Eisenstein congruences in arithmetic and geometry

Romyar Sharifi

University of Arizona

October 22, 2015

Definition

The *Riemann zeta function* is the unique meromorphic function on $\mathbb{C}$ satisfying

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$$

for $\mathrm{Re}(s) > 1$.

Remarks

1. $\zeta(s)$ is holomorphic outside $s = 1$, where it has a simple pole of residue 1,
2. $\zeta(s)$ has a *functional equation*: setting

   $$\Lambda(s) = \pi^{-\frac{s}{2}}\Gamma(\tfrac{s}{2})\zeta(s)$$

   we have $\Lambda(s) = \Lambda(1-s)$ for $s \neq 0, 1$. Here $\Gamma(s)$ is meromorphic on $\mathbb{C}$ with

   $$\Gamma(s) = \int_0^{\infty} x^{s-1}e^{-x}dx$$

   for $\mathrm{Re}(s) > 0$. It has simple poles at non-positive integers, and $\Gamma(n) = (n-1)!$ for $n \geq 1$.

Definition

For $n \geq 0$, the nth *Bernoulli number* $B_n \in \mathbb{Q}$ is given by $\dfrac{x}{e^x - 1} = \sum_{n=0}^{\infty} \dfrac{B_n}{n!} x^n$.

1. $B_1 = -\frac{1}{2}$, but $B_n = 0$ for odd $n \geq 3$, since $\dfrac{x}{e^x - 1} - \dfrac{-x}{e^{-x} - 1} = -x$.
2. $B_0 = 1$, $B_2 = \dfrac{1}{6}$, $B_4 = -\dfrac{1}{30}$, $B_6 = \dfrac{1}{42}$, $B_8 = -\dfrac{1}{30}$, $B_{10} = \dfrac{5}{66}$.
3. $B_{12} = -\dfrac{691}{2730}$. Note: 691 is prime, and $2730 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13$.

1. $\zeta(k) = (-1)^{\frac{k}{2}+1} \dfrac{(2\pi)^k B_k}{2 \cdot k!}$ for even $k \geq 0$, and $\zeta(3)$ is irrational (Apéry).
2. $\zeta(1-n) = -\dfrac{B_n}{n}$ for $n \geq 2$. In particular, $\zeta(-k) = 0$ for even $k \geq 2$.

Conjecture

The numbers $\zeta(n)$ for odd $n \geq 3$, and π, are $\mathbb{Q}$-algebraically independent.

From now on, we use k to denote a positive even integer.

Remark (Kummer congruences)

1. We have $(p-1) \mid k$ if and only if the denominator of $\frac{B_k}{k}$ is divisible by p.
2. If $(p-1) \nmid k$, then $\frac{B_k}{k} \equiv \frac{B_{k+p-1}}{k+p-1} \bmod p$.

Definition

A prime p is *regular* if $p \nmid B_2 B_4 \cdots B_{p-3}$, and it is *irregular* otherwise.

Remark

There are infinitely many irregular primes (Jensen, 1915).

Example

The smallest irregular primes are 37, 59, and 67, dividing B_{32}, B_{44}, and B_{58}, respectively. Note that 691 is irregular, as $691 \mid B_{12}$.

Cyclotomic fields

1. The *class group* of a number field F is a finite abelian group that measures the failure of ideals of the ring of integers $\mathcal{O}$ of F to be principal.

   (The class group consists of equivalence classes of nonzero ideals of $\mathcal{O}$ up to by multiplication by principal ideals.)

2. The *class number* of F is the order of the class group of F.

Definition

For $n \geq 1$, the nth *cyclotomic field* $\mathbb{Q}(\mu_n)$ is the smallest subfield of $\mathbb{C}$ containing the group of nth roots of unity μ_n.

Theorem (Dirichlet, Kummer 1847)

A prime p divides the class number of $\mathbb{Q}(\mu_p)$ if and only if p is irregular.

Conjecture (Kummer 1849, known as Vandiver's conjecture)

The class number of $\mathbb{Q}(\mu_p) \cap \mathbb{R}$ is not divisible by p.

Theorem (Buhler-Harvey 2011)

Vandiver's conjecture holds for $p < 163577356$.

The K-groups $K_n(\mathbb{Z})$ for $n \geq 0$ are abelian groups that tell us in some sense about "higher arithmetic" of $\mathbb{Z}$. We have $K_0(\mathbb{Z}) \cong \mathbb{Z}$ and $K_1(\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$.

Theorem (Borel 1974)

For $n \geq 2$, the groups $K_n(\mathbb{Z})$ are finite unless $n \equiv 1 \bmod 4$, in which case they are isomorphic to $\mathbb{Z}$ or $\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

The following is a consequence of the Quillen-Lichtenbaum conjecture, known by the work of many: Soulé, Dwyer-Friedlander, Rognes-Weibel, Rost, Voevodsky....

Theorem

For even $k \geq 2$, we have that $K_{2k-1}(\mathbb{Z})$ is a cyclic group, and

$$\frac{|K_{2k-2}(\mathbb{Z})|}{|K_{2k-1}(\mathbb{Z})|} = \left|\frac{B_k}{2k}\right| = \left|\frac{\zeta(1-k)}{2}\right|.$$

Aside from a single power of 2 if $4 \nmid k$, the leftmost fraction is reduced.

Vandiver's conjecture implies that $K_{2k}(\mathbb{Z}) = 0$ and $K_{2k-2}(\mathbb{Z})$ is cyclic for even k. It is known that $K_4(\mathbb{Z}) = 0$ (Rognes).

Let $\mathbb{H}$ denote the complex upper half-plane.

Definition

For even $k \geq 4$, the kth normalized *Eisenstein series* G_k is the holomorphic function on $\mathbb{H}$ given by

$$G_k(z) = \frac{(k-1)!}{2 \cdot (2\pi i)^k} \sum_{\substack{(a,b)\in\mathbb{Z}^2 \\ (a,b)\neq(0,0)}} \frac{1}{(a+bz)^k}.$$

It extends to a holomorphic function at ∞, with value $-\frac{1}{2}\zeta(1-k)$.

G_k is a *weight k modular form* for $\mathrm{SL}_2(\mathbb{Z})$. That is, if $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, then

$$G_k\left(\frac{az+b}{cz+d}\right) = (cz+d)^k G_k(z).$$

For $q = e^{2\pi i z}$ with $z \in \mathbb{H}$, we have

$$G_k(q) = -\frac{\zeta(1-k)}{2} + \sum_{n=1}^{\infty} \Big(\sum_{d|n} d^{k-1}\Big) q^n.$$

Definition

1. The mth *Hecke operator* T_m on the space M_k of modular forms of weight k for $\mathrm{SL}_2(\mathbb{Z})$ takes $f = \sum_{n=0}^{\infty} a_n q^n \in M_k$ to
$$T_m f = \sum_{n=0}^{\infty} \left(\sum_{d \mid \gcd(m,n)} d^{k-1} a_{mn/d^2} \right) q^n.$$
2. The Hecke algebra $\mathfrak{H}_k$ of M_k is the $\mathbb{Z}$-subalgebra of $\mathrm{End}_{\mathbb{C}}(M_k)$ generated by the operators T_m for $m \geq 1$.

Definition

$f \in M_k$ is a (normalized) *eigenform* if $T_m f = a_m f$ for all $m \geq 1$.

Example

The Eisenstein series G_k are all eigenforms.

Remark

The space M_k has a $\mathbb{C}$-basis of eigenforms.

Definition

1. A modular form in M_k is a *cusp form* if it vanishes at ∞ (i.e., $a_0 = 0$).
2. The $\mathfrak{H}_k$-submodule of weight k cusp forms in M_k is denoted S_k.

Remark

We have $M_k \cong S_k \oplus \mathbb{C}G_k$ as $\mathfrak{H}_k$-modules.

Definition

Let $\mathfrak{h}_k$ denote the *cuspidal Hecke algebra*, the image of $\mathfrak{H}_k$ in $\mathrm{End}_{\mathbb{C}}(S_k)$.

Definition

The *Eisenstein ideal* is the ideal $I_k = (T_n - \sum_{d|n} d^{k-1} \mid n \geq 1)$ of $\mathfrak{h}_k$.

Theorem (Kurihara, Harder-Pink)

We have an isomorphism $\mathfrak{h}_k/I_k \xrightarrow{\sim} \mathbb{Z}/c_k\mathbb{Z}$ *defined by* $T_n \mapsto \sum_{d|n} d^{k-1} \bmod c_k$, *where* c_k *is the numerator of* $|\frac{B_k}{2k}|$.

Definition

The *L-function* of a modular form $f = \sum_{n=0}^{\infty} a_n q^n$ is the holomorphic function on $\mathbb{C}$ such that

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

for $\mathrm{Re}(s) > k$.

Remark

The function $\Lambda(f, s) = (2\pi)^{-s}\Gamma(s)L(f, s)$ satisfies the functional equation

$$\Lambda(f, s) = (-1)^{\frac{k}{2}}\Lambda(f, k - s).$$

Example

We have $L(G_k, s) = \zeta(s)\zeta(s - k + 1)$.

Theorem (Manin 1973)

For an eigenform $f = \sum_{n=1}^{\infty} a_n q^n \in S_k$, *there exist periods* $\Omega_f^{\pm} \in \mathbb{C}$ *such that*

$$\frac{\Lambda(f,i)}{\Omega_f^{\pm}} \in K_f = \mathbb{Q}(a_1, a_2, \ldots)$$

for $1 \leq i \leq k-1$, *where* $\pm$ *is the sign of* $(-1)^{i-1}$.

Example

The space S_{12} is one-dimensional, spanned by the eigenform

$$\Delta(q) = q \prod_{n=1}^{\infty} (1-q^n)^{24}.$$

Note: $691 \mid \zeta(-11)$, and in fact, $\Delta \equiv G_{12} \bmod 691$. Take $\Omega_\Delta^+ = \Lambda(\Delta, 1)$. Then

$$\frac{\Lambda(\Delta,3)}{\Omega_\Delta^+} = \frac{-691}{2^2 \cdot 3^4 \cdot 5} \quad \text{and} \quad \frac{\Lambda(\Delta,5)}{\Omega_\Delta^+} = \frac{691}{2^3 \cdot 3^2 \cdot 5 \cdot 7}.$$

The ratio $\dfrac{\Lambda(\Delta,5)}{\Lambda(\Delta,3)}$ is $-\dfrac{9}{14} \equiv -50 \bmod 691$.

Fact

There are product maps $K_i(\mathbb{Z}) \times K_j(\mathbb{Z}) \to K_{i+j}(\mathbb{Z})$ *for all* $i, j \geq 0$.
If $x \in K_i(\mathbb{Z})$ *and* $y \in K_j(\mathbb{Z})$*, then* $xy = (-1)^{ij} yx$.

Theorem (Soulé, Beilinson-Deligne, Huber-Wildeshaus)

For odd $i \geq 3$*, there is a canonical element* κ_i *of infinite order in* $K_{2i-1}(\mathbb{Z})$.

For a finitely generated abelian group A, let us set $A' = A/(2\text{-power torsion})$.

Remark

The *Soulé element* κ_i generates $K_{2i-1}(\mathbb{Z})' \cong \mathbb{Z}$ if Vandiver's conjecture holds.

Example (S.)

We have $K_{22}(\mathbb{Z}) \cong \mathbb{Z}/691\mathbb{Z}$. For the product maps

$$K_5(\mathbb{Z}) \times K_{17}(\mathbb{Z}) \to K_{22}(\mathbb{Z}) \quad \text{and} \quad K_9(\mathbb{Z}) \times K_{13}(\mathbb{Z}) \to K_{22}(\mathbb{Z})$$

we have $\kappa_5\kappa_7 = a\kappa_3\kappa_9 \neq 0$ with $a \equiv -50 \bmod 691$.

Fact

For odd primes $p < 25{,}000$ and k with $p \mid \frac{B_k}{k}$, a computation of McCallum-S. (2003), along with results of S. and Fukaya-Kato, provides the values $\kappa_i \kappa_{k-i}$ of

$$K_{2i-1}(\mathbb{Z}) \times K_{2(k-i)-1}(\mathbb{Z}) \to K_{2k-2}(\mathbb{Z}) \otimes \mathbb{Z}/p\mathbb{Z}.$$

For small k and p with $p \mid B_k$, the following table lists $\kappa_i \kappa_{k-i} \bmod p$ for $i = 3, 5, \ldots, k-3$ under an isomorphism of the p-part of $K_{2k-2}(\mathbb{Z})$ with $\mathbb{Z}/p\mathbb{Z}$.

k	p	$\kappa_i \kappa_{k-i}$
12	691	$(222, 647, 44, 469)$
16	3617	$(1787, 2884, 3312, 305, 733, 1830)$
20	283	$(251, 194, 260, 172, 111, 23, 89, 32)$
20	617	$(144, 593, 53, 110, 507, 564, 24, 473)$
22	131	$(35, 74, 129, 81, 0, 50, 2, 57, 96)$
22	593	$(469, 77, 541, 10, 0, 583, 52, 516, 124)$
24	103	$(70, 17, 22, 77, 25, 78, 26, 81, 86, 33)$
32	37	$(26, 0, 36, 1, 35, 31, 34, 3, 6, 2, 36, 1, 0, 11)$
44	59	$(45, 21, 30, 14, 35, 5, 0, 48, 57, 7, 52, 2, 11, 0, 54, 24, 45, 29, 38, 14)$
58	67	$(45, 38, 56, 0, 47, 62, 9, 29, 15, 65, 26, 45, 57, 0, 10, 22, 41, 2, 52, 38, 58, 5, 20, 0, 11, 29, 22)$

Definition

For positive integers $r_1, \ldots, r_d$ with $r_1 \geq 2$, the value

$$\zeta(r_1, \ldots, r_d) = \sum_{n_1 > \cdots > n_d > 0} \frac{1}{n_1^{r_1} n_2^{r_2} \cdots n_d^{r_d}}$$

is called a *multiple zeta value* (MZV) of weight $k = r_1 + \ldots + r_d$ and depth d.

Remarks

1. These are values of iterated integrals yielding periods of $\pi_1(\mathbb{P}^1 - \{0, 1, \infty\})$.
2. They satisfy standard relations: e.g., $\zeta(r,s) + \zeta(s,r) = \zeta(r)\zeta(s) - \zeta(r+s)$.
3. Hoffman (1997) conjectured that the MZVs with $r_i \in \{2, 3\}$ form a basis of the $\mathbb{Q}$-span of MZVs. Using a result of Zagier, Brown (2012) proved that these MZVs span (and motivic versions are linearly independent).

Example (Gangl-Kaneko-Zagier)

We have $28\zeta(9,3) + 150\zeta(7,5) + 168\zeta(5,7) = \frac{5197}{691}\zeta(12)$. Note: $\frac{150-168}{28} = -\frac{9}{14}$.

Modular symbols

Let $Z_k = \{P \in \mathbb{Z}[X,Y] \mid P$ is homogeneous of degree $k-2\}$.

Definition

1. The group $\mathcal{M}_k$ of *modular symbols* of weight k is the maximal torsion-free quotient of Z_k by the following relations for $P \in Z_k$:

$$P(X,Y) + P(-Y,X) \quad \text{and} \quad P(X,Y) - P(X,X+Y) - P(X+Y,Y).$$

2. The group $\mathcal{S}_k$ of *cuspidal modular symbols* in $\mathcal{M}_k$ is generated by the $X^{j-1}Y^{k-1-j}$ with $1 < j < k-1$.
3. The *plus parts* $\mathcal{M}_k^+$ (and $\mathcal{S}_k^+$) are the subgroups generated by the $X^{j-1}Y^{k-1-j}$ for j odd.

The spaces of (cuspidal) modular symbols are modules for $\mathfrak{H}_k$ (resp., $\mathfrak{h}_k$).

Theorem (Eichler 1957, Shimura 1959)

For modular forms with real coefficients, we have a pairing

$$\mathcal{M}_k^+ \times M_k(\mathbb{R}) \to \mathbb{R}, \quad (X^{j-1}Y^{k-j-1}, f) = \int_0^{i\infty} z^{j-1} f(z)dz = \Lambda(f,j),$$

inducing an isomorphism $M_k(\mathbb{R}) \cong \mathrm{Hom}(\mathcal{M}_k^+, \mathbb{R})$ *of* $\mathfrak{H}_k$*-modules.*

An interesting map

Theorem (S., Fukaya-Kato)

For $k \geq 2$ even, there exists a map

$$\varpi_k \colon \mathcal{S}_k^+ / I_k \mathcal{S}_k^+ \to K_{2k-2}(\mathbb{Z})', \quad X^{i-1}Y^{k-i-1} \mapsto \kappa_i \kappa_{k-i}.$$

Remark

The map on $\mathcal{S}_k^+$ was constructed by S. and conjectured to factor through $\mathcal{S}_k^+ / I_k \mathcal{S}_k^+$. In an equivalent form, this was proven by Fukaya and Kato in 2012.

Conjecture (S.)

The map ϖ_k is an isomorphism for all k.

Remark

Surjectivity of ϖ_k is equivalent to a conjecture of McCallum-S. (2003)

Theorem (S. for $p < 1000$, Fukaya-Kato)

The map ϖ_k is an isomorphism on p-parts for $p < 163577356$.

The unramified Iwasawa module

For an odd prime p, set $\mathbb{Q}(\mu_{p^\infty}) = \bigcup_{r=1}^{\infty} \mathbb{Q}(\mu_{p^r})$ and $G = \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$.

Definition

The *p-adic cyclotomic character* is the isomorphism $\chi\colon G \to \mathbb{Z}_p^\times$ satisfying $\sigma(\zeta) = \zeta^{\chi(\sigma)}$ for all p-power roots of unity ζ.

Remark

We have $G = \Gamma \times \Delta$ with $\Gamma \cong \mathbb{Z}_p$ and $\Delta \cong (\mathbb{Z}/p\mathbb{Z})^\times$.

Definition

1. The *Iwasawa algebra* is $\Lambda = \mathbb{Z}_p[\![\Gamma]\!] = \varprojlim_r \mathbb{Z}_p[\Gamma/\Gamma^{p^r}]$.
2. X_∞ is the finitely generated, torsion Λ-module of norm compatible sequences in the p-parts of the class groups of the fields $\mathbb{Q}(\mu_{p^r})$ for $r \geq 1$.

Remarks

1. Λ is noncanonically isomorphic to a power series ring $\mathbb{Z}_p[\![T]\!]$.
2. By class field theory, X_∞ is isomorphic to Galois group of the maximal abelian pro-p extension of $\mathbb{Q}(\mu_{p^\infty})$ in which no prime ramifies.

Let $\omega\colon (\mathbb{Z}/p\mathbb{Z})^\times \hookrightarrow \mathbb{Z}_p^\times$ be the unique splitting of the reduction-mod-p map.

Definition

The *Kubota-Leopoldt p-adic L-function* $L_p(\omega^k, s)$ is the unique continuous $\mathbb{Q}_p$-valued function on $\mathbb{Z}_p$ that for positive integers $n \equiv k \bmod (p-1)$ satisfies

$$L_p(\omega^k, 1-n) = -(1-p^{n-1})\frac{B_n}{n}.$$

Remark

Every finitely generated torsion Λ-module M is isomorphic up to finite modules to a direct sum of cyclic modules $\Lambda/(f)$, where f is a non-unit in $\Lambda \cong \mathbb{Z}_p[\![T]\!]$. The product of these elements f is a *characteristic power series* of M.

Theorem (Iwasawa main conjecture, Mazur-Wiles 1984)

The Λ-module summand $X_\infty^{(1-k)}$ of elements of X_∞ on which Δ acts through χ^{1-k} has a characteristic power series interpolating $L_p(\omega^k, s)$.

Mazur and Wiles extended work of Ribet to construct unramified extensions of cyclotomic fields out of two-dimensional Galois representations attached to cusp forms satisfying congruences with Eisenstein series. That is, they studied Galois actions on the quotients of étale cohomology groups of modular curves by Eisenstein ideals (Wiles, Ohta).

Remark

As a consequence of the Quillen-Lichtenbaum conjecture, the maximal quotient of X_∞ on which G acts through χ^{1-k} is isomorphic to $K_{2k-2}(\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}_p$.

A mild refinement of the Mazur-Wiles method gives the following map on p-parts.

Theorem (S. 2011)

There is a canonical map $\Upsilon_k \colon K_{2k-2}(\mathbb{Z})' \to S_k^+/I_k S_k^+$.

The following explicitly refines the main conjecture.

Conjecture (S. 2011)

The maps ϖ_k *and* Υ_k *are inverse to each other.*

Results

Theorem (Fukaya-Kato 2012, Fukaya-Kato-S. 2015)

We have $\xi'_k \Upsilon_k \circ \varpi_k = \xi'_k$ *on* $S_k^+/I_k S_k^+$, *where* $\xi'_k = \frac{d}{ds} L_p(\omega^k, s)|_{s=1-k} \in \mathbb{Z}_p$.

Remark

Fukaya and Kato proved an analogous result up the cyclotomic tower after taking a tensor product with $\mathbb{Q}_p$. Our work removed the need to tensor with $\mathbb{Q}_p$.

Remark

If $p \nmid \xi'_k$ (or $p \nmid \frac{B_k}{k}$), the conjecture holds on p-parts by the above theorem.

Corollary

The conjecture is true on p*-parts for primes* $p < 163577356$.

The above generalizes to modular symbols of arbitrary weight and level modulo Eisenstein ideals, describing $K_{2k-2}(\mathcal{O})$ for integer rings $\mathcal{O}$ of cyclotomic fields in terms of products on special elements in $K_{2i-1}(\mathcal{O})$ for odd i.

By Hida and Iwasawa theory, it is sufficient to consider weight 2 modular symbols.

Example (Weight 2, Level N)

- A *Manin symbol* $[u : v]$ for $u, v \in \mathbb{Z}/N\mathbb{Z}$ with $(u, v) = (1)$ is a certain class in first homology of the modular curve $X_1(N)$ relative to its cusps.
- There is a map
$$[u : v]^+ \mapsto \{1 - \zeta_N^u, 1 - \zeta_N^v\}^+$$
for $u, v \neq 0$, inducing
$$\varpi \colon (H_1(X_1(N), \mathbb{Z})^+/I)' \to (K_2(\mathbb{Z}[\mu_N])^+)'$$
Here, $\{\ ,\ \}$ is the Steinberg symbol, I is an Eisenstein ideal, $+$ is fixed part under complex conjugation, and $\zeta_N = e^{2\pi i/N}$. The conjecture (S.) is that ϖ is an isomorphism outside of a trivial $(\mathbb{Z}/N\mathbb{Z})^\times$-component.
- Excluding certain exceptional components, we can construct a conjectural inverse Υ on p-parts (S.). The analogous theorems hold (F-K, F-K-S).

Over a global base field F, our philosophy is very roughly summarized by:

Philosophy (Fukaya-Kato-S.)

geometry of GL_d modulo Eisenstein $\Longleftrightarrow$ arithmetic of GL_{d-1}

The above is the special case $F = \mathbb{Q}$ and $d = 2$.

Question ($F = \mathbb{Q}$ and $d = 3$)

Can we use modular symbols for an arithmetic quotient of $\mathrm{SL}_3(\mathbb{R})/\mathrm{SO}_3(\mathbb{R})$ to construct generators of the dual of the Selmer group of a modular Galois representation out of products of three Siegel units?

Work-in-progress (F global function field, arbitrary d)

We are writing a series of papers to formulate a conjecture and prove an analogue of the Fukaya-Kato theorem in this setting. This will describe products of Siegel units on a Drinfeld modular variety (Kondo-Yasuda) in terms of modular symbols in the homology of an arithmetic quotient of a Bruhat-Tits building. Our first preprint in this series (2015) compactifies the latter quotient. We have the analogous conjecture and theorem in the case $F = \mathbb{F}_q(t)$ and $d = 2$ (2014).