

ANTS X

Proceedings of the Tenth Algorithmic Number Theory Symposium

Haberland's formula and numerical computation
of Petersson scalar products

Henri Cohen



Haberland's formula and numerical computation of Petersson scalar products

Henri Cohen

We study several methods for the numerical computation of Petersson scalar products, and in particular we prove a generalization of Haberland's formula to any subgroup of finite index G of $\Gamma = \mathrm{PSL}_2(\mathbb{Z})$, which gives a fast method to compute these scalar products when a Hecke eigenbasis is not necessarily available.

1. Introduction

Let G be a subgroup of $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ of finite index $r = [\Gamma : G]$. Recall that Γ acts on the upper half-plane \mathcal{H} via linear fractional transformations and that we have an invariant measure $d\mu = dx dy/y^2$. We will denote by $D(G)$ a “reasonable” fundamental domain for the action of G on \mathcal{H} ; see [Definition 4.1](#) below.

Given two modular forms f_1 and f_2 having the same weight k and the same multiplier system ν on G , we recall that one defines the *Petersson scalar product* $\langle f_1, f_2 \rangle_G$ (abbreviated PSP), when it exists, by the formula

$$\langle f_1, f_2 \rangle_G = \frac{1}{[\Gamma : G]} \int_{G \backslash \mathcal{H}} f_1(\tau) \overline{f_2(\tau)} y^k \frac{dx dy}{y^2} = \frac{1}{r} \int_{D(G)} f_1(\tau) \overline{f_2(\tau)} y^k d\mu.$$

This is a fundamental quantity which enters almost everywhere in the theory of modular forms, and the aim of the present paper is to study how to compute it numerically in practice. The normalizing factor $1/r$ is included so that the result does not depend on which group is taken with respect to which both f_1 and f_2 are modular.

The absolute convergence of the above integral is assured if either f_1 or f_2 is a cusp form, or if we are in weight $1/2$. Note however that it can also converge in other cases. We will always consider the case where one of f_1 and f_2 is a cusp

MSC2010: primary 11F11; secondary 11Y35.

Keywords: Petersson product.

form and we will assume that $k \geq 2$ and that k is integral. It is an interesting and nontrivial question to ask what can be done when $k = 1$.

When the space $S_k(G, v)$ of cusp forms of weight k and multiplier system v is known explicitly, and in particular when the decomposition into Hecke eigenforms is known (when $G = \Gamma_0(N)$ or $\Gamma_1(N)$ for instance), there are specific methods for computing the PSP if the decomposition of f_1 and f_2 on the eigenbasis can be easily computed; we will mention these methods below. But we are more interested in the general context where one does not need to know either $S_k(G, v)$ or the eigenbasis decompositions, but where we assume that for any $\tau \in \mathcal{H}$ one can rapidly compute $f_1(\tau)$ and $f_2(\tau)$ to reasonably high accuracy.

In the sequel we will let $(\gamma_j)_{1 \leq j \leq r}$ be a system of representatives of right cosets of $G \backslash \Gamma$, so that $\Gamma = \bigsqcup_{1 \leq j \leq r} G\gamma_j$. In particular, if \mathfrak{F} is a fundamental domain for the full modular group Γ (for instance the standard one), then $\bigcup_{1 \leq j \leq r} \gamma_j(\mathfrak{F})$ is a fundamental domain for G , where the union is essentially disjoint, with the only possible intersections being on the boundaries.

Recall that if $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ we write $f|_k \gamma$ to mean

$$f|_k \gamma(\tau) = (c\tau + d)^{-k} f\left(\frac{a\tau + b}{c\tau + d}\right),$$

so that f is an element of $M_k(G, v)$ if and only if $f|_k \gamma = v(\gamma)f$ for all $\gamma \in G$ and f is holomorphic on \mathcal{H} and at the cusps; also, f lies in $S_k(G, v)$ if in addition f vanishes at the cusps.

It is clear that $f|_k g\gamma_j = v(g)f|_k \gamma_j$, so up to the factor $v(g)$ the function $f_j = f|_k \gamma_j$ is independent of the chosen representative of the right coset $G\gamma_j$. In addition, for any $\alpha \in \Gamma$ we have by definition $\gamma_j \alpha = g_j \gamma_{a(j)}$ for some $g_j \in G$, the map $j \mapsto a(j)$ being a *permutation* of $[1, r]$, so up to the factors $v(g_j)$, the family of $f_j|_k \alpha$ is simply a permutation of the f_j .

2. Some standard methods

Before coming to the more original part of the paper, where we explain how to compute PSP's in a quite general setting, we recall with some detail some well-known methods.

Throughout the paper we will use three test examples, even though they are not completely general:

$$f_1 = f_2 = \Delta(\tau) = \eta(\tau)^{24} \in S_{12}(\Gamma),$$

$$f_1 = f_2 = \Delta_5(\tau) = (\eta(\tau)\eta(5\tau))^4 \in S_4(\Gamma_0(5)),$$

and

$$f_1 = f_2 = \Delta_{11}(\tau) = (\eta(\tau)\eta(11\tau))^2 \in S_2(\Gamma_0(11)),$$

the last of these being the cusp form associated to the elliptic curve $X_0(11)$. To 47 decimals, we have

$$\begin{aligned} \langle \Delta, \Delta \rangle_\Gamma &= 0.00000103536205680432092234781681222516459322491 \dots, \\ \langle \Delta_5, \Delta_5 \rangle_{\Gamma_0(5)} &= 0.00014513335082978187614092680220909259631066600 \dots, \\ \langle \Delta_{11}, \Delta_{11} \rangle_{\Gamma_0(11)} &= 0.00390834565612459898524738548138211386179054941 \dots \end{aligned}$$

In most cases, we assume for simplicity that $G = \Gamma$, but we will of course state the necessary modifications for a general subgroup of finite index G .

2A. Computing from the definition. A first method for computing PSP's is to use the definition directly: Assuming for instance that $G = \Gamma$, we have

$$\begin{aligned} \langle f_1, f_2 \rangle &= \int_{\mathfrak{F}} f_1(\tau) \overline{f_2(\tau)} y^{k-2} dx dy \\ &= \int_{-\frac{1}{2}}^{\frac{1}{2}} \left(\int_{\sqrt{1-x^2}}^{\infty} f_1(x+iy) \overline{f_2(x+iy)} y^{k-2} dy \right) dx. \end{aligned}$$

Since the functions f_i are holomorphic, to compute the integrals numerically one can use the *doubly exponential integration method* (see for instance [2, §9.3]). This little-known but remarkable method is especially efficient for holomorphic functions, and it can be shown that to obtain an accuracy of N decimals the method requires $O(N \log N)$ evaluations of the function to be integrated.

However, we have here a double integral, so the method requires $O(N^2 \log^2 N)$ evaluations of the functions, which can be rather expensive. Of course this can be generalized to any subgroup G by using a natural choice of fundamental domain $D(G) = \bigcup_{1 \leq j \leq r} \gamma_j(\mathfrak{F})$ and making the obvious changes of variable. Table 1 gives a selection of timings to compute $\langle f, f \rangle_G$ to a given number N of decimals using this method. The timings are in seconds, and those not given (as indicated by a dash) are greater than 30 minutes. The present timings have been made on a single processor of a standard 1.8 GHz Intel core i7 CPU, but they are highly dependent on the implementation, so this table is only indicative.

f	$N = 19$	38	57	96	250	500
Δ	11	16	87	143	—	—
Δ_5	154	219	1185	—	—	—
Δ_{11}	327	468	—	—	—	—

Table 1. Timings (in seconds, on one processor of a 1.8 GHz Intel core i7 CPU) to compute $\langle f, f \rangle_G$ to N decimal places using the definition of the pairing. Timings greater than 30 minutes are indicated with a dash.

To summarize: The advantages of this method are its complete generality and simplicity, while its main disadvantage is that it is quite slow, especially at high accuracy and/or for a subgroup of large index.

2B. Using Kloosterman sums. Thanks to the computation of the Fourier expansion of Poincaré series for Γ , it is easy to show that

$$\frac{1}{\langle \Delta, \Delta \rangle} = \frac{(4\pi)^{11}}{10! \tau(n)} \left(\delta_{n,1} + 2\pi \cdot n^{11/2} \sum_{c \geq 1} \frac{K(n, 1; c)}{c} J_{11} \left(\frac{4\pi n^{1/2}}{c} \right) \right),$$

and similar formulas exist in higher weight and for congruence subgroups.

The convergence of this type of series is essentially of the order of $O(1/c^{k-2})$ (here with $k = 12$). This shows that, although useful, the above formula has severe limitations. First, even in the case of Δ , the convergence in $O(1/c^{10})$ and the necessity of computing Kloosterman sums and Bessel functions implies that one can reasonably compute perhaps 10^6 terms if one is patient, giving an accuracy of 60 decimals. A more important limitation occurs for subgroups of Γ , for which there exist forms of lower weight than 12. For instance, in weight 2 the absolute convergence is not even clear, and in weight 4 the convergence is in $O(1/c^2)$, which is too slow to obtain any reasonable accuracy.

Table 2 presents some timings for this method, but limited to Δ since the convergence for Δ_5 would be too slow.

To summarize: The advantage of this method is its speed for high weight and reasonably low accuracy such as 19 or 38 decimals, but the method is essentially useless in all other cases. In addition, its use is restricted to congruence subgroups.

2C. Using symmetric square L-functions. Once again for simplicity we restrict to $G = \Gamma$, but there is no difficulty in generalizing.

Since there exists an explicit orthogonal basis of eigenfunctions in $M_k(\Gamma)$, computing Petersson scalar products of two arbitrary forms can easily be reduced to the computation of $\langle f, f \rangle$ for f a normalized eigenform. If

$$L(f, s) = \sum_{n \geq 1} \frac{a(n)}{n^s} = \prod_p \frac{1}{1 - a(p)p^{-s} + p^{k-1-2s}} = \prod_p \frac{1}{(1 - \alpha_p p^{-s})(1 - \beta_p p^{-s})}$$

f	$N = 19$	38	57	96	250	500
Δ	0.01	3	900	—	—	—

Table 2. Timings (in seconds) to compute $\langle f, f \rangle_G$ to N decimal places using Kloosterman sums.

with $\alpha_p + \beta_p = a(p)$ and $\alpha_p \beta_p = p^{k-1}$, recall that we define the *symmetric square L-function* $L(\text{Sym}^2(f), s)$ for $\Re(s) > k$ by the formula

$$L(\text{Sym}^2(f), s) = \prod_p \frac{1}{(1 - \alpha_p^2 p^{-s})(1 - \alpha_p \beta_p p^{-s})(1 - \beta_p^2 p^{-s})}.$$

The main properties of this function are summarized in the following result.

Theorem 2.1. *Let $f = \sum_{n \geq 1} a(n)q^n \in S_k(\Gamma)$ be a normalized Hecke eigenform.*

(1) *(Fourier expansion.) If we set*

$$A(n) = \sum_{m|n} (-1)^{\Omega(m)} m^{k-1} a(n/m)^2,$$

where $\Omega(m)$ is the number of prime divisors of m , counted with multiplicity, then

$$L(\text{Sym}^2(f), s) = \sum_{n \geq 1} \frac{A(n)}{n^s}.$$

(2) *(Functional equation.) The function $L(\text{Sym}^2(f), s)$ can be extended holomorphically to the whole of \mathbb{C} , and the completed L-function*

$$\Lambda(\text{Sym}^2(f), s) = \pi^{-3s/2} \Gamma(s/2) \Gamma((s+1)/2) \Gamma((s-k)/2 + 1) L(\text{Sym}^2(f), s)$$

satisfies the functional equation

$$\Lambda(\text{Sym}^2(f), 2k - 1 - s) = \Lambda(\text{Sym}^2(f), s).$$

(3) *(Special value.) We have*

$$L(\text{Sym}^2(f), k) = \frac{\pi}{2} \frac{(4\pi)^k}{(k-1)!} \langle f, f \rangle.$$

Proof. The meromorphic continuation, functional equation, and special value are very classical and immediate consequences of the Rankin-Selberg method. The holomorphy is more difficult, and was proved independently by Shimura and Zagier in 1975. □

Note that similar results are of course valid for subgroups.

The last statement of the theorem allows us to reduce the computation of $\langle f, f \rangle$ to that of $L(\text{Sym}^2(f), k)$. For this, the direct use of the definition is of little help, since it is not even clear that the series or product defining this L -function converge, and even if they do, the convergence will be extremely slow. However, the crucial point is the following: Any Dirichlet series satisfying a functional equation of standard type can be evaluated numerically very efficiently using *exponentially convergent* series, see for instance [1, §10.3]. Specializing to our case, it is easy to show the following theorem.

Theorem 2.2. Let $f = \sum_{n \geq 1} a(n)q^n \in S_k(\Gamma)$ be a Hecke eigenform. Set $C = 2 \cdot \pi^{\frac{3}{2}}$ and $\gamma(s) = C^{-s} \Gamma(s) \Gamma((s-k)/2 + 1)$, and as usual let H_n denote the harmonic number $\sum_{1 \leq j \leq n} 1/j$ and let γ denote Euler's constant. Let

$$\begin{aligned}
 F_{1,k}(s, x) &= \sum_{1 \leq m \leq (k-2)/2} (-1)^{k/2-m-1} \frac{(2m-1)!}{(k/2-m-1)!} \frac{(Cx)^{-2m}}{s-2m}, \\
 F_{2,k}(s, x) &= \sum_{m \geq 0} (-1)^{k/2-m-1} \frac{2^{2m+k} (m+k/2)!}{(2m+1)! (2m+k)!} \frac{(Cx)^{2m+1}}{s+2m+1}, \quad \text{and} \\
 F_{3,k}(s, x) &= \sum_{m \geq 0} (-1)^{k/2-m-1} \frac{1}{(2m)! (m+k/2-1)!} \frac{(Cx)^{2m}}{2m+s} G_m(s, x),
 \end{aligned}$$

where

$$G_m(s, x) = 2H_{2m} + H_{m+k/2-1} - 3\gamma - 2 \log(Cx) + \frac{2}{2m+s},$$

and set

$$F_k(s, x) = \gamma(s) - x^s (2F_{1,k}(s, x) + \pi^{1/2} F_{2,k}(s, x) + F_{3,k}(s, x)).$$

Then for every $s \in \mathbb{C}$ with $\Re(s) > k - 2$ and every $t_0 > 0$, we have

$$\gamma(s)L(\text{Sym}^2(f), s) = \sum_{n \geq 1} \frac{A(n)}{n^s} F_k(s, nt_0) + \sum_{n \geq 1} \frac{A(n)}{n^{2k-1-s}} F_k(2k-1-s, n/t_0)$$

where the $A(n)$ are the coefficients given in part (1) of [Theorem 2.1](#). In particular,

$$\langle f, f \rangle = 2^{1-k} \pi^{k/2-1} \left(\sum_{n \geq 1} \frac{A(n)}{n^k} (F_k(k, n) + n F_k(k-1, n)) \right).$$

Note that even though there is cancellation for large x , the series for $F_k(s, x)$ are sufficient for practical computation. One can also compute asymptotic expansions for large x , if desired, showing in particular that $F_k(s, x)$ tends to 0 exponentially.

[Table 3](#) presents a few timings; for simplicity of implementation, we again limit the table to the case $f = \Delta$.

The advantages of this method are that it is general and fast; its main disadvantage is that its implementation requires great care in writing the correct formulas,

f	$N = 19$	38	57	96	250	500
Δ	0.03	0.09	0.2	0.8	11	97

Table 3. Timings (in seconds) to compute $\langle f, f \rangle_G$ to N decimal places using symmetric-square L -functions.

especially for subgroups, and in dealing with cancellation and accuracy problems. But once these hurdles have been overcome, it is the best method that we have seen up to now, and most experts in the field would agree that it is the best available. However, as already mentioned, it assumes that the eigenfunction decomposition of f is known, and this is not always easy or possible. This leads us now to a different method, which is completely general.

3. Basic lemmas

The main computational difficulty related to Petersson products is that they are truly *double* integrals. In the first naïve approach, we have explained that nonetheless these integrals can be computed, somewhat slowly, by using doubly exponential integration techniques. A remarkable fact however, discovered by Haberland [4] (see also [7]) some time ago, is that PSP's can be reduced to the computation of a reasonably small finite number of *simple* integrals, which can now be evaluated very rapidly using doubly exponential integration.

Haberland's result was given for general weights k but only for the full modular group. In a slightly different form it was generalized long ago to $\Gamma_0(N)$ but only in weight $k = 2$ and trivial character, first by Cremona [3] and Zagier [10] in the context of computing the degree of modular parametrizations of elliptic curves (see the more recent paper of Watkins [9] on this subject), and much more recently by Merel [5] in connection with Manin symbols. It was realized that a complete generalization should not be difficult to obtain, and it is one of the purposes of this paper to give it. Note that in [6] the authors also give such a generalization, in a slightly different form, and also for noncuspsforms. In what follows, we will assume that f_1 and f_2 are both cuspforms; if one of the f_i is not a cuspform we can either find its decomposition into its Eisenstein and cuspidal part, which can usually be done with ease, or use the generalization due to [6].

Our goal in this section, which is the main step toward Haberland's formulas, is to show that PSP's are related to other double integrals, which are not "true" double integrals in the sense that they can easily be expressed in terms of simple integrals. For this, we need some preliminary definitions and results. We assume G , $(\gamma_j)_{1 \leq j \leq r}$, k , v , f_1 , and f_2 as above, and we will set $f_{1,j} = f_1|_k \gamma_j$ and $f_{2,j} = f_2|_k \gamma_j$ for $1 \leq j \leq r$. As mentioned above, for simplicity we assume that f_1 and f_2 are *both* cuspforms.

3A. The differentials ε and δ .

Definition 3.1. We set

$$\varepsilon(f_1, f_2)(\tau_1, \tau_2) = f_1(\tau_1) \overline{f_2(\tau_2)} (\tau_1 - \overline{\tau_2})^{k-2} d\tau_1 d\overline{\tau_2}$$

and

$$\delta(f_1, f_2) = \sum_{1 \leq j \leq r} \varepsilon(f_{1,j}, f_{2,j}).$$

Lemma 3.2. *Let $\alpha \in \Gamma$.*

(1) *We have*

$$\varepsilon(f_1, f_2)(\alpha\tau_1, \alpha\tau_2) = \varepsilon(f_1|_k\alpha, f_2|_k\alpha)(\tau_1, \tau_2).$$

(2) *The expression $\varepsilon(f_{1,j}, f_{2,j})$ does not depend on the choice of the right coset representative γ_j .*

(3) *If $\gamma_j\alpha = g_j\gamma_{a(j)}$ with $g_j \in G$ we have*

$$\varepsilon(f_{1,j}, f_{2,j})(\alpha\tau_1, \alpha\tau_2) = \varepsilon(f_{1,a(j)}, f_{2,a(j)}).$$

(4) *We have $\delta(f_1, f_2)(\alpha\tau_1, \alpha\tau_2) = \delta(f_1, f_2)$; in other words, $\delta(f_1, f_2)$ is invariant under Γ .*

Proof. Writing $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, we have

$$\begin{aligned} &\varepsilon(f_1, f_2)(\alpha\tau_1, \alpha\tau_2) \\ &= f_1|_k\alpha(\tau_1) \overline{f_2|_k\alpha(\tau_2)} \cdot (c\tau_1 + d)^k \overline{(c\tau_2 + d)^k} (\alpha\tau_1 - \overline{\alpha\tau_2})^{k-2} d\alpha\tau_1 d\overline{\alpha\tau_2} \\ &= f_1|_k\alpha(\tau_1) \overline{f_2|_k\alpha(\tau_2)} (\tau_1 - \overline{\tau_2})^{k-2} d\tau_1 d\overline{\tau_2} \\ &= \varepsilon(f_1|_k\alpha, f_2|_k\alpha)(\tau_1, \tau_2), \end{aligned}$$

using the immediate but fundamental identity

$$(c\tau_1 + d)^k \overline{(c\tau_2 + d)^k} (\alpha\tau_1 - \overline{\alpha\tau_2})^{k-2} d\alpha\tau_1 d\overline{\alpha\tau_2} = (\tau_1 - \overline{\tau_2})^{k-2} d\tau_1 d\overline{\tau_2}.$$

Statement (1) follows.

If $g \in G$ we have $f_1|_k g\gamma_j = v(g)f_{1,j}$, and similarly for f_2 , so statement (2) follows from $v(g)\overline{v(g)} = 1$.

By definition we have

$$f_{1,j}|_k\alpha = f_1|_k\gamma_j\alpha = f_1|_k g_j\gamma_{a(j)} = v(g_j)f_{1,a(j)}$$

since $f_1 \in M_k(G, v)$, and similarly for $f_{2,j}$. Again using $v(g_j)\overline{v(g_j)} = 1$, we obtain statement (3). Statement (4) follows by summing on j since the map $j \mapsto a(j)$ is a permutation. □

3B. The simple integral $F_{2,j}$.

Definition 3.3. Let $Z \in \overline{\mathcal{H}}$ be fixed, and set

$$F_{2,j}(Z; \tau) = F_{2,j}(\tau) = \int_Z^\tau \overline{f_{2,j}(\tau_2)} (\tau - \overline{\tau_2})^{k-2} d\overline{\tau_2}.$$

Remarks. (1) We could also define $F_{1,j}$ in a similar manner, but we will only need $F_{2,j}$ since we temporarily treat f_1 and f_2 in a nonsymmetric manner.

(2) Note that $F_{2,j}$ is in general not holomorphic, so must be considered as a function of τ and $\overline{\tau}$.

(3) We have

$$F_{2,j}(Z_1; \tau) - F_{2,j}(Z_2; \tau) = \int_{Z_1}^{Z_2} \overline{f_{2,j}(\tau_2)} (\tau - \overline{\tau_2})^{k-2} d\overline{\tau_2},$$

which is a *polynomial* (hence in particular a holomorphic function) in τ .

Lemma 3.4. (1) We have

$$\frac{\partial F_{2,j}}{\partial \overline{\tau}} = \overline{f_{2,j}(\tau)} (\tau - \overline{\tau})^{k-2}.$$

(2) For every $\alpha \in \Gamma$ we have

$$F_{2,j}|_{2-k} \alpha(\tau) = \int_{\alpha^{-1}(Z)}^\tau \overline{f_{2,j}|_k \alpha(\tau_2)} (\tau - \overline{\tau_2})^{k-2} d\overline{\tau_2}.$$

(3) In particular, if we write $\gamma_j \alpha = g_j \gamma_{a(j)}$ with $g_j \in G$, we have

$$F_{2,j}|_{2-k} \alpha(\tau) = \overline{v(g_j)} (F_{2,a(j)}(\tau) - P_{a(j)}(\alpha; \tau)),$$

where

$$P_{a(j)}(\alpha; \tau) = \int_Z^{\alpha^{-1}(Z)} \overline{f_{2,a(j)}(\tau_2)} (\tau - \overline{\tau_2})^{k-2} d\overline{\tau_2}$$

is a polynomial in τ of degree less than or equal to $k - 2$ (recall once again that we assume $k \geq 2$).

(4) We have

$$\left(\int_A^B - \int_{\alpha(A)}^{\alpha(B)} \right) \sum_{1 \leq j \leq r} f_{1,j}(\tau) F_{2,j}(\tau) d\tau = \int_A^B \sum_{1 \leq j \leq r} f_{1,j}(\tau) P_j(\alpha; \tau) d\tau.$$

Proof. We have $\overline{F_{2,j}(\tau)} = \int_Z^\tau f_{2,j}(\tau_2) (\overline{\tau} - \tau_2)^{k-2} d\tau_2$, so

$$\frac{\partial \overline{F_{2,j}(\tau)}}{\partial \tau} = f_{2,j}(\tau) (\overline{\tau} - \tau)^{k-2}.$$

Conjugating this equality proves statement (1).

Setting $\tau_2 = \alpha z$ and writing $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, we have

$$\begin{aligned} F_{2,j} |_{2-k} \alpha(\tau) &= (c\tau + d)^{k-2} \int_Z^{\alpha\tau} \overline{f_{2,j}(\tau_2)} (\alpha\tau - \overline{\tau_2})^{k-2} d\overline{\tau_2} \\ &= (c\tau + d)^{k-2} \int_{\alpha^{-1}Z}^{\tau} (c\bar{z} + d)^{k-2} \overline{f_{2,j} |_k \alpha(z)} (\alpha\tau - \alpha\bar{z})^{k-2} d\bar{z} \\ &= \int_{\alpha^{-1}Z}^{\tau} \overline{f_{2,j} |_k \alpha(z)} (\tau - \bar{z})^{k-2} d\bar{z}, \end{aligned}$$

since $\alpha u - \alpha v = (u - v) / ((cu + d)(cv + d))$; this proves statement (2).

Since we have $f_{2,j} |_k \alpha = v(g_j) f_{2,a(j)}$, it follows from statement (2) that

$$F_{2,j} |_{2-k} \alpha(\tau) = \overline{v(g_j)} \int_{\alpha^{-1}(Z)}^{\tau} \overline{f_{2,a(j)}(\tau_2)} (\tau - \overline{\tau_2})^{k-2} d\overline{\tau_2},$$

proving statement (3).

Setting $\tau = \alpha z$ with $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and as before $\gamma_j \alpha = g_j \gamma_{a(j)}$, we have

$$\begin{aligned} \int_{\alpha(A)}^{\alpha(B)} f_{1,j}(\tau) F_{2,j}(\tau) d\tau &= \int_A^B f_{1,j}(\alpha z) F_{2,j}(\alpha z) (cz + d)^{-2} dz \\ &= \int_A^B f_{1,j} |_k \alpha(z) F_{2,j} |_{2-k} \alpha(z) dz \\ &= v(g_j) \overline{v(g_j)} \int_A^B f_{1,a(j)}(\tau) (F_{2,a(j)}(\tau) - P_{a(j)}(\alpha; \tau)) d\tau, \end{aligned}$$

and since $j \mapsto a(j)$ is a bijection, we obtain

$$\int_{\alpha(A)}^{\alpha(B)} \sum_{1 \leq j \leq r} f_{1,j}(\tau) F_{2,j}(\tau) d\tau = \int_A^B \sum_{1 \leq j \leq r} f_{1,j}(\tau) (F_{2,j}(\tau) - P_j(\alpha; \tau)) d\tau,$$

proving statement (4). □

Corollary 3.5. *Let f_1 and f_2 be in $M_k(G, v)$, one of them being a cusp form. For every subgroup H of Γ of finite index $s = [\Gamma : H]$ we have*

$$(2i)^{k-1} r s \langle f_1, f_2 \rangle_G = \int_{\partial(D(H))} \sum_{1 \leq j \leq r} f_{1,j}(\tau) F_{2,j}(\tau) d\tau,$$

where $\partial(D(H))$ denotes the boundary of a reasonable fundamental domain $D(H)$ of H .

Note that the subgroup H need not have anything to do with the subgroup G .

Proof. By definition we have

$$\begin{aligned}
 (2i)^{k-1}r\langle f_1, f_2 \rangle_G &= \int_{D(G)} f_1(\tau)\overline{f_2(\tau)}(\tau - \bar{\tau})^{k-2} d\tau d\bar{\tau} \\
 &= \sum_{1 \leq j \leq r} \int_{\gamma_j(D(\Gamma))} f_1(\tau)\overline{f_2(\tau)}(\tau - \bar{\tau})^{k-2} d\tau d\bar{\tau} \\
 &= \int_{D(\Gamma)} \sum_{1 \leq j \leq r} f_{1,j}(\tau)\overline{f_{2,j}(\tau)}(\tau - \bar{\tau})^{k-2} d\tau d\bar{\tau} \\
 &= \int_{D(\Gamma)} \delta(f_1, f_2)(\tau, \tau) \\
 &= \frac{1}{s} \int_{D(H)} \delta(f_1, f_2)(\tau, \tau),
 \end{aligned}$$

after an evident change of variable, and since δ is invariant by Γ by [Lemma 3.2](#). Now since $f_{1,j}$ is holomorphic, we have $\partial f_{1,j}/\partial \bar{\tau} = 0$, so by Stokes's theorem and the above lemma we have

$$\begin{aligned}
 (2i)^{k-1}rs\langle f_1, f_2 \rangle_G &= \int_{D(H)} \sum_{1 \leq j \leq r} \frac{\partial(f_{1,j}F_{2,j})}{\partial \bar{\tau}} d\tau d\bar{\tau} \\
 &= \int_{\partial(D(H))} \sum_{1 \leq j \leq r} f_{1,j}(\tau)F_{2,j}(\tau) d\tau,
 \end{aligned}$$

as claimed. □

3C. The basic double integral \mathcal{F} . We make the following definition.

Definition 3.6. Let f_1 and f_2 be modular forms. If A_1, B_1, A_2, B_2 are in $\overline{\mathcal{H}}$, we set, when defined,

$$\begin{aligned}
 \mathcal{F}(A_1, B_1; A_2, B_2) &= \int_{A_1}^{B_1} \int_{A_2}^{B_2} \delta(f_1, f_2) \\
 &= \sum_{1 \leq j \leq r} \int_{A_1}^{B_1} \int_{A_2}^{B_2} f_{1,j}(\tau_1)\overline{f_{2,j}(\tau_2)}(\tau_1 - \bar{\tau}_2)^{k-2} d\tau_1 d\bar{\tau}_2,
 \end{aligned}$$

where $f_{1,j} = f_1|_k \gamma_j$ and $f_{2,j} = f_2|_k \gamma_j$.

When we need to emphasize the dependence in f_1 and f_2 we will of course write $\mathcal{F}(f_1, f_2; A_1, B_1; A_2, B_2)$ instead of $\mathcal{F}(A_1, B_1; A_2, B_2)$. Also, as usual when integrating on \mathcal{H} it is understood that integrals having a cusp as an endpoint must end with a hyperbolic circle. The following properties are immediate.

Lemma 3.7. (1) *The above definition does not depend on the paths of integration, as long as the conditions at the cusps are satisfied.*

- (2) *The above definition does not depend on the right coset representatives γ_j .*
- (3) *The function \mathcal{F} is transitive separately on (A_1, B_1) and on (A_2, B_2) ; in other words,*

$$\mathcal{F}(A_1, C_1; A_2, B_2) + \mathcal{F}(C_1, B_1; A_2, B_2) = \mathcal{F}(A_1, B_1; A_2, B_2),$$

and similarly for (A_2, B_2) .

- (4) *We have*

$$\mathcal{F}(f_1, f_2; A_2, B_2; A_1, B_1) = (-1)^{k-2} \overline{\mathcal{F}(f_2, f_1; A_1, B_1; A_2, B_2)}.$$

- (5) *We have*

$$\begin{aligned} &\mathcal{F}(A_1, B_1; A_2, B_2) \\ &= \sum_{1 \leq j \leq r} \sum_{0 \leq n \leq k-2} (-1)^n \binom{k-2}{n} \int_{A_1}^{B_1} \tau^{k-2-n} f_{1,j}(\tau) d\tau \overline{\int_{A_2}^{B_2} \tau^n f_{2,j}(\tau) d\tau}, \end{aligned}$$

where we must assume that f_1 and f_2 are both cusp forms if at least one of the A_i or B_i is a cusp.

In particular, this last statement shows that \mathcal{F} is much easier to compute than a PSP, and it is in this sense that we said above that it is not a “true” double integral.

Proposition 3.8. *For any $\alpha \in \Gamma$ we have*

$$\mathcal{F}(\alpha A_1, \alpha B_1; \alpha A_2, \alpha B_2) = \mathcal{F}(A_1, B_1; A_2, B_2).$$

Proof. This follows immediately from the Γ -invariance of δ , proved in [Lemma 3.2](#). □

4. The main result

4A. Fundamental domains. Before stating and proving the main result, we must discuss fundamental domains of subgroups of Γ . We first set the following definition.

Definition 4.1. Let $G \subset \Gamma$ be a subgroup of finite index r . A subset $D(G)$ of \mathcal{H} is called a *reasonable fundamental domain* (or simply a *fundamental domain*) for G if the following conditions are satisfied:

- (1) $D(G)$ is a finite union of connected and simply connected open subsets of \mathcal{H} .
- (2) The boundary $\partial(D(G)) = \overline{D(G)} \setminus D(G)$ has measure 0.
- (3) For any $\tau \in \mathcal{H}$ there exists $g \in G$ such that $g\tau \in \overline{D(G)}$. In addition, if $g\tau \in D(G)$ then g is unique, or equivalently, if g_1 and $g_2 \in G$ are such that $g_1(\tau)$ and $g_2(\tau)$ are in $D(G)$, then $g_i(\tau) \in \partial(D(G))$.

If \mathfrak{F} is the standard fundamental domain for the full modular group Γ , it is clear that $D(G) = \bigcup \gamma_j(\mathfrak{F}^\circ)$ is a reasonable fundamental domain. The following results are well-known.

Proposition 4.2. *The fundamental domain $D(G)$ can be chosen so that its boundary $\partial(D(G))$ is the union of an even number of oriented hyperbolic circles, say $[A_i, A_{i+1}[$ with $1 \leq i \leq 2n$ (where the indices are taken modulo $2n$), such that there exists a family $(\alpha_i)_{1 \leq i \leq 2n}$ of elements of Γ and a permutation τ of $[1, 2n]$ satisfying the following properties:*

- (1) τ is an involution without fixed points (that is, $\tau^2 = 1$ and $\tau(i) \neq i$ for all i); equivalently, τ is a product of n disjoint transpositions $(i_m, j_m)_{1 \leq m \leq n}$.
- (2) $\alpha_{\tau(i)} = \alpha_i^{-1}$.
- (3) $\alpha_i(A_i) = A_{\tau(i)+1}$ and $\alpha_i(A_{i+1}) = A_{\tau(i)}$, so that α_i gives a bijection from $[A_i, A_{i+1}[$ to $[A_{\tau(i)+1}, A_{\tau(i)}[$.

Corollary 4.3. *If τ is the product of the n disjoint transpositions $(i_m, j_m)_{1 \leq m \leq n}$, then α_{i_m} gives a bijection from $[A_{i_m}, A_{i_m+1}[$ to the reverse of $[A_{j_m}, A_{j_m+1}[$, and*

$$\partial(D(H)) = \bigsqcup_{1 \leq m \leq n} ([A_{i_m}, A_{i_m+1}[\sqcup [A_{j_m}, A_{j_m+1}[$$

Proof. Clear. □

4B. Examples of fundamental domains. For simplicity, we will choose subgroups G having a fundamental domain whose boundary has only 4 sides, and τ will always be the product $(1, 2)(3, 4)$ of the two transpositions exchanging 1 and 2, and 3 and 4, so $i_1 = 1$ and $i_2 = 3$. The fundamental domain is thus a hyperbolic quadrilateral given by its vertices A_1, A_2, A_3 , and A_4 , and α_1 sends $[A_1, A_2[$ bijectively to the reverse of $[A_2, A_3[$, and α_3 sends $[A_3, A_4[$ bijectively to the reverse of $[A_4, A_1[$.

We consider a number of different subgroups H of Γ , and give one or more fundamental domains of the above type for each, where as usual $\rho = e^{2i\pi/3}$:

- (1) $H = \Gamma$, with $A_1 = \rho + 1, A_2 = i\infty, A_3 = \rho, A_4 = i, \alpha_1 = T^{-1}$, and $\alpha_3 = S$, which corresponds to the standard fundamental domain \mathfrak{F} , where as usual $T = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.
- (2) $H = \Gamma$, with $A_1 = 0, A_2 = i, A_3 = i\infty, A_4 = \rho, \alpha_1 = S$, and $\alpha_3 = ST$.
- (3) $H = \Gamma_2$ the unique subgroup of index 2 in Γ , with $A_1 = \rho + 1, A_2 = i\infty, A_3 = \rho, A_4 = 0, \alpha_1 = T^{-1}$, and $\alpha_3 = TST = ST^{-1}S = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$.
- (4) $H = \Gamma_2$ the unique subgroup of index 2 in Γ , with $A_1 = 0, A_2 = i\infty, A_3 = -1, A_4 = \rho, \alpha_1 = T^{-1}$ and $\alpha_3 = T^{-1}S = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$.

- (5) $H = \Gamma_3$ one of the subgroups of index 3 in Γ , with $A_1 = 1, A_2 = i\infty, A_3 = -1, A_4 = I, \alpha_1 = T^{-2}$, and $\alpha_3 = S$.
- (6) $H = \Gamma_0(3)$, which has index 4 in Γ , with $A_1 = (\rho + 2)/3, A_2 = i\infty, A_3 = (\rho - 1)/3, A_4 = 0, \alpha_1 = T^{-1}$, and $\alpha_3 = ST^{-3}S = \begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix}$.
- (7) $H = \Gamma(2)$ the principal congruence subgroup of level 2, which has index 6 in Γ and is a free group, with $A_1 = 1, A_2 = i\infty, A_3 = -1, A_4 = 0, \alpha_1 = T^{-2}$, and $\alpha_3 = ST^{-2}S = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$.

Proof. The domain (1) is of course completely classical, and the others, which can all be found somewhere in the literature, can be usually deduced by splitting the standard fundamental domain of (1) into a finite number of pieces and then applying to those a suitable finite number of elements of Γ . One can also prove the results directly in the same way as the classical proofs of (1). □

4C. The main result.

Proposition 4.4. *Keep the above notation and let H be a subgroup of finite index s in Γ . For every $Z \in \overline{\mathfrak{H}}$ we have*

$$(2i)^{k-1}rs \langle f_1, f_2 \rangle_G = \sum_{1 \leq m \leq n} \mathcal{F}(A_{i_m}, A_{i_{m+1}}; Z, \alpha_{i_m}^{-1}(Z)).$$

Proof. By [Corollary 3.5](#) and [Lemma 3.4\(4\)](#), we have

$$\begin{aligned} (2i)^{k-1}rs \langle f_1, f_2 \rangle_G &= \sum_{1 \leq m \leq n} \left(\int_{A_{i_m}}^{A_{i_{m+1}}} - \int_{\alpha_{i_m}(A_{i_m})}^{\alpha_{i_m}(A_{i_{m+1}})} \right) \sum_{1 \leq j \leq r} f_{1,j}(\tau) F_{2,j}(\tau) d\tau \\ &= \sum_{1 \leq m \leq n} \int_{A_{i_m}}^{A_{i_{m+1}}} \sum_{1 \leq j \leq r} f_{1,j}(\tau) P_j(\alpha_{i_m}; \tau) d\tau, \end{aligned}$$

proving the proposition using the definition of P_j and \mathcal{F} . □

Since we have seen that \mathcal{F} is not a “true” double integral but an explicit finite linear combination of products of two simple integrals, we see that we have achieved our goal of expressing PSP’s in terms of simple integrals. In the next section, we will specialize this formula to the fundamental domains given above.

5. The main corollaries

5A. General formulas. From the above proposition, we can deduce infinitely many expressions of PSP’s in terms of simple integrals. We give a few here.

Theorem 5.1. *Assume that f_1 and f_2 are in $M_k(G, v)$, one of them being a cusp form. Then for all Z , we have*

$$\begin{aligned}
 (2i)^{k-1}r\langle f_1, f_2 \rangle_G &= \mathcal{F}(\rho, i\infty; Z-1, Z) + \mathcal{F}(\rho, i; Z, -\frac{1}{Z}) \\
 &= \mathcal{F}(i, i\infty; Z, -\frac{1}{Z}) + \mathcal{F}(\rho, i\infty; -\frac{Z+1}{Z}, Z) \\
 &= \left(\mathcal{F}(\rho, i\infty; Z-1, Z) + \mathcal{F}(\rho, i\infty; -\frac{Z+1}{Z}, -\frac{1}{Z}) \right) / 2 \\
 &= \left(\mathcal{F}(0, i\infty; Z, Z+1) + \mathcal{F}(-1, \rho; Z, -\frac{1}{Z+1}) \right) / 2 \\
 &= \left(\mathcal{F}(0, i\infty; Z, \frac{Z}{Z+1}) + \mathcal{F}(\rho, i\infty; -\frac{1}{Z+1}, Z) \right) / 2 \\
 &= \left(\mathcal{F}(0, i\infty; Z-1, Z+1) + \mathcal{F}(-1, i; Z, -\frac{1}{Z}) \right) / 3 \\
 &= \left(\mathcal{F}(\rho, 0; \frac{Z}{Z+1}, \frac{Z}{1-2Z}) + \mathcal{F}(\rho, 1; \frac{Z-1}{Z}, \frac{Z}{Z+1}) \right) / 4 \\
 &= \left(\mathcal{F}(0, i\infty; Z-1, Z+1) + \mathcal{F}(-1, 0; Z, \frac{Z}{1-2Z}) \right) / 6 \\
 &= \left(\mathcal{F}(0, i\infty; Z-1, Z+1) + \mathcal{F}(0, i\infty; -\frac{Z+1}{Z}, \frac{Z-1}{Z}) \right) / 6.
 \end{aligned}$$

In particular, we have

$$\begin{aligned}
 (2i)^{k-1}r\langle f_1, f_2 \rangle_G &= \mathcal{F}(i, \rho; 0, i\infty) = \mathcal{F}(i, i\infty; \rho, \rho+1) \\
 &= \mathcal{F}(\rho, i\infty; i-1, i) = \mathcal{F}(\rho, i\infty; -1, 0) / 2 \\
 &= \mathcal{F}(\rho, i\infty; \rho-1, \rho+1) / 2 = \mathcal{F}(0, i\infty; \rho, \rho+1) / 2 \\
 &= \mathcal{F}(0, i\infty; -1, \rho) / 2 = \mathcal{F}(0, i\infty; -1, \rho+1) / 4 \\
 &= \mathcal{F}(0, i\infty; -1, i) / 3 = \mathcal{F}(0, i\infty; i-1, i+1) / 3 \\
 &= \mathcal{F}(0, i\infty; -1, 1) / 6
 \end{aligned}$$

as well as

$$(2i)^{k-1}r\langle f_1, f_2 \rangle_G = (\mathcal{F}(0, i\infty; -1, 0) - \mathcal{F}(-1, 0; 0, i\infty)) / 6.$$

Proof. The first collection of formulas follows from the different subgroups H and corresponding fundamental domains given in the preceding section, together with [Proposition 3.8](#), which expresses the Γ -invariance of \mathcal{F} . The formulas in the second collection are obtained from those in the first by specializing to specific values of Z and using [Proposition 3.8](#) and transitivity of the function \mathcal{F} . The details are left to the reader. □

Note that even though the final formula in the theorem involves two evaluations of the function \mathcal{F} instead of one, and so takes longer to compute, we have included

it because it is the only formula which is symmetrical in f_1 and f_2 , and because it leads directly to Haberland’s formulas, given below.

5B. Haberland’s formulas for subgroups. Even though the above theorem is sufficient for computational needs, we now reach our goal of generalizing Haberland’s formulas to general subgroups of finite index of Γ . Recall that for any cusp form f we let $r_n(f) = \int_0^{i\infty} \tau^n f(\tau) d\tau$ denote the n -th period of f , and that $T = \begin{pmatrix} 1 & \\ 0 & 1 \end{pmatrix}$.

Theorem 5.2. *If f_1 and f_2 are in $S_k(G, v)$, we have the formula*

$$6r(-2i)^{k-1} \langle f_1, f_2 \rangle_G = \sum_{m+n \leq k-2} \binom{k-2}{m+n} \binom{m+n}{m} M_{m,n}(f_1, f_2),$$

where

$$M_{m,n}(f_1, f_2) = \sum_{1 \leq j \leq r} \left((-1)^m r_m(f_{1,j}) \overline{r_n(f_{2,j} |_k T)} - (-1)^n r_m(f_{1,j} |_k T) \overline{r_n(f_{2,j})} \right),$$

and where we recall that $f_{i,j} = f_i |_k \gamma_j$. In particular, we have

$$\begin{aligned} -6r(-2i)^{k-2} \langle f, f \rangle_G &= \sum_{m+n \leq k-2} \binom{k-2}{m+n} \binom{m+n}{m} \sum_{1 \leq j \leq r} (-1)^m \Im \left(r_m(f_{1,j}) \overline{r_n(f_{2,j} |_k T)} \right). \end{aligned}$$

Proof. As already mentioned, by the binomial theorem we have

$$\mathcal{J}(-1, 0; 0, i\infty) = \sum_{1 \leq j \leq r} \sum_{0 \leq n \leq k-2} (-1)^n \binom{k-2}{n} \overline{r_n(f_{2,j})} \int_{-1}^0 \tau^{k-2-n} f_{1,j}(\tau) d\tau.$$

Setting $\tau = -1/(z + 1) = ST(z) = U(z)$, we have

$$\begin{aligned} \int_{-1}^0 \tau^{k-2-n} f_{1,j}(\tau) d\tau &= (-1)^{k-2-n} \int_0^{i\infty} (z + 1)^n f_{1,j} |_k U(z) dz \\ &= (-1)^{k-2-n} \sum_{0 \leq m \leq n} \binom{n}{m} r_m(f_{1,j} |_k U), \end{aligned}$$

so using the trivial equality $r_{k-2-n}(f) = (-1)^{k-1-n} r_n(f |_k S)$, we obtain

$$\begin{aligned} \mathcal{J}(-1, 0; 0, i\infty) &= (-1)^{k-2} \sum_{0 \leq m \leq n \leq k-2} \binom{k-2}{n} \binom{n}{m} \sum_{1 \leq j \leq r} r_m(f_{1,j} |_k U) \overline{r_n(f_{2,j})} \\ &= \sum_{0 \leq m \leq n \leq k-2} (-1)^{n+1} \binom{k-2}{n} \binom{n}{m} \sum_{1 \leq j \leq r} r_m(f_{1,j} |_k U) \overline{r_{k-2-n}(f_{2,j} |_k S)}. \end{aligned}$$

By Lemma 3.7(2), \mathcal{J} does not depend on the chosen representatives of right cosets, so replacing γ_j by $\gamma_j S$ and then changing n into $k - 2 - n$ gives

$$\begin{aligned} &\mathcal{J}(-1, 0; 0, i\infty) \\ &= \sum_{m+n \leq k-2} (-1)^{k-1-n} \binom{k-2}{m+n} \binom{m+n}{m} \sum_{1 \leq j \leq r} r_m(f_{1,j} |_k T) \overline{r_n(f_{2,j})}. \end{aligned}$$

By symmetry, we have

$$\begin{aligned} &\mathcal{J}(0, i\infty; -1, 0) \\ &= \sum_{m+n \leq k-2} (-1)^{k-1-m} \binom{k-2}{m+n} \binom{m+n}{m} \sum_{1 \leq j \leq r} r_m(f_{1,j}) \overline{r_n(f_{2,j} |_k T)}, \end{aligned}$$

so the last formula of Theorem 5.1 gives us the first formula of Theorem 5.2. The second formula of Theorem 5.2 follows immediately. \square

Even though we will not need the following proposition, note that it can be proved in the same way.

Proposition 5.3. *Under the same assumptions as above, we have*

$$\begin{aligned} &\sum_{m+n \leq k-2} \binom{k-2}{m+n} \binom{m+n}{m} \\ &\cdot \sum_{1 \leq j \leq r} ((-1)^m r_m(f_{1,j}) \overline{r_n(f_{2,j} |_k T)} + (-1)^n r_m(f_{1,j} |_k T) \overline{r_n(f_{2,j})}) \\ &= \sum_{1 \leq j \leq r} \sum_{m+n=k-2} (-1)^m \binom{k-2}{m} r_m(f_{1,j}) \overline{r_n(f_{2,j})}. \end{aligned}$$

Proof. Simply expand as above the identity

$$\mathcal{J}(-1, 0; 0, i\infty) + \mathcal{J}(0, i\infty; -1, 0) = -\mathcal{J}(0, i\infty; 0, i\infty). \quad \square$$

Corollary 5.4 (Haberland). *Assume that $G = \Gamma$, so that $r = 1$, $v = 1$, and k is even. We have*

$$3(-2i)^{k-1} \langle f_1, f_2 \rangle = \sum_{\substack{m+n \leq k-2 \\ m+n \equiv 1 \pmod{2}}} \binom{k-2}{m+n} \binom{m+n}{m} (-1)^m r_m(f_1) \overline{r_n(f_2)},$$

and

$$\sum'_{\substack{m+n \leq k-2 \\ m+n \equiv 0 \pmod{2}}} \binom{k-2}{m+n} \binom{m+n}{m} (-1)^m r_m(f_1) \overline{r_n(f_2)} = 0,$$

where \sum' means that the term $m + n = k - 2$ occurs with coefficient $1/2$. \square

6. Using Theorem 5.1

We now consider methods for computing PSP's based on the results obtained above. First, let us consider one of the formulas of Theorem 5.1, for instance the formula

$$6r(2i)^{k-1} \langle f_1, f_2 \rangle_G = \mathcal{J}(0, i\infty; -1, 1).$$

Once again we will assume for simplicity that $G = \Gamma$ but the reasoning is completely general. We have

$$\mathcal{J}(0, i\infty; -1, 1) = \sum_{0 \leq n \leq k-2} (-1)^n \binom{k-2}{n} \int_0^{i\infty} \tau^{k-2-n} f_1(\tau) d\tau \overline{\int_{-1}^1 \tau^n f_2(\tau) d\tau},$$

so the problem boils down to the computation of $k - 1$ integrals involving f_1 and $k - 1$ integrals involving f_2 (in the general case, this becomes $r(k - 1)$ integrals).

The computation of $\int_0^{i\infty} \tau^{k-2-n} f(\tau) d\tau = r_{k-2-n}(f)$ can be done in two quite different ways. On the one hand, we can apply the above-mentioned theory of double-exponential integration, which here works very well since it is only a *simple* and not a double integral.

An important implementation remark must be noted here: Since $f(\tau)$ may be costly to compute, it is preferable to use the integration method on the *vector-valued* function $(1, \tau, \dots, \tau^{k-2})f(\tau)$ or on the *polynomial-valued* function $(X - \tau)^{k-2} f(\tau)$, instead of on each component individually, since this only requires one evaluation of f instead of $k - 1$.

On the other hand, we can use the elementary link between this integral and the value of the Λ -function attached to f : Indeed, we have trivially

$$r_j(f) = i^{j+1} \Lambda(f, j + 1),$$

where $\Lambda(f, s) = (2\pi)^{-s} \Gamma(s) L(f, s)$ satisfies the functional equation

$$\Lambda(f, k - s) = (-1)^{k/2} \Lambda(f, s).$$

Thus, using the standard method explained above, but here in a *much* simpler context because the inverse Mellin transform of $(2\pi)^{-s} \Gamma(s)$ is simply $e^{-2\pi x}$, we obtain the formula

$$\Lambda(f, s) = \sum_{n \geq 1} \frac{a(n)}{(2\pi n)^s} \Gamma(s, 2\pi n t_0) + (-1)^{k/2} \sum_{n \geq 1} \frac{a(n)}{(2\pi n)^{k-s}} \Gamma(k - s, 2\pi n / t_0),$$

where

$$\Gamma(s, x) = \int_x^\infty e^{-t} t^{s-1} dt$$

is the incomplete gamma function, which can be computed in many efficient ways.

The computation of $\int_{-1}^1 \tau^n f(\tau) d\tau$ poses slightly different problems. We can

of course still use double-exponential integration. On the other hand, the link with L -functions still exists but is slightly more subtle (unless $G = \Gamma$). Indeed, we first write $\int_{-1}^1 = \int_{-1}^0 + \int_0^1$, and then set $\tau = ST(z) = -1/(z + 1)$ in the first integral and $\tau = z/(z + 1)$ in the second integral. We obtain

$$\int_{-1}^1 \tau^n f(\tau) d\tau = (-1)^n \int_0^{i\infty} (z + 1)^{k-2-n} f(-1/(z + 1)) dz + \int_0^{i\infty} z^n (z + 1)^{k-2-n} f(z/(z + 1)) dz.$$

If $G = \Gamma$ then the transforms of f are equal to f , so by using the binomial theorem we reduce the computation to that of at most $k - 1$ periods of f . If desired we can in fact directly use Haberland's formula; see below.

If $G \neq \Gamma$, a new difficulty appears: Since the transforms of f by Γ are not in general equal to f , we have to compute their periods. The doubly exponential integration method is of course always available, but the use of the L -function explained above now requires the knowledge of the Fourier expansions at infinity of the functions $f_j = f|_k \gamma_j$, using the notation of the beginning of this section; equivalently, given $f \in M_k(G, v)$ in some way, we need to compute the Fourier expansion of f at the *cusps* of G , not only at infinity. This is still another computational problem which we do not consider here.

Table 4 presents some timings to compute $\langle f, f \rangle_G$ to the given number N of decimals using this method, without using at all the functional equation but only double-exponential integration, so as to keep it as general as possible. Note that in my implementation, the fastest among the formulas given by Theorem 5.1 for Δ , Δ_5 , and Δ_{11} is the one given above involving $\mathcal{F}(0, i\infty; -1, 1)$, but this may not be the case for other implementations.

As an illustration of the power of double-exponential integration, note that for instance to compute $\langle \Delta, \Delta \rangle$ to 500 decimal digits, we only need 500 sample points, so only 1000 evaluations of Δ (which is of course efficiently computed using the equality $\Delta(\tau) = \eta^{24}(\tau)$).

To summarize, in order to use Theorem 5.1 in the simplest possible manner, I suggest using the doubly exponential integration methods, since here they only apply to simple integrals.

f	$N = 19$	38	57	96	250	500
Δ	0.06	0.06	0.14	0.19	2.02	11.3
Δ_5	0.35	0.46	1.16	1.60	17.1	94.3
Δ_{11}	0.67	0.89	2.24	3.11	33.7	188

Table 4. Timings (in seconds) to compute $\langle f, f \rangle_G$ to N decimal places using Theorem 5.1.

f	$N = 19$	38	57	96	250	500
Δ	0.02	0.02	0.06	0.08	0.86	4.96
Δ_5	0.23	0.29	0.72	1.00	10.5	58.4
Δ_{11}	0.48	0.61	1.48	2.12	22.0	122.5

Table 5. Timings (in seconds) to compute $\langle f, f \rangle_G$ to N decimal places using [Theorem 5.2](#).

7. Using [Theorem 5.2](#)

As mentioned above, a variant is to directly use [Theorem 5.2](#). This should be done in the following way: Using either double-exponential integration or the L -function method if available, we compute the $(k-1)r$ periods $r_m(f_{1,j})$, as well as the $(k-1)r$ periods $r_n(f_{2,j})$ if $f_1 \neq f_2$ (as mentioned above, these should be computed as r vectors with $k-1$ components). It is *not* necessary to compute the periods of $f_{1,j}|_k T$ and $f_{2,j}|_k T$. Indeed, we can write $\gamma_j T = g_j \gamma_{t(j)}$, where $g_j \in G$ and $j \mapsto t(j)$ is a permutation of $[1, r]$. Thus, since $f_1 \in M_k(G, v)$, we have

$$r_m(f_{1,j}|_k T) = r_m(f_1|_k \gamma_j T) = v(g_j) r_m(f_{1,t(j)}),$$

so no additional computation is necessary. [Table 5](#) gives the corresponding timings.

Note that the main gain compared to the use of [Theorem 5.1](#) comes from the fact that since $f_2 = f_1$, the periods have to be computed only once.

8. Using rationality theorems

There is a more subtle way of using periods to compute Petersson scalar products, but only in the special case of Hecke eigenforms: It is a well-known theorem of Manin that in the case of $G = \Gamma$, if f is a normalized eigenform there exist positive real numbers ω^+ and ω^- such that the even (respectively, odd) periods are algebraic multiples of ω^+ (respectively, of ω^-), and that ω^+ and ω^- can be chosen such that $\langle f, f \rangle = \omega^+ \omega^-$. Since ω^+ and ω^- are essentially periods, they are thus very easy to compute as explained above, so this gives a very efficient way of computing $\langle f, f \rangle$. For instance, once one knows that

$$\langle \Delta, \Delta \rangle = \frac{225}{2048i} r_1(\Delta) r_2(\Delta),$$

without using any tricks and computing the periods using the doubly exponential integration method, we obtain the result to 500 decimals in only 9 seconds, while using the L -function method we obtain the result in 1 second, so there is no special advantage in this case.

However, in the case of congruence subgroups G of Γ , similar results hold, and here we may use rationality to our advantage. I thank N. Skoruppa for the precise statement of this theorem.

Theorem 8.1. *Denote by*

$$\gamma_j^+ = \begin{pmatrix} a_j & b_j \\ c_j & d_j \end{pmatrix}$$

a system of representatives of right cosets of $G \backslash \Gamma$. Set

$$\gamma_j^- = \begin{pmatrix} -b_j & -a_j \\ d_j & c_j \end{pmatrix} = P^{-1} \gamma_j S P,$$

where $P = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$, and for $f \in M_k(G, v)$ write $f_j^\pm = f|_k \gamma_j^\pm$. Finally, let

$$R_j^\pm(f)(X) = \int_0^{i\infty} (X \mp \tau)^{k-2} f_j^\pm d\tau,$$

and

$$P_j^\pm(f) = R_j^+(f) \pm R_j^-(f).$$

Assume that f is a normalized eigenfunction of all Hecke operators, so that the Fourier coefficients of f at infinity are algebraic, and denote by $K = \mathbb{Q}(f)$ the number field generated by them. There exist complex numbers ω^\pm such that the coefficients of the polynomials $P_j^\pm(f)(X)/\omega^\pm$ are in K . In addition, ω^\pm can be chosen so that $\omega^+ \omega^- = \langle f, f \rangle$.

Remarks. (1) I do not know if this theorem is stated explicitly in the literature, although it certainly is implicit.

(2) I thank an anonymous referee for pointing out that a similar theorem is valid with $\gamma_j^- = \begin{pmatrix} a_j & -b_j \\ -c_j & d_j \end{pmatrix} = P^{-1} \gamma_j P$ instead.

For $f = \Delta$, as mentioned above we choose for instance $\omega^+ = r_2(\Delta)/i$ and $\omega^- = r_1(\Delta)$, and we have

$$\langle \Delta, \Delta \rangle = (225/2048)\omega^+ \omega^-.$$

For $f = \Delta_5$, we choose for instance $\omega^+ = r_0(\Delta_5)/i$ and $\omega^- = r_1(\Delta_5)$, and we have

$$\langle \Delta_5, \Delta_5 \rangle = -(13/24)\omega^+ \omega^-.$$

For $f = \Delta_{11}$, we choose for instance $\omega^+ = r_0(\Delta_{11})/i$ and $\omega^- = \Re(r_0(\Delta_{11}; (\frac{1}{3} \ 0)))$ (which is one of the simplest choices), and we have

$$\langle \Delta_{11}, \Delta_{11} \rangle = (5/12)\omega^+ \omega^-.$$

Table 6 gives the timings.

f	$N = 19$	38	57	96	250	500
Δ	0.013	0.017	0.043	0.063	0.75	4.41
Δ_5	0.023	0.028	0.071	0.103	1.20	7.07
Δ_{11}	0.06	0.09	0.20	0.28	3.08	17.58

Table 6. Timings (in seconds) to compute $\langle f, f \rangle_G$ to N decimal places using rationality theorems.

We see that this is by far the fastest method, especially when the index $r = [\Gamma : G]$ is large, since we only need to compute two periods. Its main disadvantages are first that it is applicable only to Hecke eigenforms, and second that we need to compute the rational (or algebraic) constants which occur for each form f , which we do not know how to give in closed form, although such a formula may well exist.

References

- [1] Henri Cohen, *Advanced topics in computational number theory*, Graduate Texts in Mathematics, no. 193, Springer, New York, 2000. [MR 2000k:11144](#)
- [2] ———, *Number theory, II: Analytic and modern tools*, Graduate Texts in Mathematics, no. 240, Springer, New York, 2007. [MR 2008e:11002](#)
- [3] J. E. Cremona, *Computing the degree of the modular parametrization of a modular elliptic curve*, *Math. Comp.* **64** (1995), no. 211, 1235–1250. [MR 95j:11047](#)
- [4] Klaus Haberland, *Perioden von Modulformen einer Variabler and Gruppencohomologie, I*, *Math. Nachr.* **112** (1983), 245–282. [MR 85k:11022](#)
- [5] Loïc Merel, *Symboles de Manin et valeurs de fonctions L* , in Tschinkel and Zarhin [8], 2009, pp. 283–309. [MR 2011d:11115](#)
- [6] Vicentiu Pasol and Alexandru A. Popa, *Modular forms and period polynomials*, 2012. [arXiv 1202.5802 \[math.NT\]](#)
- [7] Alexandru A. Popa, *Rational decomposition of modular forms*, *Ramanujan J.* **26** (2011), no. 3, 419–435. [MR 2860697](#)
- [8] Yuri Tschinkel and Yuri Zarhin (eds.), *Algebra, arithmetic, and geometry: In honor of Yu. I. Manin*, vol. 2, Progress in Math., no. 270, Birkhäuser, Boston, 2009. [MR 2010k:00009](#)
- [9] Mark Watkins, *Computing the modular degree of an elliptic curve*, *Experiment. Math.* **11** (2002), no. 4, 487–502. [MR 2004c:11091](#)
- [10] D. Zagier, *Modular parametrizations of elliptic curves*, *Canad. Math. Bull.* **28** (1985), no. 3, 372–384. [MR 86m:11041](#)

HENRI COHEN: Henri.Cohen@math.u-bordeaux1.fr

Université Bordeaux I, Institut de Mathématiques de Bordeaux, 351 Cours de la Libération,
33405 Talence Cedex, France

VOLUME EDITORS

Everett W. Howe
Center for Communications Research
4320 Westerra Court
San Diego, CA 92121-1969
United States

Kiran S. Kedlaya
Department of Mathematics
University of California, San Diego
9500 Gilman Drive #0112
La Jolla, CA 92093-0112

Front cover artwork based on a detail of
Chicano Legacy 40 Años ©2010 Mario Torero.

The contents of this work are copyrighted by MSP or the respective authors.
All rights reserved.

Electronic copies can be obtained free of charge from <http://msp.org/obs/1>
and printed copies can be ordered from MSP (contact@msp.org).

The Open Book Series is a trademark of Mathematical Sciences Publishers.

ISSN: 2329-9061 (print), 2329-907X (electronic)

ISBN: 978-1-935107-00-2 (print), 978-1-935107-01-9 (electronic)

First published 2013.



MATHEMATICAL SCIENCES PUBLISHERS

798 Evans Hall #3840, c/o University of California, Berkeley CA 94720-3840
contact@msp.org <http://msp.org>

Tenth Algorithmic Number Theory Symposium

The Algorithmic Number Theory Symposium (ANTS), held biennially since 1994, is the premier international forum for research in computational number theory. ANTS is devoted to algorithmic aspects of number theory, including elementary, algebraic, and analytic number theory, the geometry of numbers, arithmetic algebraic geometry, the theory of finite fields, and cryptography. This volume is the proceedings of the tenth ANTS meeting, held July 9–13, 2012, at the University of California, San Diego. It includes revised and edited versions of the 25 refereed papers presented at the conference, together with extended abstracts of two of the five invited talks.

TABLE OF CONTENTS

Deterministic elliptic curve primality proving for a special sequence of numbers — Alexander Abatzoglou, Alice Silverberg, Andrew V. Sutherland, and Angela Wong	1
Imaginary quadratic fields with isomorphic abelian Galois groups — Athanasios Angelakis and Peter Stevenhagen	21
Iterated Coleman integration for hyperelliptic curves — Jennifer S. Balakrishnan	41
Finding ECM-friendly curves through a study of Galois properties — Razvan Bärbulescu, Joppe W. Bos, Cyril Bouvier, Thorsten Kleinjung, and Peter L. Montgomery	63
Two grumpy giants and a baby — Daniel J. Bernstein and Tanja Lange	87
Improved techniques for computing the ideal class group and a system of fundamental units in number fields — Jean-François Biasse and Claus Fieker	113
Conditionally bounding analytic ranks of elliptic curves — Jonathan W. Bober	135
A database of elliptic curves over $\mathbb{Q}(\sqrt{5})$: a first report — Jonathan Bober, Alyson Deines, Arian Klages-Mundt, Benjamin LeVeque, R. Andrew Ohana, Ashwath Rabindranath, Paul Sharaba, and William Stein	145
Finding simultaneous Diophantine approximations with prescribed quality — Wieb Bosma and Ionica Smeets	167
Success and challenges in determining the rational points on curves — Nils Bruin	187
Solving quadratic equations in dimension 5 or more without factoring — Pierre Castel	213
Counting value sets: algorithm and complexity — Qi Cheng, Joshua E. Hill, and Daqing Wan	235
Haberland's formula and numerical computation of Petersson scalar products — Henri Cohen	249
Approximate common divisors via lattices — Henry Cohn and Nadia Heninger	271
Explicit descent in the Picard group of a cyclic cover of the projective line — Brendan Creutz	295
Computing equations of curves with many points — Virgile Ducet and Claus Fieker	317
Computing the unit group, class group, and compact representations in algebraic function fields — Kirsten Eisenträger and Sean Hallgren	335
The complex polynomials $P(x)$ with $\text{Gal}(P(x) - t) \cong M_{23}$ — Noam D. Elkies	359
Experiments with the transcendental Brauer-Manin obstruction — Andreas-Stephan Elsenhans and Jörg Jahnel	369
Explicit 5-descent on elliptic curves — Tom Fisher	395
On the density of abelian surfaces with Tate-Shafarevich group of order five times a square — Stefan Keil and Remke Kloosterman	413
Improved CRT algorithm for class polynomials in genus 2 — Kristin E. Lauter and Damien Robert	437
Fast computation of isomorphisms of hyperelliptic curves and explicit Galois descent — Reynald Lercier, Christophe Ritzenthaler, and Jeroen Sijsling	463
Elliptic factors in Jacobians of hyperelliptic curves with certain automorphism groups — Jennifer Paulhus	487
Isogeny volcanoes — Andrew V. Sutherland	507
On the evaluation of modular polynomials — Andrew V. Sutherland	531
Constructing and tabulating dihedral function fields — Colin Weir, Renate Scheidler, and Everett W. Howe	557