The various faces of a pairing on $p$-units

Romyar Sharifi

Max Planck Institute of Mathematics
Bonn, Germany
Basic objects:

Let $K$ be a number field, a finite extension of $\mathbb{Q}$ in a fixed algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$.

Let $\mathcal{O}_K$ be the ring of integers of $K$, consisting of all roots in $K$ of monic polynomials with integral coefficients.

Let $\text{Cl}_K$ denote the class group of $K$, the quotient of the semigroup of nonzero ideals of $\mathcal{O}_K$ by the nonzero principal ideals.

Let $h_K$ be the class number of $K$, the order $|\text{Cl}_K|$ of $\text{Cl}_K$.

Example. The ring of integers of $\mathbb{Q}(\sqrt{-5})$ is $\mathbb{Z}[\sqrt{-5}]$. The class number $h_{\mathbb{Q}(\sqrt{-5})}$ is 2, and the image of $(2, 1 + \sqrt{-5})$ generates $\text{Cl}_{\mathbb{Q}(\sqrt{-5})}$. 
Irregular primes and Bernoulli numbers:

A prime number $p$ is called regular if $p \nmid h_{\mathbb{Q}(\mu_p)}$. Otherwise, $p$ is called irregular.

**Example.** 37, 59 and 67 are the smallest three irregular primes.

**Remark.** Kummer proved Fermat’s Last Theorem for regular odd primes in 1850.

Let $B_k$ denote the $k$th Bernoulli number, which is defined by the power series

$$
\frac{x}{e^x - 1} = \sum_{k=0}^{\infty} \frac{B_k}{k!} x^k.
$$

$p$ is regular if and only if $p$ does not divide the numerator of $B_k/k$ for any positive even $k$ (with $k \leq p - 3$).

**Example.** 37 | $B_{32}$, 59 | $B_{44}$, 67 | $B_{58}$, and 691 | $B_{12}$. 
Eigenspaces:

Henceforth, \( K = \mathbb{Q}(\mu_p) \) for an odd prime \( p \). Let \( \Delta = \text{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times \).

Consider the \( p \)-adic integers \( \mathbb{Z}_p = \lim \downarrow \mathbb{Z}/p^n\mathbb{Z} \).

We define the Teichmüller character

\[
\omega: \Delta \to \mu_{p-1}(\mathbb{Z}_p) \subset \mathbb{Z}_p^\times
\]

by \( \delta \zeta = \zeta^{\omega(\delta)} \) for \( \delta \in \Delta, \zeta \in \mu_p \).

Any \( \mathbb{Z}_p[\Delta]\)-module \( A \) breaks up into eigenspaces

\[
A = \bigoplus_{i=0}^{p-2} A^{(i)}
\]

where for \( i \in \mathbb{Z} \), an element \( \delta \in \Delta \) acts through multiplication by \( \omega(\delta)^i \) on \( A^{(i)} \).

Also, if \( \sigma \in \Delta \) has order 2, then we have a decomposition \( A = A^+ \oplus A^- \), where \( \sigma a = \pm a \) for \( a \in A^\pm \).
**L-functions:**

Recall the complex \( \zeta \)-function, which is an analytic function on \( \mathbb{C} - \{1\} \) with

\[
\zeta(s) = \sum_{n=1}^{\infty} n^{-s} = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}}
\]

for \( \text{Re } s > 1 \).

For \( k \) even, we have \( p \)-adic \( L \)-functions \( L_p(s, \omega^k) \) defined on \( s \in \mathbb{Z}_p \) (Kubota-Leopoldt).

The \( p \)-adic \( L \)-functions interpolate special values of \( \zeta(s) \) as follows:

\[
L_p(1 - k, \omega^k) = \zeta(1 - k) = -\frac{B_k}{k}
\]

when \( k \geq 2 \) and \( k \not\equiv 0 \text{ mod } p - 1 \).
Orders of class groups:

Let $A_K$ denote the $p$-part of $\text{Cl}_K$.

**Theorem (Mazur-Wiles).** For $k \not\equiv 0 \mod p-1$ even,

$$|A_{K}^{(1-k)}| = |\mathbb{Z}_p / L_p(0, \omega^k)|.$$

The above theorem is a weak form of the Main Conjecture of Iwasawa theory. It relates an arithmetic object with a ($p$-adic) analytic object.

This, plus $A_{K}^{(1)} = 0$, describes the size of $A_{K}^{-}$.
Vandiver’s conjecture:

As for $A^+_K$, we have the following conjecture.

**Conjecture (Vandiver).** $A^+_K = 0$.

Vandiver’s conjecture is known to hold for $p < 12,000,000$ (Buhler, et. al.)

If Vandiver’s conjecture holds, then $A^{(1-k)}_K$ is cyclic for any even $k$.

**Note.** For simplicity of presentation, we will assume Vandiver’s conjecture at $p$ for the remainder of the talk.

All statements can be modified, when necessary, so as to remove this assumption.
A cup product pairing:

\[ R_K = \mathbb{Z}[\mu_p, \frac{1}{p}] \] is the ring of \( p \)-integers of \( K \).
\[ \mathcal{E}_K = R_K^\times \] is the group of \( p \)-units of \( K \).

McCallum and I defined a pairing

\[ (,)_K : \mathcal{E}_K \times \mathcal{E}_K \to A_K \otimes \mu_p. \]

which arises from the cup product in étale (or Galois) cohomology

\[ H^1(\text{Spec } R_K, \mu_p)^\otimes 2 \cup H^2(\text{Spec } R_K, \mu_p^\otimes 2). \]

Conjecture (McCallum-S). \((,)_K\) is surjective.

Theorem (S). \((,)_K\) is surjective for \( p < 1000 \).
**Special values:**

Fix a primitive $p$th root of unity $\zeta$. The image of $\zeta$ generates $(E_K/E_K^p)^-$. For odd $i$, we have special $p$-units

$$\eta_i = \prod_{u=1}^{p-1} (1 - \zeta^u)^{u^{-1}}.$$

The image of $\eta_i$ generates $(E_K/E_K^p)^{(1-i)}$. For $i$ odd and $k$ even, we have

$$(\eta_i, \eta_{k-i})_K \in A^{(1-k)}_K \otimes \mu_p \hookrightarrow \mathbb{Z}/p\mathbb{Z},$$

and these values determine $(\ , \ )_K$.

McCallum and I explicitly computed these values for fixed $k$ up to a possibly zero scalar for each $k$ and $p < 10,000$. 
Table of pairings:

\[ p = 37, \, k = 32 \]
\[ (1 \, 26 \, 0 \, 36 \, 1 \, 35 \, 31 \, 34 \, 3 \, 6 \, 2 \, 36 \, 1 \, 0 \, 11 \, 36 \, 11 \, 26) \]

\[ p = 59, \, k = 44 \]
\[ (1 \, 45 \, 21 \, 30 \, 14 \, 35 \, 5 \, 0 \, 48 \, 57 \, 7 \, 52 \, 2 \, 11 \, 0 \, 54 \, 24 \, 45 \, 29 \]
\[ 38 \, 14 \, 58 \, 27 \, 32 \, 15 \, 0 \, 44 \, 27 \, 32) \]

\[ p = 67, \, k = 58 \]
\[ (1 \, 45 \, 38 \, 56 \, 0 \, 47 \, 62 \, 9 \, 29 \, 15 \, 65 \, 26 \, 45 \, 57 \, 0 \, 10 \, 22 \, 41 \, 2 \]
\[ 52 \, 38 \, 58 \, 5 \, 20 \, 0 \, 11 \, 29 \, 22 \, 66 \, 2 \, 24 \, 43 \, 65) \]

\[ p = 101, \, k = 68 \]
\[ (1 \, 56 \, 40 \, 96 \, 26 \, 63 \, 0 \, 61 \, 81 \, 71 \, 35 \, 92 \, 73 \, 64 \, 6 \, 88 \, 0 \, 0 \, 13 \]
\[ 95 \, 37 \, 28 \, 9 \, 66 \, 30 \, 20 \, 40 \, 0 \, 38 \, 75 \, 5 \, 61 \, 45 \, 100 \, 17 \, 17 \, 12 \]
\[ 66 \, 72 \, 53 \, 86 \, 31 \, 70 \, 15 \, 48 \, 29 \, 35 \, 89 \, 84 \, 84) \]

\[ p = 103, \, k = 24 \]
\[ (1 \, 70 \, 17 \, 22 \, 77 \, 25 \, 78 \, 26 \, 81 \, 86 \, 33 \, 102 \, 18 \, 4 \, 26 \, 92 \, 77 \]
\[ 54 \, 88 \, 90 \, 23 \, 26 \, 57 \, 0 \, 11 \, 86 \, 70 \, 85 \, 85 \, 97 \, 57 \, 0 \, 46 \, 6 \, 18 \]
\[ 18 \, 33 \, 17 \, 92 \, 0 \, 46 \, 77 \, 80 \, 13 \, 15 \, 49 \, 26 \, 11 \, 77 \, 99 \, 85) \]

\[ p = 131, \, k = 22 \]
\[ (1 \, 35 \, 74 \, 129 \, 81 \, 0 \, 50 \, 2 \, 57 \, 96 \, 130 \, 0 \, 38 \, 8 \, 81 \, 67 \, 83 \, 64 \]
\[ 3 \, 127 \, 107 \, 0 \, 34 \, 69 \, 23 \, 105 \, 34 \, 64 \, 100 \, 105 \, 70 \, 73 \, 37 \, 13 \]
\[ 118 \, 114 \, 124 \, 36 \, 95 \, 7 \, 17 \, 13 \, 118 \, 94 \, 58 \, 61 \, 26 \, 31 \, 67 \, 97 \]
\[ 26 \, 108 \, 62 \, 97 \, 0 \, 24 \, 4 \, 128 \, 67 \, 48 \, 64 \, 50 \, 123 \, 93 \, 0) \]
**Milnor $K$-groups:**

Define

$$K_2^M(R_K) = \frac{\mathcal{E}_K \otimes \mathcal{E}_K}{\langle x \otimes (1-x) \mid x, 1-x \in \mathcal{E}_K \rangle}.$$

We have a canonical homomorphism

$$K_2^M(R_K) \to K_2(R_K),$$

where $K_2(R_K)$ is the usual algebraic $K_2$-group.

**Remark.** If $R_K$ is replaced by any field and $\mathcal{E}_K$ by its multiplicative group, the above map is an isomorphism (Matsumoto).

Surjectivity of $(\langle \quad \rangle)_K$ can be reinterpreted as the following equivalent statement.

**Conjecture (McCallum-S).** The map

$$K_2^M(R_K) \otimes \mathbb{Z}_p \to K_2(R_K) \otimes \mathbb{Z}_p$$

is surjective.
Class groups of Kummer extensions:

Class groups of large, nonabelian number fields are notoriously hard to compute. The pairing affords us a means of doing this.

For \( i \geq 1 \) odd, let \( L_i = K(\eta_i^{1/p}) \).

Let \( A_{L_i} \) denote the \( p \)-part of \( \text{Cl}_{L_i} \).
Let \( B_{L_i} \) denote the quotient of \( A_{L_i} \) by the classes of the primes of \( L_i \) that lie above \( p \).

**Theorem (McCallum-S).** *The norm map on ideal classes \( B_{L_i} \to A_K \) is an isomorphism if and only if \( (\eta_i, \cdot)_K \) is surjective.*

As a result, we can determine exactly when \( A_{L_i} \) and \( B_{L_i} \) are isomorphic to \( A_K \) for \( p < 1000 \).
**$K$-groups of $\mathbb{Z}$:**

For each $i \geq 2$ and $j = 1, 2$, we have surjective cycle class maps (Soulé, Dwyer-Friedlander)

$$c_{i,j} : K_{2i-j}(\mathbb{Z}) \otimes \mathbb{Z}_p \to H^j(\text{Spec } \mathbb{Z}[1/p], \mathbb{Z}_p(i)).$$

Quillen and Lichtenbaum conjectured the following. It is a consequence of a conjecture of Bloch-Kato, a proof of which has recently been announced.

**Theorem (Voevodsky-Rost).** Each $c_{i,j}$ is an isomorphism.

This allows us to prove the following.

**Theorem (S).** For $i$ odd and $k$ even with $i, k - i > 1$, the product map

$$K_{2i-1}(\mathbb{Z}) \otimes K_{2(k-i)-1}(\mathbb{Z}) \to K_{2k-2}(\mathbb{Z}) \otimes \mathbb{Z}_p$$

is surjective if and only if $(\eta_i, \eta_{k-i})_K \neq 0$.

This yields which products on odd $K$-groups of $\mathbb{Z}$ are surjective onto $p$-parts for $p < 1000$. 

13
The fundamental group of $\mathbb{P}^1 - \{0, 1, \infty\}$:

\[ \pi_1 = \pi_1(\mathbb{P}^1(\mathbb{C}) - \{0, 1, \infty\}) \]
is a free group on two generators.

Let $\pi_1^{\text{pro-}p}$ be the pro-$p$ completion of $\pi_1$. There is a canonical “representation”

\[ \rho_p : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \text{Out}(\pi_1^{\text{pro-}p}). \]

through which Ihara defined a filtration on $G_{\mathbb{Q}}$, the graded pieces of which form a graded $\mathbb{Z}_p$-Lie algebra $\mathfrak{g}_p$.

For each odd $i \geq 3$, one can choose special nontrivial elements $\sigma_i \in \text{gr}^i \mathfrak{g}_p$ (Soulé-Ihara).

**Conjecture (Deligne).** The graded Lie algebra $\mathfrak{g}_p \otimes \mathbb{Z}_p \mathbb{Q}_p$ is freely generated by the $\sigma_i$.

**Theorem (Del.-Beilinson, Hain-Matsumoto).**

$\mathfrak{g}_p \otimes \mathbb{Z}_p \mathbb{Q}_p$ is generated by the $\sigma_i$. 

14
Properties of $g_p$:

As for $g_p$ itself, we have the following.

**Theorem (S).** Assume Deligne's conjecture.
1. If $p$ is regular, $g_p$ is generated by the $\sigma_i$.
2. If $p$ is irregular and $(\ , \ )_K$ is surjective, $g_p$ is not generated by the $\sigma_i$.

Ihara studied a “mysterious relation” in a certain Lie algebra of derivations containing $g_{691}$, which led him to conjecture the following.

**Theorem (S).** There is a relation in $\text{gr}^{12} g_{691}$ of the form

$$[\sigma_3, \sigma_9] - 50[\sigma_5, \sigma_7] = 691h$$

with $h \notin [g_{691}, g_{691}]$.

The coefficients 1 and $-50$ are, modulo 691 and up to a particular isomorphism

$$A_K^{(1-12)} \otimes \mu_{691} \cong \mathbb{Z}/691\mathbb{Z},$$

the values $(\eta_3, \eta_9)_K$ and $(\eta_5, \eta_7)_K$. 

15
Hecke algebras:

Let $T$ denote the ordinary cuspidal Hecke algebra of weight 2, level $p$, and character $\omega^{k-2}$.

$T$ is generated by Hecke operators $T_l$ with $l \neq p$ prime and $U_p$, and $T$ contains an ideal $I$ called the Eisenstein ideal which contains $U_p - 1$.

**Theorem (S).** $(p, \eta_{k-1})_K \neq 0$ if and only if $U_p - 1$ generates the group $I/I^2$.

This theorem and a computation imply the surjectivity of $(\cdot, \cdot)_K$ for $p < 1000$.

**Remark.** $U_p - 1$ relates directly to the value at 1 of the $p$-adic $L$-function of a cusp form congruent to an Eisenstein series modulo $p$. 

Modular Forms:

Let $k$ be a positive even integer. Let $G_k$ denote the normalized Eisenstein series of weight $k$ and level 1:

$$G_k = -\frac{B_k}{2k} + \sum_{n=1}^{\infty} \sigma_{k-1}(n)q^n,$$

where $\sigma_{k-1}(n) = \sum_{1 \leq d | n} d^{k-1}$, $q = e^{2\pi i z}$.

Assume that $p$ divides the numerator of $B_k/k$.

There exists a weight $k$ cusp form

$$f = \sum_{n=1}^{\infty} a_n q^n$$

for $SL_2(\mathbb{Z})$ which is a Hecke eigenform and satisfies a certain mod $p$ congruence with $G_k$. 
Sketch of a conjectural relationship:

There is a \( p \)-adic \( L \)-function \( L_p(f, s) \) interpolating special values of the classical \( L \)-function

\[
L(f, s) = \sum_{n=1}^{\infty} a_n n^{-s},
\]

up to certain transcendental periods (Manin, Mazur-Tate-Teitelbaum).

Normalizing, we may reduce the \( L_p(f, i) \) for odd \( i \) with \( 1 \leq i \leq k - 1 \) modulo the maximal ideal \( m \) of the ring of integers of \( \mathbb{Q}_p \).

The reductions \( \overline{L_p(f, i)} \) of the \( L_p(f, i) \) modulo \( m \) are \( \mathbb{F}_p \)-proportional.

**Conjecture (S).** The values \( \overline{L_p(f, i)} \) and the values \( (\eta_i, \eta_{k-i})_K \) for odd \( i \) with \( 1 \leq i \leq k - 1 \) define the same element of \( \mathbb{P}^{k/2-1}(\mathbb{F}_p) \).