PACIFIC JOURNAL OF MATHEMATICS
Vol. 119, No. 2, 1985

IWASAWA THEORY FOR THE ANTICYCLOTOMIC EXTENSION

RODNEY I. YAGER

We compute the structure of local units modulo elliptic units for the anticyclotomic $\mathbf{Z}_p$-extension of an imaginary quadratic field with class number one.

Introduction. Let K be an imaginary quadratic field with discriminant $-d_K$ and, for simplicity, class number one. We let p be a rational prime which splits in K, and write K_∞^- for the anticyclotomic $\mathbf{Z}_p$-extension of K, the unique $\mathbf{Z}_p$-extension of K unramified outside p such that the action of complex conjugation c on $\Gamma^- = \mathrm{Gal}(K_\infty^-/K)$ is given by

$$c \cdot \tau = c\tau c^{-1} = \tau^{-1}.$$

Let K_n^- denote the n-th layer of the extension K_∞^- over K. It is clear that both primes of K dividing (p) share the same inertia group for the extension K_n^- over K, which is unramified outside p. Under our assumption that K has class number one, it follows that both primes are totally ramified in K_n^-. Choose one of the primes $\mathfrak{p}$ of K dividing (p), and denote by U_n the group of principal units (i.e. those congruent to one modulo the maximal ideal) of the completion of K_n^- at the unique prime above $\mathfrak{p}$. The natural embedding of K_n^- in its completion sends the group of principal global units E_n of K_n^- into U_n, and we write E_n for the $\mathbf{Z}_p$-submodule of U_n which they generate. The $\mathbf{Z}_p[[\Gamma^-]]$-module $X_\infty = \varprojlim U_n/\overline{E}_n$, where the projections are the norm maps, clearly is important in the arithmetic of K, as it is the Galois group of the maximal abelian p-extension of K_∞^- unramified outside $\mathfrak{p}$, or equivalently, the $\mathfrak{p}$-primary part of the idèle class group of K_∞^-.

The $\mathbf{Z}_p[[\Gamma^-]]$-module X_∞ becomes a torsion $\lambda = \mathbf{Z}_p[[T]]$-module in the usual way if we fix a topological generator τ of Γ^- and define the action of T by setting

$$T \cdot x = (\tau - 1) \cdot x.$$

The classification theorem for torsion λ-modules shows that there is a unique set of principal λ-ideals $\{\mathscr{F}_1, \ldots, \mathscr{F}_r\}$ such that there is a λ-homomorphism $X_\infty \to \oplus_{i=1}^r \lambda/\mathscr{F}_i$ with finite kernel and co-kernel. Moreover,

there is a very precise conjecture for the invariant $\mathcal{F}_{X_\infty} = \prod_{i=1}^{r} \mathcal{F}_i$ of X_∞ which we shall now describe.

We identify the completion of the ring of integers $\mathcal{O}$ of K at $\mathfrak{p}$ with $\mathbf{Z}_p$, and let $\langle\ \rangle\colon \mathbf{Z}_p^* \to 1 + p\mathbf{Z}_p$ be the natural character which fixes $1 + p\mathbf{Z}_p$. It is not hard to see that Γ^- is equipped with a canonical character ϕ: $\Gamma^- \xrightarrow{\sim} 1 + p\mathbf{Z}_p$, whose value at the Artin symbol for the ideal generated by $\alpha \in \mathcal{O}$, α prime to p, is given by

$$\phi((\alpha), K_\infty^-/K) = \langle \alpha \rangle / \langle \bar{\alpha} \rangle.$$

Similarly, since w, the number of roots of unity in K, divides $p - 1$, there is for each integer $k \equiv 0 \bmod p - 1$ a Grossencharacter Φ^k with conductor one given by

$$\Phi^k((\alpha)) = \alpha^k \bar{\alpha}^{-k}.$$

We fix an embedding of K in $\mathbf{C}$ and write $L(\Phi^k, s)$ for the complex Hecke L-function attached to this Grossencharacter.

Choose $\Omega_\infty \in \mathbf{C}^*$ so that the discriminant of the lattice $\Omega_\infty \mathcal{O}$ is a p-unit in $\mathbf{Q}$. This determines Ω_∞^w up to a p-unit in $\mathbf{Q}$, and it is known that for all positive $k \equiv 0 \bmod p - 1$,

$$L^*(\Phi^{-k}, 0) = \left(2\pi/\sqrt{d_K}\right)^k \Omega_\infty^{-2k} L(\Phi^{-k}, 0)$$

lies in K.

Moreover, it is possible to choose a unit $\Omega_\mathfrak{p} \in \mathcal{I}$, the ring of integers of the maximal unramified extension of $K_\mathfrak{p}$ $(= \mathbf{Q}_p)$, such that there is a power series $\mathcal{G}(T) \in \mathcal{I}[[T]]$ satisfying

$$\mathcal{G}\left(\phi(\tau)^k - 1\right) = \Omega_\mathfrak{p}^{-2k}(k-1)!\,\mathrm{Eul}(k) L^*(\Phi^{-k}, 0)$$

for all positive $k \equiv 0 \bmod (p - 1)$, where

$$\mathrm{Eul}(k) = \left(1 - \Phi^k(\mathfrak{p}) p^{-1}\right)\left(1 - \Phi^{-k}(\bar{\mathfrak{p}})\right).$$

The "product" $\Omega_\infty \Omega_\mathfrak{p}$ is well-determined up to multiplication by an element of $\mathbf{Z}_p^*$, and so the ideal generated by $\mathcal{G}(T)$ is independent of the choice of these constants.

Conjecture: *The power series $\mathcal{G}(T)$ generates the same ideal of $\mathcal{I}[[T]]$ as $\mathcal{F}_{X_\infty}$.*

In this paper, we shall deduce from the results in our earlier work [Y] that the conjecture holds for the closely related λ-module $Y_\infty = \varprojlim U_n/\bar{C}_n$, where the global units E_n are replaced by the elliptic units $\bar{C}_n$ of K_n^-. However, it will be necessary to suppose not only that p splits in K, but that p is not 2 or 3, and that there is an elliptic curve E defined over $\mathbf{Q}$

with good reduction at p, which, when viewed over K, admits complex multiplication by $\mathcal{O}$.

Local units. Let E be an elliptic curve with the above properties, and choose a Weierstrass model for E

$$y^2 = 4x^3 - g_2x - g_3, \qquad g_2, g_3 \in \mathbf{Z}$$

with discriminant δ prime to p. We denote by L the period lattice of the associated Weierstrass $\wp$-function, and choose a generator Ω_∞ of L so that $L = \Omega_\infty \mathcal{O}$. We recall that w is the number of roots of unity in K, and leave it as an exercise for the reader to show that Ω_∞^w is well-determined up to a p-unit in $\mathbf{Q}$, independent of our choice of elliptic curve E.

We write $K(E_{p^{n+1}})$ for the field obtained by adjoining to K the coordinates of all the points of $E(K^{\mathrm{ab}})$ of order p^{n+1}, and let $K(E_{p^\infty})$ denote $\bigcup_{n\geq 0} K(E_{p^{n+1}})$. It is well known that $K(E_{p^\infty})$ contains K_∞, the maximal abelian p-extension of K unramified outside p, and that $\mathrm{Gal}(K(E_{p^\infty})/K)$ decomposes as $\Delta \times \Gamma$, where Δ is isomorphic to $(\mathbf{Z}/p\mathbf{Z})^{*2}$ and may be identified with $\mathrm{Gal}(K(E_p)/K)$ and $\Gamma \tilde{=} \mathbf{Z}_p^2$ and may be identified with $\mathrm{Gal}(K_\infty/K)$.

In turn, since K_∞ is Galois over $\mathbf{Q}$, $\mathrm{Gal}(K/\mathbf{Q})$ acts on Γ via inner automorphisms, and so Γ decomposes uniquely as $\Gamma = \Gamma^+ \oplus \Gamma^-$, where complex conjugation acts trivially on Γ^+ and by -1 on Γ^-. Of course, Γ^+ is the Galois group of K_∞^+ over K, where K_∞^+ is the cyclotomic $\mathbf{Z}_p$-extension of K, and $\Gamma^- = \mathrm{Gal}(K_\infty^-/K)$, where K_∞^- is the anticyclotomic $\mathbf{Z}_p$-extension mentioned in the introduction.

For each place ω of $K(E_{p^{n+1}})$ dividing $\mathfrak{p}$, we write $\mathbf{U}_{n,\omega}$ for the principal units of the completion of $K(E_{p^{n+1}})$ at ω, and set $\mathbf{U}_n = \prod_{\omega|\mathfrak{p}} \mathbf{U}_{n,\omega}$ and $\mathbf{U}_\infty = \varprojlim \mathbf{U}_n$ where, as usual, the projections are the norm maps. Similarly, we let U_∞ denote $\varprojlim U_n$.

THEOREM 1. *The natural norm map* $\mathbf{N}\colon \mathbf{U}_\infty \to U_\infty$ *is onto.*

Proof. Since $\mathfrak{p}$ is totally ramified in K_∞/K, it follows from local class field theory that an element $\alpha \in U_n$ can be extended to an element of U_∞ if and only if the norm to $K_\mathfrak{p}$ of α is one. Again, by local class field theory, such an element is a norm from $\mathbf{U}_\infty$.

The Galois group of $K(E_{p^\infty})$ over K acts on $\mathbf{U}_\infty$ in the obvious way, and we may write

$$\mathbf{U}_\infty = \bigoplus_\chi \mathbf{U}_{\infty_\chi},$$

where χ runs over the $\mathbf{Z}_p^*$-valued characters of Δ and $\mathbf{U}_{\infty_\chi}$ denotes the $\mathbf{Z}_p[[\Gamma]]$-submodule of $\mathbf{U}_\infty$ on which Δ acts via χ. Now it is easy to see that $\mathbf{N}(\mathbf{U}_\infty) = 1$ unless χ is the trivial character, and so we deduce from Theorem 1 that $\mathbf{N}$: $\mathbf{U}_{\infty_1} \to U_\infty$ is onto.

Recall that we have already chosen a topological generator τ of Γ^-. Now, choose a topological generator σ of Γ^+. The $\mathbf{Z}_p[[\Gamma]]$-module $\mathbf{U}_{\infty_1}$ becomes a $\Lambda = \mathbf{Z}_p[[S, T]]$-module by setting

$$S \cdot u = (\sigma - 1) \cdot u \quad \text{and} \quad T \cdot u = (\tau - 1) \cdot u,$$

and it was shown in Lemma 25 of [Y] that $\mathbf{U}_{\infty_1}$ is a free Λ-module of rank one.

THEOREM 2. *Let* Υ: $\Lambda \to \mathbf{U}_{\infty_1}$ *be any isomorphism of* Λ*-modules. Then there is a unique isomorphism* v: $\lambda \to U_\infty$ *of* λ*-modules such that the diagram*

$$\begin{array}{ccccc} f(S,T) & \in & \Lambda & \xrightarrow{\Upsilon} & \mathbf{U}_\infty \\ \downarrow & & \downarrow & & \downarrow \mathbf{N} \\ f(0,T) & \in & \lambda & \xrightarrow{v} & U_\infty \end{array} \qquad \textit{commutes.}$$

Proof. Clearly $\mathbf{N} \cdot \Upsilon$ is a λ-module homomorphism, so by Theorem 1, we need only show that $S\Lambda$ lies in the kernel of $\mathbf{N} \cdot \Upsilon$, and that $\ker v = 0$.

The first of these is obvious, since $\Upsilon(Sf(S, T)) = \sigma \cdot \Upsilon(f(S, T)) - \Upsilon(f(S, T))$, and this is clearly in the kernel of $\mathbf{N}$.

Suppose now that $\ker v \neq 0$, and choose a non-zero element $f(T) \in \ker v$. By the Weierstrass preparation theorem we may write

$$f(T) = p^r q(T) u(T),$$

where $r \geq 0$, $q(T)$ is a distinguished polynomial and $u(T) \in \lambda^*$.

Now $v \cdot p^r$ induces a map from $\lambda/q(T)$ onto $p^r U_\infty$, which, in turn, projects onto $p^r U_n'$, where U_n' denotes the elements of U_n whose norm to $K_\mathfrak{p}$ is one, and so it follows that $p^r U_n'$ is a finitely generated $\mathbf{Z}_p$-module of rank at most the degree of $q(T)$.

On the other hand, it is well known that U_n' contains a submodule which is a free $\mathbf{Z}_p$-module of rank $p^n - 1$, which, for n sufficiently large, must contradict the above statement. It follows that v must be an isomorphism.

Elliptic units. In [Y], we constructed an explicit Λ-module isomorphism from $\mathbf{U}_{\infty_1}$ to Λ, and computed the image in Λ of the closure in $\mathbf{U}_{\infty_1}$ of a certain subgroup of the global units of K_∞. Here we shall consider a

slightly larger subgroup of the global units, which we could equally well have used in [Y], so we shall quickly sketch their construction.

Let $\sigma(z)$ be the Weierstrass σ-function attached to the lattice L, and set

$$\theta(z) = \delta e^{-6s_2 z^2} \sigma(z)^{12},$$

where

$$s_2 = \lim_{s \to 0^+} \sum_{\substack{\omega \in L \\ \omega \neq 0}} \omega^{-2} |\omega|^{-2s}.$$

We write I for the set of ideals of K prime to $6\mathfrak{f}p$, where $\mathfrak{f}$ is the conductor of the Grossencharacter ψ attached to E over K by theory of complex multiplication, and for each $\mathfrak{a} \in I$, we set

$$\Theta(z, \mathfrak{a}) = \theta(z)^{N\mathfrak{a}} \theta(\psi(\mathfrak{a})z)^{-1}.$$

It can be shown that $\Theta(z, \mathfrak{a})$ is an elliptic function with period lattice L, and Robert [**R**] and de Shalit [**S**] have shown that if ρ is a primitive $\mathfrak{g}p^{n+1}$-division point of L for some integral ideal $\mathfrak{g}$ dividing $\mathfrak{f}$, then $\theta(\rho, \mathfrak{a})$ is a unit in the field $K(E_{\mathfrak{g}p^{n+1}})$ obtained by adjoining to K the coordinates of the points of $E(K^{\mathrm{ab}})$ of order dividing $\mathfrak{g}p^{n+1}$. The norms of $\Theta(\rho, \mathfrak{a})$ from $K(E_{\mathfrak{g}p^{n+1}})$ to $K(E_{p^{n+1}})$ for all such ρ, $\mathfrak{a}$ and $\mathfrak{g}$ generate a subgroup of finite index in the global units of $K(E_{p^{n+1}})$ which is stable under the action of $\mathrm{Gal}(K(E_{p^{n+1}})/K)$, and which we shall call the group of elliptic units of $K(E_{p^{n+1}})$.

The group of principal elliptic units of $K(E_{p^{n+1}})$, which we denote by $\mathbf{C}_n$, consists of those elliptic units which are congruent to one modulo each prime of $K(E_{p^{n+1}})$ dividing $\mathfrak{p}$. Clearly $\mathbf{C}_n$ is of finite (prime to p) index in the group of elliptic units, and may be embedded in the group of principal local units $\mathbf{U}_n$ via the diagonal map. We let $\bar{\mathbf{C}}_n$ denote the $\mathbf{Z}_p$-module generated by $\mathbf{C}_n$. We mention that the norm map sends $\mathbf{C}_{n+1}$ onto $\mathbf{C}_n$, and that $\bar{\mathbf{C}}_\infty = \varprojlim \bar{\mathbf{C}}_n$ is a Λ-submodule of $\mathbf{U}_\infty$.

In [Y] we determined the structure of $(\mathbf{U}_\infty/\bar{\mathbf{C}}_\infty)_\chi$, the submodule of $\mathbf{U}_\infty/\bar{\mathbf{C}}_\infty$ on which Δ acts via χ, for each character χ, except that there we used a slightly smaller group of principal elliptic units. We shall simply state the corresponding structure theorem in the present case, after explaining our terminology.

First, we note that the character group of Δ is generated by the $\mathbf{Z}_p^*$-valued characters $\chi_{\mathfrak{p}}$ and $\chi_{\bar{\mathfrak{p}}}$, both of order $p-1$, giving the action of Δ on $E_{\mathfrak{p}}$ and $E_{\bar{\mathfrak{p}}}$ respectively. There is also a canonical character $\mathcal{N}$: $\Gamma^+ \xrightarrow{\sim} 1 + p\mathbf{Z}_p$ whose value on the Artin symbol for the ideal generated

by $\alpha \in \mathcal{O}$, α prime to p, is given by

$$\mathcal{N}((\alpha), K_\infty^+/K) = \langle \alpha\bar{\alpha} \rangle.$$

We should mention that if $\kappa_\mathfrak{p}$ and $\kappa_{\bar{\mathfrak{p}}}$ are the $\mathbf{Z}_p^*$-valued characters of [Y] giving the action of $\mathrm{Gal}(K(E_{p^\infty})/K)$ on $E_{\mathfrak{p}^\infty}$ and $E_{\bar{\mathfrak{p}}^\infty}$ respectively, then $\mathcal{N}$ is the restriction to Γ^+ of $\kappa_\mathfrak{p}\kappa_{\bar{\mathfrak{p}}}$, while ϕ is the restriction to Γ^- of $\kappa_\mathfrak{p}\kappa_{\bar{\mathfrak{p}}}^{-1}$. We extend both $\mathcal{N}$ and ϕ to the whole of Γ by insisting that they are trivial on Γ^- and Γ^+ respectively.

Finally, we let r denote the number of primes of $K(E_p)$ dividing $\mathfrak{p}$, and M be the number of places of K_∞ dividing $\mathfrak{p}$. Clearly r divides $p-1$, and M is a power of p. It is also easy to see that if $\mathfrak{p}_\infty$ is any one of the M places of K_∞ dividing $\mathfrak{p}$, then $\mathrm{Gal}(K_{\infty_{\mathfrak{p}_\infty}}/K_\mathfrak{p}) \subset \Gamma$, and is topologically generated by σ^M and $\sigma\tau^\ell$, where $\ell \in \mathbf{Z}_p^*$ and is chosen so that $\mathcal{N}(\sigma) = \phi(\tau)^\ell$.

THEOREM 3. *For each character χ of Δ, set*

$$H_\chi = \begin{cases} \left\langle (1+S)(1+T)^\ell - \mathcal{N}(\sigma\tau^\ell), (1+S)^M - \mathcal{N}(\sigma)^M \right\rangle, \\ \qquad \chi = \chi_\mathfrak{p}\chi_{\bar{\mathfrak{p}}}^j \quad \text{with } j \equiv 1 \bmod (p-1)/r \\ \Lambda \quad \text{otherwise.} \end{cases}$$

and

$$\mathcal{H}_\chi = \begin{cases} \langle (1+S) - \mathcal{N}(\sigma), T \rangle, & \chi = \chi_\mathfrak{p}\chi_{\bar{\mathfrak{p}}} \\ \Lambda \quad \text{otherwise.} \end{cases}$$

Let $L(\bar{\psi}^{k+j}, s)$ denote the primitive Hecke L-function attached to the Grossencharacter $\bar{\psi}^{k+j}$, and observe that Damerell's theorem shows that

$$L^*(\bar{\psi}^{k+j}, k) = \left(2\pi/\sqrt{d_K}\right)^j \Omega_\infty^{-(k+j)} L(\bar{\psi}^{k+j}, k)$$

lies in K for $k > j \geq 0$.

Then $(\mathbf{U}_\infty/\bar{\mathbf{C}}_\infty)_\chi$ is Λ-isomorphic to $\mathcal{H}_\chi/H_\chi G_\chi(S,T)$ where $G_\chi(S,T)$ is any power series in Λ generating the same ideal in $\mathcal{I}[[S,T]]$ as the unique power series $\mathcal{G}_\chi(S,T) \in \mathcal{I}[[S,T]]$ satisfying the following interpolation property:

$$\mathcal{G}_\chi\left(\mathcal{N}(\sigma)^{(k-j)/2} - 1, \phi(\tau)^{(k+j)/2} - 1\right) = (k-1)!\,\mathrm{Eul}(k,j)\Omega_\mathfrak{p}^{-(k+j)} L^*(\bar{\psi}^{k+j}, k)$$

for all $k > j \geq 0$ such that $\chi = \chi_\mathfrak{p}^k \chi_{\bar{\mathfrak{p}}}^{-j}$.

Here $\mathrm{Eul}(k,j) = (1 - \bar{\psi}(\mathfrak{p})^{k+j}/N\mathfrak{p}^{j+1})(1 - \bar{\psi}(\bar{\mathfrak{p}})^{k+j}/N\bar{\mathfrak{p}}^k)$, and $\Omega_\mathfrak{p}$ is the so-called $\mathfrak{p}$-adic period of E, a unit in $\mathcal{I}$.

Main Theorem. We define the elliptic units C_n of K_n^- to be the norms to K_n^- of the elliptic units of $K(E_{p^{n+1}})$. It happens that these units are principal, and so the $\mathbf{Z}_p$-module $\overline{C}_n$ generated by C_n is none other than that generated by the norms of the principal elliptic units of $K(E_{p^{n+1}})$. It follows that $\overline{C}_\infty = \varprojlim \overline{C}_n$ is a λ-submodule of U_∞, and is the image of $\overline{\mathbf{C}}_\infty$ under the norm map $\mathbf{N}$: $\mathbf{U}_\infty \to U_\infty$.

We also observe that if we write Φ for the Grossencharacter $\psi\bar{\psi}^{-1}$, then, for each $k \equiv 0 \bmod p-1$, Φ^k is the Grossencharacter of that name mentioned in the introduction. Our main theorem is then just a consequence of Theorems 2 and 3.

THEOREM 4. *In the above notation, $U_\infty/\overline{C}_\infty$ is λ-isomorphic to λ/G, where G is a principal ideal of λ generating the same ideal in $\mathcal{I}[[T]]$ as the power series $\mathcal{G}(T)$ satisfying*

$$\mathcal{G}\big(\phi(\tau)^k - 1\big) = \Omega_{\mathfrak{p}}^{-2k}(k-1)!\,\mathrm{Eul}(k)\,L^*(\Phi^{-k}, 0)$$

for all positive $k \equiv 0 \bmod (p-1)$.

Finally, we wish to make two remarks. The first is that while the elliptic units C_n of K_n^- may depend on the auxiliary choice of an elliptic curve E, the structure of $U_\infty/\overline{C}_\infty$ does not, since, as we have seen, the power series $\mathcal{G}(T)$ is well-determined up to a unit by the field K.

The other remark is that precisely the same technique will work to prove a similar theorem for any $\mathbf{Z}_p$-extension contained in K_∞ in which $\mathfrak{p}$ is infinitely ramified. We leave it as an exercise for the reader to deduce the theorem in the two most interesting cases; K_∞^+, where the answer, of course, involves Bernoulli numbers, and the $\mathbf{Z}_p$-extension of K contained in $K(E_{\mathfrak{p}^\infty})$, which provides the missing eigenspace in Theorem 1 of Coates-Wiles [**C-W**].

REFERENCES

[**C-W**] J. Coates and A. Wiles, *On p-adic L-functions and elliptic units*, J. Austral. Math. Soc., **26** (1978), 1–25.

[**R**] G. Robert, *Unités élliptiques*, Bull. Soc. Math. France Mémoire, **36** (1973).

[**S**] E. de Shalit, *Thesis*, Princeton University, to appear.

[**Y**] R. Yager, *On two variable p-adic L-functions*, Ann. Math., **115** (1982), 411–449.

Received June 28, 1983 and in revised form December 6, 1983. Supported in part by N.S.F.Grant no. MCS 8202310.

OKLAHOMA STATE UNIVERSITY
STILLWATER, OK 74078