mass form F has Fourier expansion

$$F(z) = \underbrace{\sum_{n \geq n_0} c^+(n) q^n}_{\text{holomorphic}} - \underbrace{\sum_{n>0} c(n)\beta_k(n,y) q^{-n}}_{\text{non-holomorphic}}.$$

The $c(n)$ of the non-holomorphic part are just the Fourier coefficients of $f(z) := \sum c(n) q^n$. The "holomrphic part" $c^+(n)$ is more subtle and interesting.

Definition 2.2. A *mock modular form* is the holomorphic part of the weak harmonic Maass form (denoted $\sum c^+(n) q^n$ above).

Definition 2.3. If $\widetilde{f}$ is the holomorphic part of a weakly harmonic Maass form F, then the cusp form $f := \xi_k F$ is called the *shadow* of $\widetilde{f}$.

It's important to observe that a cusp form can be the shadow of different mock modular forms. Any two mock modular forms with the same shadow differ by a classical weakly holomorphic modular form.

Philosphy. Fourier expansion of mock modular forms encodes generating series of interesting arithmetic functions.

2.2. **The work of Duke-Li.** Let H be Hilbert class field of $K = \mathbb{Q}(\sqrt{-p})$ with $p \equiv 3 \pmod 4$. Let ψ be a class group character, and θ_ψ the associated theta series (modular of weight 1). We are interested in mock modular form whose shadow is θ_ψ.

Theorem 2.4 (Duke, Li)**.** *There exists a mock modular form $\widetilde{\theta}_\psi$ with shadow θ_ψ, for which we have (certain normalizing conditions) and the coefficients $c^+_\psi(n)$ are logarithms of $u(n)$ algebraic numbers in H (units when $n < 0$).*

Similar results were obtained more or less simultaneously by Ehlen and Viazovska, by different methods. A common feature of all three works is that the coefficients $c^+_\psi(n)$ are related to traces of singular moduli, so the theory of complex multiplication play an essential role in the proofs.

However, the statement itself certainly doesn't need complex multiplication! This suggests that we can generalize it! Let f be any classical newform of weight 1 associated to odd, irreducible, two-dimensional Artin representation *not* induced from quadratic imaginary.

Conjecture 2.5. *There is a mock modular form $\widetilde{f}$ whose Fourier coefficients are simple linear combinations with algebraic coefficients of logarithms of algebraic numbers in H, lying in the field cut out by the adjoint (ρ_f).*

There is some experimental evidence in the paper of Duke and Li, for a certain octahedral modular form.

Let K be a real quadratic field and $\psi\colon G_K \to \mathbb{C}^\times$ any character of mixed signature. Let $\theta_\psi \in S_1(N,\chi)$ be Hecke's theta series of weight one attached to ψ, and $c^+_\psi(n)$ the nth Fourier coefficient of $\widetilde{\theta}_\psi$.

Conjecture 2.6 (Yingkun Li)**.** *For all rational primes ℓ, the real and imaginary parts of $c^+_\psi(\ell)$ are logarithms of elements of $\mathcal{O}_K[1/\ell]^\times_1$.*

Li proves this in several settings, by relating the $c^+_\psi(\ell)$ to certain traces of singular moduli, on the HIlbert moduli surface attached to K.

Remark 2.7. It is disappointing that the coefficients describe things living in K, not the class field H, as that means the Fourier coefficients of $\widetilde{\theta}_\psi$ don't contain interesting information about H.

3. p-ADIC METHODS

Now I want to discuss the possibility of transposing this to the p-adic setting. There are several advantages there:

(1) analogues of Stark's conjecture are more tractable,
(2) the p-adic world allows for aesthetically pleasing parallels with the classical theory of singular moduli, in the setting of real quadratic fields,
(3) a natural p-adic analogue of the Duke-Li theorem does lead to non-trivial class invariants in ring class fields of real quadratic fields.

3.1. **Gross-Stark conjecture.** The p-adic analogue of Stark's conjecture:

Conjecture 3.1 (Gross)**.** *Let $\chi\colon \mathrm{Gal}(H/F) \to L^\times$ be a totally odd character of a totally real field F, and suppose $\chi(\mathfrak{p}) = 1$ on a single prime $\mathfrak{p}$ of F above p. Then there exists $u_\chi \in (\mathcal{O}_H[1/p])^\times \otimes L)^\chi$ satisfying*

$$L_p'(F,\chi,0) \sim \log_p \mathrm{Nm}_{F_p/\mathbb{Q}_p}(u_\chi).$$

Dasgupta, Pollack, Darmon, plus work of Ventulla (2011) proved this.
♠♠♠ TONY: [what about a more general version?]

The proof uses p-adic deformations and congruences with families of Eisenstein series, following the pioneering approach of Ribet and Mazur-Wiles.

3.2. **Singular moduli.** Let K be a quadratic imaginary field and $\tau \in \mathbb{H} \cap K$. Then one can associate the order

$$\mathcal{O}_\tau = \{\alpha \in \mathbb{C} \mid \alpha(\mathbb{Z} + \mathbb{Z}\tau) \subset \mathbb{Z} + \mathbb{Z}\tau\}.$$

This is an order in an imaginary quadratic field, and the ring class field H_τ is an extension of K with $\mathrm{Gal}(H_\tau/K) = \mathrm{Pic}(\mathcal{O}_\tau)$. The theory of complex multiplication tells us that the singular modulus $j(\tau)$ generates ring class field H_τ.

One can replace j by any rational function the j-line, or even on $X_1(N)$. We would like to extend this to real quadratic fields.

3.3. **Dasgupta's thesis.** The goal of Samit's thesis was to extend this theory of singular moduli to ring class fields of real quadratic fields. More precisely, his thesis develops a p-adic analytic theory of elliptic units for real quadratic fields.

Let $u \in \mathcal{O}^\times_{Y_0(N)}$ be a modular unit with $u(\infty) = 1$. Then $d\log u = du/u$ is weight two Eisenstein series, and

$$u(\tau) = \exp\left(\int_{i\infty}^{\tau} du/u\right).$$

We can write this in a very roundabout way as an integral over the boundary of a cycle:

$$= \exp\left(\int_{\partial^{-1}(\tau - i\infty)} E_2\right).$$

This may be seem contrived, but it is useful for understanding parallels with the formulas in Samit's thesis. His thesis works in one dimension higher: he studies cycles of real dimension 1 on a two-dimensional symmetric space.

3.4. **Mock hilbert modular surfaces.** The p-adic Poincaré upper half plane is $\mathbb{H}_p := \mathbb{C}_p - \mathbb{Q}_p$. ♠♠♠ TONY: [why?!] We also define the "congruence subgroup"

$$\Gamma_p(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}[1/p]) \colon N \mid c \right\}.$$

The group $\Gamma_p(N)$ acts discretely on $\mathbb{H}_p \times \mathbb{H}$ (the second factor is the usual upper half plane). The quotient can be thought of as "mock" (in a sense unrelated to the "mock" of "mock modular forms") modular surface.

Let p be a prime *inert* in a real quadratic K, so that $\mathbb{H}_p \cap K$ is non-empty. Let γ_τ be a generator for stabilizer of τ in $\Gamma_p(N)$.

To each $\tau \in H \cap K$, we can associate the cycle

$$Z_\tau := \{\tau\} \times (\text{geodesic from } x \text{ to } \gamma_\tau x) \subset \Gamma_p(N) \backslash (\mathbb{H}_p \times \mathbb{H}).$$

This is a cycle of real dimension one on the mock Hilbert modular surface. You want to think of it as being nullhomologous, like the zero cycle $\tau - i\infty$ in the CM theory.

Then Samit defines a Coleman-style p-adic integration theory on $\mathbb{H}_p \times \mathbb{H}$, whereby the classical Eisenstein series du/u is parlayed into a "mock Hilbert modular Eisenstein series" $E_2^{(p)}$ on $\mathbb{H}_p \times \mathbb{H}$ of parallel weight 2. This is not quite a function in reality, but you can at least make enough sense of it to talk about its periods. Then define an integral

$$u_p(\tau) = \exp_p \left(\int_{\partial^{-1} Z_r} E_2^{(p)} \right).$$

These formulas convey spirit of the construction, but it can be made concrete and rigorous.

Conjecture 3.2. *The p-adic number $u_p(\tau)$ is a global p-unit in $O_{H_\tau}[1/p]^\times$, and behaves exactly like elliptic units $u(\tau)$ attached to quadratic imaginary τ.*

Theorem 3.3. *This conjecture is compatible with Gross-Stark conjecture for totally odd ring class characters, and in fact is a non-trivial refinement of it.*

Although we proved Gross-Stark, this conjecture remains open.

3.5. **A Duke-Li style conjecture.** Let p be a prime splitting in real quadratic K.

Conjecture 3.4 (Darmon-Lauder-Rotger)**.** *There exists an overconvergent p-adic modular form g_τ of weight one satisfying, for all primes ℓ inert in K,*

$$a_\ell(g_\tau) \sim_{\mathbb{Q}^\times} \log_p u_\ell(\tau)$$

for suitable $u_\ell(\tau) \in \mathbb{Q}_{\ell^2}$.

There is good experimental confirmation.

This conjecture suggests that ring class invariants of real quadratic fields can be packaged into modular generating series, after replacing mock modular forms by p-adic modular forms.

Note that the Gross-Stark conjectures involves p-adic logarithms of p-adic units, while this involves p-adic logarithms of ℓ-adic units.

3.6. **A p-adic Duke-Li theorem.** Let ψ be a totally odd ring class character of K.

Lemma 3.5 (Tate)**.** *There is a ray class character ψ_0 of K of mixed signature, satisfying $\psi_0/\psi_0' = \psi$ (where ψ_0' is the conjugate of ψ') and hence*

$$\mathrm{Ad}(\mathrm{Ind}_K^{\mathbb{Q}} \psi_0) = \mathrm{Ind}_K^{\mathbb{Q}} \psi \oplus 1 \oplus \chi_K.$$

♠♠♠ TONY: [unwind the equivalence]

The p-adic counterpart of a mock modular form $\widetilde{\theta}_{\psi_0}$ whose shadow is θ_{ψ_0} is an overconvergent generalized eigenform attached to θ_{ψ_0}. Here the meaning of "overconverent" is as usual, and "generalized eigenform" is in the sense of "generalized eigenvetor."

Assume that θ_{ψ_0} is regular at a prime p, i.e. has p-stabilizations with distinct p-eigenvalues of U_p. Replacing by a p-stabilization, we can assume that

$$U_p \theta_{\psi_0} = \alpha \theta_{\psi_0}.$$

Theorem 3.6 (Cho-Vatsal, Bellaiche-Dimitrov, Adel Betina)**.** *The Coleman-Mazur eigencurve is smooth at the classical weight one point x_{ψ_0} attached to θ_{ψ_0}, but it is not étale above weight space at this point.*

♠♠♠ TONY: [picture: there is ramification at the point.]

Proof. Both tangent space and relative tangent space of the fiber above wiehgt 1 at x_{ψ_0} are one-dimensional. The proof uses the fact that the three irreducible constituents $\mathrm{Ad}(\mathrm{Ind}_K^{\mathbb{Q}} \psi_0)$ occurs with multiplicities $(0, 1, 0)$ in $O_H^\times \otimes \mathbb{C}$, i.e. units are concentrated χ_K.

This is the same thing that prevented Duke-Li from getting interesting units in class fields!

□

The result should be thought of as a positive one, as it's telling us about the existence of an interesting non-classical modular form. Hence:

Corollary 3.7. *The natural inclusion*

$$M_1^{p,oc}(N,\chi)[\theta_{\psi_0}] \hookrightarrow M_1^{p,oc}(N,\chi)[[\theta_{\psi_0}]]$$

is not surjective.

Hecke doesn't act semisimply on $M_1^{p,oc}(N,\chi)[[\theta_{\psi_0}]]$.

Definition 3.8. A modular form $\theta'_{\psi_0} = 0$ in $M_1^{p,oc}(N,\chi)[[\theta_{\psi_0}]]$ which is not classical (i..e. not an eigenvector) is called an *overconvergent generalized eigenform*. This is said to be *normalized* if $a_1(\theta'_{\psi_0}) = 0$ (since we can add any multiple of an honest eigenvector with this eigenavlue).

Remark 3.9. We don't need that the generalized eigenspace is 2-dimensional in order to make this normalization.

Theorem 3.10 (Darmon-Lauder-Rotger)**.** *The normalized generalized eigenform θ'_{ψ_0} attached to θ_{ψ_0} can be scaled in such a way that for all primes $\ell \nmid N$ with $\chi_K(\ell) = -1$,*

$$a_\ell(\theta'_{\psi_0}) \sim_{L^\times} \log_p u_\ell(\psi)$$

where u_ℓ has some explicit description, and is a unit.

♠♠♠ TONY: [there is also some formula for a_ℓ which I couldn't copy down]

Remark 3.11. The techniques in [DLR] are fundamentally p-adic in nature, relying only on p-adic deformations and some simple class field theory for H. In particular, the theory of CM or singular moduli plays no role in [DLR].

Also, we note that [DLR] is only 9 pages long (with 6 page intro) and handles essentially all ψ_0, while the archimedean stuff is really involved - this is why Duke-Li handles only the special case of unramified characters of quadratic imaginary fields of prime discriminant.

You might thus be skeptical that there is a convincing analogy between mock modular forms in archimedean world and overconvergent p-adic modular forms. To convince you, we remind you of a classical result:

Theorem 3.12 (Kudla-Rapoport-Yang)**.** *Let χ be an odd Dirichlet character of prime conductor N and $E_1(1,\chi)$ the associated weight one Eisenstein series. For all $n \geq 2$ with* $\gcd(n,N) = 1$,

$$a_n(\widetilde{E}_1(1,\chi)) \sim_{L^\times} \frac{1}{2}\sum_{\ell|n} \log \ell \cdot (\mathrm{ord}_\ell(n)+1) \cdot a_{n/\ell}(E_1(1,\chi)).$$

Compare with our formula [RLD] for the Fourier coefficients - there is a strong similarity! ♠♠♠ TONY: [Unfortunately, this is the formula that I didn't write down...]

The phenomena described in [DLR] can be viewed as a fragment of a "p-adic Kudla program."

THETA OPERATORS ON PICARD MODULAR SURFACES AT AN INERT PRIME

EHUD DE SHALIT

This is joint work with Eyal Goren.

1. Classical theta operators

The theta operator is a formal operator on q series

$$\theta = q\frac{d}{dq}: \sum a_n q^n \mapsto \sum n a_n q^n.$$

If you think in terms of Dirichlet series, this effects a shift in s, which is like a Tate twist.

If $q = e^{2\pi i z}$, this is essentially differentiation by z. Ramanujan observed that this destroys modularity. However, it can be corrected if you sacrifice holomorphicity. More precisely, Maass found that if $\partial = \frac{1}{2\pi i}\left(\frac{\partial}{\partial z} + \frac{k}{z-\bar{z}}\right)$ then ∂ induces

$$M_k^\infty(\Gamma, \mathbb{C}) \to M_{k+2}^\infty(\Gamma, \mathbb{C}).$$

One wants to extend this to negative weights k. Shimura knew that if you iterated this k times going from $-k$ to k, then you actually preserve holomorphicity, even though the intermediate steps do not. This plays a significant role in Borcherds' theory, and the p-adic shadow appears later in Coleman's work.

There is a theory of *Maass-Shimura operators*, which has arithmetic significance even though these are only C^∞ operators.

2. The p-adic theory

That's the story over $\mathbb{C}$. The p-adic one is much better behaved. Swinnerton-Dyer and Serre (1972) proved that for $p \geq 5$ and level 1, there is an operator

$$\theta: M_k(\Gamma, \overline{\mathbb{F}_p}) \to M_{k+p+1}(\Gamma, \overline{\mathbb{F}_p})$$

(note that the shift in weight is $2 + p - 1$, the $p - 1$ being the weight of the Hasse invariant). This is done at the level of q expansion.

Katz (1975) gave a general geometric interpretation of this. Let

- $X = X(N)$ be the open modular cuve,
- $A \xrightarrow{\pi} X$ the universal elliptic curve,
- $\omega := \omega_{A/X} \subset R^1\pi_*\Omega^\bullet_{A/X} =: D$.

Suppose $D = \omega + U$ as $\mathcal{O}_X$-modules. Then we have maps

$$\begin{array}{ccc} \omega^k & \longrightarrow & \mathrm{Sym}^k D \\ & & \downarrow{\scriptstyle \Delta \text{ Gauss-Manin}} \\ & & \mathrm{Sym}^k D \otimes \Omega^1_X \\ & & \downarrow{\scriptstyle \cong \text{ Kodaira-Spencer}} \\ & & \mathrm{Sym}^k D \otimes \omega^2 = \omega^{k+2} \oplus \dots \\ & & \downarrow{\scriptstyle \text{projection}} \\ & & \omega^{k+2} \end{array}$$

Over $\mathbb{C}$, we know that $U = \overline{\omega}$ (by the C^∞ Hodge decomp), which gives Maass-Shimura operators.

Over $\overline{\mathbb{F}_p}$, we know Frob* exists if you remove the supersingular points. We can then take $U = \mathrm{Frob}^*(D^{(p)})$, the "unit root space."

You can use this U to make $\theta\colon H^0(X^{\mathrm{ord}}, \omega^k) \to H^0(X^{\mathrm{ord}}, \omega^{k+2})$ with simple poles at X^{ss}. This is only on the ordinary locus, with poles at the supersingular locus, so you multiply by the Hasse invariant $h \in H^0(X, \omega^{p-1})$ to kill the poles on the supersingular locus, and get an operator

$$\Theta := h \circ \theta\colon H^0(X, \omega^k) \to H^0(X, \omega^{k+p+1}).$$

This has the property that on q-expansions, "$\theta = \Theta$."

This has relations to Galois representations and congruence between modular forms: see Swinnerton-Dyer and Serre on Ramanujan congruences, and Gross' theory of companion forms.

I want to explain Robert's use of this. One of his famous results is that "Overconvergent modular forms of small slope are classical." We can think of "small" as meaning that the slope is at most $k + 1$.

Key points. Although θ preserves p-adic modular forms (in the sense of Serre), it doesn't preserve overconvergent modular forms. However:

(1) We have $\theta^{k+1}\colon M^{oc}_{-k} \to M^{oc}_{k+2}$ (i.e. a power of θ *does* preserve overconvergent forms). This is geometric: analyze Gauss-Manin connection on the crystal/local system from Sym^k of the de Rham cohomology. [A $\mathbb{C}$ version of this was known by Shimura]

(2) The cokernel of θ^{k+1} above is filled out by classical forms. Moreover, for a slope $\alpha < k + 1$ this implies that

$$M_{k+2,\alpha} = \theta^{k+1}(M^{oc}_{-k})_\alpha \oplus (\mathrm{Classical})_\alpha.$$

Looking at the q-expansion of a U_p-eigenform $f = \sum a_n q^n$, then one finds: $a_{np} = \lambda a_n$ for $\mathrm{ord}_p \lambda = \alpha$. Also, one has an estimate

$a_{np^r} = O(p^{r(k+1)})$. Combining these, we find that if $\mathrm{ord}_p \lambda$ is too small, then that incompatibility forces $f = 0$, which implies that on this part everything is classical.

There are more power modern arguments, but that was Robert's proof.

3. Picard modular surfaces

Let E be a quadratic imaginary field, $V = E^3$. We have a hermitian structure on V given by

$$(u, v) = {}^t\overline{u}\begin{pmatrix} & & 1 \\ & 1 & \\ 1 & & \end{pmatrix} v$$

which has signature $(2, 1)$. Then the group $\underline{G} = GU(V, (-,-))/\mathbb{Q}$ of general linear similitudes on V is quasi-split. It is known that $G_\infty = \underline{G}(\mathbb{R})$ acts on $\mathcal{X}$, the unit ball in $\mathbb{C}^2$. If x_0 is the center, then $K_\infty = \mathrm{Stab}(x_0)$ and $K_f \subset \underline{G}(\mathbb{A}_f)$ is principal level subgroup of level $N \geq 3$.

The theory of Shimura varieties gives a canonical model S_E/E (E the reflex field) such that

$$S_E(\mathbb{C}) = \underline{G}(\mathbb{Q})\backslash\underline{G}(\mathbb{A})/K_\infty K_f \cong \bigcup_{1\leq j\leq n} \Gamma_j\backslash X.$$

Even better, this has a smooth integral model S/R_0 where $R_0 = \mathcal{O}_E[1/2ND_E]$ (N is the level and D_E is the discriminant of E).This has a smooth arithmetic compactification $\overline{S}/R_0$, worked out by Larsen, Bellaïche, Lan.

What's important for us is that this solves the moduli problem:

> Classify $\underline{A} = (A, \lambda, \iota, \alpha)/(R/R_0)$ where
> - A is an abelian 3-fold,
> - $\lambda\colon A \to \widehat{A}$ is a principal polarization,
> - $\iota\colon \mathcal{O}_E \hookrightarrow \mathrm{End}_R(A)$ is an inclusion with $\mathrm{Rosati}_\lambda(a) = \overline{a}$), and
> - $\mathrm{Lie}(A/R)$ is an $\mathcal{O}_E$-module of type $(2, 1)$, α is a level-N structure.

One gets a universal abelian variety $\pi\colon \mathcal{A} \to S$ and semi-abelian variety $\overline{\mathcal{A}} \to \overline{S}$ (the compactification).

From now on, $S := S_{\overline{\mathbb{F}_p}}$ where p is a good inert prime. We study the structure of $S_{\overline{\mathbb{F}_p}}$. There's been a lot of good work recently on Shimura varieties in characteristic p. The key tool is Rapoport-Zink local models. The structure of the special fiber was explained by Voollaard, Wedhorn and others.

There is a dense open set S_μ, the μ-ordinary stratum. Then there are a bunch of reduced curves S_{ss} which is the super-singular locus. The third stratum is S_{ssp} (super special), which just consists of points. The p-divisible group at points $x \in S_\mu, S_{ss}, S_{ssp}$ is described.

Theorem 3.1 (Voollaard)**.** *For $N \geq N_0(p)$, every irreducible component of S_{ss} is the Fermat curve*

$$C : x^{p+1} + y^{p+1} + z^{p+1} = 0.$$

Any two components intersect in at most one pont. Through each point there are $p+1$ branches, and each intersection point is transversal. There are p^3+1 intersection points on each irreducible component. Finally, $S_{ssp} = S_{ss}^{sing}$.

Remark 3.2. The generalization of this is probably in terms of Deligne-Lustzig varieties. The dual graph is related to the Bruhat-Tits building for $\mathrm{GL}_2(\mathbb{Q}_p)$.

Theorem 3.3 (Goren-de Shalit)**.** *The number of irreducible components is*

$$c_2(\overline{S})/3 = \chi_{top}/3.$$

By work of Holzapfel, this is (up to constants) $[\Gamma(1) : \Gamma(N)] \cdot L(\left(\frac{D_E}{\cdot}\right), 3)$.

Remark 3.4. This is independent of p!

Rapoport-Zink gives a parametrization of the irreducible components by certain double cosets. However, to get $c_2(\overline{S})/3$ one needs different ideas: intersection theory, and secondary Hasse invariant (needed to compute certain self-intersections).

4. Hasse invariant

Let $\Sigma, \overline{\Sigma}$ be the two maps $\mathcal{O}_E \to \mathcal{O}_E/p\mathcal{O}_E \subset \overline{\mathbb{F}_p}$. Then

$$\begin{aligned} \omega_{A/S} =: \omega &= \omega(\Sigma) \oplus \omega(\overline{\Sigma}) \\ &= \underbrace{\mathcal{P}}_{\text{rank } 2} \oplus \underbrace{\mathcal{L}}_{\text{rank } 1}. \end{aligned}$$

Then one has $\mathrm{Ver} : \mathcal{A}^{(p)} \to \mathcal{A}$ (the first being the twist of $\mathcal{A}$ by absolute Frobenius) dual to Frobenius, inducing $V : \omega \to \omega^{(p)}$. Because this is not $\mathbb{F}_p$-linear, it exchanges the Σ and $\overline{\Sigma}$ parts:

$$V_{\mathcal{P}} : \mathcal{P} \to \mathcal{L}^{(p)}$$

and

$$V_{\mathcal{L}} : \mathcal{L} \to \mathcal{P}^{(p)}.$$

Then composing gives

$$h_{\overline{\Sigma}} = V_{\mathcal{P}}^{(p)} \circ V_{\mathcal{L}} \in \mathrm{Hom}(\mathcal{L}, \mathcal{L}^{(p^2)}) = \mathrm{Hom}(\mathcal{L}, \mathcal{L}^{\otimes p^2}).$$

The Hasse invariant is the corresponding element of $H^0(\overline{S}, \mathcal{L}^{p^2-1})$, which is $M_{p^2-1}(N; \overline{\mathbb{F}}_p)$.

Proposition 4.1. *(i)* $V_{\mathcal{P}}, V_{\mathcal{L}}$ *are rank* 1 *outside* S_{ss}. *(ii)* $\mathrm{Div}(h_{\overline{\Sigma}}) = S_{ss}$.

Remark 4.2. It content of the second part is that $h_{\overline{\Sigma}}$ has a simple zero on S_{ss}.

That is, the image of $V_{\mathcal{L}}$ is tranverse to the kernel of $V_{\mathcal{P}}$ on the ordinary locus, but they come together on the supersingular locus. The simplicity of the zero is subtle, however.

This has been generalized greatly, to other Shimura varieties.

5. Igusa surfaces of level p

This is a surface Ig_μ equipped with an étale map

$$\begin{array}{c} Ig_\mu \\ \big\downarrow \tau \\ S_\mu \end{array}$$

(1) with étale Galois group $\Delta := (\mathcal{O}_E/p\mathcal{O}_E)^\times$.
(2) classifies $(\underline{A}, \epsilon\colon \mathcal{O}_E \otimes \mu_p \hookrightarrow A[p])$,
(3) can be compactified over S_{ss} to be totally ramified along S_{ss}, normal surface with singularities over S_{ssp}.
(4) It is "relatively irreducible." (inverse image of any connected component irreducible?)
(5) (most importantly) $\tau^*\mathcal{L}$ has a tautological section a, with $a^{p^2-1} = h_{\overline{\Sigma}}$ (supposedly easy to see in characteristic p, didn't catch why).

6. Definition of Θ and Main Theorem

We should say that we were very much motivated by Gross' treatment of the classical theta operator on his paper on the tameness criterion.

We have the Kodaira-Spencer isomorphism

$$KS : \mathcal{P} \otimes \mathcal{L} \xrightarrow{\sim} \Omega^1_S.$$

Over Ig_μ, we have

$$\tau^*(\mathcal{P} \otimes \mathcal{L}) \cong \Omega^1_{Ig_\mu}.$$

The operator Θ goes from $M_k(N, \overline{\mathbb{F}_p}) = H^0(S, \mathcal{L}^k)$ to $M_{k+p+1}(N, \overline{\mathbb{F}_p})$.

The map is defined as follows. For $f \in H^0(S, \mathcal{L}^k)$,

(1) Pull back f via τ to get a $\tau^* f \in H^0(IG_\mu, \tau^*\mathcal{L}^k)$,

(2) Divide by a^k to get $(\tau^* f)/a^k \in H^0(IG_\mu, \mathcal{O})$,
(3) Take the exterior derivative to get $d((\tau^* f)/a^k) \in H^0(IG_\mu, \Omega^1_S)$,
(4) Apply the inverse of KS to get $KS^{-1}(d((\tau^* f)/a^k)) \in \tau^*(\mathcal{P} \otimes \mathcal{L})$,
(5) Apply $V_{\mathcal{P}} \colon \mathcal{P} \otimes \mathcal{L} \to \mathcal{L}^{(p)} \otimes \mathcal{L} \cong \mathcal{L}^{p+1}$,
(6) Multiply by a^k to get

$$a^k \cdot (V_{\mathcal{P}} \otimes 1)((KS)^{-1} d(t^* f/a^k)) \in H^0(IG_\mu, \tau^* \mathcal{L}^{k+p+1})$$

which descends back down to S_μ.

Remark 6.1. The key is the map $V_{\mathcal{P}} \otimes 1$. Since the operator beings by dividing by a^k, it introduces a pole of order k. Differentiation turns this into a pole of order $k+1$, and if you didn't apply $V_{\mathcal{P}} \otimes 1$ then multiplying by a^k at the end leaves a pole. Multiplication by Hasse invariant is buried in $V_{\mathcal{P}} \otimes 1$, which makes this holomorphic again. However, this isn't the only thing- that would be too crude because the Hasse invariant has a zero on S_{ss} of order $p^2 - 1$!

Questions.

(1) What happens over the supersingular locus?
(2) What is the effect on q-expansions?

Theorem 6.2 (Goren-de Shalit)**.**

(1) $\Theta(f)$ *extends holomorphically across* S_{ss}
(2) $\Theta(f)$ *has the effect of "*$q\frac{d}{dq}$*" on Fourier-Jacobi expansions.*
(3) Θ *is a derivation, with image contained in the space of cusp forms.*
(4) Θ *is compatible with classical* Θ *on embedded modular curves.*

Remark 6.3.
(1) The idea to use Igusa is due to D. Gross (in the classical case).
(2) $V_{\mathcal{P}} \otimes 1$ "clears all problems at cusps and along S_{ss}."
(3) There are "arithmetic" Fourier-Jacobi expansions (in two variables: q and theta functions)
(4) Serre and Jochnovitch considered "Theta cycles." By "Fermat's little theorem" $\Theta^p f = \Theta f$. Serre defined a filtration where the weight of a form is the least weight whose reduction gives you that form. Usually the filtration grows by $p+1$ each time you apply Θ, but occasionally it drops (since you have to come back to the starting point eventually). Jochnovitch found that there are exactly two drops: exactly when the weight becomes divisible by p.

Here you get increase by the filtration $p+1$ each time, but to drop you have to divide by Hasse invariant, which has weight $p^2 - 1$. So

there can only be one step where the weight drops. But when? It has nothing to do with the weight being divisible by p.

SOME EXPLICIT COMPUTATIONS ON THE CURVES RELATED TO P-ADIC HODGE THEORY

JEAN-MARC FONTAINE

1. The Fargues-Fontaine curve

1.1. **Preliminaries.**

Definition 1.1. A *complete curve* is a pair $(X, \deg)$ where X is a separated, connected, regular scheme which is noetherian of dimension 1, and $\deg : |X| \to \mathbb{N}_{>0}$ (where $|X|$ is the set of closed points on X) is a map such that $\deg \mathrm{Div}(f) = 0$ for all $f \in k(X)^\times$.

One can check that $H^0(X, \mathcal{O}_X)$ is a field E (the field of definition of X) and E is algebraically closed in $k(X)$, the function field of X.

Example 1.2. A smooth projective curve is complete.

This is what's important for us: given such an X, there is a notion of *degree* for a vector bundle (coming from the degree of a line bundle, which is well-defined by the assumption of completeness). Then one has the notion of a semistable vector bundle of slope λ. Any vector bundle has a Harder-Narasimhan filtration by semistable vector bundles.

Suppose X has a closed point of degree one, denoted ∞. Define $X_e = X \setminus \{\infty\}$. This is an affine scheme Spec B_e, where B_e is Dedekind. There is a natural map $\mathrm{Pic}(X_e) = \mathrm{Pic}(B_e) \to \mathrm{Pic}^0(X)$, sending $[x] \mapsto [x] - (\deg x) \cdot [\infty]$.

1.2. **Review of construction and properties.**

Now fix k an algebraically closed field of characteristic $p > 0$. Consider a pair (E, F) where

- E is a locally compact non-archimedean field, whose residue field $\mathbb{F}_q$ is contained in k.
- $F \supset \mathbb{F}_q$ is a perfect field of characteristic p equipped with a non-trivial absolute value. F is not necessarily complete; a typical example we have in mind is the algebraic closure of a perfectoid field. We suppose $k_F \subset k$.

Think of E and F as having nothing to do with each other. For instance, they may have different characteristics.

From the data (E, F) we construct $X = X_{E,F}$ a complete curve defined over E with $H^0(X, \mathcal{O}_X) = E$.

Properties of $X_{E,F}$.

(1) *(Residue fields)* Let $x \in |X_{E,F}|$ be a closed point.
   (a) If ch $E = p$, then $[k(x) : \widehat{F}] = \deg x$. This is already strange because E is a discrete valuation ring, and $k(x)$ contains an indiscrete valuation ring.
   (b) If ch $E = 0$, then $k(x)$ is a perfectoid field and $[k(x)^\flat : \widehat{F}] = \deg x$.

(2) *(Functoriality)* Let E' be a finite separable extension of E. Then

$$X_{E',F} = E' \otimes_E X_{E,F}.$$

(We are cheating slightly: we need $k_{E'} \subset k$. If this is not the case, then the above is a definition.)

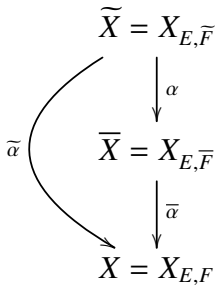
If F' is a finite extension of F (automatically separable because F is perfect), then $X_{E',F'}/X_{E,F}$ is an étale cover. If E'/E and F'/F are both Galois, then this is a Galois covering, and the Galois group $\mathrm{Gal}(E'/E) \times \mathrm{Gal}(F'/F)$.

Choose $\{\overline{x}\}$ a geometric closed point of X. This gives an algebraic closure of E and F. Then we have

$$\pi_1^{\text{ét}}(X, \{\overline{x}\}) = \mathrm{Gal}(E^s/E) \times \mathrm{Gal}(\overline{F}/F).$$

2. An equivalence of categories

2.1. **Galois Descent.** Let $\overline{F}$ be an algebraic closure of F and $\widetilde{F}$ a completion of $\overline{F}$. We have $X = X_{E,F}$ and $\overline{X} = X_{E,\overline{F}}$ with a map $\overline{X} \to X$ (careful though: this is not the limit of the curves constructed from the finite extensions of F). We also have



Then for any coherent $\mathcal{O}_X$-module $\mathcal{V}$, one has maps:

$$\mathcal{V} \to \overline{\alpha}^*\mathcal{V} \to \widetilde{\alpha}^*\mathcal{V}.$$

But there is more data here, because $G_F := \mathrm{Gal}(\overline{F}/F)$ acts on $\overline{X}$ and $\widetilde{X}$. So in fact this induces a functor from the category of coherent $\mathcal{O}_X$-modules to $\mathrm{Rep}_{\mathcal{O}_{\overline{X}}}(G_F)$ to $\mathrm{Rep}_{\mathcal{O}_{\widetilde{X}}}(G_F)$. These are both equivalences of categories.

[We're cheating separately: $\mathcal{O}_X, \mathcal{O}_{\overline{X}}, \mathcal{O}_{\widetilde{X}}$ are considered as sheaves of *topological* rings.]

When you have a field of characteristic 0, there is a way of getting rid of almost all ramification by taking a $\mathbb{Z}_p$ extension. Over a field of characteristic p, there is an even easier way: take the perfection.

2.2. **Classification of vector bundles.** Since we're on a curve, we can consider the category of vector bundles (just the coherent $\mathcal{O}_X$-modules with no torsion).

The main theorem is:

Theorem 2.1. *If $F = \widetilde{F}$ (i.e. F is complete and algebraically closed) then any semistable vector bundle of slope 0 is trivial.*

If V is any finite dimensional E-vector space, then we can form $\mathcal{O}_X \otimes V$, which is a vector bundle on X which is semi-stable of slope 0. The theorem says that this induces an equivalence of categories. The inverse functor is $\mathcal{V} \mapsto H^0(X, \mathcal{V})$.

Combing this with the Galois action, we have an equivalence of categories

$$\mathrm{Rep}_E(G_F) \xrightarrow{\sim} \{\text{semistable vector bundles of slope 0 over } X_{E/F}\}.$$

(This is even an equivalence of Tannakian categories.)

2.3. **Special case.** Choosing $\infty \in |X|$, we have $X_e = \mathrm{Spec}\ B_e$. We had the identification $\mathrm{Pic}(B_e) \cong \mathrm{Pic}^0(X)$. Under the equivalence of categories, we get an identification with Galois representations of dimension 1.

$$\mathrm{Pic}(B_e) \cong G_F^\vee := \mathrm{Hom}_{\mathrm{cont}}(G_F, \mathbb{G}_m).$$

Let I be a non-zero ideal of B_e. This defines a 1-dimensional Galois representation. What is it? We have an inclusion $B_e \subset B_{e,\widetilde{F}}$, and we can extend $I \mapsto IB_{e,\widetilde{F}} = bB_{e,\widetilde{F}}$. Now, $(B_{e,\widetilde{F}})^\times = E^\times$. If $g \in G_F$, then $g(b) = \eta(g)b$ for some $\eta(g) \in E^\times$, and this defines the corresponding character.

Let K be a p-adic field. Suppose $K \subset L \subset \overline{K}$ where L is big enough so that $\widehat{L}$ is a perfectoid field (for instance, it could be obtained by add compatible system of p^n roots of a uniformizer to K).

If $E = \mathbb{Q}_p$, then we take $F = \widetilde{L}^\flat$. We know $G_F = G_L = \mathrm{Gal}(\overline{K}/L)$, then applying this equivalence of categories we see that a representation of G_F is the same as a semistable vector bundle of slope 0 over $X_{E,F}$. If we choose L/K to be Galois and set $\Gamma = \mathrm{Gal}(L/K)$, then Γ acts on $X_{E,F}$ and we get an equivalence of categories between $\mathrm{Rep}(G_K)$ and Γ-equivariant bundles.

Then $B^+_{\mathrm{dR}} = \widehat{\mathcal{O}}_{X,\infty}$. ♠♠♠ TONY: [wow! work this out]

3. Construction of the curve

Let E, F be given. Choose π a uniformizing parameter of E. B is an E-algebra (which is equipped with a topology, but we don't care about that for now) equipped with an automorphism φ. We define

$$X_{E,F} = \mathrm{Proj}(P = \bigoplus_{d\in\mathbb{N}} P^d)$$

where P^d is the eigenspace of B associated to φ:

$$P^d = B_{(\pi^d)} := \{b \in B \mid \varphi(b) = \pi^d b\}.$$

So what is B? There are two cases.

Characteristic p. If ch $E = p$, then B is the ring of rigid analytic functions on

$$D^- := \{c \in \widetilde{F} \mid 0 < |c| < 1\}$$

with coefficients in F. How does E figure into this? The point is that if we view $\pi \in E$ as an indeterminant, then

$$B = \left\{ \sum_{n\in\mathbb{Z}} a_n \pi^n \mid a_n \in F, \forall \rho \in (0,1) : |a_n|\rho^n \to 0 \text{ as } n \to \pm\infty \right\}.$$

Then $E \subset B$ as $\sum_{n\gg-\infty} a_n\pi^n$ for $a_n \in \mathbb{F}_q$.

Characteristic 0. If ch $E = 0$, then we try to mimic the above. We define $\mathbb{A} := O_E \otimes_{W(\mathbb{F}_p)} W(O_F)$, any element of which can be expressed uniquely as $\sum_{n=0}^{\infty} \pi^n[a_n]$ for $a_n \in O_F$ (we are using the usual notation for the Teichmüller lift). We define a ring $B^b = \mathbb{A}[1/\pi, 1/[\varpi]]$ where $\varpi \in \mathfrak{m}_F$ is any non-zero element, so anything in B^b can be uniquely expressed as $\sum_{n\gg-\infty}[a_n]\pi^n$ where $a_n \in F$ and there exists C such that $|a_n| \le C$ for all n.

For any $\rho \in (0,1)$ we can define a norm

$$\left|\sum [a_n]\pi^n\right|_\rho = \sup_{n\in\mathbb{Z}} |a_n|\rho^n.$$

Let B be the completion of B^b for this family of norms.

Then $\varphi(\sum a_n\pi^n) = \sum[a_n^q]\pi^n$.

Remark 3.1. There's something that can go wrong here. If you have $\sum_{n\in\mathbb{Z}}[a_n]\pi^n$ which converges in both direction, you get an element of B, but we don't know (and I don't believe that much) that this expression exists for anything in B, or that this is unique. That is, if ch $E = 0$ then we don't have a canonical expression of $b \in B$ as a $\sum_{n\in\mathbb{Z}}[a_n]\pi^n$.

So F is the coefficient field and E is the field containing the uniformizer. In some cases, we can interchange them.

Definition 3.2. A perfectoid field F of characteristic p is *small* if there exists $u \in F$ such that $k_F(u)^{\mathrm{rad}}$ is dense in F. If this is the case, u can be chosen in $\mathfrak{m}_F$ and then $F = (k_F((u))^{\mathrm{rad}})^{\vee}$.

For all $s \in \mathbb{Z}[1/p]$, we can define z^s to be the Teichmüller lift $[u^s] \in \mathbb{A} \subset B$. Let

$$\Delta^- = \varprojlim (D^- \xrightarrow{x \mapsto x^q} D^- \xrightarrow{x \mapsto x^q} D^- \to \ldots)$$

so any $\delta \in \Delta^-$ has a representation $\delta = (\delta_k)_{k \in \mathbb{N}}$ with $\delta_k \in \widetilde{F}$ and $0 < |\delta_k| < 1$ and $\delta_{k+1}^q = \delta_k$.

We can view B as the ring of analytic functions on Δ^- with coefficients in $K_0 = E \otimes_{W(\mathbb{F}_q)} W[k_F]$. Then any element f can be written uniquely as $\sum_{s \in \mathbb{Z}[1/p]} a_s z^s$ with a condition on the a_s (exercise: describe it) and $f(S) = \sum a_s \delta^s$ where if $s = q^{-k} n$ then $\delta^s = \delta_k^n$.

In the equal characteristic case, $\mathbb{A}^- = D^-$.