Canad. J. Math. Vol. **59** (3), 2007 pp. 553–574

Computations of Elliptic Units for Real Quadratic Fields

Samit Dasgupta

Abstract. Let K be a real quadratic field, and p a rational prime which is inert in K. Let α be a modular unit on $\Gamma_0(N)$. In an earlier joint article with Henri Darmon, we presented the definition of an element $u(\alpha,\tau) \in K_p^\times$ attached to α and each $\tau \in K$. We conjectured that the p-adic number $u(\alpha,\tau)$ lies in a specific ring class extension of K depending on τ, and proposed a "Shimura reciprocity law" describing the permutation action of Galois on the set of $u(\alpha,\tau)$. This article provides computational evidence for these conjectures. We present an efficient algorithm for computing $u(\alpha,\tau)$, and implement this algorithm with the modular unit $\alpha(z) = \Delta(z)^2\Delta(4z)/\Delta(2z)^3$. Using $p = 3, 5, 7$, and 11, and all real quadratic fields K with discriminant $D < 500$ such that 2 splits in K and K contains no unit of negative norm, we obtain results supporting our conjectures. One of the theoretical results in this paper is that a certain measure used to define $u(\alpha,\tau)$ is shown to be $\mathbf{Z}$-valued rather than only $\mathbf{Z}_p \cap \mathbf{Q}$-valued; this is an improvement over our previous result and allows for a precise definition of $u(\alpha,\tau)$, instead of only up to a root of unity.

Introduction

Elliptic units, which are obtained by evaluating modular units at quadratic imaginary arguments of the Poincaré upper half-plane, yield an analytic construction of abelian extensions of imaginary quadratic fields. The Kronecker limit formula relates the complex absolute values of these units to values of zeta functions, and enabled Stark to prove his rank one archimedean conjecture for abelian extensions of quadratic imaginary fields [9].

A conjectural construction of an analogous theory for real quadratic fields K was proposed in [2], by replacing the infinite prime of $\mathbf{Q}$ with a prime p that remains inert in K. The completion K_p is a quadratic unramified extension of $\mathbf{Q}_p$. The construction of [2] associates to a modular unit α and any $\tau \in K - \mathbf{Q}$ an element $u(\alpha,\tau) \in K_p^\times$ which is conjectured to be a p-unit in a specific narrow ring class field of K depending on τ and denoted H_τ ([2, Conjecture 2.14], hereafter denoted Conjecture DD). In harmony with the fact that the role of ∞ is played by that of p, the construction of $u(\alpha,\tau)$ involves p-adic integration in a manner motivated by the definition of "Stark–Heegner points" given in [1] and generalized in [5].

The main theorems of [2] relate the p-adic valuation and p-adic logarithm of $u(\alpha,\tau)$ to values at 0 of partial zeta functions (classical and p-adic, respectively) attached to the extension H_τ/K, and thereby allow one to deduce Gross's p-adic analogue of Stark's conjecture (see [6]) for this extension from Conjecture DD.

In the present article we provide concrete computational evidence for Conjecture DD. The formulas of [2, §4.4] may be used to calculate the units $u(\alpha,\tau)$ to a high

Received by the editors September 27, 2004; revised August 15, 2005.
AMS subject classification: 11R37, 11R11, 11Y40.

p-adic accuracy. Using 50 digits of p-adic accuracy for $p = 3, 5, 7, 11$ and all ground fields K of positive discriminant less than 500, we are able to recognize the units $u(\alpha, \tau)$ as algebraic numbers for the fixed modular unit $\alpha = \Delta(z)^2\Delta(4z)/\Delta(2z)^3$ and all τ such that H_τ is the narrow Hilbert class field of K. In each case, the algebraic number approximated by $u(\alpha, \tau)$ is a p-unit in H_τ as predicted by Conjecture DD.

We begin by recalling the definition of $u(\alpha, \tau)$, and proving that a certain modular symbol of measures μ appearing in this definition is $\mathbf{Z}$-valued. In [2], it is only proven that μ is $\mathbf{Z}_p$-valued. In Sections 4 and 5 we describe the method and results of our computations that supply empirical evidence for Conjecture DD.

1 Definition of the Units

Let N be a positive integer. A *modular unit* is a holomorphic nowhere vanishing function on $\Gamma_0(N)\backslash\mathcal{H}$ that extends to a meromorphic function on the compact Riemann surface $X_0(N)(\mathbf{C})$. A typical example of such a unit is the modular function

$$\alpha(\tau) = \prod_{d|N} \Delta(d\tau)^{n_d} \tag{1}$$

for integers n_d such that $\sum_d n_d = 0$. For the remainder of the article, fix a choice of such integers n_d. We will assume that the corresponding modular unit α has no zero or pole at the cusp ∞ of the completed upper half plane $\mathcal{H}^* = \mathcal{H} \cup \mathbf{P}^1(\mathbf{Q})$. This assumption is equivalent to the equation

$$\sum_d n_d d = 0. \tag{2}$$

Let p be a prime number not dividing N. Given the modular unit α of level N, we may define a modular unit of level Np by the rule $\alpha^*(z) := \alpha(z)/\alpha(pz)$. The logarithmic derivatives of α and α^* are given by

$$\operatorname{dlog}\alpha(z) = 2\pi i F_2(z)\,\mathrm{d}z, \qquad \operatorname{dlog}\alpha^*(z) = 2\pi i F_2^*(z)\,\mathrm{d}z, \tag{3}$$

where $F_2(z)$ and $F_2^*(z)$ are the weight 2 Eisenstein series on $\Gamma_0(N)$ and $\Gamma_0(Np)$, respectively, given by the formulae

$$F_2(z) = -24 \sum_{d|N} d n_d E_2(dz), \qquad F_2^*(z) = F_2(z) - pF_2(pz). \tag{4}$$

Here $E_2(z)$ is the standard Eisenstein series of weight 2:

$$E_2(z) = \frac{1}{(2\pi i)^2}\left(\zeta(2) + \frac{1}{2}\sum_{\substack{m=-\infty \\ m\neq 0}}^{\infty}\sum_{n=-\infty}^{\infty}\frac{1}{(mz+n)^2}\right) \tag{5}$$

$$= -\frac{1}{24} + \sum_{n=1}^{\infty}\sigma_1(n)q^n, \quad q = e^{2\pi i\tau}.$$

(We remark that the double series used to define E_2 is not absolutely convergent and the resulting expression is not invariant under $\mathrm{SL}_2(\mathbf{Z})$.)

Let $\mathcal{M} = \mathrm{Div}_0(\Gamma_0(N)\infty)$ denote the group of degree-zero divisors on the set of cusps with denominator divisible by N. Note that $\mathcal{M}$ has a natural left action by $\Gamma_0(N)$. A *partial modular symbol* with values in a group A is simply a group homomorphism from $\mathcal{M}$ to A. If ψ is a partial modular symbol and $r, s \in \Gamma_0(N)\infty$, then one writes

$$\psi\{r \to s\} \text{ or } \psi_m \text{ for } \psi([r] - [s]), \text{ where } m = [r] - [s] \in \mathcal{M}.$$

Assumption (2) implies that the differential $\mathrm{d}\log\alpha$ on $\mathcal{H}^*$ is regular on $\Gamma_0(N)\infty$, so we may define a partial modular symbol ψ with values in $\mathbf{Z}$ by the rule

$$\psi\{r \to s\} := \frac{1}{2\pi i}\int_r^s \mathrm{d}\log\alpha = \int_r^s F_2(z)\,\mathrm{d}z,$$

where the complex line integral on the right side is taken along any smooth path P in $\mathcal{H}^*$ connecting the cusps r and s. The rational integer $\psi\{r \to s\}$ may be understood as the winding number of the closed loop $\alpha(P)$ around the origin in the complex plane. The function ψ (which was denoted m_α in [2]) is called the partial modular symbol attached to α, and its value will be expressed in terms of classical Dedekind sums in Section 2.

The Eisenstein series of (4) and (5) are part of a natural *family* of Eisenstein series of varying weights. For even $k \geq 2$, consider the standard Eisenstein series of weight k:

$$E_k(z) = \frac{2(k-1)!}{(2\pi i)^k}\sum_{m,n=-\infty}^{\infty}{}' \frac{1}{(mz+n)^k} = -\frac{B_k}{2k} + \sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n. \tag{6}$$

Define likewise the higher weight Eisenstein series

$$\begin{aligned} F_k(z) &= -24\sum_{d|N} n_d \cdot d \cdot E_k(dz) \\ &= -\frac{48(k-1)!}{(2\pi i)^k}\sum_{m,n=-\infty}^{\infty}{}' \Big(\frac{1}{(mz+n)^k}\sum_{d|(N,m)} n_d d\Big) \\ &= -24\sum_{n=1}^{\infty}\sigma_{k-1}(n)\sum_{d|N} n_d d q^{nd}. \end{aligned} \tag{7}$$

The F_k are modular forms of weight k on $\Gamma_0(N)$ that are holomorphic on the upper half plane. Note that these Eisenstein series have no constant term and hence are holomorphic at the cusp ∞. We also define, for the purpose of p-adic interpolation, the function $F_k^*(z) = F_k(z) - p^{k-1}F_k(pz)$. We extend the definition of $E_k(z)$ and $F_k(z)$ to all $k \geq 2$ by letting $E_k = F_k = 0$ for k odd.

Let $\mathbf{X}$ denote the subspace of $\mathbf{Z}_p \times \mathbf{Z}_p$ consisting of all pairs (a, b) such that a and b are not both divisible by p in $\mathbf{Z}_p$. This space of "primitive vectors" makes an appearance in the earlier work of Greenberg and Stevens [7].

Definition 1.1 For a subgroup $A \subset \mathbf{Q}_p$, a *distribution* on $\mathbf{X}$ with values in A is a function ν which assigns to each compact open set $U \subset \mathbf{X}$ an element $\nu(U) \in A$ such that

- $\nu(U \cup V) = \nu(U) + \nu(V)$ for disjoint compact open U and V, and
- $\nu(\mathbf{X}) = 0$.

A distribution is said to be a *measure* if A can be chosen to be a bounded subgroup of $\mathbf{Q}_p$.

The set of measures on $\mathbf{X}$ valued in A is denoted $\mathrm{Meas}(\mathbf{X}, A)$. The crucial technical ingredient in the definition of $u(\alpha, \tau)$ is the following result.

Theorem 1.2 ([2, Theorem 4.2]) *Let α be fixed as above. There is a unique $\mathrm{Meas}(\mathbf{X}, \mathbf{Z}_p)$-valued partial modular symbol μ such that for every homogeneous polynomial $h(x, y) \in \mathbf{Z}[x, y]$ of degree $k - 2$,*

$$\int_{\mathbf{X}} h(x, y)\, \mathrm{d}\mu\{r \to s\}(x, y) = \mathrm{Re}\Big((1 - p^{k-2}) \int_r^s h(z, 1) F_k(z)\, \mathrm{d}z\Big)\,. \tag{8}$$

The p-adic integral on the left side of (8) is defined to be

$$\lim_{\|\mathfrak{U}\| \to 0} \sum_{U \in \mathfrak{U}} h(x_U, y_U) \cdot \mu\{r \to s\}(U) \in \mathbf{Z}_p,$$

where $\mathfrak{U}$ is a cover of $\mathbf{X}$ by disjoint compact opens, (x_U, y_U) is an arbitrary point of $U \in \mathfrak{U}$, and the p-adic limit is taken over uniformly finer covers $\mathfrak{U}$. Implicit in the statement of Theorem 1.2 is the fact that the real numbers on the right side of (8) are in fact rational, and hence may be viewed as elements of $\mathbf{Q}_p$. We will give explicit formulas for these numbers in terms of generalized Dedekind sums in Section 2. In Section 3, we will prove the following.

Theorem 1.3 *The partial modular symbol of measures μ is $\mathbf{Z}$-valued.*

The space $\mathbf{X}$, viewed as a subspace of the larger space $\mathbf{Y} := \mathbf{Q}_p^2 - \{0\}$, forms a fundamental domain for the action of multiplication by p on $\mathbf{Y}$. Hence the measures $\mu\{r \to s\}$ can be extended uniquely to measures on $\mathbf{Y}$ which are invariant under multiplication by p:

$$\mu\{r \to s\}(pU) = \mu\{r \to s\}(U)$$

for all compact open $U \subset \mathbf{Y}$. The group $\mathrm{GL}_2(\mathbf{Q}_p)$ acts on $\mathbf{Y}$ by left multiplication by viewing the elements of $\mathbf{Y}$ as column vectors. The partial modular symbol of measures μ satisfies the following additional properties:

- For all
$$\gamma \in \tilde{\Gamma} := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2^+(\mathbf{Z}[1/p]) : N | c \right\}$$
and all compact open $U \subset \mathbf{Y}$,
$$\mu\{\gamma r \to \gamma s\}(\gamma U) = \mu\{r \to s\}(U).$$

- For every homogeneous polynomial $h(x, y) \in \mathbf{Z}[x, y]$ of degree $k - 2$,

$$\int_{\mathbf{Z}_p \times \mathbf{Z}_p^\times} h(x, y)\, \mathrm{d}\mu\{r \to s\}(x, y) = \mathrm{Re}\Big(\int_r^s h(z, 1) F_k^*(z)\, \mathrm{d}z\Big). \tag{9}$$

We are now ready to define $u(\alpha, \tau)$. Let K be a real quadratic field such that p is inert in K, and let $\tau \in K - \mathbf{Q}$. Assume that the reduction of τ modulo p, which is an element of $\mathbf{P}^1(\mathbf{F}_{p^2})$, does not lie in $\mathbf{P}^1(\mathbf{F}_p)$. Choose the real embedding of K in which τ is greater than its Galois conjugate. Denote by Γ_τ the stabilizer of τ in

$$\Gamma := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}[1/p]) : N | c \right\} \subset \tilde{\Gamma},$$

acting via linear fractional transformations. Let γ_τ be the unique element of Γ_τ whose image generates the quotient $\Gamma_\tau / \langle \pm 1 \rangle \cong \mathbf{Z}$ such that

$$\gamma_\tau \begin{pmatrix} \tau \\ 1 \end{pmatrix} = \varepsilon \begin{pmatrix} \tau \\ 1 \end{pmatrix} \tag{10}$$

with $\varepsilon > 1$. Write $\gamma_\tau = \left(\begin{smallmatrix} a & b \\ Nc & d \end{smallmatrix}\right)$.

We define the element $u(\alpha, \tau) \in K_p^\times$ by the formula

$$u(\alpha, \tau) = p^{\psi\{\infty \to \frac{a}{Nc}\}} \cdot \times\!\!\!\!\!\!\int_{\mathbf{X}} (x - y\tau)\, d\mu\Big\{\infty \to \frac{a}{Nc}\Big\}(x, y). \tag{11}$$

The p-adic multiplicative integral on the right side of (11) is defined to be

$$\lim_{\|\mathcal{U}\| \to 0} \prod_{U \in \mathcal{U}} (x_U - y_U \tau)^{\mu\{\infty \to \frac{a}{Nc}\}(U)} \in \mathcal{O}_p^\times,$$

with the notation as in (8). Here $\mathcal{O}_p$ denotes the ring of integers of K_p. Note that the definition of the multplicative integral is contingent on Theorem 1.3. This constitutes an improvement over the definition of [2], where $u(\alpha, \tau)$ was defined only up to a root of unity in $K_p^\times$.

The element $u(\alpha, \tau) \in K_p^\times$ is conjectured to lie in a ring class field extension of K. To be precise, assume that the minimal quadratic polynomial with integer coefficients satisfied by τ has the form

$$A\tau^2 + B\tau + C = 0, \quad (A, B, C) = 1, \quad A > 0$$

where

$$N | A \text{ and } D = B^2 - 4AC \text{ is relatively prime to } Np. \tag{12}$$

Conjecture DD The element $u(\alpha, \tau) \in K_p^\times$ is a p-unit in the narrow ring class field H_D attached to the discriminant $D > 0$.

2 Dedekind Sums

In this section we relate the integrals appearing in the right of (8) and (9) to generalized Dedekind sums. The explicitly calculable formulas of this section will be used in the computations of $u(\alpha,\tau)$.

The classical Bernoulli polynomials B_n are defined by the power series

$$\frac{e^{tx}}{e^t-1}=\sum_{n=0}^{\infty}\frac{B_n(x)}{n!}t^{n-1}.$$

We use the Bernoulli polynomials to define periodic functions

$$\tilde{B}_s(x):=\begin{cases}0 & \text{if } s=1 \text{ and } x\in\mathbf{Z}\\ B_s(x-[x]) & \text{otherwise,}\end{cases}$$

where $[x]$ denotes the greatest integer less than or equal to x. Let s and t be positive integers. For a and c relatively prime and $c\geq 1$, the generalized Dedekind sum $D_{s,t}(a/c)$ is defined by

$$D_{s,t}(a/c):=\frac{c^{s-1}}{st}\sum_{h=1}^{c}\tilde{B}_s(h/c)\tilde{B}_t(ha/c).$$

In terms of these generalized Dedekind sums, we have from [2, §4.4, §4.7],

(13)

$$\operatorname{Re}\Big[\int_{\infty}^{\frac{a}{Nc}} z^nF_k(z)\,\mathrm{d}z\Big]=-12\sum_{\ell=0}^{n}\binom{n}{\ell}\Big(\frac{a}{Nc}\Big)^{n-\ell}(-1)^{\ell}\sum_{d|N}\frac{n_d}{d^{\ell}}D_{k-\ell-1,\ell+1}\Big(\frac{a}{Nc/d}\Big),$$

$$(14)\qquad \operatorname{Re}\Big[\int_{\infty}^{\frac{a}{Nc}} z^nF_k^*(z)\,\mathrm{d}z\Big]=-12\sum_{\ell=0}^{n}\binom{n}{\ell}\Big(\frac{a}{Nc}\Big)^{n-\ell}(-1)^{\ell}$$
$$\times\sum_{d|N}\frac{n_d}{d^{\ell}}\Big[D_{k-\ell-1,\ell+1}\Big(\frac{a}{Nc/d}\Big)-p^{k-\ell-2}D_{k-\ell-1,\ell+1}\Big(\frac{pa}{Nc/d}\Big)\Big].$$

Equation (13) for $k=2$ and $n=0$ yields the formula

$$\psi\Big\{\infty\to\frac{a}{Nc}\Big\}=-12\sum_{d|N}n_dD\Big(\frac{a}{Nc/d}\Big),$$

where $D=D_{1,1}$ is the classical Dedekind sum.

3 Integrality of the Measures

In this section we prove that the measures μ_m, which are proved in [2] to be only $\mathbf{Z}_p$-valued, actually take on integer values. We begin by reviewing the single-variable measures arising from Bernoulli polynomials; our presentation is motivated by [8, §10.2]. Let $e \geq 1$ be a positive integer divisible by N but not by p, and let

$$Z = \varprojlim \mathbf{Z}/ep^n\mathbf{Z} \cong \mathbf{Z}/e\mathbf{Z} \times \mathbf{Z}_p.$$

For each integer $k \geq 1$, define a distribution $\mathcal{F}_k$ on Z corresponding to the Eisenstein series F_{2k} by the rule

$$\mathcal{F}_k(a + ep^n \cdot Z) := \sum_{d|N} n_d \Big(\frac{ep^n}{d}\Big)^{k-1} \cdot \frac{1}{k} \cdot \tilde{B}_k\Big(\frac{a}{ep^n/d}\Big)$$

for each integer a. The "distribution relation"

$$\sum_{a=1}^{f} \tilde{B}_k\Big(x + \frac{a}{f}\Big) = f^{1-k}\tilde{B}_k(fx) \tag{15}$$

for Bernoulli polynomials demonstrates that $\mathcal{F}_k$ is indeed a distribution for each $k \geq 1$. For $x \in Z$, let x_p denote the projection of x onto $\mathbf{Z}_p$.

Proposition 3.1 *The distributions $\mathcal{F}_k$ are $\mathbf{Z}_p$-valued measures, and for every compact open set $U \subset Z$ and every $k \geq 1$ we have $\mathcal{F}_k(U) = \int_U x_p^{k-1}\, d\mathcal{F}_1(x)$.*

Proof It suffices to consider U of the form $U = a + ep^nZ$ for integers a. We will prove that

$$\mathcal{F}_k(U) \equiv a^{k-1}\mathcal{F}_1(U) \pmod{p^{n-\epsilon}\mathbf{Z}_p} \tag{16}$$

where ϵ depends only on k. The key fact is that the Bernoulli polynomial $B_k(x)$ begins $x^k - \frac{1}{2}kx^{k-1} + \cdots$. Therefore,

$$\mathcal{F}_k(U) \equiv \sum_{d|N} n_d \Big(\frac{ep^n}{d}\Big)^{k-1} \frac{1}{k}\bigg(\Big(\frac{da}{ep^n} - \Big[\frac{da}{ep^n}\Big]\Big)^k - \frac{k}{2}\Big(\frac{da}{ep^n} - \Big[\frac{da}{ep^n}\Big]\Big)^{k-1}\bigg) \tag{17}$$

modulo $p^{n-\epsilon}\mathbf{Z}_p$, where ϵ is the largest power of p appearing in the denominators of the coefficients of $B_k(x)/k$. The congruence (17) yields:

$$\mathcal{F}_k(U) \equiv \sum_{d|N} \frac{n_d}{k}\Big(\Big(\frac{d}{ep^n}\Big)a^k - ka^{k-1}\Big[\frac{da}{ep^n}\Big] - \frac{k}{2}a^{k-1}\Big) \pmod{p^{n-\epsilon}\mathbf{Z}_p}$$

$$\equiv -\sum_{d|N} n_d a^{k-1}\Big[\frac{da}{ep^n}\Big], \tag{18}$$

where (18) uses $\sum n_d = \sum n_d d = 0$. The congruence (18) implies that $\mathcal{F}_k$ is $\mathbf{Z}_p$-valued. Meanwhile we find

$$a^{k-1}\mathcal{F}_1(U) = a^{k-1}\sum_{d|n} n_d\Big(\frac{d}{ep^n} - \Big[\frac{da}{ep^n}\Big] - \frac{1}{2}\Big) = -\sum_{d|N} n_d a^{k-1}\Big[\frac{da}{ep^n}\Big]. \tag{19}$$

Equations (18) and (19) yield (16), proving the proposition. ■

https://doi.org/10.4153/CJM-2007-023-0 Published online by Cambridge University Press

The measures $\mathcal{F}_k$ may be used to calculate the modular symbol of measures μ. Let the fraction $\frac{a}{Nc}$ be fixed; we will write ν for $\mu\{\infty \to \frac{a}{Nc}\}$.

Let V be a compact open subset of $\mathbf{Z}_p^\times$, and let $f_i(y) = \sum_{n=0}^{d_i} c_n(i) y^n$ be a sequence of polynomials such that $\lim_{i\to\infty} f_i(y)$ is the characteristic function of V. Then equations (8) and (13) for the moments of ν yield

$$\nu(\mathbf{Z}_p \times V) = \lim_{i\to\infty} -12 \sum_{d|N} n_d \sum_{n=0}^{d_i} (1-p^n) c_n(i) \cdot D_{n+1,1}\Big(\frac{a}{Nc/d}\Big). \tag{20}$$

From the distribution relation (15) with $k = 1$, we have

$$\begin{aligned} D_{n+1,1}\Big(\frac{a}{Nc/d}\Big) &= \Big(\frac{Nc}{d}\Big)^n \sum_{h=1}^{Nc/d} \frac{\tilde{B}_{n+1}\big(\frac{h}{Nc/d}\big)}{n+1} \cdot \tilde{B}_1\Big(\frac{ha}{Nc/d}\Big) \\ &= \Big(\frac{Nc}{d}\Big)^n \sum_{h=1}^{Nc} \frac{\tilde{B}_{n+1}\big(\frac{h}{Nc/d}\big)}{n+1} \cdot \tilde{B}_1\Big(\frac{ha}{Nc}\Big). \end{aligned}$$

Hence (20) becomes

$$\nu(\mathbf{Z}_p \times V) = \lim_{i\to\infty} -12 \sum_{h=1}^{Nc} \tilde{B}_1\Big(\frac{ha}{Nc}\Big) \sum_{n=0}^{d_i} (1-p^n) \sum_{d|N} n_d \Big(\frac{Nc}{d}\Big)^n \frac{\tilde{B}_{n+1}\big(\frac{h}{Nc/d}\big)}{n+1} c_n(i). \tag{21}$$

Write $Nc = ep^r$ with p not dividing e. Then N divides e, and in terms of the measure $\mathcal{F}_1$ above we have

$$\sum_{n=0}^{d_i} (1-p^n) \sum_{d|N} n_d \Big(\frac{Nc}{d}\Big)^n \frac{\tilde{B}_{n+1}\big(\frac{h}{Nc/d}\big)}{n+1} c_n(i) = \int_{h+ep^rZ} \Big(f_i(x_p) - f_i(px_p)\Big)\, \mathrm{d}\mathcal{F}_1(x)$$

by Proposition 3.1. Let us now specify V of the form $V = b + p^s\mathbf{Z}_p$, with $s \geq r$ and $b \in \mathbf{Z}_p^\times$. In the limit as $i \to \infty$, the value $f_i(x_p)$ approaches 1 or 0 according to whether $x_p \in V$, and $f_i(px_p)$ approaches 0. Therefore (21) becomes

$$\begin{aligned} \nu(\mathbf{Z}_p \times V) &= -12 \sum_{h=1}^{Nc} \tilde{B}_1\Big(\frac{ha}{Nc}\Big) \mathcal{F}_1\big(\{x \in h + ep^rZ : x_p \in V\}\big) \\ &= -12 \sum_{\substack{h=1 \\ h\in b+p^r\mathbf{Z}_p}}^{Nc} \tilde{B}_1\Big(\frac{ha}{ep^r}\Big) \sum_{d|N} n_d \tilde{B}_1\Big(\frac{y}{ep^s/d}\Big) \qquad (22) \end{aligned}$$

https://doi.org/10.4153/CJM-2007-023-0 Published online by Cambridge University Press

where y is an integer such that $y \equiv h \pmod{e}$ and $y \equiv b \pmod{p^s}$. Fixing one such y for each h, we obtain

$$\nu(\mathbf{Z}_p \times V) = 12 \sum_{\substack{h=1 \\ h\in b+p^r\mathbf{Z}_p}}^{Nc} \tilde{B}_1\Big(\frac{ha}{ep^r}\Big) \sum_{d|N} n_d \Big[\frac{y}{ep^s/d}\Big] \tag{23}$$

$$\equiv 12\frac{a}{Nc} \sum_{\substack{h=1 \\ h\in b+p^r\mathbf{Z}_p}}^{Nc} h \sum_{d|N} n_d \Big[\frac{y}{ep^s/d}\Big] \pmod{\mathbf{Z}},$$

where (23) uses $\sum n_d = \sum n_d d = 0$. Hence to prove integrality, it suffices to consider the case $a = 1$. For this purpose, we return to (22) with $a = 1$ and rewrite the expression in terms of a generalized Dedekind sum:

$$\nu(\mathbf{Z}_p \times V) = -12 \sum_{d|N} n_d \sum_{\substack{h=1 \\ h\in b+p^r\mathbf{Z}_p}}^{ep^r/d} \tilde{B}_1\Big(\frac{h}{ep^r/d}\Big) \tilde{B}_1\Big(\frac{y}{ep^s/d}\Big). \tag{24}$$

The inner sum is the generalized Dedekind sum denoted $C(1, 1, p^{s-r}, \frac{e}{d}, \frac{ke/d}{p^s}, 0)$ in [10], where k is an integer chosen so that $ke/d \equiv b \pmod{p^s}$. The reciprocity law governing these Dedekind sums [10, Theorem 2] shows that this value equals

$$\sum_{\substack{h=1 \\ h\in b+p^r\mathbf{Z}_p}}^{ep^r/d} \tilde{B}_1\Big(\frac{h}{ep^r/d}\Big) \tilde{B}_1\Big(\frac{y}{ep^s/d}\Big) = \frac{(e/d)^2}{2p^{s-r}} - \sum_{i=1}^{p^{s-r}} \tilde{B}_1\Big(\frac{i}{p^{s-r}}\Big) \tilde{B}_1\Big(\frac{(ip^r - k)e/d}{p^{s-r}}\Big)$$

$$+ \frac{p^{s-r}}{2e/d}\tilde{B}_2\Big(-\frac{b}{p^r}\Big) + \frac{p^{s-r}}{2e/d}\tilde{B}_2\Big(\frac{b}{p^s}\Big) \tag{25}$$

$$- \tilde{B}_1\Big(\frac{b}{p^s}\Big). \tag{26}$$

Using this expression in equation (24), the terms from lines (25) and (26) vanish since $\sum n_d d = 0$. The remaining line yields only terms in $\mathbf{Z}[1/p]$. Since we know that ν is $\mathbf{Z}_p$-valued, we thus conclude that $\nu(\mathbf{Z}_p \times V) \in \mathbf{Z}$. Since the $\tilde{\Gamma}$ translates of the sets $\mathbf{Z}_p \times V$ form a basis of compact opens for $\mathbf{Q}_p^2 - \{0\}/p^{\mathbf{Z}} \cong \mathbf{X}$, the $\tilde{\Gamma}$-invariance of μ therefore implies that the modular symbol of measures μ is $\mathbf{Z}$-valued, proving Theorem 1.3.

For future reference, we record the following corollary of our calculations above.

Proposition 3.2 *Let $u, v \in \mathbf{Z}$ such that $(u, v) \in \mathbf{X}$. For a positive integer s, let $U_{u,v,s}$ denote the ball of radius p^{-s} around (u, v) in $\mathbf{X}$,* i.e., $U_{u,v,s} = (u + p^s\mathbf{Z}_p) \times (v + p^s\mathbf{Z}_p) \subset \mathbf{X}$. *Let $\frac{a}{c} \in \Gamma_0(N)\infty$. Then*

$$\mu\Big\{\infty \to \frac{a}{c}\Big\}(U_{u,v,s}) = -12 \sum_{\ell \pmod{c}} \tilde{B}_1\Big(\frac{a}{c}\Big(\ell + \frac{v}{p^s}\Big) - \frac{u}{p^s}\Big) \sum_{d|N} n_d \tilde{B}_1\Big(\frac{d}{c}\Big(\ell + \frac{v}{p^s}\Big)\Big).$$

Proof We provide only a sketch. Write $c = ep^r$ with $p \nmid e$. Equation (22) states that if $s \geq r$, then

(27)

$$\mu\left\{\infty \to \frac{a}{ep^r}\right\}(\mathbf{Z}_p \times (v + p^s\mathbf{Z}_p)) = -12 \sum_{\substack{h=1 \\ h\equiv v \pmod{p^r}}}^{Nc} \tilde{B}_1\Big(\frac{ha}{ep^r}\Big) \sum_{d|N} n_d \tilde{B}_1\Big(\frac{yd}{ep^s}\Big),$$

where $y \equiv h \pmod{e}$ and $y \equiv v \pmod{p^s}$. When $s \leq r$, the analogous formula is

(28)

$$\mu\Big\{\infty \to \frac{a}{ep^r}\Big\}(\mathbf{Z}_p \times (v + p^s\mathbf{Z}_p)) = -12 \sum_{\substack{h=1 \\ h\equiv v \pmod{p^s}}}^{Nc} \tilde{B}_1\Big(\frac{ha}{ep^r}\Big) \sum_{d|N} n_d \tilde{B}_1\Big(\frac{hd}{ep^r}\Big).$$

Suppose now that $p \nmid v$, and let $j \in \mathbf{Z}$ such that $u \equiv jv \pmod{p^s}$. Consider the matrix $\gamma = \left(\begin{smallmatrix} p^s & j \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma$, and note that $\gamma(\mathbf{Z}_p \times (v + p^s\mathbf{Z}_p)) = U_{u,v,s}$. The Γ-invariance of μ then yields

$$\mu\Big\{\infty \to \frac{a}{c}\Big\}(U_{u,v,s}) = \mu\Big\{\infty \to \frac{a - jc}{cp^s}\Big\}(\mathbf{Z}_p \times (v + p^s\mathbf{Z}_p)). \tag{29}$$

An elementary calculation shows that the right-hand side of (29) equals the result stated in the proposition, using 28 when the fraction $\frac{a-jc}{cp^s}$ has denominator divisible by p^s and using (27) when it does not.

To handle the case when p divides v, let $\tilde{\mu}$ be the partial modular symbol *defined* by the formula of the proposition, *i.e.*,

$$\tilde{\mu}\Big\{\infty \to \frac{a}{c}\Big\}(U_{u,v,s}) := -12 \sum_{\ell \pmod{c}} \tilde{B}_1\Big(\frac{a}{c}\Big(\ell + \frac{v}{p^s}\Big) - \frac{u}{p^s}\Big) \sum_{d|N} n_d \tilde{B}_1\Big(\frac{d}{c}\Big(\ell + \frac{v}{p^s}\Big)\Big).$$

Since any $\gamma \in \Gamma_0(N) - \Gamma_0(Np)$ sends $U_{u,v,s}$ with $p|v$ to $U_{u',v',s}$ with $p \nmid v'$, to conclude the proof it suffices to prove that $\tilde{\mu}$ is a $\Gamma_0(N)$-invariant partial modular symbol. In terms of the notation of [10], we have

$$\tilde{\mu}\Big\{\infty \to \frac{a}{c}\Big\}(U_{u,v,s}) = -12 \sum_{d|N} n_d C\Big(1, 1, a, \frac{c}{d}, \frac{v}{p^s}, -\frac{ud}{p^s}\Big),$$

and the desired $\Gamma_0(N)$-invariance follows from the transformation formula regarding the generalized Dedekind sums $C(-)$ [10, Theorem 2]. The computation is lengthy but elementary, and we omit it. ■

4 Method to Compute Elliptic Units

As before, let K denote a real quadratic field in which p is inert. The completion K_p is a quadratic unramified extension of $\mathbf{Q}_p$. Let $\log_p : K_p^\times \to \mathcal{O}_p$ denote the branch of the p-adic logarithm which vanishes on p. Let β be a primitive (p^2-1)-st root of unity in $K_p^\times$, and let $\log_\beta$ denote the discrete logarithm with base β:

$$\log_\beta \colon K_p^\times \to \mathbf{Z}/(p^2-1)\mathbf{Z},$$

where

$$\frac{x}{p^{\operatorname{ord}_p(x)}\beta^{\log_\beta(x)}} \in 1 + p\mathcal{O}_p \text{ for all } x \in K_p^\times.$$

For $p > 2$, we then have the decomposition:

$$K_p^\times \cong \mathbf{Z} \times \mathbf{Z}/(p^2-1)\mathbf{Z} \times p\mathcal{O}_p \text{ given by } x \mapsto (\operatorname{ord}_p(x), \log_\beta(x), \log_p(x)).$$

(The function $\log_p$ is invertible only on $1 + p^2\mathcal{O}_p$ for $p = 2$; for notational reasons only, we will assume $p > 2$ throughout.) For $x = u(\alpha, \tau)$ and $\gamma_\tau = \left(\begin{smallmatrix} a & * \\ Nc & * \end{smallmatrix}\right)$, these three components are given by the formulas

$$\operatorname{ord}_p(u(\alpha,\tau)) = -12 \sum_{d|N} n_d \cdot D\Big(\frac{a}{Nc/d}\Big), \tag{30}$$

$$\log_\beta(u(\alpha,\tau)) = \int_{\mathbf{X}} \log_\beta(x - y\tau)\, \mathrm{d}\mu\Big\{\infty \to \frac{a}{Nc}\Big\}(x,y), \tag{31}$$

$$\log_p(u(\alpha,\tau)) = \int_{\mathbf{X}} \log_p(x - y\tau)\, \mathrm{d}\mu\Big\{\infty \to \frac{a}{Nc}\Big\}(x,y). \tag{32}$$

The computations of (30) and (31) are easy to execute in practice (note that for (31) it suffices to take a cover of $\mathbf{X}$ in which x and y are determined modulo p), so we only elaborate upon the computation of (32).

Suppose we are content to calculate (32) to an accuracy of M p-adic digits. Let $m = [\infty] - \left[\frac{a}{Nc}\right] \in \mathcal{M}$. Then $\log_p(u(\alpha,\tau))$ is equal to

$$\int_{\mathbf{Z}_p \times \mathbf{Z}_p^\times} \log_p(y)\, \mathrm{d}\mu_m(x,y) + \int_{\mathbf{Z}_p \times \mathbf{Z}_p^\times} \log_p\left(\frac{x}{y} - \tau\right) \mathrm{d}\mu_m(x,y) \tag{33}$$

$$+ \int_{\mathbf{Z}_p^\times \times p\mathbf{Z}_p} \log_p(x)\, \mathrm{d}\mu_m(x,y) + \int_{\mathbf{Z}_p^\times \times p\mathbf{Z}_p} \log_p\left(1 - \frac{y\tau}{x}\right) \mathrm{d}\mu_m(x,y). \tag{34}$$

The first term of (33) is independent of τ. To evaluate this term to an accuracy of M p-adic digits, one finds a polynomial $f(y)$ that is congruent to $\log_p(y)$ modulo p^M for all $y \in \mathbf{Z}_p^\times$. This can be done as follows. For each $i = 1, \dots, p-1$, let

$$g_i(y) = \prod_{\substack{j=1 \\ j \neq i}}^{p-1} (y - j)^M,$$

https://doi.org/10.4153/CJM-2007-023-0 Published online by Cambridge University Press

and let $h_i(y)$ denote the power series of $\log_p(y)/g_i(y)$ on the residue disc $i + p\mathbf{Z}_p$, truncated after $M+\log M$ terms (the extra $\log M$ terms account for the denominators divisible by powers of p in the power series of $\log_p$). Then letting

$$f(y) = \sum_{i=1}^{p-1} g_i(y)h_i(y) \tag{35}$$

produces the desired polynomial; it has degree $p(M + \log M)$. The first term of (33) may then be evaluated be replacing $\log_p(y)$ by $f(y)$ and using (9) and (14) to evaluate the integral of y^n on $\mathbf{Z}_p \times \mathbf{Z}_p^\times$ against the measure μ_m.

There is a $\mathbf{Z}_p^\times$-bundle map $\pi\colon \mathbf{X} \to \mathbf{P}^1(\mathbf{Q}_p)$ given by $(x, y) \mapsto x/y$. Given the measure μ_m on $\mathbf{X}$, its push forward to $\mathbf{P}^1(\mathbf{Q}_p)$ is defined by the rule

$$\overline{\mu}_m(U) = \pi_*\mu_m(U) = \mu_m(\pi^{-1}(U)) \in \mathbf{Z}$$

for compact open $U \subset \mathbf{P}^1(\mathbf{Q}_p)$ (the measure-valued partial modular symbol $\overline{\mu}$ was denoted μ_α in [2]). The second term of (33) may be recognized as a push forward from $\mathbf{X}$ to $\mathbf{P}^1(\mathbf{Q}_p)$, and equals

$$\begin{aligned}\int_{\mathbf{Z}_p} \log_p(t-\tau)\,\mathrm{d}\overline{\mu}_m(t) &= \sum_{i=0}^{p-1} \int_{i+p\mathbf{Z}_p} \log_p(t-i+(i-\tau))\,\mathrm{d}\overline{\mu}_m(t)\\ &= \sum_{i=0}^{p-1} \Big[\log_p(\tau-i)\overline{\mu}_m(i+p\mathbf{Z}_p)\\ &\qquad + \int_{i+p\mathbf{Z}_p} \log_p\Big(1-\frac{t-i}{\tau-i}\Big)\,\mathrm{d}\overline{\mu}_m(t)\Big].\end{aligned} \tag{36}$$

The final integrand in (36) may be expanded as a power series in the residue disc $i + p\mathbf{Z}_p$, and hence to calculate the integral modulo p^M, it suffices to calculate the moments

$$\int_{i+p\mathbf{Z}_p} (t-i)^n\,\mathrm{d}\overline{\mu}_m(t) = p^n \int_{\mathbf{Z}_p} u^n\,\mathrm{d}\overline{\mu}_{P_i^{-1}m}(u) \pmod{p^M} \tag{37}$$

for $n = 0, \dots, M-1$, where $P_i = \left(\begin{smallmatrix} p & i \\ 0 & 1 \end{smallmatrix}\right)$, and (37) uses the invariance of $\overline{\mu}$ under $P_i \in \tilde{\Gamma}$. Writing $P_i^{-1}m = \tilde{w} = [\infty] - [w]$, we calculate (37) by pulling back to $\mathbf{X}$:

$$\begin{aligned}\int_{\mathbf{Z}_p} u^n\,\mathrm{d}\overline{\mu}_{\tilde{w}}(u) &= \int_{\mathbf{Z}_p\times\mathbf{Z}_p^\times} x^n y^{-n}\,\mathrm{d}\mu_{\tilde{w}}(x,y)\\ &= \lim_{\substack{j\to\infty\\ g=(p-1)p^j}} \int_{\mathbf{Z}_p\times\mathbf{Z}_p^\times} x^n y^{g-n}\,\mathrm{d}\mu_{\tilde{w}}(x,y)\\ &= \lim_{\substack{j\to\infty\\ g=(p-1)p^j}} 12\sum_{\ell=0}^{n} \binom{n}{l} w^{n-\ell}(-1)^\ell \sum_{d\mid N} n_d d^{-\ell} D_{g-\ell+1,\ell+1}(dw).\end{aligned} \tag{38}$$

https://doi.org/10.4153/CJM-2007-023-0 Published online by Cambridge University Press

Writing $w = b/ep^r$ (with $p \nmid e$ and $N|e$) and employing the distribution relation (15), expression (38) may be expressed in terms of the single-variable measures of Section 3:

(39)

$$\lim_{\substack{j\to\infty \\ g=(p-1)p^j}} \sum_{d|N} n_d d^{-\ell} D_{g-\ell+1,\ell+1}\Big(\frac{bd}{ep^r}\Big) = \sum_{h=1}^{ep^r} \frac{\tilde{B}_{\ell+1}(\frac{hb}{ep^r})}{\ell+1} \lim_{\substack{j\to\infty \\ g=(p-1)p^j}} \mathcal{F}_{g-\ell+1}(h+ep^r\cdot Z)$$
$$= \sum_{h=1}^{ep^r} \frac{\tilde{B}_{\ell+1}(\frac{hb}{ep^r})}{\ell+1} \int_{h+ep^rZ} x^{-\ell}\, \mathrm{d}\mathcal{F}_1(x),$$

by Proposition 3.1. The integrals of (39) may be computed modulo p^M by expanding $x^{-\ell}$ as a power series and using Proposition 3.1 to calculate the moments of $\mathcal{F}_1$.

The terms of (34) may be calculated similarly using the methods described above for (33). Our method has broken down the computation of (32) into two parts. The first step is the calculation of the following integrals, which are independent of τ:

(i) $\int_{\mathbf{Z}_p\times\mathbf{Z}_p^\times} \log_p(y)\, \mathrm{d}\mu_m(x,y)$,
(ii) $\int_{i+p\mathbf{Z}_p} (t-i)^n\, \mathrm{d}\overline{\mu}_m(t), i = 0,\dots,p=1, n=0,\dots,M-1$,
(iii) $\int_{\mathbf{Z}_p^\times\times p\mathbf{Z}_p} \log_p(x)\, \mathrm{d}\mu_m(x,y)$,
(iv) $\int_{\mathbf{P}^1(\mathbf{Q}_p)-\mathbf{Z}_p} t^{-n}\, \mathrm{d}\overline{\mu}_m(t), n=0,\dots M-1$.

(The last moment arises in the computation of (34).) The second step is to calculate $\log_p u(\alpha,\tau)$ from these integrals, using the decomposition of (33)–(34).

Hence our algorithm is to execute one program, which calculates for a given α, p, and M, the integrals (i)–(iv) once and for all as m ranges over a $\Gamma_0(N)$-module basis for $\mathcal{M}$, to an accuracy of p^M. (Using the $\Gamma_0(N)$-invariance of the indefinite integral, it suffices to calculate (i)–(iv) for a $\Gamma_0(N)$-module basis of $\mathcal{M}$ in order to evaluate the indefinite integral for all $m \in \mathcal{M}$.) This program executes $O(pM^2)$ arithmetic operations involving p-adic numbers stored to an accuracy of M p-adic digits. The output is stored in a file.

A second program is then run, inputting the integrals (i)–(iv) from the output file of the first program, and calculating $u(\alpha,\tau)$ to an accuracy of p^M as described above. This calculation executes $O(pM)$ arithmetic operations, and hence is rather quick even when M is large. Thus to compute the p-units $u(\alpha,\tau)$ to a high accuracy for various real quadratic fields K, it suffices to execute the (much slower) first program only once.

We summarize our method to compute the unit $u(\alpha,\tau)$ below. We assume that α has been fixed as in (1), as well as a prime p and a p-adic accuracy p^M. We further assume that a $\Gamma_0(N)$-basis $\{m_1,\dots,m_r\}$ of $\mathcal{M}$ is known, as well as an algorithm to write any $m \in \mathcal{M}$ as a linear combination

$$m = \sum_{i=1}^{r} \sum_{\gamma\in\Gamma_0(N)} a_{\gamma,i}\cdot\gamma m_i,$$

https://doi.org/10.4153/CJM-2007-023-0 Published online by Cambridge University Press

with $a_{\gamma,i} \in \mathbf{Z}$ and all but finitely many of the $a_{\gamma,i}$ equal to zero. For the case $N = 4$, we remark that $\mathcal{M}$ is a free $\mathbf{Z}[\Gamma_0(4)]$-module, generated by $[\infty] - \left[\frac{1}{4}\right]$. A recursive algorithm to write any element of $\mathcal{M}$ as an element of $\mathbf{Z}[\Gamma_0(4)]([\infty] - \left[\frac{1}{4}\right])$ is given below.

Algorithm 4.1 Let $N = 4$. This algorithm expresses any $[\infty] - \left[\frac{a}{4c}\right] \in \mathcal{M}$ with $c \geq 0$ as a linear combination $\sum a_\gamma \cdot \gamma([\infty] - \left[\frac{1}{4}\right])$ with $a_\gamma \in \mathbf{Z}$ and $\gamma \in \Gamma_0(4)$.

1. If $c = 0$, then $[\infty] - \left[\frac{a}{4c}\right] = 0$. Terminate. Otherwise, proceed with the remainder of the algorithm.
2. Let d be the unique integer such that $ad \equiv 1 \pmod{4c}$ and $-2c < d < 2c$, and let $b = (ad-1)/(4c)$. Define $\gamma \in \Gamma_0(4)$ by

$$\gamma = \begin{cases} \begin{pmatrix} a & b \\ 4c & d \end{pmatrix} & \text{if } d < 0, \\ \begin{pmatrix} a-4b & b \\ 4c-4d & d \end{pmatrix} & \text{if } d > 0. \end{cases}$$

3. We have

$$[\infty] - \left[\frac{a}{4c}\right] = \begin{cases} \left([\infty] - \left[\dfrac{a+4b}{4c+4d}\right]\right) - \gamma\left([\infty] - \left[\frac{1}{4}\right]\right) & \text{if } d < 0 \\ \left([\infty] - \left[\dfrac{a-4b}{4c-4d}\right]\right) + \gamma\left([\infty] - \left[\frac{1}{4}\right]\right) & \text{if } d > 0. \end{cases} \tag{40}$$

   In both cases, return to Step 1 to express the first term in parentheses on the right side of (40) in the desired form.

In each case in (40), the denominator of the fraction involved in the first term on the right-hand side (namely, $4c + 4d$ when $d < 0$ and $4c - 4d$ when $d > 0$) has absolute value smaller than $4c$. Thus the recursive procedure will terminate when we have reached the case $c = 0$.

We return now to the case of general N and the algorithm to compute $u(\alpha, \tau)$. The following procedure computes certain integrals specific only to the data (α, p, M) and hence must be executed only once if that data is fixed.

Algorithm 4.2 This algorithm computes certain auxiliary integrals which are needed to compute $u(\alpha, \tau)$.

1. [Calculate integral (i)] As described in (35), define a polynomial $f(y)$ such that $f(y) \equiv \log_p(y) \pmod{p^M}$ for all $y \in \mathbf{Z}_p^\times$. Then compute

$$\int_{\mathbf{Z}_p \times \mathbf{Z}_p^\times} \log_p(y)\, d\mu_{m_i}(x, y) \equiv \int_{\mathbf{Z}_p \times \mathbf{Z}_p^\times} f(y)\, d\mu_{m_i}(x, y) \pmod{p^M}$$

   for $i = 1, \ldots, r$ using equations (9) and (14).

https://doi.org/10.4153/CJM-2007-023-0 Published online by Cambridge University Press

2. [Calculate integral (ii)] For each $i = 1, \dots, r$, $j = 0, \dots, p-1$, and $n = 0, \dots, M-1$, calculate
$$\int_{j+p\mathbf{Z}_p} (t-j)^n \, d\mu_{m_i}(t) \pmod{p^M}$$
using equations (37)–(39). The integral in (39) can be evaluated by expanding $x^{-\ell}$ as a power series and using Proposition 3.1 to calculate the moments of $\mathcal{F}_1$.
3. [Calculate integral (iii)] With the polynomial f as in Step 1 above, for each $i = 1, \dots, r$ calculate
$$\int_{\mathbf{Z}_p^\times \times p\mathbf{Z}_p} \log_p(x) \, d\mu_{m_i}(x,y) \equiv \int_{\mathbf{Z}_p^\times \times p\mathbf{Z}_p} f(x) \, d\mu_{m_i}(x,y) \pmod{p^M},$$
where the right-hand side can be computed using the formula
$$\begin{aligned}(41)\quad \int_{\mathbf{Z}_p^\times \times p\mathbf{Z}_p} x^n \, d\mu\Big\{\infty \to \frac{a}{Nc}\Big\}(x,y) &= -12 \sum_{\ell=0}^{n} \binom{n}{\ell} \Big(\frac{a}{Nc}\Big)^{n-\ell} (-1)^\ell \\ &\times \sum_{d|N} \frac{n_d}{d^\ell} \Big[p^{n-\ell} D_{n-\ell+1,\ell+1}\Big(\frac{pa}{Nc/d}\Big) - p^n D_{n-\ell+1,\ell+1}\Big(\frac{a}{Nc/d}\Big)\Big].\end{aligned}$$
Equation (41) follows by subtracting (9) from (8), using (13) and (14).
4. [Calculate integral (iv)] For $i = 1, \dots, r$ and $n = 0, \dots, M-1$, calculate
$$(42)\qquad \int_{\mathbf{P}^1(\mathbf{Q}_p) - \mathbf{Z}_p} t^{-n} \, d\overline{\mu}_{m_i}(t) \pmod{p^M}$$
as follows. The invariance of $\overline{\mu}$ under $\gamma = \left(\begin{smallmatrix} 1 & 0 \\ N & 1 \end{smallmatrix}\right)$ implies that (42) equals
$$(43)\qquad \int_{\frac{1}{N} + p\mathbf{Z}_p} \Big(\frac{u}{-Nu+1}\Big)^{-n} d\overline{\mu}_{\gamma^{-1}m_i}(u) \pmod{p^M}.$$
Let j be the positive integer less than p which is congruent to $1/N$ modulo p. The function $(\frac{u}{-Nu+1})^{-n}$ can be expanded as a power series in $u - j$ in the residue disc $j + p\mathbf{Z}_p$; this reduces the computation of (43) to the computation of integrals of the form
$$\int_{j+p\mathbf{Z}_p} (u-j)^n \, d\overline{\mu}_{\gamma^{-1}m_i}(u) \pmod{p^M}.$$
These may in turn be computed as in Step 2.

Once Algorithm 4.2 has been executed and its results stored in a file, the $u(\alpha,\tau) \in K_p^\times$ for varying real quadratic fields K and elements $\tau \in K$ can be computed to an accuracy of p^M by the following algorithm, which assumes the results of Algorithm 4.2 as input.

https://doi.org/10.4153/CJM-2007-023-0 Published online by Cambridge University Press

Algorithm 4.3 (Computing $u(\alpha,\tau)$) Fix $\tau \in K \subset \mathbf{P}^1(K_p)$ such that the reduction of τ modulo p does not lie in $\mathbf{P}^1(\mathbf{F}_p)$. Let $\gamma_\tau = \left(\begin{smallmatrix} a & * \\ Nc & * \end{smallmatrix}\right)$ be as in (10). The following algorithm computes $u(\alpha,\tau)$.

1. [Calculate $\operatorname{ord}_p u(\alpha,\tau)$] Define

$$\operatorname{ord}_p(u(\alpha,\tau)) = -12\sum_{d|N} n_d \cdot D\Big(\frac{a}{Nc/d}\Big) \in \mathbf{Z}.$$

2. [Calculate $\log_\beta u(\alpha,\tau)$] Define

$$\begin{aligned}\log_\beta(u(\alpha,\tau)) &= \int_{\mathbf{X}} \log_\beta(x-y\tau)\,\mathrm{d}\mu\Big\{\infty \to \frac{a}{Nc}\Big\}(x,y) \\ &= \sum_{(u,v)} \log_\beta(u-v\tau)\mu\Big\{\infty\to\frac{a}{Nc}\Big\}(U_{u,v,1}) \in \mathbf{Z}/(p^2-1)\mathbf{Z},\end{aligned} \tag{44}$$

where the sum in (44) is over representatives (u,v) in $\mathbf{Z}\times\mathbf{Z}$ for the nonzero elements of $\mathbf{F}_p\times\mathbf{F}_p$. The right side of (44) may be computed using Proposition 3.2.

3. [Calculate $\log_p u(\alpha,\tau)$] Write $[\infty]-[\frac{a}{Nc}]$ in terms of the given $\Gamma_0(N)$-basis for $\mathcal{M}$:

$$[\infty] - \Big[\frac{a}{Nc}\Big] = \sum_{i=1}^{r}\sum_{\gamma\in\Gamma_0(N)} a_{\gamma,i}\cdot\gamma m_i,$$

for example, using Algorithm 4.1 when $N=4$. Then calculate

$$\begin{aligned}\log_p(u(\alpha,\tau)) &= \int_{\mathbf{X}} \log_p(x-y\tau)\,\mathrm{d}\mu\Big\{\infty\to\frac{a}{Nc}\Big\}(x,y) \\ &= \sum_{i,\gamma} a_{i,\gamma}\int_{\mathbf{X}} \log_p(x-y\gamma^{-1}\tau)\,\mathrm{d}\mu_{m_i}(x,y)\end{aligned} \tag{45}$$

modulo p^M, using the decomposition (33)–(34). The first terms of (33) and (34) were calculated in Steps 1 and 3 of Algorithm 4.2. The second terms in (33) and (34) are push forwards from $\mathbf{Z}_p\times\mathbf{Z}_p^\times$ to $\mathbf{Z}_p$ under π; they can be expanded as power series in the residue discs $i+p\mathbf{Z}_p$ as described in (36), and calculated using the moments from Steps 2 and 4 of Algorthm 4.2.

4. [Define $u(\alpha,\tau)$] Define

$$u(\alpha,\tau) = p^{\operatorname{ord}_p(u(\alpha,\tau)}\cdot\beta^{\log_\beta(u(\alpha,\tau))}\cdot\exp(\log_p(u(\alpha,\tau))),$$

where $\exp\colon p\mathcal{O}_p \to 1+p\mathcal{O}_p$ is the exponential map inverting $\log_p$ on $1+p\mathcal{O}_p$.

5 Results

We used the methods of Section 4 with the modular unit $\alpha(z) = \Delta(z)^2\Delta(2z)^{-3}\Delta(4z)$ of level $N = 4$ and various p. We used a p-adic accuracy of $M = 50$ digits. In our calculations, we restricted to fields K and $\tau \in K$ such that the resulting elements $u(\alpha, \tau)$ would be (conjecturally) defined over the narrow Hilbert class field H^+ of K. Assumption (12) lead us to restrict to K of discriminant D congruent to 1 modulo 8. For each p we considered all $D < 500$ for which p is inert in K and $\mathcal{O}_K$ contains no unit of norm -1.

We used the programming language Magma for the computations. In each case, we computed representatives for each of the h classes of quadratic forms to produce a τ_i (see [1, §5.2]) and the corresponding $u(\alpha, \tau_i) \in K_p^\times$. Conjecture 2.14 of [2] predicts that the conjugate of $u(\alpha, \tau_i) \in H^+$ over H is $u(\alpha, \tau_i)^{-1}$. Thus the characteristic polynomial of the $u(\alpha, \tau_i) \in H^+$ over K should be

$$P(x) = \prod_{i=1}^{h} \bigl(x - u(\alpha, \tau_i)\bigr)\bigl(x - u(\alpha, \tau_i)^{-1}\bigr).$$

We computed the polynomial $P(x)$ in $K_p[x]$ to an accuracy of 50 p-adic digits, and used a simple algorithm involving shortest lattice vectors (see [3, §1.6]) to recognize the resulting p-adic numbers as elements of K.

Remark 5.1 The modular symbol ψ attached to α actually takes values in $3\mathbf{Z}$, since α is the cube of the modular function $\eta(z)^8\eta(2z)^{-12}\eta(4z)^4$ of level 4. In order to minimize the heights of the points $u(\alpha, \tau)$, it is preferable to replace ψ with $\psi/3$.

Furthermore, after executing our algorithm, it was clear that in most cases our p-units were still powers of smaller units. If the integers $\operatorname{ord}_p(u(\alpha, \tau_i))$ and

$$\mu\Bigl\{\infty \to \frac{a}{Nc}\Bigr\}((u + p\mathbf{Z}_p) \times (v + p\mathbf{Z}_p))$$

for $(u, v) \in \mathbf{X}$ are divisible by a common integer r relatively prime to p, then formulas (30)–(32) yield a canonical r-th root of $u(\alpha, \tau)$ in $K_p^\times$, by replacing ψ by ψ/r. In each case where $\operatorname{ord}_p u(\alpha, \tau) \neq 0$, we calculated the largest r for which this was the case.

The tables below present our results; we list for each discriminant the class number h of $\mathcal{O}_K$ (so $[H^+ : K] = 2h$), the maximal value of r as described in Remark 5.1, the values $\frac{1}{r}\operatorname{ord}_p u(\alpha, \tau)$, and the polynomial $P(x)$ of the $u(\alpha, \tau)^{1/r}$ scaled to clear powers of p from the denominator. In each case, the polynomials produced are indeed characteristic polynomials of p-units in H^+. In many cases, the units listed are powers of smaller p-units in H^+; in these cases, the polynomial $P(x)$ of the largest root lying in H^+ is listed in the table on the following line (with the root taken implied by the value of r). This root is not necessarily uniquely defined, depending on the presence of roots of unity in H^+.

Remark 5.2 Since the units we produce conjecturally have trivial valuation at each place not lying above p, they are determined uniquely by their valuations at the places

Table 1: Characteristic Polynomial of $u(\alpha,\tau)$ for $p = 3$

D	h	r	$\mathrm{ord}_p\, u(\alpha,\tau)^{1/r}$	$P(x)$
161	1	6	± 0	$x^2 - 2x + 1$
209	1	6	± 6	$729x^2 + 1358x + 729$
		36	± 1	$3x^2 + 5x + 3$
305	2	6	$\pm 2, \pm 4$	$6561x^4 - \frac{675\sqrt{D}+3987}{2}x^3 + \frac{75\sqrt{D}+4607}{2}x^2 - \frac{675\sqrt{D}+3987}{2}x + 6561$
		12	$\pm 1, \pm 3$	$81x^4 - \frac{9\sqrt{D}+345}{2}x^3 + \frac{15\sqrt{D}+419}{2}x^2 - \frac{9\sqrt{D}+345}{2}x + 81$
329	1	6	± 0	$x^2 - 2x + 1$
377	2	12	$\pm 1, \pm 3$	$81x^4 - \frac{21\sqrt{D}+207}{2}x^3 + \frac{21\sqrt{D}+499}{2}x^2 - \frac{21\sqrt{D}+207}{2}x + 81$
473	3	6	$\pm 2, \pm 2, \pm 6$	$3^{10}x^6 + \frac{15795\sqrt{D}+101493}{2}x^5 + \frac{12285\sqrt{D}+620541}{2}x^4 + \frac{34905\sqrt{D}+336763}{2}x^3 + \frac{12285\sqrt{D}+620541}{2}x^2 + \frac{15795\sqrt{D}+101493}{2}x + 3^{10}$
		12	$\pm 1, \pm 1, \pm 3$	$243x^6 + \frac{-9\sqrt{D}+945}{2}x^5 + \frac{15\sqrt{D}+1167}{2}x^4 + \frac{21\sqrt{D}+815}{2}x^3 + \frac{15\sqrt{D}+1167}{2}x^2 + \frac{-9\sqrt{D}+945}{2}x + 243$
497	1	6	± 0	$x^2 - 2x + 1$

above p. In particular, when the class number of K is 1 and $\mathrm{ord}_p\, u(\alpha,\tau) = 0$, we expect $u(\alpha,\tau)$ to be a root of unity. To produce non-trivial units in this case, one must work with a different modular unit α to avoid the "accidental zero" caused by the particular linear combination of Δ-functions weighted by n_d used to define α.

Similarly, if K has class number 2 and the values $\mathrm{ord}_p\, u(\alpha,\tau_i)$ for the distinct Γ-orbits of τ_i are equal, then we expect the corresponding units to be equal, and our polynomial $P(x)$ to factor as a square. A different modular unit must be used to generate the full narrow Hilbert class field. These features of the construction are evident in the tables.

Acknowledgements This work grew out of discussions with H. Darmon, and the computations were done in Magma on W. Stein's MECCAH machines at Harvard University. The results were included in my Ph.D. thesis at the University of California-Berkeley, under the guidance of K. Ribet. I am grateful to all of them for their assistance. I am also indebted to the referee, whose comments greatly improved the final exposition.

Table 2: Characteristic Polynomial of $u(\alpha, \tau)$ for $p = 5$

D	h	r	$\operatorname{ord}_p u(\alpha,\tau)^{1/r}$	$P(x)$
33	1	6	± 2	$25x^2 + \frac{3\sqrt{D}-49}{2}x + 25$
		12	± 1	$5x^2 + \frac{3\sqrt{D}-1}{2}x + 5$
57	1	12	± 1	$5x^2 + \frac{-\sqrt{D}+9}{2}x + 5$
177	1	6	± 6	$5^6x^2 + \frac{4011\sqrt{D}+5231}{2}x + 5^6$
		12	± 3	$125x^2 + \frac{21\sqrt{D}-191}{2}x + 125$
217	1	6	± 0	$x^2 - 2x + 1$
273	2	6	$\pm 2, \pm 2$	$(25x^2 + \frac{3\sqrt{D}-41}{2}x + 25)^2$
		12	$\pm 1, \pm 1$	$(5x^2 + \frac{-\sqrt{D}+3}{2}x + 5)^2$
297	1	12	± 3	$125x^2 - 74x + 125$
		36	± 1	$5x^2 + x + 5$
377	2	6	$\pm 2, \pm 6$	$5^8x^4 + \frac{30375\sqrt{D}+533925}{2}x^3 + \frac{76545\sqrt{D}+102167}{2}x^2 + \frac{30375\sqrt{D}+533925}{2}x + 5^8$
		12	$\pm 1, \pm 3$	$625x^4 + \frac{75\sqrt{D}-655}{2}x^3 + \frac{-15\sqrt{D}+1447}{2}x^2 + \frac{75\sqrt{D}-655}{2}x + 625$
393	1	6	± 10	$5^{10}x^2 + 2275534x + 5^{10}$
		12	± 5	$3125x^2 + 4154x + 3125$
417	1	6	± 6	$5^6x^2 - \frac{2109\sqrt{D}+18929}{2}x + 5^6$
		12	± 3	$125x^2 + \frac{19\sqrt{D}+111}{2}x + 125$
473	3	6	$\pm 2, \pm 2, \pm 6$	$5^{10}x^6 + \frac{-253125\sqrt{D}-4501875}{2}x^5 + \frac{496125\sqrt{D}+5836125}{2}x^4 + \frac{-59535\sqrt{D}-13546883}{2}x^3 + \frac{496125\sqrt{D}+5836125}{2}x^2 + \frac{-253125\sqrt{D}-4501875}{2}x + 5^{10}$
		12	$\pm 1, \pm 1, \pm 3$	$3125x^6 + \frac{-1125\sqrt{D}-1475}{2}x^5 + \frac{225\sqrt{D}+47345}{2}x^4 + \frac{-2655\sqrt{D}-6797}{2}x^3 + \frac{225\sqrt{D}+47345}{2}x^2 + \frac{-1125\sqrt{D}-1475}{2}x + 3125$
497	1	6	± 0	$x^2 - 2x + 1$

Table 3: Characteristic Polynomial of $u(\alpha,\tau)$ for $p = 7$

D	h	r	$\mathrm{ord}_p\, u(\alpha,\tau)^{1/r}$	$P(x)$
33	1	6	± 2	$49x^2 + 94x + 49$
		12	± 1	$7x^2 + 2x + 7$
129	1	12	± 1	$7x^2 - 2x + 7$
201	1	6	± 2	$49x^2 + 94x + 7$
		12	± 1	$7x^2 + 2x + 7$
209	1	12	± 3	$343x^2 - 610x + 343$
		36	± 1	$7x^2 + 5x + 7$
297	1	6	± 6	$7^6x^2 + 153502x + 7^6$
		36	± 1	$7x^2 + 2x + 7$
321	3	6	$\pm 2, \pm 2, \pm 6$	$7^{10}x^6 - \frac{1188495\sqrt{D}+567084987}{2}x^5 + \frac{-557865\sqrt{D}+433702773}{2}x^4 + \frac{5083155\sqrt{D}-475485877}{2}x^3 + \frac{-557865\sqrt{D}+433702773}{2}x^2 - \frac{1188495\sqrt{D}+567084987}{2}x + 7^{10}$
		12	$\pm 1, \pm 1, \pm 3$	$7^5x^6 - \frac{2205\sqrt{D}+53361}{2}x^5 + \frac{3465\sqrt{D}+48699}{2}x^4 - \frac{4455\sqrt{D}+21791}{2}x^3 + \frac{3465\sqrt{D}+48699}{2}x^2 - \frac{2205\sqrt{D}+53361}{2}x + 7^5$
377	2	6	$\pm 2, \pm 6$	$7^8x^4 + \frac{-1210545\sqrt{D}+3900253}{2}x^3 + \frac{-172935\sqrt{D}+31066815}{2}x^2 + \frac{-1210545\sqrt{D}+3900253}{2}x + 7^8$
		12	$\pm 1, \pm 3$	$2401x^4 + \frac{315\sqrt{D}+10017}{2}x^3 + \frac{405\sqrt{D}+15155}{2}x^2 + \frac{315\sqrt{D}+10017}{2}x + 2401$
465	2	6	± 4 , ± 4	$(2401x^2 - 4034x + 2401)^2$
		24	± 1 , ± 1	$(7x^2 + 2x + 7)^2$
489	1	6	± 2	$49x^2 + 94x + 49$
		12	± 1	$7x^2 + 2x + 7$

Table 4: Characteristic Polynomial of $u(\alpha, \tau)$ for $p = 11$

D	h	r	$\operatorname{ord}_p u(\alpha,\tau)^{1/r}$	$P(x)$
57	1	6	± 2	$121x^2 - \frac{15\sqrt{D}+233}{2}x + 121$
		12	± 1	$11x^2 - \frac{5\sqrt{D}+3}{2}x + 11$
105	2	6	$\pm 2, \pm 2$	$(121x^2 - \frac{39\sqrt{D}+73}{2}x + 121)^2$
		12	$\pm 1, \pm 1$	$(11x^2 - \frac{3\sqrt{D}+13}{2}x + 11)^2$
129	1	6	± 2	$121x^2 + \frac{-21\sqrt{D}+199}{2}x + 121$
		12	± 1	$11x^2 + \frac{\sqrt{D}+21}{2}x + 11$ [1pt]
161	1	6	± 0	$x^2 - 2x + 1$
217	1	6	± 0	$x^2 - 2x + 1$
249	1	6	± 6	$11^6x^2 - \frac{167295\sqrt{D}+3198553}{2}x + 11^6$
		12	± 3	$11^3x^2 - \frac{285\sqrt{D}+587}{2}x + 11^3$
305	2	6	$\pm 2, \pm 6$	$11^8x^4 + \frac{10372725\sqrt{D}+344443077}{2}x^3 + \frac{23917275\sqrt{D}-61466353}{2}x^2$ $+\frac{10372725\sqrt{D}+344443077}{2}x + 11^8$
		12	$\pm 1, \pm 3$	$11^4x^4 + \frac{-2475\sqrt{D}+6853}{2}x^3 + \frac{-225\sqrt{D}+44467}{2}x^2$ $+\frac{-2475\sqrt{D}+6853}{2}x + 11^4$
321	3	6	$\pm 2, \pm 2, \pm 6$	$11^{10}x^6 - (1967882169\sqrt{D} + 60603418095)x^5+$ $\frac{10953497049\sqrt{D}+178199983335}{2}x^4$ $-\frac{13842699651\sqrt{D}+210615242059}{2}x^3$ $+\frac{10953497049\sqrt{D}+178199983335}{2}x^2-$ $(1967882169\sqrt{D} + 60603418095)x + 11^{10}$
		12	$\pm 1, \pm 1, \pm 3$	$11^5x^6 + (-4719\sqrt{D} + 427251)x^5+$ $\frac{-37257\sqrt{D}+801537}{2}x^4 + \frac{-55935\sqrt{D}+531929}{2}x^3$ $+\frac{-37257\sqrt{D}+801537}{2}x^2 + (-4719\sqrt{D} + 427251)x + 11^5$
329	1	6	± 0	$x^2 - 2x + 1$
393	1	6	± 10	$11^{10}x^2 - 50395911602x + 11^{10}$
		12	± 5	$11^5x^2 - 319798x + 11^5$
417	1	6	± 6	$11^6x^2 + \frac{174795\sqrt{D}-2882153}{2}x + 11^6$
		12	± 3	$11^3x^2 + \frac{215\sqrt{D}-813}{2}x + 11^3$
497	1	6	± 0	$x^2 - 2x + 1$

https://doi.org/10.4153/CJM-2007-023-0 Published online by Cambridge University Press

References

[1] H. Darmon, *Integration on $\mathcal{H}_p \times \mathcal{H}$ and arithmetic applications.* Ann. of Math. **154**(2001), no. 3, 589–639.

[2] H. Darmon and S. Dasgupta, *Elliptic units for real quadratic fields.* Ann. of Math. **163**(2006), no. 1, 301–345.

[3] H. Darmon and R. Pollack. *The efficient calculation of Stark–Heegner points via overconvergent modular symbols.* Israel J. Math **153**(2006), 319–354.

[4] S. Dasgupta. *Gross–Stark units, Stark–Heegner Points, and Class Fields of Real Quadratic Fields.* Ph.D. thesis, University of California-Berkeley, 2004.

[5] ———, *Stark–Heegner points on modular jacobians.* Ann. Sci. École Norm. Sup. **38**(2005), no. 3, 427–469.

[6] B. H. Gross. *p-adic L-series at $s = 0$.* J. Fac. Sci. Univ. Tokyo Sect. IA Math. **28**(1981), no. 3, 979–994.

[7] R. Greenberg and G. Stevens, *p-adic L-functions and p-adic periods of modular forms*. Invent. Math. **111**(1993), no. 2, 407–447.

[8] S. Lang. *Cyclotomic fields. I and II.* Combined second edition. Graduate Texts in Mathematics 121, Springer-Verlag, New York, 1990.

[9] H. M. Stark, *L-functions at $s = 1$. IV. First derivatives at $s = 0$.* Adv. in Math. **35**(1980), no. 3, 197–235.

[10] U. Halbritter, *Some new reciprocity formulas for generalized Dedekind sums*. Results Math. **8**(1985), no. 1, 21–46.

Department of Mathematics
Harvard University
Cambridge, MA 02138
U.S.A.
e-mail: dasgupta@math.harvard.edu