Euler systems and the conjectures of Stark
(Working paper)

David R. Hayes*
University of Massachusetts
Amherst, MA 01003
email: dhayes@qmodz.math.umass.edu

January 26, 1990

Introduction

The *Euler systems* introduced by Kolyvagin [K] have been applied with great success to the arithmetic theory of elliptic curves and to the theory of cyclotomic number fields. For these applications, the reader may consult [Gr], [R1], [R2] and [R3]. In this paper, we consider Euler systems which arise from the abelian Stark conjectures (cf. [T]). In §§2 and 3 below, we construct a new Euler system using the Brumer-Stark elements in cyclotomic function fields. In §§4 and 5, we apply the insights gained from the function field case to elucidate the Gauss sum Euler system in cyclotomic number fields.

Our analysis in §5 leads to an identity theorem for Gauss sums which may be new. The author would greatly appreciate receiving information about where this theorem might appear in the literature. It may be stated as follows: For an odd prime p, let $\mathbf{F}_*$ be the algebraic closure of $\mathbf{F}_p$, and let $\omega : \mathbf{F}_* \to \mu(\mathbf{Q}_p^{\mathrm{nr}})$ be an isomorphism onto the roots of unity in the maximal unramified extension field of $\mathbf{Q}_p$. For $m > 0$ prime to $p(p-1)$, let $f(m)$ be the order of p in the multiplicative group modulo m and put

$$a_m = \frac{p^{f(m)} - 1}{(p-1)m}.$$

---

*Partially supported by NSF grant DMS-8702716.

Write $\mathbf{F}_m = \mathbf{F}_{p^{f(m)}}$. After fixing any non-trivial additive character $e_1 : \mathbf{F}_p \to \mathbf{Q}_p(\zeta_p)^\times$, put

$$e_m(z) = e_1(i(m) \cdot S_m(z))$$

for $z \in \mathbf{F}_m$, where $S_m : \mathbf{F}_m \to \mathbf{F}_p$ is the trace map and where $i(m)$ is a multiplicative inverse for m modulo p. Put $p^* = (-1/p)p$, where $(-1/p)$ is the Legendre symbol, and fix $\sqrt{p^*} \in \mathbf{Q}_p(\zeta_p)$. We may now define the normalized Gauss sum

$$G(m) = \left(\frac{(p^*/m)}{\sqrt{p^*}}\right)^{f(m)} \cdot \sum_{z \in \mathbf{F}_m^\times} \omega(z)^{a_m} \cdot e_m(z),$$

(p^*/m) denoting the Jacobi symbol.

Theorem 1 *Suppose $m'f(m) = mf(m')$, where m and m' are positive integers prime to $p(p-1)$ such that* Supp(m) = Supp(m'). *Then $G(m) = G(m')$.*

1 The cyclotomic Euler system over Q

Throughout this §, m always denotes a positive integer which is either odd or divisible by 4. For every such integer m, let ζ_m be some primitive m-th root of unity in the algebraic closure $\mathbf{Q}^{\mathrm{ac}}$ of $\mathbf{Q}$, and let $K_m = \mathbf{Q}(\zeta_m)$ be the corresponding cyclotomic number field. For $t \in \mathbf{Z}$ prime to m, let σ_t be the element of the Galois group $G_m = \mathrm{Gal}(K_m/\mathbf{Q})$ which maps ζ_m to ζ_m^t. The element $\lambda_m = \zeta_m - 1$ is a unit in the ring of integers $\mathcal{O}_m$ of K_m except when $m = \ell^e$ is a power of a prime number ℓ, in which case λ_m generates the unique prime ideal of $\mathcal{O}_m$ lying over ℓ.

The real subfield K_m^+ of K_m is the fixed field of the conjugation $\tau = \sigma_{-1}$. Since the archimedean place of $\mathbf{Q}$ splits in $K_m^+/\mathbf{Q}$, there will be a non-trivial Stark "unit" associated to each archimedean place of K_m^+. These Stark units are defined by the values at $s = 0$ of the derivatives of the incomplete Artin L-functions attached to the abelian extension $K_m^+/\mathbf{Q}$. One such Stark unit is

$$\varepsilon_m = \lambda_m^{1+\tau} = (\zeta_m - 1)(\zeta_m^{-1} - 1) \tag{1}$$

and the others are its conjugates under the action of $G_m^+ = \mathrm{Gal}(K_m^+/\mathbf{Q})$. The reader will observe that ε_m is a true unit only when m is not a prime power. The best reference for these results is Stark's beautiful paper [S].

If $r \mid m$, we write $N_{m\to r}$ for the norm map from K_m to K_r and $N_{m\to r}^+$ for the norm map from K_m^+ to K_r^+. Consider now the lattice $\mathcal{L}_1(\mathbf{Q})$ of extension fields of $\mathbf{Q}$ defined by $\mathcal{L}_1(\mathbf{Q}) = \{K_m\}_{m \in \mathcal{S}}$, where $\mathcal{S} = \{m \in \mathbf{Z} : m \geq 3,\ m \text{ odd and square-free}\}$. We wish to choose roots of unity ζ_m for $m \in \mathcal{S}$ so that the system of elements $\{\lambda_m = \zeta_m - 1\}$ satisfies the following properties (cf. [R3]): For $m = r\ell \in \mathcal{S}$, ℓ an odd prime,

ES1 $N_{m \to r}(\lambda_m) = \lambda_r^{\sigma_\ell - 1}$.

ES2 $\lambda_m \equiv \lambda_r$ modulo every prime ideal of $\mathcal{O}_m$ dividing ℓ.

Suppose we choose primitive roots of unity ζ_ℓ for every odd prime ℓ in a random manner and then define

$$\zeta_m = \prod_{\ell | m} \zeta_\ell. \tag{2}$$

This choice leads to elements λ_m which satisfy **ES1** and **ES2**, as the reader may verify.

We can understand the construction (2) in a way which emphasizes the elements λ_m themselves. For $x, y \in \mathbf{Q}^{\mathrm{ac}}$, define $x * y = x + y + xy$. The binary operation $*$ restricts to a group law on $\mathbf{Q}^{\mathrm{ac}} - \{-1\}$, which is just the multiplicative group of $\mathbf{Q}^{\mathrm{ac}}$ translated so that its identity element becomes zero instead of one. Now λ_m is an m-division point for this translated group; and if $m = \ell_1 \ell_2 \ldots \ell_n \in \mathcal{S}$, then

$$\lambda_m = \lambda_{\ell_1} * \lambda_{\ell_2} * \cdots * \lambda_{\ell_n}. \tag{3}$$

If for $\ell = \ell_n$ we replace λ_ℓ by zero in this equation, we obtain **ES2** since λ_ℓ is divisible by every prime ideal of $\mathcal{O}_m$ dividing ℓ.

Because of (1), it is natural to try to understand the Euler system $\{\lambda_m\}$ from the point of view of Stark's conjectures. For this purpose, it is convenient to work with the full lattice $\mathcal{L}(\mathbf{Q}) = \{K_m\}$ of cyclotomic extensions of $\mathbf{Q}$ rather than the sub-lattice $\mathcal{L}_1(\mathbf{Q})$. Let

$$\mathbf{e} : \mathbf{Q}^{\mathrm{ab}} \longrightarrow \mathbf{C}$$

be an embedding of the abelian closure $\mathbf{Q}^{\mathrm{ab}} = \cup K_m$ of $\mathbf{Q}$ into the complex numbers $\mathbf{C}$. Let '∞' denote any one of the consistent family of archimedean places induced by $\mathbf{e}$ on the fields K_m^+. The Stark unit ε_m associated to the archimedean place ∞ on K_m^+ may be defined as follows:

$$\varepsilon_m = \lambda_m^{1+\tau} \quad \text{with} \quad \lambda_m = \zeta_m - 1 \quad \text{where} \quad \mathbf{e}(\zeta_m) = e^{2\pi i/m}. \tag{4}$$

The reader should note that each λ_m defined in (4) is the pull-back through $\mathbf{e}$ of a special value of the complex analytic function $e^z - 1$. The system of elements λ_m satisfies the following variants of **ES1** and **ES2**: For $m = rt$, with $t = \ell^e$ a prime power such that $\ell \nmid r$,

ES3 $N_{m\to r}(\lambda_m) = \lambda_r^{1-\sigma_\ell^{-1}}$.

ES4 $\lambda_m \equiv \lambda_r^{\sigma_t^{-1}}$ modulo every prime ideal of $\mathcal{O}_m$ dividing ℓ.

To prove **ES4**, we write $ct + dr = 1$ for suitable integers c and d and note that

$$e^{2\pi i/m} - 1 = e^{2\pi ic/r} \cdot e^{2\pi id/t} - 1 \Longrightarrow \lambda_m = \zeta_r^{\sigma_c} \zeta_t^{\sigma_d} - 1.$$

Since $\sigma_c = \sigma_t^{-1}$ on K_r and since $\zeta_t \equiv 1$ modulo any prime ideal of $\mathcal{O}_m$ dividing ℓ, **ES4** is established.

One can easily demonstrate **ES3** by similar direct calculations. Instead, we will show that **ES3** follows from **ES4** and the functorial properties of the Stark conjectures. Because the archimedean place ∞ splits completely in K_m^+/K_r^+, we have ([T], Proposition 3.5)

$$N_{m\to r}^+(\varepsilon_m) = \pm\varepsilon_r^{1-\sigma_\ell^{-1}}. \tag{5}$$

That is to say, the norm of the Stark unit ε_m at ∞ in K_m is a Stark unit at ∞ in K_r. Since λ_m is constructed out of the derivatives at $s = 0$ of L-functions deprived of their Euler factors at the primes dividing m, $N_{m\to r}^+(\varepsilon_m)$ will be a Stark unit constructed out of the derivatives at $s = 0$ of L-functions with the same missing factors. The exponent $1 - \sigma_\ell^{-1}$ in (5) adjusts for the fact that the Euler factor at ℓ is present in ε_r but missing in ε_m. Now, it follows easily from (1) that $\lambda_m^2 = -\zeta_m^{-1}\varepsilon_m$; and this together with (5) shows that

$$N_{m\to r}(\lambda_m) \in \mu(K_r) \cdot \lambda_r^{1-\sigma_\ell^{-1}}. \tag{6}$$

Let $\mathcal{L}_m$ be a prime ideal of $\mathcal{O}_m$ dividing ℓ, and let $\mathcal{L}_r$ be the prime ideal of $\mathcal{O}_r$ which lies under $\mathcal{L}_m$. Since $\mathcal{L}_r$ is totally ramified in K_m/K_r, **ES4** and (6) imply that

$$N_{m\to r}(\lambda_m) \equiv \lambda_m^{\varphi(t)} \equiv \lambda_r^{\varphi(t)\sigma_t^{-1}} \equiv \mu \cdot \lambda_r^{1-\sigma_\ell^{-1}} \pmod{\mathcal{L}_m}$$

for some $\mu \in \mu(K_r)$, where $\varphi(t) = [K_m : K_r]$. Applying σ_t to the last two terms of this congruence, we see that

$$\lambda_r^{\varphi(t)} \equiv \mu^{\sigma_t} \cdot \lambda_r^{\sigma_t - \sigma_{t/\ell}} \equiv \mu^{\sigma_t} \cdot \lambda_r^{\varphi(t)} \pmod{\mathcal{L}_r^{\sigma_t}}$$

since $\sigma_\ell \in G_r$ is the Frobenius automorphism at ℓ. As $\mathcal{L}_r$ is unramified in $K_r/\mathbf{Q}$, this last congruence shows that $\mu = 1$.

2 A cyclotomic Euler system in function fields

We begin by defining 'cyclotomic function fields' and describing some of their properties. More details and proofs may be found in [G] or [H3].

Let k be a global function field with exact constant field $\mathbf{F}_q$. Fix any place ∞ of k, and let $\mathbf{A}_\infty$ be the ring of functions in k which are holomorphic away from ∞. We view ∞ as an analog for the archimedean place of $\mathbf{Q}$ and $\mathbf{A}_\infty$ as an analog for $\mathbf{Z}$. Let k_∞ be the completion of k at ∞. Then $\mu(k_\infty) \cong \mathbf{F}_{q^\delta}^\times$, where $\delta = \deg(\infty)$. A *sign-function* on k_∞ is a group morphism $\mathrm{sgn} : k_\infty^\times \to \mu(k_\infty)$ such that $u \equiv \mathrm{sgn}(u) \pmod{\infty}$ for every unit u of the valuation ring in k_∞. It is convenient also to put $\mathrm{sgn}(0) = 0$. One can show that there are $q^\delta - 1$ distinct sign-functions on k_∞. We fix one of them and take the triple $(k, \infty, \mathrm{sgn})$ as our base object. Of course, we view k_∞ with it's sign-function as an analog for the real numbers. An element $x \in k_\infty$ is called *positive* (or *monic*) if $\mathrm{sgn}(x) = 1$.

The *Hilbert Class Field of* $\mathbf{A}_\infty$ is the maximal unramified, abelian extension field H of k in which ∞ splits completely. The prime ideals of $\mathbf{A}_\infty$ which split completely in H/k are precisely the principal prime ideals, and the Artin map induces an isomorphism $\mathrm{Pic}(\mathbf{A}_\infty) \to \mathrm{Gal}(H/k)$. By class field theory, there is a finite abelian extension H^*/k in which the prime ideals that split completely are precisely those which can be generated by a positive element of $\mathbf{A}_\infty$. This field contains H and is called the *narrow Hilbert Class field* or the *normalizing field* relative to the choice of sign-function sgn. Let $\phi : \mathbf{A}_\infty \to \mathrm{End}(\mathbf{G}_{a/k^{\mathrm{ac}}})$ be a rank one sgn-normalized Drinfield $\mathbf{A}_\infty$-module defined over the algebraic closure k^{ac} of k (see [H3], §4). Then H^* is the minimal field of definition for ϕ. Let $\mathbf{A}_\infty$ act on k^{ac} through ϕ. For a given non-zero ideal $m \subseteq \mathbf{A}_\infty$, the submodule Λ_m of m-torsion points for this action is a cyclic $\mathbf{A}_\infty$-module isomorphic to $\mathbf{A}_\infty/m$. Throughout this section, 'm' will always denote a non-zero, proper ideal in $\mathbf{A}_\infty$, and 'λ_m' will denote some generator of Λ_m. The extension field $K_m = H^*(\Lambda_m) = H^*(\lambda_m)$ is abelian over H^* with $\mathrm{Gal}(K_m/H^*) \cong (\mathbf{A}_\infty/m)^\times$. The field K_m is actually abelian over the base field k and is independent of the choice of ϕ.

Let $\mathcal{I}(m)$ be the group of fractional ideals of $\mathbf{A}_\infty$ which are prime to m. If $a \in \mathcal{I}(m)$, then the Artin automorphism $\sigma_a \in G_m = \mathrm{Gal}(K_m/k)$ is well defined and

$$\lambda^{\sigma_a} = \phi_a(\lambda) \tag{7}$$

for every $\lambda \in \Lambda_m$. For $x \in \mathbf{A}_\infty$ prime to m, we put $\sigma_x = \sigma_{x\mathbf{A}_\infty}$. As in [H3], §4, we find that $\mathrm{Gal}(K_m/H^*)$ is the group of elements σ_x such that x

$$\begin{tikzcd}
 & K_m \arrow[dd, no head, "(\mathbf{A}_\infty/m)^\times"] \\
K_m^+ \arrow[ur, no head, "G_\infty"] \arrow[dd, no head] & \\
 & H^* \\
H \arrow[ur, no head] \arrow[d, no head] & \\
k &
\end{tikzcd}$$

Figure 1: The cyclotomic function field *et al.*

is positive and prime to m. Further

$$x \equiv 1 \pmod{m} \Longrightarrow \lambda^{\sigma_x} = s_\phi(x)^{-1} \cdot \lambda \tag{8}$$

for every $\lambda \in \Lambda_m$, where $s_\phi = \mathrm{sgn} \circ \gamma_\phi$ is a *twisting* of the sign-function sgn by an $\mathbf{F}_q$-automorphism γ_ϕ of $\mathbf{F}_{q^\delta}$ which depends upon the choice of ϕ. By class field theory,

$$G_\infty = \{\sigma_x : x \equiv 1 \pmod{m}\} \subseteq G_m$$

is the decomposition group and the inertia group at the place ∞ of k. Let K_m^+ be the fixed field of G_∞. Then ∞ splits completely in K_m^+/k, and every place of K_m^+ which lies over ∞ is totally ramified in K_m/K_m^+. Any one of these places over ∞ is called an *infinite* place of K_m or K_m^+. By [H3], the element

$$\varepsilon_m = \prod_{\tau \in G_\infty} \lambda_m^\tau = -\lambda_m^{q^\delta - 1} \tag{9}$$

is a Stark "unit" at one of the infinite places of K_m^+. If $\mathcal{O}_m$ is the integral closure of $\mathbf{A}_\infty$ in K_m, then ([H3], Lemma 4.19) $\lambda_m \in \mathcal{O}_m^\times$ except when $m = \ell^e$ is a power of a prime ideal ℓ. When $m = \ell^e$, $\lambda_m \mathcal{O}_m = [\ell]_m$, where $[\ell]_m$ is the simple product of the $\mathcal{O}_m$-prime ideals lying over ℓ. The second equality in (9) is a consequence of (8).

If r is an ideal dividing m, we write $N_{m \to r}$ for the norm map from K_m to K_r. Consider now the lattice $\mathcal{L}_1(k)$ of extension fields of k defined by $\mathcal{L}_1(k) = \{K_m\}_{m \in \mathcal{S}}$, where $\mathcal{S} = \{m : m \text{ is square-free}\}$. We wish to choose a system of torsion points $\{\lambda_m\}_{m \in \mathcal{S}}$ which satisfy **ES1** and **ES2** of §1. Once again, we may choose a generator $\lambda_\ell \in \Lambda_\ell$ for every non-zero prime ideal of

$\mathbf{A}_\infty$ in a random manner. Since our torsion points are now *additive* rather than *multiplicative*, the analog of (3) is

$$\lambda_m = \lambda_{\ell_1} + \lambda_{\ell_2} + \cdots + \lambda_{\ell_n}$$

for every $m = \ell_1 \ell_2 \ldots \ell_n \in \mathcal{S}$. If for $\ell = \ell_n$ we replace λ_ℓ by zero in this equation, we obtain **ES2** since $[\ell]_m$ is divisible by every prime ideal of $\mathcal{O}_m$ dividing ℓ. In order to prove **ES1**, we use the fact that the conjugates of λ_ℓ over K_r are precisely the non-zero elements of Λ_ℓ and therefore precisely the roots of the polynomial $\phi_\ell(X)/X \in H^*[X]$. Therefore

$$N_{m \to r}(\lambda_m) = \prod_{\lambda \in \Lambda_\ell - \{0\}} (\lambda_r + \lambda) = \frac{\phi_\ell(\lambda_r)}{\lambda_r} = \lambda_r^{\sigma_\ell - 1}$$

by (7).

As in §1, we can adapt the Euler system $\{\lambda_m\}$ so that it reflects the point of view of Stark. We work with the complete lattice $\mathcal{L}(k) = \{K_m\}$ of 'cyclotomic' extension fields over $(k, \infty, \mathrm{sgn})$, and we select elements λ_m which define Stark units ε_m via (9) at a compatible system of infinite places on the fields $\{K_m^+\}$. Such a selection forces the Drinfeld module ϕ to vary with m. Our aim is to choose λ_m which satisfy **ES3** and **ES4**. Put $L = \cup K_m$, and let

$$\mathbf{e} : L \to \mathbf{C}_p$$

be an embedding of L into the completion $\mathbf{C}_p$ of the algebraic closure of k_∞. Let '∞' also denote any one of the consistent family of infinite places induced by $\mathbf{e}$ on the subfields K_m^+ of L.

The Stark unit ε_m at ∞ in K_m^+ can be constructed by analytic processes in $\mathbf{C}_p$ via the embedding $\mathbf{e}$. A *1-lattice* is any rank one $\mathbf{A}_\infty$-submodule Γ of $\mathbf{C}_p$. The analytic function $e_\Gamma(z)$ defined for $z \in \mathbf{C}_p$ by the infinite product

$$e_\Gamma(z) = z \prod_{\gamma \in \Gamma - \{0\}} \left(1 - \frac{z}{\gamma}\right) \tag{10}$$

is called the *exponential function* associated to Γ. By multiplying out the infinite product in (10), one can show that $e_\Gamma(z)$ is defined by an everywhere convergent power series on $\mathbf{C}_p$. Any 1-lattice Γ is the *root lattice* of a rank one Drinfeld module ϕ^Γ over $\mathbf{C}_p$ defined by the complex multiplications

$$\phi_x^\Gamma(e_\Gamma(z)) = e_\Gamma(xz) \tag{11}$$

for $x \in \mathbf{A}_\infty$. The *invariant* of Γ is an element $\xi(\Gamma) \in \mathbf{C}_p$ having the property that $\xi(\Gamma) \cdot \Gamma$ is the root lattice of a sgn-normalized Drinfeld module. Let us write $[m] = \xi(m) \cdot m$. Then $\phi^{[m]}$ is sgn-normalized, and the Stark unit at ∞ in K_m^+ may be constructed as follows:

$$\varepsilon_m = \prod_{\tau \in G_\infty} \lambda_m^\tau \quad \text{where} \quad \mathbf{e}(\lambda_m) = e_{[m]}(\xi(m)) = \xi(m) \cdot e_m(1). \tag{12}$$

It is clear from (11) that this λ_m is an m-torsion point for $\phi^{[m]}$. Comparing (12) with (4), we see that $\xi(m)$ is an analog of $2\pi i$. As noted in [H3], Theorem 4.17, the element ε_m defined by (12) is the unique Stark unit at ∞ in K_m^+ which is *totally positive.* This means that ε_m is positive in any embedding of K_m^+ into k_∞.

Now, although the Stark unit ε_m at ∞ is uniquely defined by the analytic construction (12), the invariant $\xi(m)$ and the torsion point λ_m are determined only up to a multiplier in $\mu(k_\infty)$. In §3 below, we will show how one may normalize the invariants $\xi(m)$ so that the following essential properties are valid for any factorization $m = rt$:

$$\phi_r^{[m]}(\lambda_m) = \lambda_t \qquad \text{and} \qquad r * \phi^{[m]} = \phi^{[t]} \tag{13}$$

with λ_m and λ_t determined by (12). By [H1], Proposition 5.10 and [H3], Theorem 5.1, each left hand side above equals some constant multiple of the corresponding right hand side. Let us assume for the moment that equations (13) hold for an appropriate choice of the invariants $\xi(m)$. Assume that $m = rt$ with $t = \ell^e$ a prime power such that $\ell \nmid r$ and choose $x \in t$ and $y \in r$ so that $x + y = 1$. Since m contains positive elements of arbitrarily high degree, we may assume that x is positive. Write $x\mathbf{A}_\infty = ct$ and $y\mathbf{A}_\infty = dr$ for integral ideals c and d of $\mathbf{A}_\infty$; and put $s_{[m]} = s_{\phi^{[m]}}$ to ease the notation. We have then via (13) for any prime ideal $\mathcal{L}_m$ of $\mathcal{O}_m$ dividing ℓ

$$\begin{aligned}
\lambda_m &= \phi_{x+y}^{[m]}(\lambda_m) = \phi_x^{[m]}(\lambda_m) + \phi_y^{[m]}(\lambda_m) \\
&= s_{[m]}(x) \cdot (t * \phi^{[m]})_c(\phi_t^{[m]}(\lambda_m)) + s_{[m]}(y) \cdot (r * \phi^{[m]})_d(\phi_r^{[m]}(\lambda_m)) \\
&= \phi_c^{[r]}(\lambda_r) + s_{[m]}(y) \cdot \phi_d^{[t]}(\lambda_t) \\
&\equiv \lambda_r^{\sigma_c} \pmod{\mathcal{L}_m}
\end{aligned}$$

by (7) and since λ_t is divisible by every prime ideal of $\mathcal{O}_m$ lying over ℓ. For this calculation, we have used the fact that

$$\phi_z^{[m]} = s_{[m]}(z) \cdot \phi_{z\mathbf{A}_\infty}^{[m]} = s_{[m]}(z) \cdot (b * \phi^{[m]})_a \cdot \phi_b^{[m]}$$

for $z \in \mathbf{A}_\infty$ and any factorization $z\mathbf{A}_\infty = ab$ by integral ideals a and b. Since x is positive and $x \equiv 1 \pmod{r}$, (8) implies that

$$\lambda_m \equiv \lambda_r^{\sigma_c} = \lambda_r^{\sigma_x \cdot \sigma_t^{-1}} = \lambda_r^{\sigma_t^{-1}} \pmod{\mathcal{L}_m}.$$

Thus, **ES4** holds for the system $\{\lambda_m\}$. Because of (9), we may deduce **ES3** from **ES4** and the functorial properties of the Stark units as in §1 above.

3 A normalization of the invariants $\xi(m)$

In this section, we will show how to normalize the system of invariants $\xi(m)$ so as to produce root lattices $\xi(m) \cdot m$ for which the equations (13) are always valid. Our aim is to prove the following

Theorem 2 *Suppose the invariant $\xi(\mathbf{A}_\infty)$ is specified in any arbitrary manner. Then there is a unique choice of invariants $\xi(m)$ associated to the non-zero, proper ideals in $\mathbf{A}_\infty$ which implies the validity of (13) for any factorization $m = rt$.*

For any choice of $\xi(m)$, let $[m] = \xi(m) \cdot m$ and let $\phi^{[m]}$ be the sgn-normalized Drinfeld module with root lattice $[m]$. The proof of Theorem 2 is based on the following analytic identity: for $z \in \mathbf{C}_p$

$$\phi_r^{[m]}\left(\xi(m) \cdot e_m(z)\right) = D(\phi_r^{[m]})\xi(m) \cdot e_t(z). \tag{14}$$

This identity is a consequence of equation (5.11) and Proposition 5.10 of [H1].

Let $\mathcal{I}_0$ be the set of non-zero integral ideals a of $\mathbf{A}_\infty$ such that $\deg a \equiv 0 \pmod{\delta}$. We begin by specifying $\xi(m)$ for $m \in \mathcal{I}_0$. The set of Drinfeld modules $\phi^{s[m]} = s^{-1}\phi^{[m]}s$ for $s \in \mu(k_\infty)$ is precisely the set of sgn-normalized modules which are isomorphic to $\phi^{[m]}$. From the definitions, we have

$$D(\phi_a^{s[m]}) = s^{1-q^{\deg a}} \cdot D(\phi_a^{[m]}) \tag{15}$$

for every ideal $a \subseteq \mathbf{A}_\infty$. Therefore if $a \in \mathcal{I}_0$, then $D(\phi_a^{[m]})$ is independent of the choice of $\xi(m)$.

Definition 1 *For $a \in \mathcal{I}_0$ and any fractional ideal b of $\mathbf{A}_\infty$, let*

$$< a \mid b >= D(\phi_a^{[ab]})$$

where $\phi^{[ab]}$ is any sgn*-normalized Drinfeld module with root lattice $[ab] = \xi(ab) \cdot ab$. By (15), this definition is independent of the choice of $\xi(ab)$.*

Let 'B' denote the integral closure of $\mathbf{A}_\infty$ in the Hilbert Class Field H. As in §1 of [H2], we may verify that the symbol $< a \mid b >$ enjoys the following properties:

P1 $< a \mid b > \in B$ and generates the ideal aB.

P2 For all $x \in k^\times$, $< a \mid xb > = < a \mid b >$.

P3 $c \in \mathcal{I}_0 \Longrightarrow < ac \mid b > = < a \mid b > \cdot < c \mid ab >$.

P4 $< a \mid b >^{\sigma_c} = < a \mid bc^{-1} >$.

P5 $x \in a^{-1} \Longrightarrow < xa \mid b > = \bar{x} < a \mid b >$ where $\bar{x} = x/\mathrm{sgn}(x)$.

If we fix one of the $q^\delta - 1$ values of the invariant $\xi(\mathbf{A}_\infty)$, we can specify $\xi(m)$ for any ideal $m \in \mathcal{I}_0$ by requiring that

$$\frac{\xi(\mathbf{A}_\infty)}{\xi(m)} = < m \mid \mathbf{A}_\infty > . \tag{16}$$

Since $m * \phi^{[\mathbf{A}]}$ is sgn-normalized, there exists a determination of $\xi(m)$ for which (16) holds by Proposition 5.10 of [H1]. Now for $m = rt$ with $r, t \in \mathcal{I}_0$, (16) and **P3** imply that

$$\frac{\xi(t)}{\xi(m)} = \frac{\xi(\mathbf{A}_\infty)/\xi(m)}{\xi(\mathbf{A}_\infty)/\xi(t)} = \frac{< m \mid \mathbf{A}_\infty >}{< t \mid \mathbf{A}_\infty >} = < r \mid t >$$

so that

$$\xi(t) = D(\phi_r^{[m]}) \cdot \xi(m). \tag{17}$$

Lemma 1 *If $m = rt$ with $r, t \in \mathcal{I}_0$, then (13) holds when the invariants of r, t and m are determined by (16).*

Proof. We obtain the first equation in (13) from (17) by setting $z = 1$ in (14). The second equation then follows from (17) and Proposition 5.10 of [H1]. ∎

We now specify $\xi(m)$ for arbitrary m by the equation

$$\xi(m) \cdot e_m(1) = \phi_a^{[am]}(\xi(am) \cdot e_{am}(1)) \tag{18}$$

where a is any ideal such that $am \in \mathcal{I}_0$. Viewing K_m as a subfield of $\mathbf{C}_p$ via the embedding $\mathbf{e}$, we note by (12) that (18) can be written as

$$\lambda_m = \phi_a^{[am]}(\lambda_{am}).$$

We must verify that this specification of $\xi(m)$ is independent of the choice of am. Let $bm \in \mathcal{I}_0$. Then

$$\phi_{abm}^{[ambm]}(\lambda_{ambm}) = \left(am * \phi^{[ambm]}\right)_b \phi_{am}^{[ambm]}(\lambda_{ambm}) = \phi_b^{[bm]}(\lambda_{bm})$$

by Lemma 1 since $am, bm \in \mathcal{I}_0$. Interchanging a and b in this equation, we obtain our result.

Lemma 2 *Suppose $m \in \mathcal{I}_0$. Then (13) holds for any factorization $m = rt$ when the invariants of r and t are determined by (18).*

Proof. Write (18) with t replacing m and r replacing a. Comparing this form of (18) and (14) with $z = 1$, we deduce (17) for factorizations $m = rt$ restricted only by the condition $m \in \mathcal{I}_0$. Now we argue just as we did in the proof of Lemma 1 above. ∎

We must now verify (13) for any factorization $m = rt$ without any restrictions on m. Choose a so that $am \in \mathcal{I}_0$. Then we have

$$\begin{aligned} \phi_r^{[m]}(\lambda_m) &= \phi_r^{[m]}\left(\phi_a^{[am]}(\lambda_{am})\right) = \left(a * \phi^{[am]}\right)_r \left(\phi_a^{[am]}(\lambda_{am})\right) \\ &= \phi_{ar}^{[am]}(\lambda_{am}) = \lambda_t \end{aligned}$$

by Lemma 2 as $am \in \mathcal{I}_0$. Comparing this equation with (14), we deduce (17) now with no restriction on the factorization $m = rt$. Equations (13) follow by the argument in the proof of Lemma 1.

4 The Gauss sum Euler system over Q

Given a global function field k, we showed in §§2 and 3 how to construct an Euler system out of Stark units associated to a compatible system of places lying over *any* fixed place ∞ of k. Motivated by the function field case, we ask if Stark units associated to a compatible system of places lying over any fixed rational prime p define an analogous Euler system with base field $\mathbf{Q}$. In this §, we show that the answer to this question is 'yes' for $p \neq 2$. Stickelberger's Theorem implies that Stark units over p exist in every abelian extension field of $\mathbf{Q}$.

In order to clarify the relationship between §§2 and 3 and the p-adic theory developed in this §, we introduce a canonical sign-function sgn_p on the p-adic completion $\mathbf{Q}_p$. For $z \in \mathbf{Q}_p^\times$, we define

$$\mathrm{sgn}_p(z) = \omega_p\left(z/p^{\mathrm{v}_p(z)}\right)$$

$$\begin{tikzcd}
 & K_m = K_m^+(\zeta_p) \\
K_m^+ \arrow[ur, dash, "G_p"] \arrow[dd, dash, "(\mathbf{Z}/m\mathbf{Z})^\times/<p>"'] & \\
 & H^* = H(\zeta_p) \arrow[uu, dash] \\
H = \mathbf{Q}(\zeta_{p-1}) \arrow[ur, dash] \arrow[d, dash] & \\
\mathbf{Q} &
\end{tikzcd}$$

Figure 2: p splits in $K_m^+/\mathbf{Q}$

where $\omega_p : \mathbf{Z}_p^\times \to \mu(\mathbf{Q}_p)$ is the Teichmüller character. We say that an element $z \in \mathbf{Q}_p^\times$ is *p-positive* if $\mathrm{sgn}_p(z) = 1$. Let $\theta_p : \mathbf{Q}_p^\times \to \mathrm{Gal}(\mathbf{Q}_p^{\mathrm{ab}}/\mathbf{Q}_p)$ be the map of local class field theory, where $\mathbf{Q}_p^{\mathrm{ab}}$ is the abelian closure of $\mathbf{Q}_p$. By local class field theory, we have

$$z \text{ is } p\text{-positive} \Leftrightarrow \theta_p(z) \text{ restricts to the identity map on } \mathbf{Q}_p(\zeta_p) \tag{19}$$

for every $z \in \mathbf{Q}_p^\times$.

Let $\mathcal{S} = \{m \in \mathbf{Z} : m \geq 1,\, m \text{ prime to } p(p-1)\}$. Throughout this §, '$m$' always denotes an integer belonging to $\mathcal{S}$. Our first task is to specify a lattice of abelian extension fields of $\mathbf{Q}$ in which p splits completely. The largest cyclotomic field in which p splits is $H = \mathbf{Q}(\zeta_{p-1})$. Let D_m be the decomposition group of p in the cyclotomic extension $H(\zeta_m)/\mathbf{Q}$, and let K_m^+ be the fixed field of D_m. Then $K_m^+ \supseteq H$ is the largest subfield of $H(\zeta_m)$ in which p splits completely. We put $H^* = H(\zeta_p)$ and $K_m = K_m^+(\zeta_p)$. We have then

$$\mathrm{Gal}(K_m/H^*) \cong \mathrm{Gal}(K_m^+/H) \cong (\mathbf{Z}/m\mathbf{Z})^\times/ < p >$$

where $< p >$ is the subgroup of $(\mathbf{Z}/m\mathbf{Z})^\times$ generated by p. The group

$$G_p = \mathrm{Gal}\,(K_m/K_m^+) \cong \mathbf{F}_p^\times$$

is the decomposition group and the inertia group at p for the extension $K_m/\mathbf{Q}$. Since H is the largest cyclotomic field contained in K_m^+, $\mu(K_m^+)$ is the group of $(p-1)$-st roots of unity.

Definition 2 *We say that an element $x \in K_m^+$ is* totally p-positive *if x is p-positive in every embedding of K_m^+ into $\mathbf{Q}_p$.*

Proposition 1 *Let $N_m^- : K_m \to K_m^+$ be the norm map. The subgroup $N_m^-(K_m^\times)$ of the multiplicative group of K_m^+ consists of totally p-positive elements.*

Proof. Since p is totally ramified in the extension K_m/K_m^+, N_m^- is the restriction to K_m of the local norm map from $\mathbf{Q}_p(\zeta_p)$ to $\mathbf{Q}_p$. By (19), the elements of $N_m^-(K_m^\times)$ are p-positive in any embedding of K_m^+ into $\mathbf{Q}_p$. ∎

The fields K_m^+ are the class fields associated to the "ray class groups" of the ring $\mathbf{A}_p = \mathbf{Z}[1/p]$ with respect to the moduli $(p-1)m$. Since $\mathbf{A}_p^\times = \{\pm 1\} \times p^{\mathbf{Z}}$ is infinite, distinct moduli may very well define the same class group and therefore the same class field. This happens, e.g., for the moduli $\{(p-1)\ell^n : n \geq 1\}$ whenever p is a primitive root modulo the square of a prime number ℓ. In this case, all the fields $K_{\ell^n}^+$ coincide. We might restrict the elements of $\mathcal{S}$ to "conductors" of the ring $\mathbf{A}_p$, but it is actually more convenient to simple accept the fact that some of the fields in our lattices are multiply defined. We adopt this strategy in what follows.

Put $T_m = \mathrm{Supp}((p-1)m)$. Our Euler system over p will be defined on the lattice of ordered pairs $\mathcal{L}_p(\mathbf{Q}) = \{(K_m, T_m)\}_{m \in \mathcal{S}}$. Put $L = \cup K_m$, and let

$$\mathbf{e} : L \to \mathbf{Q}_p^{\mathrm{ab}}$$

be an embedding of L into $\mathbf{Q}_p^{\mathrm{ab}}$. This embedding defines a unique place $\mathcal{P}_m$ over p in each of the fields K_m. Let $\mathcal{P}_m^+$ be the place of K_m^+ which lies under $\mathcal{P}_m$. The Stark "unit" at $\mathcal{P}_m^+$ (it is actually a p-unit) is the norm of a normalized Gauss sum λ_m lying in K_m. In writing down the Gauss sum which defines λ_m, we will follow Weil ([W], §14).

Once and for all, we fix a primitive p-th root of unity $\zeta_p \in \mathbf{Q}_p^{\mathrm{ab}}$. Let S_m be the trace map from $\mathbf{Q}_p(\zeta_m)$ down to $\mathbf{Q}_p$. Define an additive character $\psi_m : \mathbf{Z}_p[\zeta_m] \to \mathbf{Q}_p(\zeta_p)^\times$ by setting

$$\psi_m(z) = \zeta_p^{i(m) \cdot S_m(z)}$$

for every $z \in \mathbf{Z}_p[\zeta_m]$, where $i(m)$ is an inverse of m modulo p. Now, the number of roots of unity in $\mathbf{Q}_p(\zeta_m)$ is $p^{f(m)} - 1$, where $f(m) = \mathrm{Card}(D_m)$ is the order of p modulo m. For $0 \leq a < p^{f(m)} - 1$, define

$$g_m(a) = -\sum_{\mu} \mu^a \cdot \psi_m(\mu)$$

where μ runs over the roots of unity in $\mathbf{Q}_p(\zeta_m)$. Since

$$S_m(\mu) = \mu + \mu^p + \ldots + \mu^{p^{f(m)-1}}$$

on the roots of unity μ, a standard calculation shows that

$$g_m(a)^{\theta_p(x)} = \Big[\mathrm{sgn}_p(x)\Big]^a \cdot g_m(a) \tag{20}$$

for every $x \in \mathbf{Q}_p^\times$. We learn from this last equation that $g_m(a) \in \mathbf{e}(K_m)$.

Put $p^* = (-1/p)p$, where $(-1/p)$ is the Legendre symbol. Once and for all, we fix a determination of $\sqrt{p^*} \in \mathbf{Q}_p(\zeta_p)$. Let

$$a_m = \frac{p^{f(m)} - 1}{(p-1)m}$$

and let (p^*/m) be the Jacobi symbol. The Stark unit ε_m associated to the place $\mathcal{P}_m^+$ on K_m^+ may be defined as follows:

$$\varepsilon_m = \prod_{\tau \in G_p} \lambda_m^\tau = (-1)^{a_m} \lambda_m^{p-1} \text{ where } \mathbf{e}(\lambda_m) = g_m(a_m) \cdot \left(\frac{(p^*/m)}{\sqrt{p^*}}\right)^{f(m)} \tag{21}$$

the second equality in (21) being a consequence of (20). The Stark unit ε_m is independent of our choices of ζ_p and $\sqrt{p^*}$ because modifying these choices has the effect of multiplying λ_m by a $(p-1)$-st root of unity. Since ε_m is a norm from K_m, Proposition 1 implies

Proposition 2 *The element ε_m defined by (21) is the unique Stark unit at $\mathcal{P}_m^+$ which is totally p-positive.*

It may happen that $\lambda_m \neq \lambda_{m'}$ even thought $K_m = K_{m'}$. However ε_m is determined by the pair (K_m^+, T_m) and Proposition 2, as is proved in [T], Chapitre IV, §6 with $T = T_m$. Therefore if $(K_m, T_m) = (K_{m'}, T_{m'})$, then $\lambda_m = –\lambda_{m'}$ where – is some $(p-1)$-st root of unity. We will show in §5 below that – always equals one. We have therefore associated a well-define normalized Gauss sum to every point in the lattice $\mathcal{L}_p(\mathbf{Q})$.

Let $m = rt$, with $t = \ell^e > 1$ a prime power such that $\ell \not| \, r$. We write $\mathcal{O}_m$ for the ring of integers in K_m, and we write $N_{m \to r}$ for the norm map from K_m to K_r. We will now show that the system of normalized Gauss sums $\{\lambda_m\}$ satisfies **ES3** and the following variant of **ES4**:

ES5 $\lambda_m \equiv \lambda_r^{h\sigma_t^{-1}}$ modulo every prime ideal of $\mathcal{O}_m$ dividing ℓ, where $h = f(m)/f(r)$ is the order of $p^{f(r)}$ modulo t.

We note that since $[K_m : H^*] = \varphi(m)/f(m)$, the integer h is also defined by the equation

$$[K_m : K_r] = \frac{\varphi(t)}{h} \quad . \tag{22}$$

Suppose that **ES5** is valid for $m = rt$, and let $\mathcal{L}_m$ be a prime ideal of $\mathcal{O}_m$ dividing ℓ. Since $\mathcal{L}_m$ is totally ramified over K_r,

$$N_{m\to r}(\lambda_m) \equiv \lambda_m^{\varphi(t)/h} \equiv \lambda_r^{\varphi(t)\sigma_t^{-1}} \pmod{\mathcal{L}_m}$$

by (22) and **ES5**. As in §1, **ES3** follows from this congruence by the functorial properties of the Stark conjectures.

Property **ES5** for the system $\{\lambda_m\}$ is a consequence of the well-known theorem of Davenport-Hasse ([L], Chapter 1, §5). We observe first that

$$a_m = \frac{p^{f(m)}-1}{p^{f(r)}-1} \cdot \frac{p^{f(r)}-1}{(p-1)rt} = \frac{N}{t} \cdot a_r \tag{23}$$

where

$$N = 1 + p^{f(r)} + p^{2f(r)} + \ldots + p^{(h-1)f(r)}$$

is an integer having the property that, for any root of unity $\mu \in \mathbf{Q}_p(\zeta_m)$, μ^N is the norm of μ from $\mathbf{Q}_p(\zeta_m)$ down to $\mathbf{Q}_p(\zeta_r)$. Choose integers c and d such that $ct + d(p-1)r = 1$. Then

$$a_m = cta_m + d(p-1)ra_m = cNa_r + d \cdot \frac{p^{f(m)}-1}{t}$$

by (23). Because $\mu^{(p^{f(m)}-1)/t}$ is a t-th root of unity, $\mu^{a_m} \equiv \mu^{cNa_r} \pmod{\mathcal{L}_m}$; and this implies that

$$\begin{aligned} g_m(a_m) &\equiv -\sum_{\mu} \mu^{N\cdot ca_r} \cdot \psi_m(\mu) \pmod{\mathcal{L}_m} \\ &= \left(-\sum_{\mu} \mu^{ca_r} \cdot \psi_r(c\mu)\right)^h \\ &= g_r(a_r)^{h\sigma_c} \end{aligned} \tag{24}$$

by the Davenport-Hasse Theorem, where the second summation above is over the roots of unity $\mu \in \mathbf{Q}_p(\zeta_r)$. Since $\sqrt{p^*} \in H^*$, we have

$$\left(\frac{(p^*/m)}{\sqrt{p^*}}\right)^{f(m)} = \left(\frac{(p^*/r)}{\sqrt{p^*}}\right)^{f(r)\cdot h\sigma_c}$$

which together with (24) and (21) implies that $\lambda_m \equiv \lambda_r^{h\sigma_c} \pmod{\mathcal{L}_m}$. Property **ES5** follows because $\sigma_c = \sigma_t^{-1}$ on K_r.

5 An identity theorem for Gauss sums

In this final §, we show that

$$(K_m, T_m) = (K_{m'}, T_{m'}) \Longrightarrow \lambda_m = \lambda_{m'}, \tag{25}$$

which is equivalent to Theorem 1 of the introduction. The key element in the proof is property **ES5** of §4. Throughout this §, m and m' are elements of $\mathcal{S}$ satisfying the hypothesis of (25), and $d = \mathrm{GCD(m, m')}$.

Lemma 3 *We have* $(K_m, T_m) = (K_d, T_d)$.

Proof. First, we observe that $H(\zeta_m) \cap H(\zeta_{m'}) = H(\zeta_d)$. This follows because $[H(\zeta_m) : H(\zeta_d)] = \varphi(m)/\varphi(d) = m/d$ and $[H(\zeta_{m'}) : H(\zeta_d)] = m'/d$ are relatively prime. Therefore

$$H(\zeta_d) \supseteq K_m^+ = K_{m'}^+ \Longrightarrow K_d^+ = K_m^+ \Longrightarrow K_d = K_m$$

as K_d^+ is the largest subfield of $H(\zeta_d)$ in which p splits completely. ∎

By this lemma, we see that it suffices to prove (25) when $m' = d$. Now clearly, $(K_n, T_n) = (K_m, T_m)$ whenever $d \mid n$ and $n \mid m$. Thus, the proof of (25) reduces to the special case $m' = n$ and $m = n\ell$, where $\ell \in \mathcal{S}$ is prime. From the remarks after Proposition 2 above, we know that $\lambda_{n\ell} = -\lambda_n$ for some $(p-1)$-st root of unity $-$. Put $n = rt$, where $t = \ell^e$ with $\ell \not| \, r$ and $e \geq 1$. Then with $h = f(n)/f(r)$ and $h' = f(n\ell)/f(r)$, we have

$$\frac{h'}{h} = \frac{\varphi(n\ell)}{\varphi(n)} = \frac{\varphi(\ell^{e+1})}{\varphi(\ell^e)} = \ell$$

by (22) as $K_{n\ell} = K_n$. Let $\mathcal{L}_n$ be a prime ideal of $\mathcal{O}_{n\ell} = \mathcal{O}_n$ lying over ℓ. Invoking **ES5**, we see that

$$-\lambda_n = \lambda_{n\ell} \equiv \lambda_r^{\ell h \cdot \sigma_{t\ell}^{-1}} \equiv \lambda_r^{h \cdot \sigma_t^{-1}} \equiv \lambda_n \pmod{\mathcal{L}_n}$$

since σ_ℓ is the Frobenius automorphism at ℓ for the extension $K_r/\mathbf{Q}$. Therefore $- = 1$ as ℓ is unramified in $H/\mathbf{Q}$. This completes the proof of (25).

References

[G] E.-U. Gekeler, *Drinfeld Modular Curves*, Lecture Notes in Mathematics No. 1231. Springer-Verlag, Berlin, 1986.

[Gr] B. Gross, Kolyvagin's work on modular elliptic curves, *Durham Conference Proceedings* (1989).

[H1] D. R. Hayes, Explicit class field theory in global function fields, *Studies in algebra and number theory, Advances in Mathematics Supplementary Studies*, 6 (1979) 173-217.

[H2] D. R. Hayes, Elliptic units in function fields, in *Proceedings of a Conference on Modern Developments Related to Fermat's Last Theorem*, D. Goldfeld ed., Birkhäuser, Boston (1982).

[H3] D. R. Hayes, Stickelberger elements in function fields, *Compositio Mathematica*, 55 (1985) 209-239.

[K] V. A. Kolyvagin, Euler Systems, (1988). To appear in a Birkhäuser volume in honor of Grothendieck.

[L] S. Lang, *Cyclotomic Fields I*, Springer-Verlag, New York (1978).

[R1] K. Rubin, The work of Kolyvagin on the arithmetic of elliptic curves. To appear in *Arithmetic of Complex Manifolds, Erlangen, 1988.* Springer Lecture Notes in Mathematics.

[R2] K. Rubin, The work of Kolyvagin on ideal class groups, to appear.

[R3] K. Rubin, The Main Conjecture, to appear as an appendix to the new edition of S. Lang, *Cyclotomic Fields.*

[S] H. Stark, L-functions at $s = 1$. IV. First derivatives at $s = 0$, *Advances in Mathematics* 35 (1980) 197-235.

[T] J. Tate, *Les conjectures de Stark sur les fonctions L d'Artin en $s = 0$*, Birkhäuser, Boston (1984).

[W] A. Weil, La cyclotomie jadis et naguère, *Enseign. Math.* XX (1974) 247-263.