Arakelov theory and height bounds

Peter Bruin
Berlin, 17 November 2009

Abstract

In the work of Edixhoven, Couveignes et al. (see [5] and [4]) on computing two-dimensional Galois representations associated to modular forms over finite fields, part of the output of the algorithm is a certain polynomial with rational coefficients that is approximated numerically. Arakelov's intersection theory on arithmetic surfaces is applied to modular curves in order to bound the heights of the coefficients of this polynomial. I will explain the connection between Arakelov theory and heights, indicate what quantities need to be estimated, and give methods for doing this that lead to explicit height bounds.

1. Motivation

The motivaton for the work I am presenting is the computation of Galois representations attached to modular forms over finite fields, and of coefficients of modular forms. S. J. Edixhoven and J.-M. Couveignes have developed (in collaboration with several others) an algorithm for this; see [5] and [4]. So far it has only been worked out for modular forms of level 1; in my thesis [in preparation] I intend to give a generalisation to arbitrary levels.

We begin by explaining what the Galois representation attached to a modular form is. Let n and w be positive integers, and let let f be a (classical) modular form of weight w for $\Gamma_1(n)$, with q-expansion

$$f = a_0 + a_1 q + a_2 q^2 + \cdots.$$

Assume that f is an eigenform for all the Hecke operators of level n. In this case we may assume that $a_1 = 1$, and then we have

$$T_m f = a_m f \quad \text{for all } m \geq 1$$

and

$$\langle d \rangle f = \epsilon(d) f \quad \text{for all } d \in (\mathbf{Z}/m\mathbf{Z})^\times$$

for some character

$$\epsilon\colon (\mathbf{Z}/n\mathbf{Z})^\times \to \mathbf{C}^\times.$$

Theorem 1.1. *Let E_f be the number field generated by the a_m, let λ be a finite place of E_f, let l be the residue characteristic of λ, and let $E_{f,\lambda}$ be the completion of E_f at λ. There exists a continuous representation*

$$\rho_{f,\lambda}\colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(E_{f,\lambda})$$

which is unramified at all primes $p \nmid nl$ and with the property that for every such p the characteristic polynomial of a Frobenius element at p equals $x^2 - a_p x + \epsilon(p)p^{w-1}$. If we require $\rho_{f,\lambda}$ to be semi-simple, it is unique up to isomorphism.

If f is an Eisenstein series, then $\rho_{f,\lambda}$ is reducible and straightforward to write down. The situation is much more complicated when $\rho_{f,\lambda}$ is irreducible. In this case the representations were constructed by Eichler, Shimura and Igusa for $w = 2$, by Deligne for $w > 2$, and by Deligne and Serre for $w = 1$. The construction uses étale cohomology (or Tate modules in the case $w = 2$).

From the l-adic representations $\rho_{f,\lambda}$, we can construct *reduced representations* as follows. For a suitable choice of basis, the image of $\rho_{f,\lambda}$ lies has coefficients in the ring of integers of $E_{f,\lambda}$. We can then reduce the representation modulo λ to obtain a representation

$$\bar{\rho}_{f,\lambda}\colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(k_{f,\lambda}).$$

Here $k_{f,\lambda}$ denotes the residue field of E_f at λ. (If $\bar{\rho}_{f,\lambda}$ is reducible, it depends on the choice of basis above, but it becomes unique up to isomorphism if we require in addition that $\bar{\rho}_{f,\lambda}$ be semi-simple.)

Remark. Serre's conjecture—proved recently by Khare and Wintenberger—says that in fact *every* continuous, odd, irreducible representation over a finite field arises from a modular form.

We assume that $\bar{\rho}_{f,\lambda}$ is irreducible. Furthermore, we may assume without much loss of generality that

$$2 \le w \le l+1,$$

since it is known that all modular representations over finite fields are twists (by some character) of representations coming from modular forms satisfying this inequality. Let $K_{f,\lambda}$ be the fixed field of the kernel of $\bar{\rho}_{f,\lambda}$; then the question is how to find $K_{f,\lambda}$ and the (injective) homomorphism

$$\mathrm{Gal}(K_{f,\lambda}/\mathbf{Q}) \to \mathrm{GL}_2(k_{f,\lambda})$$

such that $\bar{\rho}_{f,\lambda}$ factors as

$$\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{Gal}(K_{f,\lambda}/\mathbf{Q}) \to \mathrm{GL}_2(k_{f,\lambda}).$$

One key ingredient for our strategy to compute $\bar{\rho}_{f,\lambda}$ is the following theorem, which follows from work of Mazur, Ribet, Gross, and others.

Theorem 1.2. *Write*

$$n' = \begin{cases} n & \text{if } w = 2; \\ nl & \text{if } 3 \le w \le l+1. \end{cases}$$

Let $\mathrm{J}_1(n')$ *denote the Jacobian of the modular curve* $\mathrm{X}_1(n')$ *over* $\mathbf{Q}$*, and let* $\mathrm{T}_1(n')$ *denote the subring of* $\mathrm{End}\,\mathrm{J}_1(n')$ *generated by the Hecke operators* T_m *for* $m \ge 1$ *and* $\langle d \rangle$ *for* $d \in (\mathbf{Z}/n'\mathbf{Z})^\times$*. There exists a surjective ring homomorphism*

$$\begin{aligned} \mathrm{T}_1(n') &\to k_{f,\lambda} \\ T_m &\mapsto a_m \\ \langle d \rangle &\mapsto \begin{cases} \epsilon(d) & \text{if } w = 2; \\ \epsilon(d \bmod n)(d \bmod l)^{w-2} & \text{if } 3 \le w \le l+1. \end{cases} \end{aligned}$$

We let $\mathfrak{m}_{f,\lambda}$ denote the kernel of this homomorphism; this is a maximal ideal of the Hecke algebra $\mathrm{T}_1(n')$. We define a closed subscheme $\mathrm{J}_1(n')[\mathfrak{m}_{f,\lambda}]$, finite over $\mathrm{Spec}\,\mathbf{Q}$, as the intersection of the kernels of the elements of $\mathfrak{m}_{f,\lambda}$. Note that $k_{f,\lambda}$ acts on $\mathrm{J}_1(n')[\mathfrak{m}_{f,\lambda}]$.

Theorem 1.3. *The* $k_{f,\lambda}[\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})]$*-module* $\mathrm{J}_1(n')[\mathfrak{m}_{f,\lambda}](\overline{\mathbf{Q}})$ *is, up to semi-simplification, a direct sum of copies of* $\bar{\rho}_{f,\lambda}$*.*

Remark. In the vast majority of cases, $\mathrm{J}_1(n')[\mathfrak{m}_{f,\lambda}](\overline{\mathbf{Q}})$ is in fact *isomorphic* to $\bar{\rho}_{f,\lambda}$. We will assume for simplicity that this is the case.

The question is now how to give an explicit description of $\bar{\rho}_{f,\lambda}$, or equivalently of the finite $k_{f,\lambda}$-vector space scheme $\mathrm{J}_1(n')[\mathfrak{m}_{f,\lambda}]$ over $\mathbf{Q}$. The strategy is as follows. We abbreviate

$$X = \mathrm{X}_1(n'), \quad J = \mathrm{J}_1(n'), \quad g = \mathrm{genus}(X) = \dim(J), \quad \mathfrak{m} = \mathfrak{m}_{f,\lambda}.$$

Fix a point $O \in X(\mathbf{Q})$ (for example a rational cusp) and consider the surjective morphism

$$\begin{aligned} \mathrm{Sym}^g X &\to J \\ D &\mapsto [D - gO]. \end{aligned}$$

This map is an isomorphism above a dense open subset of J, and we assume—again for simplicity—that it is an isomorphism above $J[\mathfrak{m}]$. Then $J[\mathfrak{m}]$ is isomorphic via the above map to a closed subscheme D of $\mathrm{Sym}^g X$. In other words, every point $x \in J[\mathfrak{m}](\overline{\mathbf{Q}})$ corresponds to a unique divisor D_x of degree g on $X \times \mathrm{Spec}\,\overline{\mathbf{Q}}$ such that

$$x = [D_x - gO].$$

We choose a function

$$\psi \colon X \to \mathbf{P}^1_{\mathbf{Q}}$$

such that the map

$$\psi_*\colon \mathrm{Sym}^g X \to \mathrm{Sym}^g \mathbf{P}^1_{\mathbf{Q}} \xrightarrow{\sim} \mathbf{P}^g_{\mathbf{Q}}$$

is a closed immersion on D; the last isomorphism comes from the symmetrisation map

$$\Sigma^g\colon (\mathbf{P}^1)^g \to \mathbf{P}^g$$

given by the elementary symmetric functions. Furthermore, we choose a rational map

$$\gamma\colon \mathbf{P}^g_{\mathbf{Q}} \to \mathbf{P}^1_{\mathbf{Q}}$$

that is well defined and a closed immersion on the image of D in $\mathbf{P}^g_{\mathbf{Q}}$. We have now constructed a closed immersion

$$\Psi\colon J[\mathfrak{m}] \to \mathbf{P}^1_{\mathbf{Q}}.$$

Let $F_\Psi \in \mathbf{Q}[u,v]$ be the homogeneous polynomial (defined up to multiplication by an element of $\mathbf{Q}^\times$) whose zero locus V is the image of Ψ. The idea is now to approximate F_Ψ to sufficient precision, and to reconstruct F_Ψ from this approximation.

Remark. There are various ways to obtain such an approximation of F_Ψ. J. G. Bosman [1] has done computations using computations on the complex modular curve $\mathrm{X}_1(n')(\mathbf{C})$. Using algorithms for computing in Jacobians of curves over finite fields invented by K. Khuri-Makdisi [8], J.-M. Couveignes [3] and myself [2], F_Ψ can also be computed modulo many small prime numbers.

Remark. Of course, to describe $J[\mathfrak{m}]$ as a $k_{f,\lambda}$-vector space scheme, we need some extra structure. Let A denote the affine coordinate ring of V. Then the extra structure consists of a $\mathbf{Q}$-algebra homomorphism

$$m^\#\colon A \to A \otimes_{\mathbf{Q}} A$$

describing addition, as well as $\mathbf{Q}$-algebra endomorphisms

$$\alpha^\#\colon A \to A$$

for all $\alpha \in k_{f,\lambda}$, describing scalar multiplication. It is possible to compute this extra structure together with A, but we will not describe this.

To be able to reconstruct F_Ψ from an approximation, we need a bound on the *height* $h(F_\Psi)$ of F_Ψ. This is simply the maximum of the absolute values of the coefficients of F_Ψ when these coefficients are chosen to be coprime integers.

2. First estimates

We first apply some preliminary estimates for the height of F_Ψ. For this it is useful to talk about heights in slightly greater generality.

Let r be a non-negative integer and let $x = (x_0 : x_1 : \ldots : x_r)$ be a point of $\mathbf{P}^r(\overline{\mathbf{Q}})$. The *height* of x is defined as follows. If K is a number field over which x is defined, then

$$h_{\mathbf{P}^r}(x) = \frac{1}{[K : \mathbf{Q}]} \sum_v \log \max\{|x_0|_v, \ldots, |x_r|_v\},$$

where v runs over all places of K and $|t|_v$ is the corresponding absolute value, normalised such that multiplication by t on the local field K_v scales the Haar measure by a factor $|t|_v$.

We use the following results without proof; they follow from basic considerations about valuations.

Lemma 2.1. *Let $\Sigma^r \colon (\mathbf{P}^1)^r \to \mathbf{P}^r$ be the symmetrisation map. Then for all $p_1, \ldots, p_r$ in $\mathbf{P}^r(\overline{\mathbf{Q}})$, have*

$$h_{\mathbf{P}^r}(\Sigma^r(p_1, \ldots, p_r)) \leq r \log 2 + \sum_{i=1}^{r} h_{\mathbf{P}^1}(p_i).$$

Lemma 2.2. *Let $\gamma \colon \mathbf{P}^r \dashrightarrow \mathbf{P}^s$ be a rational map given by a non-zero $(s+1) \times (r+1)$-matrix over $\mathbf{Q}$. Let $h(\gamma)$ be the height of this matrix, viewed as an element of $\mathbf{P}^{rs+r+s}(\mathbf{Q})$. Then for any $p \in \mathbf{P}^r(\overline{\mathbf{Q}})$ such that γ is defined at p,*

$$h_{\mathbf{P}^s}(\gamma(p)) \leq \log r + h(\gamma) + h_{\mathbf{P}^r}(p).$$

For every $x \in J[\mathfrak{m}](\overline{\mathbf{Q}})$ we decompose the corresponding divisor D_x as

$$D_x = P_{x,1} + \cdots + P_{x,g} \quad \text{with } P_{x,i} \in X(\overline{\mathbf{Q}}).$$

Then a computation using the above two lemmata gives the inequality

$$\begin{aligned} h(F_\Psi) \leq \sum_{x \in J[\mathfrak{m}](\overline{\mathbf{Q}})} \sum_{i=1}^{g} h_{\mathbf{P}^1}(\psi(P_{x,i})) \\ + \#J[\mathfrak{m}](\overline{\mathbf{Q}}) \cdot \big((g+1)\log 2 + \log g + h(\gamma)\big). \end{aligned} \tag{2.1}$$

The next step is to study $h_{\mathbf{P}^1}(\psi(P_{x,i}))$ using Arakelov theory.

3. Basics of Arakelov theory

We start with some analytic definitions. Let $\mathfrak{X}$ be a Riemann surface of genus $g \geq 1$, and let $(\alpha_1, \ldots, \alpha_g)$ be an orthonormal basis of $\Omega^1(\mathfrak{X})$ with respect to the inner product

$$\langle \alpha, \beta \rangle = \frac{i}{2} \int_{\mathfrak{X}} \alpha \wedge \bar{\beta}.$$

The *canonical* $(1,1)$*-form* on $\mathfrak{X}$ is defined as

$$\mu_{\mathfrak{X}} = \frac{i}{2g} \sum_{j=1}^{g} \alpha_j \wedge \bar{\alpha}_j.$$

The *canonical Green function* of $\mathfrak{X}$ is the unique smooth function $\mathrm{gr}_{\mathfrak{X}}$ outside the diagonal on $\mathfrak{X} \times \mathfrak{X}$ such that

$$\frac{1}{\pi i} \partial\bar{\partial}\, \mathrm{gr}_{\mathfrak{X}}(\ \ , y) = \mu_{\mathfrak{X}} - \delta_y$$

and

$$\int_{\mathfrak{X}} \mathrm{gr}_{\mathfrak{X}}(\ \ , y) \mu_{\mathfrak{X}} = 0$$

for every $y \in \mathfrak{X}$.

Let K be a number field, and let $\mathbf{Z}_K$ be its ring of integers. We write K_{fin} and K_{inf} for the sets of finite and infinite places of K. For every $v \in K_{\mathrm{inf}}$ the completion K_v (which is isomorphic to $\mathbf{R}$ or $\mathbf{C}$) we choose an algebraic closure $\bar{K}_v$; we do not need to choose an isomorphism $\bar{K}_v \cong \mathbf{C}$.

Definition. An *arithmetic surface* over $\mathbf{Z}_K$ is a projective flat scheme $X_{\mathbf{Z}_K}$ whose geometric fibres are semi-stable curves and whose generic fibre X_K is smooth.

Remark. We have adopted the definition of Moret-Bailly [9]; it implies that $X_{\mathbf{Z}_K}$ is normal. (Faltings has the stronger requirement that $X_{\mathbf{Z}_K}$ be regular.) This definition has the advantage that is stable under any base change of the form $\operatorname{Spec} \mathbf{Z}_L \to \operatorname{Spec} \mathbf{Z}_K$, where L is a finite extension of K. The assumption that the geometric fibres are semi-stable is to ensure that the relative dualising sheaf $\Omega_{X/\mathbf{Z}_K}$ exists and is a line bundle.

For each $f \in K_{\mathrm{inf}}$, we define $\mathfrak{X}_v$ to be the Riemann surface $X_K(\bar{K}_v)$. A *metrised line bundle* on X is a line bundle $\mathcal{L}$ together with a Hermitean metric $\| \ \|_v$ on the line bundle $\mathcal{L}_v$ on the Riemann surface $\mathfrak{X}_v$ for each $v \in K_{\mathrm{inf}}$.

Now assume that the fibres of $X_{\mathbf{Z}_K}$ are of genus $g \geq 1$. Then for each $v \in K_{\mathrm{inf}}$ we have the canonical $(1,1)$-form $\mu_{\mathfrak{X}_v}$ on $\mathfrak{X}_v$ and the canonical Green function $\mathrm{gr}_{\mathfrak{X}_v}$ on $fX_v \times fX_v$; these are independent of an identification of $\bar{K}_v$ with $\mathbf{C}$. A metrised line bundle $\mathcal{L}$ is *admissible* if $\| \ \|_v$ is smooth for each v and for some (hence any) local generating section s we have

$$\frac{1}{\pi i} \partial\bar{\partial} \log \|s\|_v = (\deg \mathcal{L}) \mu_{\mathfrak{X}_v}.$$

Given $\mathcal{L}$, there is a one-dimensional family of admissible metrics on each of the $\mathcal{L}_v$. Furthermore, if D is a Cartier divisor on $X_{\mathbf{Z}_K}$, there is a natural admissible metric on the line bundle $\mathcal{O}_X(D)$, given by

$$\log \|1\|_v(x) = \sum_{P \in \mathfrak{X}_v} n_P \, \mathrm{gr}_{\mathfrak{X}_v}(x, P)$$

for x outside the support of $D_v = \sum_{P \in \mathfrak{X}_v} n_P P$. Finally, the dualising sheaf $\Omega_{X/\mathbf{Z}_K}$, which is a line bundle since $X_{\mathbf{Z}_K}$ is semi-stable, has a canonical admissible metric.

Let $\operatorname{Pic} X_{\mathbf{Z}_K}$ denote the group of isomorphism classes of admissible line bundles on $X_{\mathbf{Z}_K}$. Then we have a symmetric bilinear *intersection pairing*

$$\begin{aligned} \operatorname{Pic} X_{\mathbf{Z}_K} \times \operatorname{Pic} X_{\mathbf{Z}_K} &\to \mathbf{R} \\ (\mathcal{L}, \mathcal{M}) &\mapsto (\mathcal{L} \,.\, \mathcal{M}). \end{aligned}$$

If D and E are Cartier divisors without common components, we have

$$(\mathcal{O}_X(D) \,.\, \mathcal{O}_X(E)) = \sum_{v \in K_{\mathrm{fin}}} \log \#k(v) \cdot (\mathcal{O}_X(D) \,.\, \mathcal{O}_X(E))_v + \sum_{v \in K_{\mathrm{inf}}} [K_v : \mathbf{R}](\mathcal{O}_X(D) \,.\, \mathcal{O}_X(E))_v,$$

where $(\mathcal{O}_X(D) \,.\, \mathcal{O}_X(E))_v$ is the sum of the usual local intersection numbers at points above v if v is finite, and

$$(\mathcal{O}_X(D) \,.\, \mathcal{O}_X(E))_v = -\sum_{P,Q \in \mathfrak{X}_v} m_P n_Q \,\mathrm{gr}_{\mathfrak{X}_v}(P,Q)$$

if v is an infinite place and

$$D_v = \sum_{P \in \mathfrak{X}_v} m_P P, \quad E_v = \sum_{Q \in \mathfrak{X}_v} n_Q Q.$$

4. Applying Arakelov theory

We return to estimating the height of the polynomial F_Ψ, starting from (2.1). Let K be a number field such that all the points $P_{x,i}$ are K-rational and such that X has a semi-stable model $X_{\mathbf{Z}_K}$ over $\operatorname{Spec} \mathbf{Z}_K$. We extend each $P_{x,i}$ to a section

$$P_{x,i} \colon \operatorname{Spec} \mathbf{Z}_K \to X_{\mathbf{Z}_K}.$$

After blowing up $X_{\mathbf{Z}_K}$ if necessary, the morphism $\psi \colon X \to \mathbf{P}^1_{\mathbf{Q}}$ extends to a morphism

$$\psi \colon X_{\mathbf{Z}_K} \to \mathbf{P}^1_{\mathbf{Z}_K}.$$

By composing these morphisms, we extend $\psi(P_{x,i})$ to a section

$$\psi(P_{x,i}) \colon \operatorname{Spec} \mathbf{Z}_K \to \mathbf{P}^1_{\mathbf{Z}_K}.$$

We endow the line bundle $\mathcal{O}_{\mathbf{P}^1}(\infty)$ on $\mathbf{P}^1_{\mathbf{Z}_K}$ with the metric defined by

$$\log \|1\|_{\mathcal{O}_{\mathbf{P}^1}(\infty)}(z) = -\log \max\{1, |z|\}.$$

Then it follows from the definition of local intersection numbers (at the finite and infinite places of K) that

$$h_{\mathbf{P}^1}(\psi(P_{x,i})) = \frac{1}{[K : \mathbf{Q}]} (\mathcal{O}_{\mathbf{P}^1}(\infty) \,.\, \psi(P_{x,i})).$$

Now we apply the projection formula; here we have to be careful since the pull-back of the given metric on $\mathcal{O}_{\mathbf{P}^1}(\infty)$ differs from the canonical admissible metric on $\mathcal{O}_{\mathbf{P}^1}(\psi^{-1}\infty)$. After compensating for this, we obtain

$$h_{\mathbf{P}^1}(\psi(P_{x,i})) = \frac{1}{[K : \mathbf{Q}]} \left((\mathcal{O}_X(P_{x,i}) \,.\, \mathcal{O}_X(\psi^{-1}\infty)) + \sum_{v \in K_{\mathrm{inf}}} [K_v : \mathbf{R}] \phi_v((P_{x,i})_v) \right), \tag{4.1}$$

where ϕ_v is the real-valued function on $\mathfrak{X}_v$ defined by

$$\phi_v(x) = -i \int_{\substack{y \in \mathfrak{X}_v \\ |\psi(y)|=1}} \mathrm{gr}_{\mathfrak{X}_v}(x,y) d \log \psi(y) + \int_{y \in \mathfrak{X}_v} \log \max\{1, |\psi(y)|\} \mu_{\mathfrak{X}_v}(y);$$

this can be estimated (independently of x) by

$$\phi_v(x) \leq (\deg \psi) \sup_{\mathfrak{X}_v \times \mathfrak{X}_v} \mathrm{gr}_{\mathfrak{X}_v} + \int_{y \in \mathfrak{X}_v} \log \max\{1, |\psi(y)|\} \mu_{\mathfrak{X}_v}(y).$$

Remark. Equivalently, we have

$$\phi_v(x) = \int_{y \in \mathfrak{X}_v} \mathrm{gr}_{\mathfrak{X}_v}(x,y) \psi^* \mu_{\mathbf{P}^1}(y) + \int_{y \in \mathfrak{X}_v} \log \max\{1, |\psi(y)|\} \mu_{\mathfrak{X}_v}(y),$$

where $\mu_{\mathbf{P}^1}$ is the current on $\mathbf{P}^1(\mathbf{C})$ given by

$$\mu_{\mathbf{P}^1}(\chi) = \int_{\alpha=0}^{1} \chi(\exp(it)) dt.$$

The function $-\log\{1, |z|\}$ on $\mathbf{P}^1(\mathbf{C})$ is a Green function for this current.

Combining (4.1), (2.1) and the estimate for ϕ_v, we get

$$h(F_\Psi) \leq \frac{1}{[K:\mathbf{Q}]}(\mathcal{O}_X(\mathfrak{D}) \,.\, \mathcal{O}_X(\psi^{-1}\infty)) + \#J[\mathfrak{m}](\overline{\mathbf{Q}}) \times \left((g+1)\log 2 + \log g + h(\gamma) + g(\deg\psi) \sup_{\mathfrak{X}\times\mathfrak{X}} \mathrm{gr}_{\mathfrak{X}} + g\int_{\mathfrak{X}} \log\max\{1,|\psi|\}\mu_{\mathfrak{X}}\right),$$

where

$$\mathfrak{X} = \mathrm{X}_1(n')(\mathbf{C})$$

and where $\mathfrak{D}$ is the divisor defined by

$$\mathfrak{D} = \sum_{x\in\#J[\mathfrak{m}](\overline{\mathbf{Q}})} D_x.$$

5. Sketch of what remains to be done

We take ψ of the form

$$\psi = f_{12}/\Delta,$$

where f_{12} is some cusp form of weight 12 and Δ is the usual discriminant modular form. Let us pretend that $\mathrm{X}_1(n')$ has a smooth model $X_{\mathbf{Z}}$ over $\operatorname{Spec}\mathbf{Z}$ (even though we know that this is not the case). Then we can have

$$h(F_\Psi) \leq (\mathcal{O}_X(\mathfrak{D}) \,.\, \mathcal{O}_X(\psi^{-1}\infty)) + \#J[\mathfrak{m}](\overline{\mathbf{Q}})\times \left((g+1)\log 2 + \log g + h(\gamma) + g(\deg\psi) \sup_{\mathfrak{X}\times\mathfrak{X}} \mathrm{gr}_{\mathfrak{X}} + g\int_{\mathfrak{X}} \log\max\{1,|\psi|\}\mu_{\mathfrak{X}}\right),$$

where the intersection number is now taken on the (imaginary) smooth model of $\mathrm{X}_1(n')$ over $\operatorname{Spec}\mathbf{Z}$. We assume in addition that we do not have to blow up $X_{\mathbf{Z}}$ in order to make ψ well defined. Then $\psi^{-1}\infty$ is an effective linear combination of cusps.

Using a lot of Arakelov theory (the adjunction formula, Faltings's arithmetic Riemann–Roch theorem, the Faltings–Hriljac formula relating intersection numbers to Néron–Tate heights) one can then derive the estimate

$$(\mathcal{O}_X(\mathfrak{D}) \,.\, \mathcal{O}_X(\psi^{-1}\infty)) \leq \#J[\mathfrak{m}](\overline{\mathbf{Q}})(\deg\psi)\left(3\pi g(g-1)\sup_{\mathfrak{X}\times\mathfrak{X}} \mathrm{gr}_{\mathfrak{X}} + g\sup_{\langle\alpha,\alpha\rangle=1}\sup_{\mathfrak{X}} \|\alpha\|_{\Omega_{\mathfrak{X}}} - h_{\mathrm{Faltings}}(X) + \frac{g(g-1)}{2}(O \,.\, \Omega_{X/\mathbf{Z}})\right).$$

Here $h_{\mathrm{Faltings}}(X)$ is the Faltings height of X, defined by

$$h_{\mathrm{Faltings}}(X) = \deg\det \mathrm{R}\pi(X,\mathcal{O}_X),$$

where $\pi\colon X \to \operatorname{Spec}\mathbf{Z}$ is the structure morphism. By an unpublished result of Bost, there is a constant B such that the Faltings height of any curve of genus g over a number field is at least $-Bg$.

Again, all of the above is under the assumption that the map from $\mathrm{Sym}^g X$ to $J_{\mathbf{Q}}$ is injective above $J[\mathfrak{m}]$. If this is not the case, we need in addition Zhang's bound for the Néron–Tate height below which there exist infinitely many algebraic points. Furthermore, we still have to take into account the fact that $\mathrm{X}_1(n')$ is not smooth over $\operatorname{Spec}\mathbf{Z}$ and that we may need to blow up $\mathrm{X}_1(n')$ in order to make ψ well defined. One also has to show that γ can be taken such that $h(\gamma)$ is small, and that ψ can be taken such that $\int_{\mathfrak{X}} \log\max\{1,|\psi|\}\mu_{\mathfrak{X}}$ is small.

In the end, everything is reduced to estimating the following quantities related to $\mathrm{X}_1(n')$:

(1) the canonical Green function;
(2) suprema of cusp forms of weight two;
(3) integrals of the form $\int_{\mathfrak{X}} \log\max\{1,|\psi|\}\mu_{\mathfrak{X}}$, where ψ is of the form f_{12}/Δ with f_{12} a cusp form of weight 12.

I am currently working on estimates that are as explicit as possible, using the spectral theory for the Laplace operator on $\mathrm{X}_1(n')(\mathbf{C})$. In part, this work builds on ideas of Jorgenson and Kramer; see [6] and [7].

References

[1] J. G. Bosman, *Explicit computations with modular Galois representations*. Proefschrift, Universiteit Leiden, 2008.

[2] P. J. Bruin, Computing in Picard groups of curves over finite fields. Notes of a talk held at the Institut für Experimentelle Mathematik, Essen, 10 November 2009.
Available online: `http://www.math.leidenuniv.nl/~pbruin/`.

[3] J.-M. Couveignes, Linearizing torsion classes in the Picard group of algebraic curves over finite fields. *Journal of Algebra* **321** (2009), 2085–2118.

[4] J.-M. Couveignes and S. J. Edixhoven (editors), *Computational aspects of modular forms and Galois representations*. Princeton University Press, to appear.

[5] S. J. Edixhoven (with J.-M. Couveignes, R. S. de Jong, F. Merkl and J. G. Bosman), On the computation of coefficients of a modular form. Preprint, 2006/2009.
Available online: `http://arxiv.org/abs/math.NT/0605244`.

[6] J. Jorgenson and J. Kramer, Bounding the sup-norm of automorphic forms. *Geometric and Functional Analysis* **14** (2004), no. 6, 1267–1277.

[7] J. Jorgenson and J. Kramer, Bounds on canonical Green's functions. *Compositio Mathematica* **142** (2006), no. 3, 679–700.

[8] K. Khuri-Makdisi, Asymptotically fast group operations on Jacobians of general curves. *Mathematics of Computation* **76** (2007), no. 260, 2213–2239.

[9] L. Moret-Bailly, Métriques permises. Dans: L. Szpiro, *Séminaire sur les pinceaux arithmétiques : la conjecture de Mordell*, Astérisque **127** (1985), 29–87.