p-adic computation of mod ℓ (modular) Galois representations

Nicolas Mascot

Trinity College Dublin

PARI/GP day
June 2nd 2021

Disclaimer

The code demonstrated in this talk is not yet well-polished.

I would be happy to hear your suggestions / remarks!

Topics

1. Computations in Jacobians over finite fields
2. p-adic computations in Jacobians
3. p-adic computation of mod ℓ Galois representations
4. p-adic computation of mod ℓ Galois representations attached to modular forms

Computations in Jacobians over finite fields

Curves and Jacobians

Let C be a curve of genus $g \in \mathbb{N}$.

The Jacobian J of C is an Abelian variety of dimension g.

Abelian: group law on J, similarly to elliptic curves.

Curves and Jacobians

Let C be a curve of genus $g \in \mathbb{N}$.

The Jacobian J of C is an Abelian variety of dimension g.

Abelian: group law on J, similarly to elliptic curves.

However, typically the equations of J are really horrible!
$\rightsquigarrow$ We want to compute in J by just looking at C.

NB Jacobian of a curve = Picard group of the curve $\approx$ class group of a number field.

This is possible thanks to Makdisi's algorithms.

Makdisi's algorithms

All we need is the matrix

$$V = \begin{pmatrix} v_1(P_1) & v_2(P_1) & \cdots \\ \vdots & \vdots & \\ v_1(P_n) & v_2(P_n) & \cdots \end{pmatrix}$$

where v_1, v_2 are "functions" on C forming a basis of the space of global sections of a line bundle $\mathcal{L}$ on C ($\approx$ Riemann-Roch space), and $P_1, P_2, \cdots \in C$ are sufficiently many points.

Makdisi's algorithms

All we need is the matrix

$$V = \begin{pmatrix} v_1(P_1) & v_2(P_1) & \cdots \\ \vdots & \vdots & \\ v_1(P_n) & v_2(P_n) & \cdots \end{pmatrix}$$

where v_1, v_2 are "functions" on C forming a basis of the space of global sections of a line bundle $\mathcal{L}$ on C ($\approx$ Riemann-Roch space), and $P_1, P_2, \cdots \in C$ are sufficiently many points.

A point on J is then represented by a matrix

$$W = \begin{pmatrix} w_1(P_1) & w_2(P_1) & \cdots \\ \vdots & \vdots & \\ w_1(P_n) & w_2(P_n) & \cdots \end{pmatrix}$$

where $w_1, w_2, \cdots$ is a basis of a subspace.

Example: Smooth quartic over a finite field

We construct the Jacobian J of the curve

$$C : x^4 + 2y^4 + x^3 - 3xy - 2 = 0$$

over $\mathbb{F}_{29^3}$, and generate a random point on J.

```
J = smoothplanepicinit(x^4+2*y^4+x^3-3*x*y-2,29,3)
W = picrand(J)
picmember(J,W)
piciszero(J,W)
W2 = picrand(J);
piceq(J,W,W2)
picadd(J,W,W2)
```

Example: Smooth quartic over a finite field

We construct the Jacobian J of the curve

$$C : x^4 + 2y^4 + x^3 - 3xy - 2 = 0$$

over $\mathbb{F}_{29^3}$, and generate a random point on J.

```
J = smoothplanepicinit(x^4+2*y^4+x^3-3*x*y-2,29,3)
W = picrand(J)
picmember(J,W)
piciszero(J,W)
W2 = picrand(J);
piceq(J,W,W2)
picadd(J,W,W2)
```

Hyperelliptic and superelliptic curves are also available.

We plan to implement general curves; the only missing ingredient is Riemann-Roch spaces.

Point counting and random torsion points

The zeta function of $C/\mathbb{F}_p$ is

$$Z(C/\mathbb{F}_p, x) \overset{\text{def}}{=} \exp\left(\sum_{n\geq 1} \#C(\mathbb{F}_{p^n})\frac{x^n}{n}\right) = \frac{L(x)^{\text{rev}}}{(1-x)(1-px)}$$

where $L(x) = \det(x - \text{Frob}_p\,|_J) \in \mathbb{Z}[x]$.

Theorem

We have $\#J(\mathbb{F}_{p^n}) = \text{Res}(L(x), x^n - 1) \in \mathbb{N}$ for all $n \in \mathbb{N}$.

```
factor(piccard(J))
W = picrandtors(J,13);
picmember(J,W)
piciszero(J,picmul(J,W,13))
piciszero(J,W)
picistorsion(J,W,13)
```

Frobenius and pairings

If $\mu_\ell \subset \mathbb{F}_q$, we have the Frey-Rück pairing

$$J(\mathbb{F}_q)[\ell] \times J(\mathbb{F}_q)/\ell J(\mathbb{F}_q) \longrightarrow \mathbb{F}_q^\times/\mathbb{F}_q^{\times \ell} \xrightarrow{\sim} \mathbb{Z}/\ell\mathbb{Z}.$$

```
P = pictorspairinginit(J,13);
X = picrand(J);
pictorspairing(J,P,W,X)
pictorspairing(J,P,picmul(J,W,2),X)
```

$\rightsquigarrow$ We can analyse the action of Frobenius on $J(\mathbb{F}_q)[13]$:

```
FW = picfrob(J,W);
pictorspairing(J,P,FW,X)
piceq(J,picmul(J,W,9),picfrob(J,W))
```

p-adic computations in Jacobians

Truncated p-adics

Instead of working over $\mathbb{F}_q = \mathbb{F}_p[t]/T(t) = \mathbb{Z}[t]/(T(t), p)$ where $T(t)$ is irreducible mod p, we can work over

$$\mathbb{Z}_q/p^e = \mathbb{Z}[t]/(T(t), p^e)$$

for any $e \in \mathbb{N}$.

```
J2 = picsetprec(J,21); \\ Now mod 29^e, e=21
Y = picrand(J2)
picmul(J2,Y,-3)
picmember(J2,W)
picmemberval(J2,W)
picmemberval(J2,Y)
```

Hensel-lifting torsion points

If $p \nmid \ell$ is a prime of good reduction of C, the reduction map

$$J(\mathbb{Z}_q)[\ell] \twoheadrightarrow J(\mathbb{F}_q)[\ell]$$

is étale, so we can lift ℓ-torsion points.

```
W2 = piclifttors(J2,W,13);
picmember(J2,W2)
picistorsion(J2,W2,13)
piciszero(J2,W2)
piceq(J2,picmul(J2,W2,9),picfrob(J2,W2))
```

p-adic computation of mod ℓ Galois representations

Jacobians and Galois representations

Let C be a curve of genus g over $\mathbb{Q}$, let J be its Jacobian, and let $\ell \in \mathbb{N}$.

Then $J(\overline{\mathbb{Q}})[\ell] \simeq (\mathbb{Z}/\ell\mathbb{Z})^{2g}$, and the points of $J[\ell]$ are not defined over $\mathbb{Q}$ in general
$\rightsquigarrow$ Galois representation

$$\rho_{J,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Aut}(J[\ell]) \simeq \mathrm{GSp}_{2g}(\mathbb{Z}/\ell\mathbb{Z}).$$

Jacobians and Galois representations

Let C be a curve of genus g over $\mathbb{Q}$, let J be its Jacobian, and let $\ell \in \mathbb{N}$.

Then $J(\overline{\mathbb{Q}})[\ell] \simeq (\mathbb{Z}/\ell\mathbb{Z})^{2g}$, and the points of $J[\ell]$ are not defined over $\mathbb{Q}$ in general
$\rightsquigarrow$ Galois representation

$$\rho_{J,\ell} : \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \operatorname{Aut}(J[\ell]) \simeq \operatorname{GSp}_{2g}(\mathbb{Z}/\ell\mathbb{Z}).$$

If $p \nmid \ell$ is a prime of good reduction of C, then $\rho_{J,\ell}$ is unramified at p, and the characteristic polynomial of $\rho_{J,\ell}(\operatorname{Frob}_p)$ is $L(x) \bmod \ell$, where $Z(C/\mathbb{F}_p) = \dfrac{L(x)^{\text{rev}}}{(1-x)(1-px)}$.

Jacobians and Galois representations

Let C be a curve of genus g over $\mathbb{Q}$, let J be its Jacobian, and let $\ell \in \mathbb{N}$.

Then $J(\overline{\mathbb{Q}})[\ell] \simeq (\mathbb{Z}/\ell\mathbb{Z})^{2g}$, and the points of $J[\ell]$ are not defined over $\mathbb{Q}$ in general
$\rightsquigarrow$ Galois representation

$$\rho_{J,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Aut}(J[\ell]) \simeq \mathrm{GSp}_{2g}(\mathbb{Z}/\ell\mathbb{Z}).$$

If $p \nmid \ell$ is a prime of good reduction of C, then $\rho_{J,\ell}$ is unramified at p, and the characteristic polynomial of $\rho_{J,\ell}(\mathrm{Frob}_p)$ is $L(x)$ mod ℓ, where $Z(C/\mathbb{F}_p) = \dfrac{L(x)^{\mathrm{rev}}}{(1-x)(1-px)}$.

We wish to compute $\rho_{J,\ell}$.

p-adic strategy to compute $\rho_{J,\ell}$

1. Choose prime $p \nmid \ell$ of good reduction of C,
2. Find $q = p^a$ such that $J[\ell]$ is defined over $\mathbb{F}_q$,
3. Generate random points of $J(\mathbb{F}_q)[\ell]$ until we get an $\mathbb{F}_\ell$-basis,
4. Lift this basis from $J(\mathbb{F}_q)$ to $J(\mathbb{Z}_q/p^e)$, $e \gg 1$,
5. Form all linear combinations of these points in $J(\mathbb{Z}_q/p^e)[\ell]$,
6. $F(x) = \prod_{t \in J[\ell]} \big(x - \theta(t)\big)$, where $\theta : J \dashrightarrow \mathbb{A}^1$,
7. Identify $F(x) \in \mathbb{Q}[x]$.

Example: 2-torsion of the Klein quartic

Let $C : x^3y + y^3 + x = 0$. We compute $\rho_{J,2}$.

```
f = x^3*y+y^3+x;
P = [1,0,0]; \\ Points on C
Q = [0,1,0]; \\ Needed to construct J -> A1
l = 2; \\ Look at J[2]
p = 5; e = 60; \\ Work mod 5^60
R = smoothplanegalrep(f,l,p,e,[[P],[Q]])
fa = factor(R[1])
Mat(apply(polredabs,fa[,1]))
```

We see that the field of definition of $J[2]$ is $\mathbb{Q}(\zeta_7)$.

Sub-representations of $\rho_{J,\ell}$

Frequently, we only want the representation ρ_T coming from the points of a Galois-stable $\mathbb{F}_\ell$-subspace $T \subset J[\ell]$.

Given $p \in \mathbb{N}$ prime, let

$$L(x) = \det(x - \mathrm{Frob}_p |_{J[\ell]}) \quad \text{and} \quad \chi_T(x) = \det(x - \mathrm{Frob}_p |_T),$$

so that $\chi_T \mid L$.

If χ_T is coprime with $\psi_T = L/\chi_T$, then we can generate random points of T by applying $\psi_T(\mathrm{Frob}_p)$ to random points of $J[\ell]$
$\rightsquigarrow$ We can compute ρ_T.

Example: A piece of hyperelliptic 7-torsion

```
h = x^3+x+1; \\ C : y^2+h(x)*y = f(x)
f = x^5+x^4; \\ Good reduction away from 13
P = [-1,0]; \\ Points on C
Q= [0,0]; \\ Needed to construct J -> A1
p = 17; e = 30; \\ Work mod 17^30
l = 7; \\ Look at piece of J[7]
chi = x^2-x-2;  \\ Where Frob17 acts like this
R = hyperellgalrep([f,h],l,p,e,[P,Q],chi)
PR = projgalrep(R);
F = polredabs(PR[1])
polgalois(F)
factor(nfdisc(F))
```

We obtain a polynomial with Galois group $PGL_2(\mathbb{F}_7)$ which ramifies only at 7 and at 13.

p-adic computation of mod ℓ Galois representations attached to modular forms

Galois representations attached to modular forms

Let $f = q + \sum_{n=2}^{+\infty} a_n q^n \in S_k\big(\Gamma_1(N), \varepsilon\big)$, $k \geqslant 2$, be a newform with coefficient field $K_f = \mathbb{Q}(a_n, n \geqslant 2)$.

Pick a prime $\mathfrak{l}$ of K_f above some $\ell \in \mathbb{N}$.

Galois representations attached to modular forms

Let $f = q + \sum_{n=2}^{+\infty} a_n q^n \in S_k\big(\Gamma_1(N), \varepsilon\big)$, $k \geqslant 2$, be a newform with coefficient field $K_f = \mathbb{Q}(a_n, n \geqslant 2)$.

Pick a prime $\mathfrak{l}$ of K_f above some $\ell \in \mathbb{N}$.

Theorem (Deligne, Serre)

There exists a Galois representation

$$\rho_{f,\mathfrak{l}} \colon \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \operatorname{GL}_2(\mathbb{F}_{\mathfrak{l}}),$$

which is unramified outside ℓN, and such that the image of any Frobenius element at $p \nmid \ell N$ has characteristic polynomial

$$x^2 - a_p x + \varepsilon(p) p^{k-1} \in \mathbb{F}_{\mathfrak{l}}[x].$$

Galois representations attached to modular forms

Let $f = q + \sum_{n=2}^{+\infty} a_n q^n \in S_k\big(\Gamma_1(N), \varepsilon\big)$, $k \geqslant 2$, be a newform with coefficient field $K_f = \mathbb{Q}(a_n, n \geqslant 2)$.

Pick a prime $\mathfrak{l}$ of K_f above some $\ell \in \mathbb{N}$.

Theorem (Deligne, Serre)

There exists a Galois representation

$$\rho_{f,\mathfrak{l}} \colon \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \operatorname{GL}_2(\mathbb{F}_{\mathfrak{l}}),$$

which is unramified outside ℓN, and such that the image of any Frobenius element at $p \nmid \ell N$ has characteristic polynomial

$$x^2 - a_p x + \varepsilon(p) p^{k-1} \in \mathbb{F}_{\mathfrak{l}}[x].$$

We wish to compute $\rho_{f,\mathfrak{l}}$.

Modular Galois representations in Jacobians

Under reasonable hypotheses, $\rho_{f,\mathfrak{l}}$ is afforded by a Galois-stable piece $T \subseteq J[\ell]$, where J is the Jacobian of the modular curve $X_1(N')$,

$$N' = \begin{cases} N & \text{if } k = 2, \\ \ell N & \text{if } k > 2. \end{cases}$$

Modular curves

Curves	Points
$X(N)$	Pairs (E, α) where $\alpha : (\mathbb{Z}/N\mathbb{Z})^2 \simeq E[N]$ and $e_N(\alpha(1,0), \alpha(0,1)) = \zeta_N$
$\downarrow$	
$X_1(N)$	Pairs (E, P) where $P \in E$ has exact order N
$\downarrow$	
$X(1)$	Elliptic curves E

where ζ_N is a fixed primitive N-th root of 1.

Makdisi for $X(N)$

Need line bundle $\mathcal{L}$:
Pick $\mathcal{L}$ whose sections are modular forms of weight 2.

Need points $P_1, \cdots, P_n$ to evaluate forms at:
Fix (E, α), take the

$$(E, \alpha \circ \gamma)$$

for $\gamma \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\pm 1$.

Still need to "evaluate" a basis of the space of forms of weight 2 at the P_i...

Algebraic modular forms

Let $k \in \mathbb{N}$, and R a commutative ring such that $6N \in R^\times$.

Algebraic modular forms

Let $k \in \mathbb{N}$, and R a commutative ring such that $6N \in R^\times$.

Definition

An algebraic modular form of weight k for $X(N)$ over R is a rule f assigning a value to isomorphism classes of triples $(E/R, \alpha, \omega)$ where ω generates the differential forms on E/R

Algebraic modular forms

Let $k \in \mathbb{N}$, and R a commutative ring such that $6N \in R^\times$.

Definition

An algebraic modular form of weight k for $X(N)$ over R is a rule f assigning a value to isomorphism classes of triples $(E/R, \alpha, \omega)$ where ω generates the differential forms on E/R, and such that

$$f(E, \alpha, u\omega) = u^{-k} f(E, \alpha, \omega)$$

for all $u \in R^\times$.

Algebraic modular forms

Definition

An algebraic modular form of weight k for $X(N)$ over R is a rule f assigning a value to triples $(E/R, \alpha, \omega)$, such that

$$f(E, \alpha, u\omega) = u^{-k} f(E, \alpha, \omega)$$

for all $u \in R^\times$.

Algebraic modular forms

Definition

An algebraic modular form of weight k for $X(N)$ over R is a rule f assigning a value to triples $(E/R, \alpha, \omega)$, such that

$$f(E, \alpha, u\omega) = u^{-k} f(E, \alpha, \omega)$$

for all $u \in R^\times$.

Short Weierstrass

$$(\mathcal{E}) \ : \ y^2 = x^3 + Ax + B$$

$$\rightsquigarrow \omega = dx/2y.$$

Algebraic modular forms

Definition

An <u>algebraic modular form</u> of weight k for $X(N)$ over R is a rule f assigning a value to triples $(E/R, \alpha, \omega)$, such that

$$f(E, \alpha, u\omega) = u^{-k} f(E, \alpha, \omega)$$

for all $u \in R^\times$.

Short Weierstrass

$$(\mathcal{E}) \ : \ y^2 = x^3 + Ax + B$$

$$\rightsquigarrow \omega = dx/2y.$$

Isomorphic to

$$(\mathcal{E}') \ : \ y^2 = x^3 + A'x + B'$$

by $(x, y) \mapsto (u^2 x, u^3 y)$, $A' = u^4 A$, $B' = u^6 B$, $\omega' = u^{-1}\omega$.

Algebraic modular forms

Definition

An algebraic modular form of weight k for $X(N)$ over R is a rule f assigning a value to pairs $(\mathcal{E}/R, \alpha)$, such that

$$f(\mathcal{E}', \alpha) = u^k f(\mathcal{E}, \alpha)$$

for all $u \in R^\times$.

Short Weierstrass

$$(\mathcal{E}) \ : \ y^2 = x^3 + Ax + B$$

$$\rightsquigarrow \omega = dx/2y.$$

Isomorphic to

$$(\mathcal{E}') \ : \ y^2 = x^3 + A'x + B'$$

by $(x, y) \mapsto (u^2 x, u^3 y)$, $A' = u^4 A$, $B' = u^6 B$, $\omega' = u^{-1}\omega$.

Algebraic modular forms

Definition

An algebraic modular form of weight k for $X(N)$ over R is a rule f assigning a value to pairs $(\mathcal{E}/R, \alpha)$, such that

$$f(\mathcal{E}', \alpha) = u^k f(\mathcal{E}, \alpha)$$

for all $u \in R^\times$.

Examples

$\mathcal{E} \mapsto A$ is a modular form of weight 4.

$\mathcal{E} \mapsto \Delta := -64A^3 - 432B^2$ is a modular form of weight 12.

by $(x, y) \mapsto (u^2 x, u^3 y)$, $A' = u^4 A$, $B' = u^6 B$, $\omega' = u^{-1}\omega$.

Makdisi's moduli-friendly forms

$$\alpha : (\mathbb{Z}/N\mathbb{Z})^2 \simeq \mathcal{E}[N]$$

For $v, w \in (\mathbb{Z}/N\mathbb{Z})^2$ such that $v, w, v + w$ are all nonzero, let

$$\lambda_{v,w} : (\mathcal{E}, \alpha) \longmapsto \text{slope of line joining } \alpha(v) \text{ to } \alpha(w).$$

Makdisi's moduli-friendly forms

$$\alpha : (\mathbb{Z}/N\mathbb{Z})^2 \simeq \mathcal{E}[N]$$

For $v, w \in (\mathbb{Z}/N\mathbb{Z})^2$ such that $v, w, v+w$ are all nonzero, let

$$\lambda_{v,w} : (\mathcal{E}, \alpha) \longmapsto \text{slope of line joining } \alpha(v) \text{ to } \alpha(w).$$

Theorem (Makdisi, 2011)

1. *$\lambda_{v,w}$ is a modular form of weight 1 for $X(N)$.*

Makdisi's moduli-friendly forms

$$\alpha : (\mathbb{Z}/N\mathbb{Z})^2 \simeq \mathcal{E}[N]$$

For $v, w \in (\mathbb{Z}/N\mathbb{Z})^2$ such that $v, w, v+w$ are all nonzero, let

$$\lambda_{v,w} : (\mathcal{E}, \alpha) \longmapsto \text{slope of line joining } \alpha(v) \text{ to } \alpha(w).$$

Theorem (Makdisi, 2011)

1. *$\lambda_{v,w}$ is a modular form of weight 1 for $X(N)$.*
2. *The R-algebra generated by the $\lambda_{v,w}$ contains all modular forms for $X(N)$, except cuspforms of weight 1.*

Makdisi's moduli-friendly forms

$$\alpha : (\mathbb{Z}/N\mathbb{Z})^2 \simeq \mathcal{E}[N]$$

For $v, w \in (\mathbb{Z}/N\mathbb{Z})^2$ such that $v, w, v+w$ are all nonzero, let

$$\lambda_{v,w} : (\mathcal{E}, \alpha) \longmapsto \text{slope of line joining } \alpha(v) \text{ to } \alpha(w).$$

Theorem (Makdisi, 2011)

1. $\lambda_{v,w}$ *is a modular form of weight* 1 *for* $X(N)$*.*
2. *The R-algebra generated by the* $\lambda_{v,w}$ *contains all modular forms for* $X(N)$*, except cuspforms of weight* 1*.*
3. *The* $\lambda_{v,w}$ *are moduli-friendly!*

Makdisi's moduli-friendly forms

$$\alpha : (\mathbb{Z}/N\mathbb{Z})^2 \simeq \mathcal{E}[N]$$

For $v, w \in (\mathbb{Z}/N\mathbb{Z})^2$ such that $v, w, v + w$ are all nonzero, let

$$\lambda_{v,w} : (\mathcal{E}, \alpha) \longmapsto \text{slope of line joining } \alpha(v) \text{ to } \alpha(w).$$

Theorem (Makdisi, 2011)

1. *$\lambda_{v,w}$ is a modular form of weight 1 for $X(N)$.*
2. *The R-algebra generated by the $\lambda_{v,w}$ contains all modular forms for $X(N)$, except cuspforms of weight 1.*
3. *The $\lambda_{v,w}$ are moduli-friendly!*

$\rightsquigarrow$ We can compute in the Jacobian of $X(N)$ without equations nor q-expansions, just by looking at $\mathcal{E}[N]$ for one $\mathcal{E}$!

Example 1

Let

$$f = q + (-i-1)q^2 + (i-1)q^3 + O(q^4) \in S_2\big(\Gamma_1(16)\big)$$

and

$$\mathfrak{l} = (5, i-2).$$

We catch $\rho_{f,\mathfrak{l}}$ in the 5-torsion of the Jacobian of $X_1(16)$ (genus 2).

```
S = mfinit([16,2,0],1);
f = mfeigenbasis(S[1])[1];
R = mfgalrep(f,[5,[[2,2]]],[30,50],5)
factor(projgalrep(R)[1])
```

Example 2

Let

$$f = \Delta = q - 24q^2 + 252q^3 + O(q^4) \in S_{12}\big(\Gamma_1(1)\big)$$

and

$$\mathfrak{l} = 17.$$

We catch $\rho_{f,\mathfrak{l}}$ in the 17-torsion of the Jacobian of $X_1(17)$ (genus 5).

```
f = mfDelta();
R = mfgalrep(f,17,100,200)
F = polredbest(projgalrep(R)[1])
factor(nfdisc(F))
```