Integrality Properties of a Special Value of the Partial Zeta Functions of Certain Abelian Field Extensions

Barry Smith

November 9, 2005

Advisor: Cristian D. Popescu

Basic Terminology I

A *number field* is a finite extension field of $\mathbb{Q}$

The following objects are associated to any number field K:

$\mathcal{O}_K$ – the ring of integers of K
Every ideal of $\mathcal{O}_K$ factors uniquely as a product of prime ideals.
For any prime ideal $\mathfrak{p} \in \mathcal{O}_K$, $\mathcal{O}_K/\mathfrak{p}$ is a finite field.

μ_K – the group of roots of unity contained inside of K

U_K – the group of units inside of the ring $\mathcal{O}_K$
U_K/μ_K is a finitely generated abelian group.

Basic Terminology II

I_K – the *ideal group* of K, composed of the fractional ideals of K
P_K – the subgroup of principal ideals of I_K
$C_K = I_K/P_K$ – the ideal class group of K

The ideal class group is always finite, so we let $h_K = |C_K|$

Infinite Places – The "primes at infinity" correspond to the embeddings $K \hookrightarrow \mathbb{R}$ and the pairs of conjugate embeddings $K \hookrightarrow \mathbb{C}$

For an ideal $\mathfrak{a} \in \mathcal{O}_K$, the *norm* of $\mathfrak{a}$ is given by $N\mathfrak{a} = [\mathcal{O}_K : \mathfrak{a}]$

Field Extensions

If K/k is an abelian Galois extension of number fields and $\mathfrak{p} \in I_k$, then $\mathfrak{p}\mathcal{O}_K \in I_K$ factors as

$$\mathfrak{p}\mathcal{O}_K = \left(\prod_{i=1}^{g} \mathfrak{P}_i \right)^e .$$

$\mathfrak{p}$ *splits completely* in K/k if $g = [K : k]$
$\mathfrak{p}$ *ramifies* in K/k if $e > 1$.
K/k is unramified if no places (finite or inifinite!) ramify in K/k.
The *decomposition group* of $\mathfrak{P}_i$ is the subgroup

$$\mathsf{D}(\mathfrak{P}_i/\mathfrak{p}) = \{ \sigma \in \mathsf{Gal}(K/k) | \sigma\mathfrak{P}_i = \mathfrak{P}_i \}$$

The Artin Map

If $\mathfrak{p}$ and $\mathfrak{P}_i$ are as before, and if $e = 1$, then $\mathrm{D}(K/k) \cong \mathrm{Gal}((\mathcal{O}_K/\mathfrak{P}_i)/(\mathcal{O}_k/\mathfrak{p}))$.

Furthermore, if $\mathrm{Gal}(K/k)$ is abelian, there is an automorphism $(\mathfrak{p}, K/k) \in \mathrm{Gal}(K/k)$ depending only on $\mathfrak{p}$ that maps to the Frobenius automorphism under the above isomorphism.

Let S be a finite set of prime ideals of $\mathcal{O}_k$ containing the ramified primes.

The *Artin map* is the homomorphism $(\ \cdot\ , K/k) : I_{k,S} \to \mathrm{Gal}(K/k)$ given by $\mathfrak{p} \mapsto (\mathfrak{p}, K/k)$ for prime ideals not in S, and extended multiplicatively to all fractional ideals of k prime to the ideals in S.

Partial Zeta Functions

Let K/k be a finite abelian extension of number fields with Galois group G, and let S be a finite set of places $\mathcal{O}_k$ including all infinite places and primes that ramify in K/k.

For any $\tau \in G$, the associated *partial zeta function* is defined by

$$\zeta_S(\tau, s) = \sum (N\mathfrak{a})^{-s}$$

where the sum is over all integral ideals $\mathfrak{a} \in I_{k,S}$ with $(\mathfrak{a}, K/k) = \tau$.

These functions can be analytically continued to the entire complex plane with at most a simple pole at $s = 1$.

The L-function Evaluator

With K/k, G, and S as before, the *L-function evaluator* $\theta_{K/k,S} \in \mathbb{C}[G]$ is given by

$$\theta = \sum_{\sigma \in G} \zeta_{K/k}(\sigma, 0)\sigma^{-1}.$$

Let $W_K = |\mu(K)|$. Then

- **Theorem** (Siegel 1970, Shintani 1976)
  $\theta \in \mathbb{Q}[G]$

- **Theorem** (Deligne-Ribet, Cassou-Nogués, Barsky, 1979)
  $\xi\theta \in \mathbb{Z}[G]$ for all $\xi \in \mathrm{Ann}_{\mathbb{Z}[G]}(\mu(K))$

- In particular, $w_K\theta \in \mathbb{Z}[G]$

- If $|S| \geq 2$ and some prime of S splits completely in K, then $\theta = 0$

Example

Let $m \geq 2$ be such that $m \equiv 0, 1,$ or $3 \pmod 4$.
Let $\zeta = e^{\frac{2\pi i}{m}}$.
Set $k = \mathbb{Q}$, $K = \mathbb{Q}(\zeta)$, and let $S = \{\infty, p \mid m\}$.

Under the canonical isomorphism $G \cong (\mathbb{Z}/m\mathbb{Z})^*$, if $(a, m) = 1$, $(a, K/k) \mapsto \overline{a}$. Then

$$\zeta_S(\overline{a}, s) = \sum_{n \equiv a(m)} n^{-s}$$

is the *Hurwitz zeta function*.
It is known that

$$\zeta_S(\overline{a}, 0) = \frac{1}{2} - \frac{a}{m}$$

so that

$$\theta = \sum_{\substack{a=1 \\ (a,m)=1}}^{m} \left(\frac{1}{2} - \frac{a}{m}\right) \overline{a}^{-1}.$$

A Closer Look At θ

Write

$$\omega = W_K \theta_{K/k,S} = \sum_{\sigma \in G} a_\sigma \sigma^{-1},$$

where a_1 is the coefficient of $\mathbf{1}$.

For $\tau \in G$, choose $N\tau \in \mathbb{Z}$ so that $\zeta^\tau = \zeta^{N\tau}$ for all $\zeta \in \mu(K)$. $\mathrm{Ann}_{\mathbb{Z}[G]}(\mu(K))$ is generated as a $\mathbb{Z}$-module by $\{\tau - N\tau \mid \tau \in G\}$.

It follows from the theorem of Deligne and Ribet that there exists a $\gamma \in \mathbb{Z}[G]$ such that

$$\omega = a_1 \left(\sum_{\sigma \in G} N\sigma \cdot \sigma^{-1} \right) + w_K \gamma.$$

.

Definition: $e = e_{K/k,S} = \gcd(w_K, a_1)$.

e is the largest divisor of w_K for which $\frac{w_K}{e}\theta \in \mathbb{Z}[G]$.

Ankeny, Artin, and Chowla's formula

If $p \equiv 1 \pmod 4$ and $k = \mathbb{Q}(\sqrt{p})$, then U_k/μ_k is a cyclic group.
Let $\varepsilon = \frac{t+u\sqrt{p}}{2}$ be its unique generator > 1.

In 1952, Ankeny, Artin, and Chowla published the following congruences:

$$4h(k)\frac{u}{t} \equiv \sum_{\nu=1}^{p-1} \frac{1}{g\nu}\left(\frac{\nu}{p}\right)\left[\frac{g\nu}{p}\right] \pmod p$$

where g is any quadratic non-residue $\pmod p$ and also

$$h(k)\frac{u}{t} \equiv B_{\frac{p-1}{2}} \pmod p$$

The Corresponding Partial Zeta Function

For $k = \mathbb{Q}(\sqrt{p})$ and $K = \mathbb{Q}(\zeta_p)$, and S consisting of the places of k at infinity and the prime ideal above p, $\theta_{K/k,S}$ can be computed from $\theta_{K/Q,S'}$.

It can be shown that in this case,

$$a_1 \equiv \sum_{\substack{1 \leq \mu,\nu \leq p-1 \\ \mu\nu \equiv 1 \mod p}} \left(\frac{\nu}{p}\right) \left\lfloor \frac{\mu\nu}{p} \right\rfloor \pmod{p}$$

Using Ankeny, Artin, and Chowla's formula, it follows that

$$a_1 \equiv -8h(k)\frac{u}{t} \equiv -8B_{\frac{p-1}{2}} \pmod{p}$$

An Alternative to Voronoi's Congruence

This uses a reformulation of Voronoi's congruence, one version of which says that for $(\mu, p) = 1$ and $m > 1$:

$$(\mu^m - 1)\frac{B_m}{m} \equiv \mu^{m-1} \sum_{\nu=1}^{p-1} \nu^{m-1} \left\lfloor \frac{\mu\nu}{p} \right\rfloor$$

The equivalent reformulation is, for $(c, p) = 1$,

$$c\left(\frac{B_m}{m} + c^m \frac{B_{p-1-m}}{p-1-m}\right) \equiv \sum_{\substack{1 \le \mu,\nu < p \\ \mu\nu \equiv c \mod p}} \nu^m \left\lfloor \frac{\mu\nu}{p} \right\rfloor$$

A Similar Type of Extension

Let $d \in \mathbb{Z}$ be the discriminant of the real quadratic field $k = \mathbb{Q}(\sqrt{d})$, and assume d is square free, $3 \nmid d$ and $(\phi(d), d) = 1$.

Set $K = \mathbb{Q}(\zeta_d)$ and let S consist of the places of k at infinity and the rational primes dividing d.

Like the previous case, it can be shown that if $p|d$ and $d = mp$,

$$\sum_{\substack{1 \leq nu \leq d-1 \\ (\nu,d)=1}} \frac{1}{g\nu} \left(\frac{d}{v}\right) \left\lfloor \frac{g\nu}{d} \right\rfloor \equiv -4h(k)\frac{u}{t} \pmod{p}$$

when $\left(\frac{d}{g}\right) = -1$ and also that

$$a_1 \equiv -8h(k)\frac{u}{t} \equiv -8B_{\frac{p-1}{2},\chi_m}$$

Slavutskii's Congruences

Let $p \equiv 1 \pmod 4$, $l \geq 1$, $k = \mathbb{Q}(\sqrt{p})$, let ε be as before, and set $\varepsilon^{p^{l-1}} = t_l + u_l\sqrt{p}$. Also, let $r = \frac{p-1}{2}p^{l-1}$.

In 1961, Slavutskii published the following analogues of Ankeny, Artin, and Chowla's formulae:

$$h(k)\frac{u_l}{p^{l-1}} \equiv -\frac{t_l}{4}\sum_{\nu=1}^{p^l}\left(\frac{k}{p}\right)\frac{1}{gk}\left\lfloor\frac{gk}{p^l}\right\rfloor \pmod{p^l}$$

and

$$2h(k)\frac{u_l}{p^{l-1}} \equiv -t_l\frac{B_r}{r} \pmod{p^l}$$

These appear to be exactly what is needed to evaluate $a_1 \pmod{p^l}$ when $K = \mathbb{Q}(\zeta_{p^l})$ and $k = \mathbb{Q}(\sqrt{p})$.

The Cubic Base Field Case

If $p \equiv 1 \pmod 3$, let $K = \mathbb{Q}(\zeta_p)$ and let k be the subfield of K of degree 3 over $\mathbb{Q}$. Let S be as usual. Let χ be a primitive cubic character (mod p).

The formula for a_1 can be reduced (mod p^2) to the equation:

$$pa_1 \equiv -2 \sum_{\substack{\mu\nu\omega \equiv 1 \bmod p \\ 1 \le \mu,\nu,\omega < p}} \chi(\mu)\overline{\chi}(\nu) \left\lfloor \frac{\mu\nu\omega}{p} \right\rfloor$$

Using elementary methods again, this can be simplified to:

$$a_1 \equiv -6 \frac{B_{\frac{p-1}{3}}}{\frac{p-1}{3}} \frac{B_{\frac{2(p-1)}{3}}}{\frac{2(p-1)}{3}} \pmod p$$

Two Identities

The proof of the preceding identity uses the reformulation of Voronoi's congruence as well as the following two identities:

$$\sum_{\substack{1\le\mu,\nu<p\\ \mu\nu\equiv c \pmod p}} \mu^m\nu^n \equiv mc^n\frac{B_{m-n}}{m-n}p + nc^m\frac{B_{p-1-(m-n)}}{p-1-(m-n)}p \pmod{p^2}$$

under some minor hypotheses on m, n, and

$$\sum_{\mu=1}^{p-1}\sum_{\nu=1}^{p-1}\mu^{p\frac{p-1}{3}-1}\nu^{p\frac{2(p-1)}{3}-1}\left\lfloor\frac{\mu\nu}{p}\right\rfloor \equiv \left(\left(\frac{B_{\frac{p-1}{3}}}{\frac{p-1}{3}}\right)^2 - \frac{B_{\frac{p-1}{3}}}{\frac{p-1}{3}}\frac{B_{\frac{2(p-1)}{3}}}{\frac{2(p-1)}{3}} + \left(\frac{B_{\frac{2(p-1)}{3}}}{\frac{2(p-1)}{3}}\right)^2\right)p$$

Connection With Units I

If k is a cubic field as above, it can be shown that k contains a strong Minkowski unit δ, i.e. δ and its Galois conjugates generate U_k/μ_k.

It can be shown that δ is, in some sense, unique.

Let β_0, β_1, and β_2 be the Lagrange normal basis for $\mathcal{O}_k$, and write $\delta = x\beta_0 + y\beta_1 + z\beta_2$.

Ke-Qin Feng showed that

$$ch_k \equiv \frac{3}{4} B_{\frac{p-1}{3}} B_{\frac{2(p-1)}{3}} \pmod{p}$$

where c is a rational symmetric function in x, y, z.

Connection With Units II

Choosing δ with norm -1, let the minimal polynomial for δ be $x^3 + ax^2 + bx - 1$. Then it can be shown that Feng's result is equivalent to

$$4h(k)\frac{ab+9}{p} \equiv a_1 \pmod{p}$$

For every $p \equiv 1 \pmod 3$, $4p$ can be written uniquely (up to sign changes) in the form $4p = k^2 + 27c^2$.

For primes satisfying $4p = 1 + 27c^2$, the above result implies that $a_1 \equiv -4h(k) \pmod{p}$.

For primes satisfying $4p = k^2 + 27$, the above result implies that $a_1 \equiv -108h(k) \pmod{p}$.

Higher Degree Base Fields

Let l be an odd prime and p be a prime $\equiv 1 \pmod{l}$. Let $K = \mathbb{Q}(\zeta_p)$ and let k be the subfield of K of degree l over $\mathbb{Q}$. Let S be as usual.

Some empirical evidence supports the hypothesis that in this case,

$$a_1 \equiv -2l \prod_{r=1}^{l-1} \frac{B_{\frac{r(p-1)}{l}}}{\frac{r(p-1)}{l}} \pmod{p}$$

Furthermore, Jakubec has extended Feng's result to such fields k.

If p is an irregular prime dividing B_k, then it would appear that the integer $d_{p,k} = \frac{p-1}{(p-1,k)}$ is of some interest.

Search For Small $\mathbf{d_{p,k}}$

Using Buhler's table of irregular primes up to $16,000,000$, one can find the following table of pairs $(d_{p,k}, p)$ for which $d_{p,k} < 20$:

dp,k	p
3	5479, 15646243
5	130811
7	421, 44563
9	37, 13411
13	90247, 163307
14	633473
15	1446901
17	103, 3484729
19	43093, 3962603

Remarks

Only one odd value of $d_{p,k}$ is missing, and only one even value appears.

The Ankeny-Artin-Chowla conjecture can be reinterpreted as saying 2 will never appear in the $d_{p,k}$ column.

There is a heuristic argument that the density of irregular primes should be about $1 - e^{-\frac{1}{2}}$. Perhaps this heuristic can be strengthened into one giving the density of irregular primes and corresponding indices for which $d_{p,k} = c$, for some fixed $c \in \mathbb{Z} \geq 2$.

An Application

Hayes has defined a certain unramified Kummer extension F of K (sometimes $F = K$) and asked if the exponent of Gal(F/K) will always divide e.

If so, then it is possible to reformulate a stronger version of the Brumer-Stark conjecture – slight evidence has been found to support this stronger conjecture.

If proved, would imply the existence of a certain Hecke character on the idèle class group A_K^* which produces an L-function with "nice" properties.

All of the formulae and the conjecture previously mentioned can be shown to imply that Hayes' question has an affirmative answer in these cases. However, the Ankeny-Artin-Chowla conjecture would imply that this question is trivial for $\mathbb{Q}(\zeta_p)/\mathbb{Q}(\sqrt{p})$.

Further Evidence I

If K/k is quadratic and $G = \{1, \tau\}$, let Coker denote the cokernel of the map $C_{k,S} \to C_{K,S}$.

Tate showed that

$$\theta_{K/k,S} = \frac{2^{|S|-2}|\text{Coker}|}{W_K}(1-\tau).$$

When $p \equiv 1 \pmod 4$, $K = \mathbb{Q}(\zeta_p)$, $k = \mathbb{Q}(\zeta_p)^+$, and S is as usual,

$$|\text{Coker}| = \frac{h_K}{h_K^+} = h_K^-$$

In this case, p divides the exponent of the Galois group of an unramified abelian extension of $K \Rightarrow p|h_K \Rightarrow p|h_K^- \Rightarrow p|e$

Further Evidence II

For $p \equiv 1 \pmod 3$, $k = \mathbb{Q}(\sqrt{p})$, $K = k(\sqrt{-3})$, and S consisting of the places of k at infinity and the prime ideals of $\mathcal{O}_K$ which contain rational primes that ramify in $K/\mathbb{Q}$.

Set $\tilde{k} = \mathbb{Q}(\sqrt{-3p})$. Then I believe it can be shown that

$$a_1 = 2^{|S|-1}|\text{Coker}| = \begin{cases} 2h(\tilde{k}), \text{if } p \equiv 1 \pmod 4; \\ 4h(\tilde{k}), \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Then it follows from a classical theorem of Scholz about the 3-rank of $C_{\tilde{k}}$ that 3 divides the exponent of some cubic unramified abelian extension of $K \Rightarrow 3|h(\tilde{k}) \Rightarrow 3|a_1$, so Hayes' question as an affirmative answer in this case as well.

Using PARI, I calculated that there are 6 primes $p < 500$ for which 3 divides the exponent of the Galois group of this unramified abelian extension of K, providing nontrivial cases of Hayes' conjecture.

Future Work I

To finish proving my conjecture for the value of the numerator of $\zeta_S(\mathbf{1}, 0)$ for $K = \mathbb{Q}(\zeta_m)$ and k a subfield of prime degree over $\mathbb{Q}$.

To formulate corresponding results in the case where k has composite degree over $\mathbb{Q}$.

To find new proofs of these results using p-adic L-functions and/or Bernoulli distributions.

To convert Jakubec's extension of Feng's results into statements involving the coefficients of minimal polynomials of certain units of k.

Future Work II

To formulate and prove Hayes' conjecture for function fields.

Note 1: There are two kinds of L-functions here.

Note 2: Anglès proved function-field analogue of the formula of Ankeny-Artin-Chowla involving the *Bernoulli-Carlitz* numbers.

To proved a corresponding stronger version of the Brumer-Stark conjecture in this case, using Deligne's 1-motives.