IWASAWA THEORY FOR THE ANTICYCLOTOMIC EXTENSION

RODNEY IAN YAGER
We compute the structure of local units modulo elliptic units for the anticyclotomic $\mathbb{Z}_p$-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 $K_\infty^-$ for the anticyclotomic $\mathbb{Z}_p$-extension of $K$, the unique $\mathbb{Z}_p$-extension of $K$ unramified outside $p$ such that the action of complex conjugation $c$ on $\Gamma^- = \text{Gal}(K_\infty^-/K)$ is given by

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

Let $K_n^-$ denote the $n$-th layer of the extension $K_\infty^-$ 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 $\mathbb{Z}_p$-submodule of $U_n$ which they generate. The $\mathbb{Z}_p[[\Gamma^-]]$-module $X_\infty = \varprojlim U_n/E_n$, 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 $\mathfrak{p}$-extension of $K_\infty^-$ unramified outside $\mathfrak{p}$, or equivalently, the $\mathfrak{p}$-primary part of the idèle class group of $K_\infty^-$. The $\mathbb{Z}_p[[\Gamma^-]]$-module $X_\infty$ becomes a torsion $\lambda = \mathbb{Z}_p[[T]]$-module in the usual way if we fix a topological generator $\tau$ of $\Gamma^-$ and define the action of $T$ by setting

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

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

\[
\phi((\alpha), K_{\infty}/K) = \frac{\langle \alpha \rangle}{\langle \alpha \rangle}.
\]

Similarly, since \( \omega \), the number of roots of unity in \( K \), divides \( p - 1 \), there is for each integer \( k \equiv 0 \mod p - 1 \) a Grossencharacter \( \Phi^k \) with conductor one given by

\[
\Phi^k((\alpha)) = \alpha^k \alpha^{-k}.
\]

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

Choose \( \Omega_{\infty} \in \mathbb{C}^* \) so that the discriminant of the lattice \( \Omega_{\infty} \mathfrak{O} \) is a \( p \)-unit in \( \mathbb{Q} \). This determines \( \Omega_{\infty}^\omega \) up to a \( p \)-unit in \( \mathbb{Q} \), and it is known that for all positive \( k \equiv 0 \mod p - 1 \),

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

lies in \( K \).

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

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

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

\[
\text{Eul}(k) = (1 - \Phi^k(p^{-1})p^{-1})(1 - \Phi^{-k}(\mathfrak{p})).
\]

The “product” \( \Omega_{\infty} \Omega_{\mathfrak{p}} \) is well-determined up to multiplication by an element of \( \mathbb{Z}_p^* \), 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 \( \mathfrak{S}[[T]] \) 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 \( \lambda \)-module \( Y_{\infty} = \lim U_n / \mathcal{C}_n \), where the global units \( E_n \) are replaced by the elliptic units \( \mathcal{C}_n \) of \( K_{\mathfrak{n}}^{-} \). 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 \( \mathbb{Q} \).
with good reduction at $p$, which, when viewed over $K$, admits complex multiplication by $\Theta$.

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

$$y^2 = 4x^3 - g_2x - g_3,$$  

with discriminant $\delta$ prime to $p$. We denote by $L$ the period lattice of the associated Weierstrass $\wp$-function, and choose a generator $\Omega_\infty$ 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 $\Omega_\infty$ is well-determined up to a $p$-unit in $\mathbb{Q}$, independent of our choice of elliptic curve $E$.

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

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

For each place $\omega$ of $K(E_{p^{n+1}})$ dividing $p$, we write $U_{n,\omega}$ for the principal units of the completion of $K(E_{p^{n+1}})$ at $\omega$, and set $U_n = \prod_{\omega \mid p} U_{n,\omega}$ and $U_\infty = \bigcap_{\omega} U_n$ where, as usual, the projections are the norm maps. Similarly, we let $U_\infty$ denote $\lim_{\leftarrow} U_n$.

**Theorem 1.** The natural norm map $N: U_\infty \to U_\infty$ is onto.

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

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

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

Recall that we have already chosen a topological generator \( \tau \) of \( \Gamma^- \). Now, choose a topological generator \( \sigma \) of \( \Gamma^+ \). The \( \mathbb{Z}_p[[\Gamma]] \)-module \( U_{\infty, 1} \) becomes a \( \Lambda = \mathbb{Z}_p[[S, T]] \)-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 \( U_{\infty, 1} \) is a free \( \Lambda \)-module of rank one.

**Theorem 2.** Let \( \mathcal{T}: \Lambda \to U_{\infty, 1} \) be any isomorphism of \( \Lambda \)-modules. Then there is a unique isomorphism \( v: \lambda \to U_{\infty} \) of \( \lambda \)-modules such that the diagram

\[
\begin{array}{ccc}
  f(S, T) & \in & \Lambda \\
  \downarrow & \mathcal{T} & \downarrow \\
  f(0, T) & \in & \lambda
\end{array}
\]

commutes.

**Proof.** Clearly \( N \cdot \mathcal{T} \) is a \( \lambda \)-module homomorphism, so by Theorem 1, we need only show that \( S\Lambda \) lies in the kernel of \( N \cdot \mathcal{T} \), and that \( \ker v = 0 \).

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

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 \( K_p \) is one, and so it follows that \( p^r U_n' \) is a finitely generated \( \mathbb{Z}_p \)-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 \( \mathbb{Z}_p \)-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 \( \Lambda \)-module isomorphism from \( U_{\infty, 1} \) to \( \Lambda \), and computed the image in \( \Lambda \) of the closure in \( U_{\infty, 1} \) of a certain subgroup of the global units of \( K_{\infty} \). 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 $\sigma$-function attached to the lattice $L$, and set

$$\theta(z) = \delta e^{-6s_2z^2}\sigma(z)^{12},$$

where

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

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

$$\Theta(z, \alpha) = \theta(z)^{N_\alpha}\theta(\psi(\alpha)z)^{-1}.$$

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

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

In [Y] we determined the structure of $(U^\pi/\overline{C}_\infty)_\chi$, the submodule of $U^\pi/\overline{C}_\infty$ on which $\Delta$ acts via $\chi$, for each character $\chi$, 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 $\Delta$ is generated by the $\mathbb{Z}_p^*$-valued characters $\chi_\mathfrak{p}$ and $\chi_{\mathfrak{p}^{-1}}$, both of order $p - 1$, giving the action of $\Delta$ on $E_\mathfrak{p}$ and $E_{\mathfrak{p}^{-1}}$ respectively. There is also a canonical character $N^\pi: \Gamma + \sim 1 + p\mathbb{Z}_p$ whose value on the Artin symbol for the ideal generated
by \( \alpha \in \mathcal{O} \), \( \alpha \) prime to \( p \), is given by
\[
\mathcal{N}((\alpha), K^+ / K) = \langle \alpha \bar{\alpha} \rangle.
\]

We should mention that if \( \kappa_p \) and \( \kappa_{\bar{p}} \) are the \( \mathbb{Z}_p^* \)-valued characters of \( [Y] \) giving the action of \( \text{Gal}(K(E_p^\infty) / K) \) on \( E_p^\infty \) and \( E_{\bar{p}}^\infty \) respectively, then \( \mathcal{N} \) is the restriction to \( \Gamma^+ \) of \( \kappa_p \kappa_{\bar{p}} \), while \( \phi \) is the restriction to \( \Gamma^- \) of \( \kappa_p \kappa_{\bar{p}}^{-1} \). We extend both \( \mathcal{N} \) and \( \phi \) to the whole of \( \Gamma \) by insisting that they are trivial on \( \Gamma^- \) and \( \Gamma^+ \) 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 \( K_\infty \) dividing \( \mathfrak{p} \). Clearly \( r \) divides \( p - 1 \), and \( M \) is a power of \( p \). It is also easy to see that if \( p_\infty \) is any one of the \( M \) places of \( K_\infty \) dividing \( \mathfrak{p} \), then \( \text{Gal}(K_{\infty_\mathfrak{p}} / K) \subset \Gamma \), and is topologically generated by \( \sigma^M \) and \( \sigma \tau^\ell \), where \( \ell \in \mathbb{Z}_p^\infty \) and is chosen so that \( \mathcal{N}(\sigma) = \phi(\tau)^\ell \).

**Theorem 3.** For each character \( \chi \) of \( \Delta \), set
\[
H_\chi = \left\{ \begin{array}{ll}
\langle (1 + S)(1 + T)^\ell - \mathcal{N}(\sigma \tau^\ell), (1 + S)^M - \mathcal{N}(\sigma)^M \rangle, \\
\chi = \chi_p \chi_{\bar{p}}^j \text{ with } j \equiv 1 \mod (p - 1)/r
\end{array} \right.
\]
and
\[
\mathcal{H}_\chi = \left\{ \begin{array}{ll}
\langle (1 + S) - \mathcal{N}(\sigma), T \rangle, \\
\chi = \chi_p \chi_{\bar{p}}^j
\end{array} \right. \text{ otherwise.}
\]

Let \( L(\overline{\psi}^{k+j}, s) \) denote the primitive Hecke \( L \)-function attached to the Grossencharacter \( \overline{\psi}^{k+j} \), and observe that Damerell’s theorem shows that
\[
L^*(\overline{\psi}^{k+j}, k) = \left( 2\pi / \sqrt{d_K} \right)^j \Omega_{\infty}^{-(k+j)} L(\overline{\psi}^{k+j}, k)
\]
lies in \( K \) for \( k > j \geq 0 \).

Then \( (U_\infty / \mathcal{C}_\infty)_\chi \) is \( \Delta \)-isomorphic to \( \mathcal{H}_\chi / H_\chi G_\chi(S, T) \) where \( G_\chi(S, T) \) is any power series in \( \Delta \) generating the same ideal in \( \mathcal{I}[[S, T]] \) as the unique power series \( G_{\chi}(S, T) \in \mathcal{I}[[S, T]] \) satisfying the following interpolation property:
\[
\mathcal{G}_\chi(\mathcal{N}(\sigma)^{(k-j)/2} - 1, \phi(\tau)^{(k+j)/2} - 1) = (k - 1)! \text{Eul}(k, j) \Omega_{\mathfrak{p}}^{-(k+j)} L^*(\overline{\psi}^{k+j}, k)
\]
for all \( k > j \geq 0 \) such that \( \chi = \chi_p \chi_{\bar{p}}^j \).

Here \( \text{Eul}(k, j) = (1 - \overline{\psi}(\mathfrak{p})^{k+j}/N\mathfrak{p}^{j+1})(1 - \overline{\psi}(\mathfrak{p})^{k+j}/N\mathfrak{p}^k) \), 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 $\mathbb{Z}_p$-module $C_n$ 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 $\overline{C}_\infty = \varprojlim C_n$ is a $\lambda$-submodule of $U_\infty$, and is the image of $C_\infty$ under the norm map $N: U_\infty \to U_\infty$.

We also observe that if we write $\Phi$ for the Grossencharacter $\psi \bar{\psi}^{-1}$, then, for each $k \equiv 0 \mod{p-1}$, $\Phi^k$ 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, $U_\infty / C_\infty$ is $\lambda$-isomorphic to $\lambda / G$, where $G$ is a principal ideal of $\lambda$ generating the same ideal in $\mathcal{S}[[T]]$ as the power series $\mathcal{G}(T)$ satisfying

$$\mathcal{G}(\phi(T)^k - 1) = \Omega_p^{-2k}(k-1)! \text{Eul}(k) L^*(\Phi^{-k}, 0)$$

for all positive $k \equiv 0 \mod{p-1}$.

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 $U_\infty / C_\infty$ 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 $\mathbb{Z}_p$-extension contained in $K_\infty$ 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; $K_\infty^+$, where the answer, of course, involves Bernoulli numbers, and the $\mathbb{Z}_p$-extension of $K$ contained in $K(E_{\mathfrak{p}^\infty})$, which provides the missing eigenspace in Theorem 1 of Coates-Wiles [C-W].

**References**


Received June 28, 1983 and in revised form December 6, 1983. Supported in part by N.S.F. Grant no. MCS 8202310.
Mustafa Agah Akcoglu and Meira Falkowitz (Soshniak), A general local ergodic theorem in $L_1$ .......................................................... 257

W. Wistar (William) Comfort and Lewis Chandlee Robertson, Cardinality constraints for pseudocompact and for totally dense subgroups of compact topological groups .......................... 265

John Morse Delaurentis and Boris G. Pittel, Random permutations and Brownian motion ................................................................. 287

José Esteban Galé, Gel’fand theory in algebras of differentiable functions on Banach spaces ......................................................... 303

Harry Gingold, On the location of zeroes of oscillatory solutions of $y^{(n)} = c(x)y$ ................................................................. 317

Kei Ji Izuchi, Zero sets of interpolating Blaschke products .................. 337

Mahesh Nerurkar, Ergodic continuous skew product actions of amenable groups ................................................................. 343

R. Owens, A maximal function characterization of a class of Hardy spaces ................................................................. 365

Judith Anne Packer, Point spectrum of ergodic abelian group actions and the corresponding group-measure factors ............................. 381

Judith Anne Packer, On the embedding of subalgebras corresponding to quotient actions in group-measure factors .......................... 407

Iain Raeburn and Joseph L. Taylor, The bigger Brauer group and étale cohomology ................................................................. 445

David Rosen, The Diophantine equation $ax + by = c$ in $Q(\sqrt{5})$ and other number fields ............................................................. 465

Mau-Hsiang Shih and Kok Keong Tan, Noncompact sets with convex sections ................................................................. 473

Lee Barlow Whitt, Codimension two isometric immersions between Euclidean spaces ............................................................. 481

Rodney Ian Yager, Iwasawa theory for the anticyclotomic extension .... 489