MATHEMATICS OF COMPUTATION
VOLUME 58, NUMBER 198
APRIL 1992, PAGES 807–814

ON THE COMPUTATIONAL COMPLEXITY OF MODULAR SYMBOLS

DORIAN GOLDFELD

ABSTRACT. Efficient algorithms are obtained for integrating holomorphic differential one-forms along simple geodesic lines on those compact Riemann surfaces which are given as quotients of the upper half-plane by a congruence subgroup Γ of $\mathrm{SL}(2, \mathbb{Z})$. We may assume that every geodesic line passes through a cusp which is unique up to Γ-equivalence. The algorithms we construct run in polynomial time in the height of this cusp.

1. INTRODUCTION AND STATEMENT OF RESULTS

Let Γ be a congruence subgroup of finite index in $\mathrm{SL}(2, \mathbb{Z})$. Then Γ acts properly discontinuously on $\mathfrak{h}$, the upper half-plane, and this action extends naturally to $\mathbb{Q} \cup \{i\infty\}$. Consider the compactified Riemann surface $X = \Gamma\backslash\mathfrak{h} \cup \{i\infty\} \cup \mathbb{Q}$ of genus $g > 0$. Let $f(z)dz$ be a holomorphic differential one-form on X. For $\alpha, \beta \in \mathbb{Q} \cup \{i\infty\}$ we let $\{\alpha, \beta\}_\Gamma$ denote the geodesic line joining α to β. Recall that the geodesic lines are either semicircles intersecting the real axis at α, β, or lines $\{\alpha + it | t \geq 0\}$ with $\alpha \in \mathbb{Q}$. Modular symbols are period integrals

$$2\pi i \int_{\{\alpha, \beta\}_\Gamma} f(z)\, dz,$$

and our aim is to provide fast algorithms for their computation. Such computations are necessary, for example, in the verification of the Taniyama-Weil conjecture (see Cremona [2]). If $\{\Omega_1, \Omega_2, \ldots, \Omega_{2g}\}$ denote the periods of X, then it is known [5, 7], that for $\alpha, \beta \in \mathbb{Q} \cup \{i\infty\}$

$$2\pi i \int_{\{\alpha, \beta\}_\Gamma} f(z)\, dz = \sum_{j=1}^{2g} c_j \Omega_j, \tag{1}$$

where c_j lies in the totally real field generated by $\mathbb{Q}$ and the Fourier coefficients of $f(z)$. It follows that the c_j may be determined exactly after a finite amount of computation.

In order to define the complexity of our algorithms, we introduce some simple notation. Every rational number α may be written in the form $\alpha = a/b$, where a, b are a pair of relatively prime integers. Define a height function h on $\mathbb{Q}$ by setting $h(\alpha) = \max(|a|, |b|)$. Extend h to $\mathbb{Q}(i) \cup \{i\infty\}$ by putting $h(i\infty) = 0$

Received July 2, 1990.
1991 *Mathematics Subject Classification.* Primary 11F67, 11Y16.
Supported in part by NSF grant no. 9003907.

and $h(\alpha+i\beta) = \max(h(\alpha), h(\beta))$ for $\alpha, \beta \in \mathbb{Q}$. We shall use the terminology "arithmetic operation" to denote an exact arithmetic operation on $\mathbb{Q}(i)$ of type $\alpha \pm \beta$, $\alpha \cdot \beta$ or α/β, and we assume the existence of a machine that can perform such operations. Clearly, we may extend the domain of our operations to $\mathbb{Q}(i) \cup \{i\infty\}$. Given a function $F: \mathbb{Q}(i) \cup \{i\infty\} \to \mathbb{C}$ and $\alpha \in \mathbb{Q}$, we shall say $F(\alpha)$ can be computed to within an error ε by our machine if after a finite number of arithmetic operations it can find a rational complex number $c \in \mathbb{Q}(i)$ such that $|F(\alpha) - c| < \varepsilon$. For each $\varepsilon > 0$, the complexity of our algorithm for computing $F(\alpha)$ is given by an integer $C = C(F(\alpha), \varepsilon)$ which denotes the number of arithmetic operations needed to compute $F(\alpha)$ to within error ε.

For simplicity of exposition, we specialize to the case where

$$\Gamma = \Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z}) \;\middle|\; c \equiv 0 \pmod{N} \right\},$$

and $X = X_0(N) = \Gamma_0(N) \backslash \mathfrak{h} \cup \mathbb{Q} \cup \{i\infty\}$. We shall let $\{\alpha, \beta\} = \{\alpha, \beta\}_{\Gamma_0(N)}$ denote an arbitrary geodesic line on $X_0(N)$ with $\alpha, \beta \in \mathbb{Q} \cup \{i\infty\}$.

Theorem 1. *Let $f(z)dz$ be a holomorphic Hecke differential one-form on $X_0(N)$ whose Fourier coefficients are known. Let $\{\alpha, \beta\}$ be a geodesic line on $X_0(N)$ of height $H = \max(h(\alpha), h(\beta))$. Fix $\varepsilon > 0$, $\rho \geq 0$. Then there exists a constant $c = c(\varepsilon) > 0$ such that for squarefree $N > c$, the modular symbol*

$$2\pi i \int_{\{\alpha, \beta\}} f(z)\, dz$$

may be computed to within an error $\exp(-N^{\rho+\varepsilon/2})(\log H)$ in at most

$$N^{1+\rho+\varepsilon}(\log H)$$

exact arithmetic operations.

The question remains as to whether Theorem 1 is strong enough to be able to exactly determine the coefficients c_j (of formula (1)), assuming the periods Ω_j of $X_0(N)$ are known. In this case we say that the modular symbol can be "evaluated exactly." Unfortunately, this appears to be an extremely difficult problem, since it depends on lower bounds for the periods. If the Jacobian variety $J_0(N)$ of $X_0(N)$ contains an elliptic curve E as a factor, and if Ω_1, Ω_2 denote the periods of E, then it can be shown that

$$N^{-N} \ll |\Omega_1|, \; |\Omega_2|. \tag{2}$$

The stronger estimate

$$N^{-\kappa} \ll |\Omega_1|, \; |\Omega_2| \tag{3}$$

for sufficiently large κ is equivalent to a well-known conjecture of Szpiro for E (see [3]). At present, lower bounds of the above type for the periods of $X_0(N)$ associated to higher-dimensional abelian varieties seem to be completely unknown. It seems likely, however, that estimates of type (3) should hold (see Lockhart [4]).

Theorem 2. *Let $f(z)dz$ be a holomorphic Hecke differential one-form on $X_0(N)$ whose Fourier coefficients are rational and known. Let $\{\alpha, \beta\}$ be a geodesic line*

on $X_0(N)$ *of height* $H = \max(h(\alpha), h(\beta))$. *Fix* $\varepsilon > 0$. *Then there exists a constant* $c = c(\varepsilon) > 0$ *such that for squarefree* $N > c$, *the modular symbol*

$$2\pi i \int_{\{\alpha, \beta\}} f(z)\, dz$$

may be computed exactly in at most

$$N^{2+\varepsilon} (\log H)$$

exact arithmetic operations.

If we assume Szpiro's conjecture [3], then Theorem 2 can be improved. In this case the number of exact arithmetic operations will be bounded by $N^{1+\varepsilon}(\log H)$. The algorithms found run in polynomial time in the height of the cusp, but not in polynomial time in the level N. It is probable that the number of exact arithmetic operations needed in Theorem 2 should be at most $(\log N)^{\kappa}(\log H)$ for some constant $\kappa > 2$, but this seems completely out of reach at present.

2. Proof of Theorems

Theorem 1 can be proved rather simply in the special case that N is prime. The proof is based on the following elementary lemma.

Lemma 3. *Let* N *be a prime number. Then every* $g = \left(\begin{smallmatrix} a & b \\ cN & d \end{smallmatrix}\right) \in \Gamma_0(N)$ *may be factored in the form*

$$g = w_1 \cdot g_1 \cdot w_2 \cdot g_2 \cdots w_\tau \cdot g_\tau,$$

where

$$g_i = \begin{pmatrix} a_i & b_i \\ N & d_i \end{pmatrix} \in \Gamma_0(N), \qquad w_i = \begin{pmatrix} 1 & u_i \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ q_i N & 1 \end{pmatrix}$$

with $q_i, u_i \in \mathbb{Z}$, *and* $\tau \leq \log|c|/\log 2$.

Proof. Choose an integer u so that

$$g' = \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} g = \begin{pmatrix} a' & b' \\ cN & d \end{pmatrix}$$

with $|a'| < |cN|/2$. If $|a'| < |c|$, then consider

$$\begin{pmatrix} 1 & 0 \\ qN & 1 \end{pmatrix} g' = \begin{pmatrix} a' & b' \\ (a'q + c)N & d' \end{pmatrix}.$$

Clearly, we may choose an integer q so that $|a'q + c| < |a'|/2 < \cdots < |c|/2$. Hence,

$$g = \begin{pmatrix} 1 & -u \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -qN & 1 \end{pmatrix} \begin{pmatrix} a' & b' \\ c'N & d' \end{pmatrix}$$

with $|c'| < |c|/2$.

On the other hand, if $|a'| > |c|$, then we may choose integers x, y such that $cx + dy = 1$. In fact $x = -b'N - md$, $y = a' + mc$, for any integer m. Choose m so that $|y| < |c|/2$. For this choice, we must have $0 < |m| < N$, since $|c| < |a'| < |Nc|/2$. Hence, $(m, N) = 1$, and by the Euclidean algorithm, we can find integers v, z such that $xz - vyN = 1$. It follows that

$$g = \begin{pmatrix} 1 & -u \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a_1 & b_1 \\ N & d_1 \end{pmatrix} \begin{pmatrix} v & -z \\ -yN & x \end{pmatrix},$$

where $|y| < |c|/2$ and

$$\begin{pmatrix} a_1 & b_1 \\ N & d_1 \end{pmatrix} = \begin{pmatrix} a' & b' \\ cN & d \end{pmatrix} \begin{pmatrix} x & z \\ yN & v \end{pmatrix}.$$

Continuing inductively, the proof of the lemma can be completed. □

Proof of Theorem 1. The homomorphism $\phi : \Gamma_0(N) \to H_1(X_0(N), \mathbb{Z})$ given by

$$\phi(g) = \{z, g(z)\}$$

is independent of $z \in \mathfrak{h} \cup \mathbb{Q} \cup \{i\infty\}$. Moreover, $\ker(\phi)$ is generated by the commutators, elliptic and parabolic elements of $\Gamma_0(N)$ (see [5]). Following [3], we obtain from the functional equation for the Hecke cusp form $f(z)$ for $g = \left(\begin{smallmatrix} a & b \\ cN & d \end{smallmatrix}\right) \in \Gamma_0(N)$ that

$$2\pi i \int_{\phi(g)} f(z)\, dz = \sum_{n=1}^{\infty} \frac{A(n)}{n} \exp\left(\frac{-2\pi n}{|cN|}\right) \left[\exp\left(\frac{2\pi i n a}{cN}\right) - \exp\left(\frac{-2\pi i n d}{cN}\right)\right], \tag{4}$$

where

$$f(z) = \sum_{n=1}^{\infty} A(n) \exp(2\pi i n z)$$

is the Fourier expansion of $f(z)$. Since $|A(n)| \ll n^{1/2+\varepsilon}$, it is easy to see that the integral on the left side of (4) may be computed to within an error $\exp(-N^{\rho+\varepsilon/2})$ in at most $N^{1+\rho+\varepsilon}$ exact arithmetic operations. □

We now give the algorithm for computing the modular symbol

$$2\pi i \int_{\{\alpha, \beta\}} f(z)\, dz$$

in the case when N is prime.

Step 1. Determine if $\{\alpha, \beta\}$ is a closed cycle. If it is, find $g \in \Gamma_0(N)$ such that $\beta = g(\alpha)$ and immediately continue with Step 2. If it is not a closed cycle, go to Step 3.

To see if g exists, and to find g, we may proceed as follows. For $x \in \mathbb{Q} \cup \{i\infty\}$, the Euclidean algorithm allows us to find $\sigma_x \in \mathrm{SL}(2, \mathbb{Z})$ such that $\sigma_x(0) = x$. Namely, if $x = x_1/x_2$ with $(x_1, x_2) = 1$, then $\sigma_x = \left(\begin{smallmatrix} u & x_1 \\ v & x_2 \end{smallmatrix}\right)$ with $ux_2 - vx_1 = 1$. If $x = i\infty$, then $\sigma_x = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. Since the stabilizer of 0 is the subgroup $\left(\begin{smallmatrix} 1 & 0 \\ * & 1 \end{smallmatrix}\right)$, it follows that the element

$$\sigma_y \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} \sigma_x^{-1} \in \mathrm{SL}(2, \mathbb{Z})$$

with $b \in \mathbb{Z}$ is the most general element that maps x to y. Hence, the existence of $g \in \Gamma_0(N)$ such that $\beta = g(\alpha)$ is equivalent to the existence of $0 \le b < N$ such that

$$g = \sigma_\beta \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} \sigma_\alpha^{-1} \in \Gamma_0(N).$$

Step 2. Factor the element $g = w_1 \cdot g_1 \cdot w_2 \cdot g_2 \cdots w_\tau \cdot g_\tau$ found in Step 1 according to Lemma 3. Since the elements w_i are in $\ker(\phi)$, it follows that

$$2\pi i \int_{\{\alpha,\beta\}} f(z)\,dz = \sum_{i=1}^{\tau} 2\pi i \int_{\phi(g_i)} f(z)\,dz,$$

where each $\int_{\phi(g_i)} f(z)\,dz$ can be computed by (4).

Step 3. If $\{\alpha, \beta\}$ is not a closed cycle, let

$$\{\alpha, \beta\} = \{\alpha, i\infty\} + \{i\infty, \beta\}.$$

This reduces to the case $\{\alpha, i\infty\}$, which we may assume is not a closed cycle. We may, therefore, apply the formula of Manin ([5, Theorem 3.5]), to get

$$(3 - A(2)) \int_{\alpha}^{i\infty} f(z)\,dz = \sum_{\substack{d|2 \\ b \bmod d}} \int_{\{\alpha, \frac{2}{d^2}\alpha + \frac{b}{d}\}} f(z)\,dz.$$

Since each cycle $\{\alpha, \frac{2}{d^2}\alpha + \frac{b}{d}\}$ above is closed, this reduces the problem to a sum of modular integrals over closed cycles which may be evaluated by Steps 1 and 2.

If N is not a prime, then the previous algorithm does not work. There seems to be no simple analogue of Lemma 3. A more subtle procedure is required.

Writing $\{\alpha, \beta\} = \{0, \beta\} - \{0, \alpha\}$, we need only consider $\{0, \alpha\}$ with height $h(\alpha) = H$. Let

$$\frac{p_{-2}}{q_{-2}}, \frac{p_{-1}}{q_{-1}}, \ldots, \frac{p_\tau}{q_\tau} = \alpha$$

denote the continued fraction convergents to α, where

$$\frac{p_{-2}}{q_{-2}} = \frac{0}{1}, \quad \frac{p_{-1}}{q_{-1}} = \frac{1}{0}, \quad \frac{p_0}{q_0} = \frac{p_0}{1}, \ldots.$$

It is well known that

$$p_r q_{r-1} - p_{r-1} q_r = (-1)^{r-1} \qquad (-1 \le r \le \tau),$$

$p_r \ge p_{r-1} + p_{r-2}$ and $q_r \ge q_{r-1} + q_{r-2}$, from which it is easy to show that $\tau \ll \log H$. It follows that

$$\{0, \alpha\} = \sum_{r=1}^{\tau} \left\{ \frac{p_{r-1}}{q_{r-1}}, \frac{p_r}{q_r} \right\} = \sum_{r=1}^{\tau} \{\sigma_r(0), \sigma_r(i\infty)\},$$

where

$$\sigma_r = \begin{pmatrix} (-1)^{r-1} p_r & p_{r-1} \\ (-1)^{r-1} q_r & q_{r-1} \end{pmatrix}.$$

We obtain

$$\int_{\{0,\alpha\}} f(z)\,dz = \sum_{r=1}^{\tau} \int_0^{i\infty} f(\sigma_r(z))\,d(\sigma_r(z)). \tag{5}$$

The problem is reduced to evaluating

$$\int_0^{i\infty} f(\sigma(z))\,d(\sigma(z)),$$

where

$$\sigma = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z}).$$

Since $f(z)dz$ is a Hecke differential one-form, it is an eigenfunction of the Hecke algebra $\mathfrak{H}$, which is a commutative semisimple $\mathbb{Q}$-algebra generated by the Hecke operators T_p (for primes $p \nmid N$), where

$$T_p = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} + \sum_{j=0}^{p-1} \begin{pmatrix} 1 & j \\ p & 0 \end{pmatrix},$$

and the involutions W_M (for $M|N$), where

$$W_M = \begin{pmatrix} Mx & y \\ Nz & Mw \end{pmatrix}, \qquad M^2xw - Nzy = M.$$

The W_M normalize $\Gamma_0(N)$ and satisfy

$$W_{M'M''} = W_{M'}W_{M''} \qquad (\text{for } (M', M'') = 1 \text{ and } M'M'' \mid N),$$

$$\prod_{q^r \| N} W_{q^r} = W_N = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix},$$

where the above product goes over all prime powers q^r exactly dividing N.

The action of $\mathfrak{H}$ on $f(z)dz$ is given as follows:

$$T_p f(z)dz = f(pz)d(pz) + \sum_{j=0}^{p-1} f\left(\begin{pmatrix} 1 & j \\ p & 0 \end{pmatrix} z\right) d\left(\begin{pmatrix} 1 & j \\ p & 0 \end{pmatrix} z\right)$$

$$= A(p)f(z)dz,$$

where $A(p)$ is the pth Fourier coefficient of $f(z)$. Furthermore,

$$W_M f(z)dz = f(W_M z)d(W_M z) = \lambda_M f(z)dz,$$

where the eigenvalue λ_M is independent of $x, y, z, w \in \mathbb{Z}$, since all the involutions of type W_M (with M fixed) are equivalent under left or right multiplication by $\Gamma_0(N)$. There is a simple relation between λ_M and the Fourier coefficient $A(m)$. Namely (see [1]),

$$\lambda_q = -A(q)$$

for primes $q|N$. In addition, both functions are completely multiplicative with respect to $M|N$.

Let $M_1 = \gcd(t, N)$, $t = M_1 t_1$ and $N = MM_1$. It follows that we may express

$$\sigma = \begin{pmatrix} r & s_1 \\ t & Mu_1 \end{pmatrix} \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix},$$

where $h, s_1, u_1 \in \mathbb{Z}$ are chosen so that $th + Mu_1 = u$ and $rh + s_1 = s$.

Furthermore,

$$\sigma = \begin{pmatrix} Mr & s_1 \\ Nt_1 & Mu_1 \end{pmatrix} \begin{pmatrix} \frac{1}{M} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix},$$

where $t_1 = Mt/N$ is an integer. Hence,

$$(6) \qquad \int_0^{i\infty} f(\sigma(z))\, d(\sigma(z)) = \lambda_M \int_0^{i\infty} f\left(\begin{pmatrix} 1 & h \\ 0 & M \end{pmatrix} z\right) d\left(\begin{pmatrix} 1 & h \\ 0 & M \end{pmatrix} z\right).$$

Let $W_N = \left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right)$. Then

$$\begin{pmatrix} 1 & h \\ 0 & M \end{pmatrix} = W_N \begin{pmatrix} M & 0 \\ -hN & 1 \end{pmatrix} W_N^{-1},$$

from which it easily follows that for any $U > 0$

$$\begin{aligned} &\int_0^{i\infty} f\left(\begin{pmatrix} 1 & h \\ 0 & M \end{pmatrix} z\right) d\left(\begin{pmatrix} 1 & h \\ 0 & M \end{pmatrix} z\right) \\ &\quad = \int_{\frac{iU}{\sqrt{N}}}^{i\infty} f\left(\begin{pmatrix} 1 & h \\ 0 & M \end{pmatrix} z\right) d\left(\begin{pmatrix} 1 & h \\ 0 & M \end{pmatrix} z\right) \\ &\qquad + \int_{\frac{i}{U\sqrt{N}}}^{i\infty} f\left(W_N \begin{pmatrix} M & 0 \\ -hN & 1 \end{pmatrix} z\right) d\left(W_N \begin{pmatrix} M & 0 \\ -hN & 1 \end{pmatrix} z\right). \end{aligned} \tag{7}$$

We now consider the second integral on the right side of (7). Let $M_h = \gcd(M, h)$. Clearly,

$$\begin{pmatrix} M & 0 \\ -hN & 1 \end{pmatrix} = \begin{pmatrix} \frac{M}{M_h} & l \\ \frac{-hN}{M_h} & \frac{-hNl}{M} + 1 \end{pmatrix} \begin{pmatrix} M_h & \frac{-lM_h}{M} \\ 0 & 1 \end{pmatrix}.$$

Since $(\frac{hN}{M}, \frac{M}{M_h}) = 1$, we may choose l such that

$$\frac{hN}{M} l \equiv 1 \left(\bmod \frac{M}{M_h}\right).$$

It easily follows from the above matrix identity that

$$\begin{aligned} &\int_{\frac{i}{U\sqrt{N}}}^{i\infty} f\left(W_N \begin{pmatrix} M & 0 \\ -hN & 1 \end{pmatrix} z\right) d\left(W_N \begin{pmatrix} M & 0 \\ -hN & 1 \end{pmatrix} z\right) \\ &\quad = \lambda_N \cdot \lambda_{M/M_h} \int_{\frac{i}{U\sqrt{N}}}^{i\infty} f\left(\begin{pmatrix} M_h & \frac{-lM_h}{M} \\ 0 & 1 \end{pmatrix} z\right) d\left(\begin{pmatrix} M_h & \frac{-lM_h}{M} \\ 0 & 1 \end{pmatrix} z\right) \\ &\quad = \lambda_N \cdot \lambda_{M/M_h} \int_{\frac{iM_h}{U\sqrt{N}}}^{i\infty} f(z - lM_h/M)\, dz. \end{aligned} \tag{8}$$

Combining (6), (7), (8) yields

$$\begin{aligned} &2\pi i \int_0^{i\infty} f(\sigma(z))\, d(\sigma(z)) \\ &\quad = \lambda_M \int_{\frac{U}{M\sqrt{N}}}^{\infty} \sum_{n=1}^{\infty} A(n) \exp[-2\pi ny + 2\pi inh/M]\, i dy \\ &\qquad + \lambda_N \lambda_M \lambda_{M/M_h} \int_{\frac{M_h}{U\sqrt{N}}}^{\infty} \sum_{n=1}^{\infty} A(n) \exp[-2\pi ny - 2\pi inlM_h/M]\, i dy. \end{aligned}$$

Finally,

$$\begin{aligned} &2\pi i \int_0^{i\infty} f(\sigma(z))\, d(\sigma(z)) \\ &\quad = \sum_{n=1}^{\infty} \frac{A(n)}{n} [\lambda_M \exp[-(2\pi nU/M\sqrt{N}) + 2\pi inh/M] \\ &\qquad + \lambda_N \lambda_M \lambda_{M/M_h} \exp[-(2\pi nM_h/U\sqrt{N}) - 2\pi inlM_h/M]]. \end{aligned} \tag{9}$$

Now choose $U = \sqrt{MM_h}$. Since $1 \leq M_h \leq M \leq N$, it is easy to see that the integral on the left side of (9) can be computed to within an error $\exp(-N^{\rho+\varepsilon/2})$ in at most $N^{1+\rho+\varepsilon}$ exact arithmetic operations. The proof of Theorem 1 now immediately follows from (5), since it is only necessary to compute $\tau \ll \log H$ such integrals. □

Proof of Theorem 2. It follows from the work of Shimura (see [6, 3]) that if $f(z)$ has rational Fourier coefficients, then the modular symbol (for $\sigma \in \mathrm{SL}(2, \mathbb{Z})$) is

$$2\pi i \int_0^{i\infty} f(\sigma(z))\, d(\sigma(z)) = c_1\Omega_1 + c_2\Omega_2, \tag{10}$$

where $c_1, c_2 \in \mathbb{Q}$ and Ω_1, Ω_2 denote the real and imaginary periods of an elliptic curve. Moreover, the denominators of c_1 and c_2 are absolutely bounded. In view of (8) and the lower bound (2), it is enough to compute (10) to within an error $\exp(-N^{1+\varepsilon/2})$ to be able to exactly determine c_1, c_2. As shown in the proof of Theorem 1, this may be done in $N^{2+\varepsilon}$ exact arithmetic operations. Finally, the modular symbol $2\pi i \int_{\{\alpha,\beta\}} f(z)\, dz$ is a sum of at most $O(\log H)$ integrals of type (10). This completes the proof. □

Bibliography

1. A. O. L. Atkin and J. Lehner, *Hecke operators on* $\Gamma_0(m)$, Math. Ann. **185** (1970), 134–160.
2. J. E. Cremona, *Computation of modular elliptic curves and the Birch-Swinnerton Dyer conjecture*, preprint.
3. D. Goldfeld, *Modular elliptic curves and diophantine problems*, Proc. First Canadian Number Theory Assoc. (Banff, Canada 1988), de Gruyter, New York, 1989.
4. P. T. Lockhart, *Diophantine equations and the arithmetic of hyperelliptic curves*, Ph.D. Thesis, Columbia University, 1990.
5. Ju. I. Manin, *Parabolic points and zeta-functions of modular curves,* Math. USSR Izvestija **6** (1972), 19–64.
6. G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Princeton Univ. Press, 1971.
7. G. Shimura, *On the factors of the Jacobian variety of a modular function field,* J. Math. Soc. Japan **25** (1973), 523–544.

Department of Mathematics, Columbia University, New York, New York 10027