Mod ℓ congruences and *p*-adic ramification, in general and for HGMs

David P. Roberts
University of Minnesota, Morris

November 2, 2015

1. Review of curves: good L-factors

Let X be a smooth projective geometrically connected curve over $\mathbb{Q}$ of genus g, with good reduction outside a finite set of primes S.

Then for $p \notin S$, one can count points, to get $|X(\mathbb{F}_p)|$, $|X(\mathbb{F}_{p^2})|$, ...

The first g counts determine the others via

$$|X(\mathbb{F}_{p^k})| = p^k - \left(\alpha_1^k + \cdots + \alpha_{2g}^k\right) + 1,$$

the α_j being algebraic integers with $|\alpha_j| = \sqrt{p}$.

For these good p, define

$$F_p(x) = \prod_{j=1}^{2g}(1 - \alpha_j x) = 1 - a_p x + \cdots + p^g x^{2g}.$$

Then the partial L-function is

$$L_S(X, s) = \prod_{p \notin S} \frac{1}{F_p(p^{-s})}.$$

Review of curves: Galois reps and bad L-factors

Let $M = H^1(X(\mathbb{C}), \mathbb{Z})$ and let $\langle \cdot, \cdot \rangle$ be the symplectic form on M. Let $M_\ell = M \otimes \mathbb{Z}_\ell$. Via étale cohomology, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on each M_ℓ, respecting $\langle \cdot, \cdot \rangle$ up to specified scalars.

Always require $\ell \neq p$. For $p \notin S$, the inertia group $I_p \subset \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts trivially on M_ℓ. For a Frobenius element Fr_p, one has

$$F_p(x) = \det(1 - \mathrm{Fr}_p x | M_\ell).$$

For general p, we can define $F_p(x) = \det(1 - \mathrm{Fr}_p x | M_\ell^{I_p})$, the right side being again independent of ℓ. Similarly, the character of the action of wild inertia P_p on M_ℓ is rational-valued and independent of ℓ, allowing a well-defined Swan conductor $w_p \geq 0$. The conductor of $L(X, s)$ is

$$N = \prod_p p^{t_p + w_p}$$

where $t_p = 2g - \mathrm{degree}(F_p(x))$.

2. Mod ℓ Galois representations

$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on each M/ℓ. A polynomial describing this action is called an ℓ-division polynomial for M.

The good news: even just one of these ℓ-division polynomials contains a lot of information. In particular, it gives lower bounds on the Sato-Tate group of X and it identifies the Swan conductors w_p for $p \neq \ell$.

Example with $\ell = 2$. Let X be given by $y^2 = f(x)$ with $f(x)$ of degree $2g + 1 \geq 5$. Then $f(x)$ is a 2-division polynomial.

- The image of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $M/2$ is $\mathrm{Gal}(f) \subseteq S_{2g+1} \subset Sp_{2g}(\mathbb{F}_2)$. If it is all of S_{2g+1}, then the Sato-Tate group must be all of Sp_{2g}.

- At common good primes p, one has $F_p(x) \stackrel{2}{\equiv} F_p^*(x)$. Here $L^*(s) = \zeta(K, s)/\zeta(s)$ with $K = \mathbb{Q}[x]/f(x)$. If $2g + 1 = p^j$ and p is totally ramified, then $\mathrm{ord}_p(N) = \mathrm{ord}_p(\mathrm{Disc}(K))$.

Mod ℓ Galois representations

There are a few more situations where ℓ-division polynomials are readily accessible. For elliptic curves, the situation is ideal via classical division polynomials. For plane quartics, the 28 bitangents give a 2-division polynomial with generic Galois group $Sp_6(\mathbb{F}_2) \subset S_{28}$.

The bad news: there is no systematic way to pass from a variety X and a prime ℓ to an ℓ-division polynomial for X.

Example at the limit of computation: Let X be given by $y^2 = x^5 + ax^3 + bx^2 + cx + d$. Then a 3-division polynomial is

$$f_{80}(a, b, c, d; x) \;=\; x^{80} + 15120ax^{76} + 2620800bx^{74} + 1670 \text{ terms},$$

with generic Galois group $GSp_4(\mathbb{F}_3) \subset S_{80}$.

To say the bad news again, now with reference to two examples: 5-division polynomials for a generic genus two curve ($PGSp_4(\mathbb{F}_5) \subset S_{156}$) or 3-division polynomials for a generic genus 3 curve ($PGSp_6(\mathbb{F}_3) \subset S_{364}$) seem presently out of reach.

3. Mod ℓ Galois representations for motives

Now let X be a general smooth projective variety and $M \subseteq H^w(X(\mathbb{C}), \mathbb{Z})$ a motive with a $\mathbb{Z}$-structure. Then, as before, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on M/ℓ. The situation is very similar to the situation for curves, modulo some caveats:

• For general X, independence of ℓ of the actions on $H^w(X(\mathbb{C}), \mathbb{Z}_\ell)$ is known at good p, but only expected at bad p (and if this fails all hell breaks loose in our vision of the world).

• For M cut out by non-algebraic projectors, independence of ℓ is not even known at good places.

HGMs are cut out by algebraic projectors. I'll proceed assuming independence of ℓ at the bad places too.

So far, we have been using integrality as a crutch. It suffices to start with just a motive $M \subseteq H^w(X(\mathbb{C}), \mathbb{Q})$. Then we interpret "$M/\ell$" as a semisimple representation, well-defined up to isomorphism.

The ℓ-p principle

Let M and M^* be motives. We write

$$M \stackrel{\ell}{\equiv} M^*$$

if $F_p(x) \stackrel{\ell}{\equiv} F_p^*(x)$ for all common good primes p. Equivalently, $M \stackrel{\ell}{\equiv} M^*$ if the semisimplified representations M/ℓ and M^*/ℓ are isomorphic. We write

$$M \sim_p M^*$$

if P_p acts the same way on M and M^*. In general:

The ℓ-p principle. *If $M \stackrel{\ell}{\equiv} M^*$, then $M \sim_p M^*$ for all primes p different from ℓ.*

The proof is that the characteristic 0 character theory of a p-group agrees with the characteristic ℓ character theory if $\ell \neq p$.

4. HGMs: allowing degenerate defining data

Let

$$\alpha = \{\alpha_1, \dots, \alpha_d\}, \qquad \beta = \{\beta_1, \dots, \beta_d\},$$

be multisets of elements of $\mathbb{Q}/\mathbb{Z}$. Impose the rationality condition that the multiplicity of $r \in \mathbb{Q}/\mathbb{Z}$ in either α or β depends only on $\mathrm{denom}(r)$. Then the monodromy matrices m_α and m_β are in $GL_d(\mathbb{Z})$.

If $\alpha \cap \beta = \emptyset$, one has an irreducible family of motives $H(\alpha, \beta, t)$ indexed by $\mathbb{Q} - \{0, 1\}$. We normalize these motives to have weight $w = \mathrm{mult}_0(\alpha) + \mathrm{mult}_0(\beta) - 1$. The formula for good traces $\mathrm{Tr}(\mathrm{Fr}_p^k | H(\alpha, \beta, t))$ then makes sense even when $\alpha \cap \beta = \gamma$, giving motives

$$H(\alpha, \beta, t) = H(\alpha - \gamma, \beta - \gamma, t) \oplus J(\alpha, \beta, \gamma, t).$$

Here $J(\alpha, \beta, \gamma, t)$ has lower weight and is a simpler motive, a sum of Kummer twists of Jacobi motives.

5. ℓ-p formalism for HGMs

In $\mathbb{Q}/\mathbb{Z} = \prod_p \mathbb{Q}_p/\mathbb{Z}_p$, let

$\alpha \mapsto \alpha_p$ be the projection onto $\mathbb{Q}_p/\mathbb{Z}_p$,
$\alpha \mapsto \alpha^p$ be the projection away from $\mathbb{Q}_p/\mathbb{Z}_p$.

(Thus $\alpha = \alpha_p + \alpha^p$ as in $\frac{23}{30} = \frac{1}{2} + \frac{4}{15}$ for $p = 2$.) Applying these operators to all indices has nice interpretations:

Theorem ℓ. $H(\alpha, \beta, t) \stackrel{\ell}{\equiv} H(\alpha^\ell, \beta^\ell, t)$.
One would expect something like this because the monodromy matrices underlying the left and right sides are *exactly the same matrices* modulo ℓ. The proof is that $\mathrm{Tr}(\mathrm{Fr}_p^k|\cdot)$ yields *exactly the same numbers* when applied to the two sides, by the trace formula.

Corollary p. $H(\alpha, \beta, t) \sim_p H(\alpha_p, \beta_p, t)$.
The proof is to use Theorem ℓ to remove one ℓ at a time until (α, β) becomes (α_p, β_p), applying the ℓ-p principle at every step.

Magma Demonstration

```
H := HypergeometricData;
H1 := H([1/4,1/4,3/4,3/4],[0,0,0,0]);
H2 := H([1/4,1/4,3/4,3/4],[1/5,2/5,3/5,4/5]);
L1 := LSeries(H1,-1: BadPrimes:=[<2,13,1>]);
L2 := LSeries(H2,-1: Precision := 5, Weight01:=-1,
            BadPrimes := [<2,13,1>],  Identify:=false);
E1 := EulerFactor(L1,17); E1;
24137569*x^4 + 58956*x^3 - 442*x^2 + 12*x + 1
E2 := EulerFactor(L2,17); E2;
1/289*y^4 - 1/289*y^3 + 22/289*y^2 - 1/17*y + 1
ChangeRing(E1-E2,FiniteField(5)); 0 (Illustrating Thm ℓ)
CFENew(L1); 0.000000000000000000000000000000 (8 seconds)
Factorization(Conductor(L1)); [<2,13>]
CFENew(L2); 0.00000 (12 seconds)
Factorization(Conductor(L2)); [<2,13>,<5,5>] (Cor p)
```

ℓ-degeneracy is common for HGMs

A common behavior of say symplectic motives is that $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ has image very close to all of $GSp_d(\mathbb{Z}_\ell)$ for all ℓ (in fact universally surjective for elliptic curves 37.a1, 43.a1, ...). For hypergeometric motives, severe degeneracies are common. They are also group-theoretically intelligible in terms of m_α and m_β failing to generate $Sp_d(\mathbb{F}_\ell)$. *Examples:*

• If $\alpha^\ell \cap \beta^\ell = \gamma$, then the main part of the mod ℓ image is typically $Sp_{d-|\gamma|}(\mathbb{F}_\ell)$.

• If there is a part of the form $1/2^j$, then the mod 2 image is inside one of the subgroups $O_d^\pm(\mathbb{F}_2) \subset Sp_d(\mathbb{F}_2)$.

Example. $H(\frac{1}{3}, \frac{2}{3}, \frac{1}{5}, \frac{2}{5}, \frac{3}{5}, \frac{4}{5};\ 0, 0, 0, 0, 0, 0;\ t)$ have typical images involving $O_6^-(\mathbb{F}_2)$, $Sp_4(\mathbb{F}_3)$, and $Sp_2(\mathbb{F}_5)$, before stabilizing to images involving $Sp_6(\mathbb{F}_7)$, $Sp_6(\mathbb{F}_{11})$, ...

6. Explicit ℓ-division polynomials for HGMs

We have 2-division polynomials for all HGMs in degree ≤ 7. E.g. a 2-division polynomial for

$$H\left(\frac{1}{3},\frac{1}{3},\frac{1}{3},\frac{2}{3},\frac{2}{3},\frac{2}{3};\ 0,0,0,0,0,0;\ t\right) \overset{2}{\equiv} \cdots$$

is

$$t2^4x^3(x^2-3)^{12} \quad -3^9(x-2)(x-1)^8(x^2-2x-1)^8$$

with Galois group the "27 lines" group $SO_6^-(\mathbb{F}_2)$. Similarly, a 2-division polynomial for

$$H\left(\frac{1}{9},\frac{2}{9},\frac{4}{9},\frac{5}{9},\frac{7}{9},\frac{8}{9};\ \frac{1}{3},\frac{1}{3},\frac{1}{3},\frac{2}{3},\frac{2}{3},\frac{2}{3};\ t\right) \overset{2}{\equiv} \cdots$$

is

$$t2^{18}(x^3+3x^2-3)^9 \quad -3^6x^3(3x+4)(x^2+6x+6)^{12}$$

with Galois group the "28 bitangents" group $Sp_6(\mathbb{F}_2)$.

Explicit ℓ-division polynomials for HGMs

We also have 3-division polynomials of almost all HGMs in degree ≤ 5. E.g. a 3-division polynomial for

$$H(\frac{1}{4}, \frac{1}{4}, \frac{3}{4}, \frac{3}{4};\ 0, 0, 0, 0;\ t) \overset{3}{\equiv} \cdots$$

is $f_{80}(6t, 16t, 9t^2, 0; x)$. Similarly, a 3-division polynomial for

$$H\left(\frac{1}{4}, \frac{1}{4}, \frac{3}{4}, \frac{3}{4};\ \frac{1}{5}, \frac{2}{5}, \frac{3}{5}, \frac{4}{5};\ t\right) \overset{3}{\equiv} \cdots$$

is $f_{80}(-10t, 0, 25t^2, 16^2; x)$.

All these division polynomials are more than enough to identify wild ramification in low degree HGMs, because there is a lot of redundancy. For example, the last two families are $\sim_2$.

Some references

Hypergeometric Motives, with Fernando Rodriguez Villegas and Mark Watkins, in preparation. Several presentations by each of us available online.

Finite hypergeometric functions, by Frits Beukers, Henri Cohen, and Anton Mellit. ArXiv May 12, 2015.

Hypergeometric functions over finite fields, by John Greene, Trans. Amer. Math. Soc. **301** (1987), 77-101.

Exponential Sums and Differential Equations, by Nicholas M. Katz, Annals of Math Studies, **124**, (1990) is an early work emphasizing motivic aspects of hypergeometric functions.

Some references, continued

Plane quartics and Mordell-Weil lattices of type E_7, by Tetsuji Shioda. Comment. Math. Univ. St. Paul. 42 (1993) no. 1, 61–79.

Monodromy for the hypergeometric function ${}_nF_{n-1}$, by Frits Beukers and Gert Heckman, Invent. Math. **95** (1989), 325-354. Many of our division polynomials fit into the framework of this paper.

The HGM package in *Magma* is by Mark Watkins. The L-function package is by Tim Dokchitser.