Bernouilli numbers, Eisenstein Series and Cyclotomic units

Michael Zhao Memorial Student Colloquium

Eric Urban

Columbia University

November 20th, 2019

Fermat Last Theorem

Let p be an odd prime number.

Fermat Last Theorem

Let $x, y, z \in \mathbf{Z}$ such that $x^p + y^p = z^p$ then $xyz = 0$.

Fermat Last Theorem

Let p be an odd prime number.

Fermat Last Theorem

Let $x, y, z \in \mathbf{Z}$ such that $x^p + y^p = z^p$ then $xyz = 0$.

Let F be the cyclotomic field $\mathbf{Q}(\zeta_p)$ where $\zeta_p = e^{2i\pi/p}$. Using the factorization

$$\prod_{a=0}^{p-1}(x + \zeta_p^a y) = z^p,$$

one can show that FLT follows for p, if we know that $O_F = \mathbf{Z}[\zeta_p]$ is a UFD. It is false in general but Kummer proved that if p does not divide the class number of $\mathbf{Q}(\zeta_p)$, then FLT follows for p. Such prime numbers are called regular primes.

Bernouilli numbers

The Bernouilli numbers are the rational numbers B_n for $n \geq 1$ defined by

$$\frac{t}{1-e^{-t}} = 1 + \sum_{n=1}^{\infty} B_n \cdot \frac{t^n}{n!}$$

Example: $B_1 = \frac{1}{2}$, $B_2 = \frac{1}{6}$, $B_{2n+1} = 0$ for $n \geq 1$, $B_4 = -\frac{1}{30} \ldots$.

Bernouilli numbers

The Bernouilli numbers are the rational numbers B_n for $n \geq 1$ defined by

$$\frac{t}{1-e^{-t}} = 1 + \sum_{n=1}^{\infty} B_n \cdot \frac{t^n}{n!}$$

Example: $B_1 = \frac{1}{2}$, $B_2 = \frac{1}{6}$, $B_{2n+1} = 0$ for $n \geq 1$, $B_4 = -\frac{1}{30} \ldots$.

Kummer's Criterion (1850)

If $p \nmid B_2 B_4 \ldots B_{p-3}$, then p is a regular prime.

Bernouilli numbers

The Bernouilli numbers are the rational numbers B_n for $n \geq 1$ defined by

$$\frac{t}{1-e^{-t}} = 1 + \sum_{n=1}^{\infty} B_n \cdot \frac{t^n}{n!}$$

Example: $B_1 = \frac{1}{2}$, $B_2 = \frac{1}{6}$, $B_{2n+1} = 0$ for $n \geq 1$, $B_4 = -\frac{1}{30} \dots$.

Kummer's Criterion (1850)

If $p \not| B_2 B_4 \dots B_{p-3}$, then p is a regular prime.

More generally, if χ is a Dirichlet character modulo N, we define the generalized Bernouilli numbers $B_{n,\chi}$ as follows:

$$\sum_{a=1}^{N-1} \chi(a) \frac{te^{at}}{e^{Nt}-1} = \sum_{n=0}^{\infty} B_{n,\chi} \cdot \frac{t^n}{n!}$$

Example: $B_{1,\chi} = \frac{1}{N} \sum_{a=1}^{N-1} \chi(a)a$.

A refinement:The theorem of Herbrand-Ribet

Let $G := Gal(\mathbf{Q}(\zeta_p)/\mathbf{Q})$ and let $\omega : G \to (\mathbf{Z}/p\mathbf{Z})^\times$ be the Teichmüller character. Consider the action of G on the p-Sylow subgroup C of the class group $Cl_{\mathbf{Q}(\zeta_p)}$.

A refinement:The theorem of Herbrand-Ribet

Let $G := Gal(\mathbf{Q}(\zeta_p)/\mathbf{Q})$ and let $\omega : G \to (\mathbf{Z}/p\mathbf{Z})^\times$ be the Teichmüller character. Consider the action of G on the p-Sylow subgroup C of the class group $Cl_{\mathbf{Q}(\zeta_p)}$. We have a decomposition:

$$C = \bigoplus_{i=0}^{p-1} C(i)$$

where $C(i)$ is the maximal subgroup of C for which G acts via ω^i. We then denotes by $h(i)$ the order of $C(i)$. Then a refinement of Kummer's criterion is given by the following

A refinement:The theorem of Herbrand-Ribet

Let $G := Gal(\mathbf{Q}(\zeta_p)/\mathbf{Q})$ and let $\omega : G \to (\mathbf{Z}/p\mathbf{Z})^\times$ be the Teichmüller character. Consider the action of G on the p-Sylow subgroup C of the class group $Cl_{\mathbf{Q}(\zeta_p)}$. We have a decomposition:

$$C = \bigoplus_{i=0}^{p-1} C(i)$$

where $C(i)$ is the maximal subgroup of C for which G acts via ω^i. We then denotes by $h(i)$ the order of $C(i)$. Then a refinement of Kummer's criterion is given by the following

Theorem (Herbrand(1932)-Ribet(1976))

Let i be an odd integer between 3 and $p-2$, then p divides $h(i)$ if and only if p divides B_{p-i}

Further refinement: The theorem of Mazur-Wiles.

Using elementary method, one can see from the definition of Bernouilli numbers that

$$B_{p-i} \equiv B_{1,\omega^{-i}} \pmod{p}$$

Further refinement: The theorem of Mazur-Wiles.

Using elementary method, one can see from the definition of Bernouilli numbers that

$$B_{p-i} \equiv B_{1,\omega^{-i}} \pmod p$$

Theorem (Mazur-Wiles(1984))

Let i be an odd integer between 3 and $p-2$, then

$$h(i) \sim B_{1,\omega^{-i}}.$$

Further refinement: The theorem of Mazur-Wiles.

Using elementary method, one can see from the definition of Bernouilli numbers that

$$B_{p-i} \equiv B_{1,\omega^{-i}} \pmod p$$

Theorem (Mazur-Wiles(1984))

Let i be an odd integer between 3 and $p-2$, then

$$h(i) \sim B_{1,\omega^{-i}}.$$

For a Dirichlet character χ, we consider the L-series

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} \qquad \text{CV for } Re(s) > 1.$$

It has a meromorphic continuation to $\mathbf{C}$ (holomorphic if χ is non trivial) and the following formula holds

$$L(1-n,\chi) = -\frac{B_{n,\chi}}{n} \text{ if } n \geq 1 \text{ and } \chi(-1) = (-1)^n.$$

Idea of proof of Mazur-Wiles's theorem

The idea is an elaborate refinement of Ribet's idea using Iwasawa theory.

Idea of proof of Mazur-Wiles's theorem

The idea is an elaborate refinement of Ribet's idea using Iwasawa theory.

- Let L be the maximal abelian unramified extension of $\mathbf{Q}(\zeta_p)$. Use Class Field Theory to view $C(i)$ as

$$C(i) \cong Hom_G(Gal(L/\mathbf{Q}(\zeta_p)), \mathbf{Q}_p/\mathbf{Z}_p(\omega^{-i})).$$

Idea of proof of Mazur-Wiles's theorem

The idea is an elaborate refinement of Ribet's idea using Iwasawa theory.

- Let L be the maximal abelian unramified extension of $\mathbf{Q}(\zeta_p)$. Use Class Field Theory to view $C(i)$ as

$$C(i) \cong Hom_G(Gal(L/\mathbf{Q}(\zeta_p)), \mathbf{Q}_p/\mathbf{Z}_p(\omega^{-i})).$$

- Use congruence between Eisenstein series and cusp forms and their associated Galois representations to prove the divisibility

$$B_{1,\omega^{-i}} \sim L(0, \omega^{-i}) \mid h(i)$$

for odd integer i between 3 and $p-2$.

Idea of proof of Mazur-Wiles's theorem

The idea is an elaborate refinement of Ribet's idea using Iwasawa theory.

- Let L be the maximal abelian unramified extension of $\mathbf{Q}(\zeta_p)$. Use Class Field Theory to view $C(i)$ as

$$C(i) \cong Hom_G(Gal(L/\mathbf{Q}(\zeta_p)), \mathbf{Q}_p/\mathbf{Z}_p(\omega^{-i})).$$

- Use congruence between Eisenstein series and cusp forms and their associated Galois representations to prove the divisibility

$$B_{1,\omega^{-i}} \sim L(0, \omega^{-i}) \mid h(i)$$

for odd integer i between 3 and $p-2$.

- Use Dirichlet class Number Formulas for $\mathbf{Q}(\zeta_p)$ and $\mathbf{Q}(\zeta_p)^+$ that tell us that

$$\prod_{\substack{i=3 \\ odd}}^{p-2} L(0, \omega^{-i}) \sim h^- = \prod_{\substack{i=3 \\ odd}}^{p-2} h(i)$$

Modular forms

A modular forms of weight k and nebentypus χ is an holomorphic function on the Poincaré upper half plane $\mathbf{H}$ such that

$$f(\frac{az+b}{cz+d}) = \chi(d)(cz+d)^k \cdot f(z) \qquad \forall \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$$

and if $f(z)$ has a limit at the each of the cusps of $\Gamma_0(N)\backslash\mathbf{H}$.

Modular forms

A modular forms of weight k and nebentypus χ is an holomorphic function on the Poincaré upper half plane $\mathbf{H}$ such that

$$f(\frac{az+b}{cz+d}) = \chi(d)(cz+d)^k \cdot f(z) \qquad \forall \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$$

and if $f(z)$ has a limit at the each of the cusps of $\Gamma_0(N)\backslash\mathbf{H}$. It is said cuspidal if the value at the cusps are zero.

Modular forms

A modular forms of weight k and nebentypus χ is an holomorphic function on the Poincaré upper half plane $\mathbf{H}$ such that

$$f(\frac{az+b}{cz+d}) = \chi(d)(cz+d)^k \cdot f(z) \qquad \forall \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$$

and if $f(z)$ has a limit at the each of the cusps of $\Gamma_0(N)\backslash\mathbf{H}$. It is said cuspidal if the value at the cusps are zero. A modular form f is called an eigenform if it is an eigen vector for all the Hecke operators T_q defined by

$$T_q.f(z) = \sum_{i=0}^{q-1} f(\frac{z+i}{q}) + \chi(q) f(qz)$$

for q prime to N, then

$$f(z) = a_0(f) + \sum_{n=1}^{\infty} a_n(f) e^{2i\pi nz}. \qquad (a_1 = 1 \textit{ if } f \textit{ normalized})$$

where $a_q(f)$ is the eigenvalue of T_q and $a_0(f)$ is called the constant term at the cusp ∞.

Eisenstein series

For each integer $k \geq 3$, one can form the series

$$G_{k,\chi}(z) := \sum_{\substack{(c,d)=1 \\ N|c}} \chi(d)(cz+d)^{-k}$$

this defines a modular form of weight k and nebentypus χ. After renormalization, one gets

$$E_{k,\chi}(z) = \frac{L(1-k,\chi)}{2} + \sum_{n=1}^{\infty}\Big(\sum_{\substack{d|n \\ (d,N)=1}} \chi(d)d^{k-1}\Big)e^{2i\pi nz}$$

Eisenstein series

For each integer $k \geq 3$, one can form the series

$$G_{k,\chi}(z) := \sum_{\substack{(c,d)=1 \\ N|c}} \chi(d)(cz+d)^{-k}$$

this defines a modular form of weight k and nebentypus χ. After renormalization, one gets

$$E_{k,\chi}(z) = \frac{L(1-k,\chi)}{2} + \sum_{n=1}^{\infty}\Big(\sum_{\substack{d|n \\ (d,N)=1}} \chi(d)d^{k-1}\Big)e^{2i\pi nz}$$

It is an eigenform satisfying

$$T_q \cdot E_{k,\chi} = (1+\chi(q)q^{k-1}) \cdot E_{k,\chi}$$

Galois representations

If f is an eigenform of weight k and nebentypus χ, it is known thanks to the works of Eichler-Shimura and Deligne, that there exists a continuous Galois representation

$$\rho_f : \mathrm{G}_{\mathbf{Q}} \to GL_2(\mathbf{Z}_p)$$

unramified away from Np such that $tr(\rho_f(Frob_q)) = a_q(f)$ for $q \not| Np$ and $det(\rho_f) = \epsilon_{cyc}^{1-k}\chi$.

Galois representations

If f is an eigenform of weight k and nebentypus χ, it is known thanks to the works of Eichler-Shimura and Deligne, that there exists a continuous Galois representation

$$\rho_f : \mathrm{G}_{\mathbf{Q}} \to GL_2(\mathbf{Z}_p)$$

unramified away from Np such that $tr(\rho_f(Frob_q)) = a_q(f)$ for $q \not| Np$ and $det(\rho_f) = \epsilon_{cyc}^{1-k}\chi$. Moreover if $p \not| a_p$, the restriction of ρ_f to the decomposition subgroup at p is ordinary i.e.

$$\rho_f|_{I_p} \sim \begin{pmatrix} 1 & * \\ 0 & \epsilon_{cyc}^{1-k}\chi \end{pmatrix}$$

Galois representations

If f is an eigenform of weight k and nebentypus χ, it is known thanks to the works of Eichler-Shimura and Deligne, that there exists a continuous Galois representation

$$\rho_f : \mathrm{G}_{\mathbf{Q}} \to GL_2(\mathbf{Z}_p)$$

unramified away from Np such that $tr(\rho_f(Frob_q)) = a_q(f)$ for $q \not| Np$ and $det(\rho_f) = \epsilon_{cyc}^{1-k}\chi$. Moreover if $p \not| a_p$, the restriction of ρ_f to the decomposition subgroup at p is ordinary i.e.

$$\rho_f|_{I_p} \sim \begin{pmatrix} 1 & * \\ 0 & \epsilon_{cyc}^{1-k}\chi \end{pmatrix}$$

Ribet proved that ρ_f is absolutely irreducible whenever f is cuspidal. On the other hand, if f is the Eisenstein series $E_{k,\chi}$, the corresponding Galois representation is reducible.

Galois representations

If f is an eigenform of weight k and nebentypus χ, it is known thanks to the works of Eichler-Shimura and Deligne, that there exists a continuous Galois representation

$$\rho_f : \mathrm{G}_{\mathbf{Q}} \to GL_2(\mathbf{Z}_p)$$

unramified away from Np such that $tr(\rho_f(Frob_q)) = a_q(f)$ for $q \not| Np$ and $det(\rho_f) = \epsilon_{cyc}^{1-k}\chi$. Moreover if $p \not| a_p$, the restriction of ρ_f to the decomposition subgroup at p is ordinary i.e.

$$\rho_f|_{I_p} \sim \begin{pmatrix} 1 & * \\ 0 & \epsilon_{cyc}^{1-k}\chi \end{pmatrix}$$

Ribet proved that ρ_f is absolutely irreducible whenever f is cuspidal. On the other hand, if f is the Eisenstein series $E_{k,\chi}$, the corresponding Galois representation is reducible. More precisely, it is given by

$$\rho_{E_{k,\chi}} = \begin{pmatrix} \epsilon_{cyc}^{1-k}\chi & 0 \\ 0 & 1 \end{pmatrix}$$

I

Ordinary Eisenstein congruences

If $p^m | L(1-k,\chi)$, then $E_{k,\chi}$ looks cuspidal modulo p^m. In fact, on can show that there exists g cuspidal of the same weight and level as $E_{k,\chi}$ such that

$$g \equiv E_{k,\chi} \pmod{p^m}$$

Ordinary Eisenstein congruences

If $p^m | L(1-k,\chi)$, then $E_{k,\chi}$ looks cuspidal modulo p^m. In fact, on can show that there exists g cuspidal of the same weight and level as $E_{k,\chi}$ such that

$$g \equiv E_{k,\chi} \pmod{p^m}$$

If g is an eigenform, we deduce that ρ_g becomes reducible modulo p^m. Since ρ_g is itself irreducible, one can show (Ribet's lemma) that there exists a stable lattice in the space of the representation ρ_g such that modulo p^m, we have

$$\rho_g \equiv \begin{pmatrix} \chi\epsilon_{cyc}^{1-k} & * \\ 0 & 1 \end{pmatrix} \pmod{p^m}$$

Ordinary Eisenstein congruences

If $p^m | L(1-k,\chi)$, then $E_{k,\chi}$ looks cuspidal modulo p^m. In fact, on can show that there exists g cuspidal of the same weight and level as $E_{k,\chi}$ such that

$$g \equiv E_{k,\chi} \pmod{p^m}$$

If g is an eigenform, we deduce that ρ_g becomes reducible modulo p^m. Since ρ_g is itself irreducible, one can show (Ribet's lemma) that there exists a stable lattice in the space of the representation ρ_g such that modulo p^m, we have

$$\rho_g \equiv \begin{pmatrix} \chi\epsilon_{cyc}^{1-k} & * \\ 0 & 1 \end{pmatrix} \pmod{p^m}$$

where the upper right shoulder $*$ defines a non trivial extension and therefore an element in $H^1(G_{\mathbf{Q}}, \mathbf{Z}/p^m\mathbf{Z}(\chi\epsilon_{cyc}^{1-k}))$ which is unramified at p. By refining this argument and making it precise, Mazur and Wiles prove that $B_{1,\omega^{-i}}$ divides $h(i)$.

Cyclotomic units and the Kummer map

For any number field $F \subset \bar{\mathbf{Q}}$ and integer n, recall that we have the Kummer map

$$k_F \colon F^{\times} \to H^1(F, \mathbf{Z}_p(1))$$

Cyclotomic units and the Kummer map

For any number field $F \subset \bar{\mathbf{Q}}$ and integer n, recall that we have the Kummer map

$$k_F \colon F^\times \to H^1(F, \mathbf{Z}_p(1))$$

For any integer N, we consider the subgroup $\mathcal{E}_N \subset \mathbf{Z}[\zeta_N]^\times$ generated by the elements $\zeta_N^a \prod_b (1 - \zeta_N^b)^{r_b}$ with $r_b, a \in \mathbf{Z}$ such that $\sum_b r_b = 0$. We denote by $c_N \in H^1(\mathbf{Q}(\zeta_N), \mathbf{Z}_p(1))$ defined by

$$c_N = k_{\mathbf{Q}(\zeta_N)}(1 - \zeta_N)$$

Cyclotomic units and the Kummer map

For any number field $F \subset \bar{\mathbf{Q}}$ and integer n, recall that we have the Kummer map

$$k_F \colon F^\times \to H^1(F, \mathbf{Z}_p(1))$$

For any integer N, we consider the subgroup $\mathcal{E}_N \subset \mathbf{Z}[\zeta_N]^\times$ generated by the elements $\zeta_N^a \prod_b (1-\zeta_N^b)^{r_b}$ with $r_b, a \in \mathbf{Z}$ such that $\sum_b r_b = 0$. We denote by $c_N \in H^1(\mathbf{Q}(\zeta_N), \mathbf{Z}_p(1))$ defined by

$$c_N = k_{\mathbf{Q}(\zeta_N)}(1-\zeta_N)$$

It satisfies the **Norm Relations** of an Euler system:

$$Cores_{\mathbf{Q}(\zeta_N)}^{\mathbf{Q}(\zeta_{N\ell})}(c_{N\ell}) = \begin{cases} (1-\mathrm{F}r_\ell^{-1}) \cdot c_N & \text{if } \ell \not| N \\ c_N & \text{if } \ell | N \end{cases}$$

Another proof of MW theorem using this Euler system:

Using these classes, following ideas of Thaine and Kolyvagin, K. Rubin (1990) gave another proof of the Mazur-Wiles theorem. Grosso modo, his proof

Another proof of MW theorem using this Euler system:

Using these classes, following ideas of Thaine and Kolyvagin, K. Rubin (1990) gave another proof of the Mazur-Wiles theorem. Grosso modo, his proof

- Uses the classes c_N to construct torsion classes $\kappa_N \in H^1(\mathbf{Q}, \mu_{p^n})$ satisfying precise ramification conditions

Another proof of MW theorem using this Euler system:

Using these classes, following ideas of Thaine and Kolyvagin, K. Rubin (1990) gave another proof of the Mazur-Wiles theorem. Grosso modo, his proof

- Uses the classes c_N to construct torsion classes $\kappa_N \in H^1(\mathbf{Q}, \mu_{p^n})$ satisfying precise ramification conditions
- Uses Tate and Poitou-Tate duality theorems, the reciprocity law of Class Field Theory to exhibit many relations among elements in C. This allows him to bound the size of the class groups $C(i)$:

$$h(i) \mid L(0, \omega^{-i})$$

for odd integer i between 3 and $p-2$.

Another proof of MW theorem using this Euler system:

Using these classes, following ideas of Thaine and Kolyvagin, K. Rubin (1990) gave another proof of the Mazur-Wiles theorem. Grosso modo, his proof

- Uses the classes c_N to construct torsion classes $\kappa_N \in H^1(\mathbf{Q}, \mu_{p^n})$ satisfying precise ramification conditions
- Uses Tate and Poitou-Tate duality theorems, the reciprocity law of Class Field Theory to exhibit many relations among elements in C. This allows him to bound the size of the class groups $C(i)$:

$$h(i) \mid L(0, \omega^{-i})$$

  for odd integer i between 3 and $p-2$.
- Uses the Dirichlet class Number Formula as in the original proof of Mazur-Wiles.

$$\prod_{\substack{i=3 \\ odd}}^{p-2} L(0, \omega^{-i}) \sim h^- = \prod_{\substack{i=3 \\ odd}}^{p-2} h(i)$$

Ordinary Eisenstein congruences and Euler systems combined

Using Eisenstein congruences and the Euler system of cyclotomic units one obtains a proof of MW theorem without invoking Dirichlet class number formula. Here is another example where these two technics are combined.

Ordinary Eisenstein congruences and Euler systems combined

Using Eisenstein congruences and the Euler system of cyclotomic units one obtains a proof of MW theorem without invoking Dirichlet class number formula. Here is another example where these two technics are combined.

Theorem (Kato(2004),Skinner-U.(2013))

Let E be an elliptic curve over the rational having good ordinary reduction at p such that $L(E,1) \neq 0$ and having no p-torsion point over an abelian extension of $\mathbf{Q}$ Then the p-part of the BSD formula holds

$$\frac{L(E,1)}{\Omega_E} \sim \#\text{Ш}_p(E) \prod_{\ell | N_E} c_\ell(E)$$

Ordinary Eisenstein congruences and Euler systems combined

Using Eisenstein congruences and the Euler system of cyclotomic units one obtains a proof of MW theorem without invoking Dirichlet class number formula. Here is another example where these two technics are combined.

Theorem (Kato(2004),Skinner-U.(2013))

Let E be an elliptic curve over the rational having good ordinary reduction at p such that $L(E,1) \neq 0$ and having no p-torsion point over an abelian extension of $\mathbf{Q}$ Then the p-part of the BSD formula holds

$$\frac{L(E,1)}{\Omega_E} \sim \#\text{Ш}_p(E) \prod_{\ell | N_E} c_\ell(E)$$

- The Euler system construction using Siegel units and the upper bound is obtained by the work of K. Kato.

Ordinary Eisenstein congruences and Euler systems combined

Using Eisenstein congruences and the Euler system of cyclotomic units one obtains a proof of MW theorem without invoking Dirichlet class number formula. Here is another example where these two technics are combined.

Theorem (Kato(2004),Skinner-U.(2013))

Let E be an elliptic curve over the rational having good ordinary reduction at p such that $L(E,1) \neq 0$ and having no p-torsion point over an abelian extension of $\mathbf{Q}$ Then the p-part of the BSD formula holds

$$\frac{L(E,1)}{\Omega_E} \sim \#\text{Ш}_p(E) \prod_{\ell | N_E} c_\ell(E)$$

- The Euler system construction using Siegel units and the upper bound is obtained by the work of K. Kato.
- The Eisenstein congruences argument uses Klingen-Eisenstein series for $GU(2,2)$ to obtain the right lower bound by the work of Skinner-U .

Non-ordinary Eisenstein congruences

Consider the Eisenstein series

$$E_{2,\chi}^{crit}(z) := E_{2,\chi}(z) - E_{2,\chi}(pz)$$

It is p-adically cuspidal.

Non-ordinary Eisenstein congruences

Consider the Eisenstein series

$$E_{2,\chi}^{crit}(z) := E_{2,\chi}(z) - E_{2,\chi}(pz)$$

It is p-adically cuspidal. Using the theory of overconvergent forms, for each integer n, one can find a cusp form g_n of weight k_n such that

$$g_n \equiv E_{k,\chi}^{crit} \pmod{p^n}$$

Non-ordinary Eisenstein congruences

Consider the Eisenstein series

$$E_{2,\chi}^{crit}(z) := E_{2,\chi}(z) - E_{2,\chi}(pz)$$

It is p-adically cuspidal. Using the theory of overconvergent forms, for each integer n, one can find a cusp form g_n of weight k_n such that

$$g_n \equiv E_{k,\chi}^{crit} \pmod{p^n} \text{ and } k_n \to 2 \text{ } p\text{-adically}$$

Non-ordinary Eisenstein congruences

Consider the Eisenstein series

$$E^{crit}_{2,\chi}(z) := E_{2,\chi}(z) - E_{2,\chi}(pz)$$

It is p-adically cuspidal. Using the theory of overconvergent forms, for each integer n, one can find a cusp form g_n of weight k_n such that

$$g_n \equiv E^{crit}_{k,\chi} \pmod{p^n} \text{ and } k_n \to 2 \ p\text{-adically}$$

One can patch these congruences and use Ribet's lemma to construct a class $c_\chi \in H^1(\mathbf{Q}, \mathbf{Q}_p(1)(\chi)) = H^1(\mathbf{Q}(\zeta_N), \mathbf{Q}_p(1))^\chi$.

Non-ordinary Eisenstein congruences

Consider the Eisenstein series

$$E_{2,\chi}^{crit}(z) := E_{2,\chi}(z) - E_{2,\chi}(pz)$$

It is p-adically cuspidal. Using the theory of overconvergent forms, for each integer n, one can find a cusp form g_n of weight k_n such that

$$g_n \equiv E_{k,\chi}^{crit} \pmod{p^n} \text{ and } k_n \to 2 \text{ } p\text{-adically}$$

One can patch these congruences and use Ribet's lemma to construct a class $c_\chi \in H^1(\mathbf{Q}, \mathbf{Q}_p(1)(\chi)) = H^1(\mathbf{Q}(\zeta_N), \mathbf{Q}_p(1))^\chi$.
This class c_χ is a multiple of the χ-isotypical component of c_N. However, the c_χ's are defined up to an element in $\mathbf{Q}_p^\times$. Moreover, if one wants to use these classes in a way an Euler system is constructed, we need them to satisfy

Non-ordinary Eisenstein congruences

Consider the Eisenstein series

$$E_{2,\chi}^{crit}(z) := E_{2,\chi}(z) - E_{2,\chi}(pz)$$

It is p-adically cuspidal. Using the theory of overconvergent forms, for each integer n, one can find a cusp form g_n of weight k_n such that

$$g_n \equiv E_{k,\chi}^{crit} \pmod{p^n} \text{ and } k_n \to 2 \ p\text{-adically}$$

One can patch these congruences and use Ribet's lemma to construct a class $c_\chi \in H^1(\mathbf{Q}, \mathbf{Q}_p(1)(\chi)) = H^1(\mathbf{Q}(\zeta_N), \mathbf{Q}_p(1))^\chi$.
This class c_χ is a multiple of the χ-isotypical component of c_N. However, the c_χ's are defined up to an element in $\mathbf{Q}_p^\times$. Moreover, if one wants to use these classes in a way an Euler system is constructed, we need them to satisfy
(i) The classes are integrals

Non-ordinary Eisenstein congruences

Consider the Eisenstein series

$$E_{2,\chi}^{crit}(z) := E_{2,\chi}(z) - E_{2,\chi}(pz)$$

It is p-adically cuspidal. Using the theory of overconvergent forms, for each integer n, one can find a cusp form g_n of weight k_n such that

$$g_n \equiv E_{k,\chi}^{crit} \pmod{p^n} \text{ and } k_n \to 2 \text{ } p\text{-adically}$$

One can patch these congruences and use Ribet's lemma to construct a class $c_\chi \in H^1(\mathbf{Q}, \mathbf{Q}_p(1)(\chi)) = H^1(\mathbf{Q}(\zeta_N), \mathbf{Q}_p(1))^\chi$.
This class c_χ is a multiple of the χ-isotypical component of c_N. However, the c_χ's are defined up to an element in $\mathbf{Q}_p^\times$. Moreover, if one wants to use these classes in a way an Euler system is constructed, we need them to satisfy
(i) The classes are integrals
(ii) They satisfy some norm relations

Non-ordinary Eisenstein congruences II

This raises the following questions:

Non-ordinary Eisenstein congruences II

This raises the following questions:

Question 1:

Can we normalize the classes c_χ 's in a canonical way so that

$$c_N := \frac{1}{\#(\mathbf{Z}/N\mathbf{Z})^\times} \sum_{\chi \in \widehat{(\mathbf{Z}/N\mathbf{Z})}^\times} c_\chi \in H^1(\mathbf{Q}(\zeta_N), \mathbf{Z}_p(1))?$$

Non-ordinary Eisenstein congruences II

This raises the following questions:

Question 1:

Can we normalize the classes c_χ 's in a canonical way so that

$$c_N := \frac{1}{\#(\mathbf{Z}/N\mathbf{Z})^\times} \sum_{\chi \in \widehat{(\mathbf{Z}/N\mathbf{Z})^\times}} c_\chi \in H^1(\mathbf{Q}(\zeta_N), \mathbf{Z}_p(1))?$$

Question 2:

If the answer to Q1 is positive, can we relate the classes c_N's to L-values or Bernouilli numbers? Or equivalently, are the c_N's related to the cyclotomic units $(1 - \zeta_N)$ via the Kummer map?

Non-ordinary Eisenstein congruences II

This raises the following questions:

Question 1:

Can we normalize the classes c_χ 's in a canonical way so that

$$c_N := \frac{1}{\#(\mathbf{Z}/N\mathbf{Z})^\times} \sum_{\chi \in \widehat{(\mathbf{Z}/N\mathbf{Z})^\times}} c_\chi \in H^1(\mathbf{Q}(\zeta_N), \mathbf{Z}_p(1))?$$

Question 2:

If the answer to Q1 is positive, can we relate the classes c_N's to L-values or Bernouilli numbers? Or equivalently, are the c_N's related to the cyclotomic units $(1-\zeta_N)$ via the Kummer map?

Question 3:

Can we prove Mazur-Wiles theorem using only Eisenstein congruences? (i.e. without invoking the class number formula)

Euler system via Eisenstein congruences

Theorem (U.)

There is a positive answer to three questions above. In other words, let a *be an odd integer distinct from* 1 *modulo* $p-1$*. For each integer* N*, the exists a class* $\mathcal{C}_{N,a} \in H^1_{Iw}(\mathbf{Q}(\zeta_N), \mathbf{Z}_p(1))^{\omega^a}$ *constructed using Eisenstein congruences and satisfying the norm relation of an Euler system. Moreover, the image of* $\mathcal{C}_{1,a}$ *in* $H^1_{Iw}(\mathbf{Q}_p, \mathbf{Z}_p(1))^{\omega^a}$ *is related to the* ω^a*-branch of the Kubota-Leopold p-adic L-function.*

Euler system via Eisenstein congruences

Theorem (U.)

There is a positive answer to three questions above. In other words, let a be an odd integer distinct from 1 modulo $p-1$. For each integer N, the exists a class $\mathcal{C}_{N,a} \in H^1_{Iw}(\mathbf{Q}(\zeta_N), \mathbf{Z}_p(1))^{\omega^a}$ constructed using Eisenstein congruences and satisfying the norm relation of an Euler system. Moreover, the image of $\mathcal{C}_{1,a}$ in $H^1_{Iw}(\mathbf{Q}_p, \mathbf{Z}_p(1))^{\omega^a}$ is related to the ω^a-branch of the Kubota-Leopold p-adic L-function.

Remarks: (i)The non-triviality of the classes come from the non triviality of the c_χ's constructed above. The norm relations follow from the very definition of the construction where a normalization factor comes from the ordinary Eisenstein congruence number.

Euler system via Eisenstein congruences

Theorem (U.)

There is a positive answer to three questions above. In other words, let a be an odd integer distinct from 1 modulo $p-1$. For each integer N, the exists a class $\mathcal{C}_{N,a} \in H^1_{Iw}(\mathbf{Q}(\zeta_N), \mathbf{Z}_p(1))^{\omega^a}$ constructed using Eisenstein congruences and satisfying the norm relation of an Euler system. Moreover, the image of $\mathcal{C}_{1,a}$ in $H^1_{Iw}(\mathbf{Q}_p, \mathbf{Z}_p(1))^{\omega^a}$ is related to the ω^a-branch of the Kubota-Leopold p-adic L-function.

Remarks: (i)The non-triviality of the classes come from the non triviality of the c_χ's constructed above. The norm relations follow from the very definition of the construction where a normalization factor comes from the ordinary Eisenstein congruence number.
(ii) On the other hand, proving that the classes are integral is difficult. There are two proofs. One uses the Stickelberger theorem and is therefore not generalizable. The second proof (which is generalizable) uses the local-global compatibility property for the p-adic Langlands correspondence for $GL_2(\mathbf{Q}_p)$ using V. Paškūnas formalism.

Sketch of the construction I

We fix $N > 1$ prime to p and denote by $\mathbf{t}_N$ the Hecke algebra generated by T_ℓ's for ℓ prime to Np. There is a pseudorepresenation

$$t_N \colon \mathbf{G}_\mathbf{Q} \to T_N$$

unramified away from Np and such that $t_N(Frob_\ell) = T_\ell$. We consider $\mathbf{T}_N^{red}$ the maximal quotient of $\mathbf{T}_N$ such that the push forward of t_N to $\mathbf{T}_N^{red}$ becomes reducible after restriction to $G_{\mathbf{Q}_p}$. We have a natural maps

$$\mathbf{T}_N \to \mathbf{T}_N^{red} \to \mathbf{T}_N^{ord}$$

and we set $Q_N := Ker(\mathbf{T}_N \to \mathbf{T}_N^{ord})$ and we define Q_N^{red} similarly.

Sketch of the construction I

We fix $N > 1$ prime to p and denote by $\mathbf{t}_N$ the Hecke algebra generated by T_ℓ's for ℓ prime to Np. There is a pseudorepresenation

$$t_N \colon \mathbf{G}_{\mathbf{Q}} \to T_N$$

unramified away from Np and such that $t_N(Frob_\ell) = T_\ell$. We consider $\mathbf{T}_N^{red}$ the maximal quotient of $\mathbf{T}_N$ such that the push forward of t_N to $\mathbf{T}_N^{red}$ becomes reducible after restriction to $G_{\mathbf{Q}_p}$. We have a natural maps

$$\mathbf{T}_N \to \mathbf{T}_N^{red} \to \mathbf{T}_N^{ord}$$

and we set $Q_N := Ker(\mathbf{T}_N \to \mathbf{T}_N^{ord})$ and we define Q_N^{red} similarly.
Let

$$\lambda_N \colon \mathbf{T}_N \to \Lambda_N := \mathbf{Z}_p[[1 + p\mathbf{Z}_p]][\mathbf{Z}/N\mathbf{Z})^\times]$$

interpolating the Hecke eigenvalues of Eisenstein series.

Sketch of the construction II

Sketch of the construction II

- There exists a canonical exact sequence

$$0 \to \varprojlim_N \Lambda_N \to \varprojlim_N (Q_N \otimes_{\lambda_N} \Lambda_N) \to \varprojlim_N (Q_N^{red} \otimes_{\lambda_N} \Lambda_N) \to 0$$

Sketch of the construction II

- There exists a canonical exact sequence

$$0 \to \lim_{\substack{\leftarrow \\ N}} \Lambda_N \to \lim_{\substack{\leftarrow \\ N}} (Q_N \otimes_{\lambda_N} \Lambda_N) \to \lim_{\substack{\leftarrow \\ N}} (Q_N^{red} \otimes_{\lambda_N} \Lambda_N) \to 0$$

- Using the pseudo-representation t_N, it is possible to construct a canonical element

$$(y_N)_N \in H^1(\mathbf{Q}, \lim_{\substack{\leftarrow \\ N}} Q_N \otimes \Lambda_N(1))$$

Sketch of the construction II

- There exists a canonical exact sequence

$$0 \to \varprojlim_N \Lambda_N \to \varprojlim_N (Q_N \otimes_{\lambda_N} \Lambda_N) \to \varprojlim_N (Q_N^{red} \otimes_{\lambda_N} \Lambda_N) \to 0$$

- Using the pseudo-representation t_N, it is possible to construct a canonical element

$$(y_N)_N \in H^1(\mathbf{Q}, \varprojlim_N Q_N \otimes \Lambda_N(1))$$

The difficulty left is to show that $Q_N^{red} \otimes_{\lambda_N} \Lambda_N$ is annihilated by an element $\mathcal{L}_N \in \Lambda_N$ defined such that for all even character χ of level Np^∞ with $\chi|_{(\mathbf{Z}/p\mathbf{Z})^\times} \neq 1$, we have

$$\chi(\mathcal{L}_N) = L^{Np}(1,\chi) \prod_{\ell | N} (1 - \chi(\ell)^{-1})$$

Sketch of the construction III

Using some local-global compatibility with p-adic Landlands correspondence, we can replace $Q_N \otimes \Lambda_N$ by a suitable quotient such that the exact sequence still holds and the corresponding co-kernel is killed by $\mathcal{L}_N$.

Sketch of the construction III

Using some local-global compatibility with p-adic Landlands correspondence, we can replace $Q_N \otimes \Lambda_N$ by a suitable quotient such that the exact sequence still holds and the corresponding co-kernel is killed by $\mathcal{L}_N$.

Let us call y'_N the projection of y_N the Galois cohomology of this quotient. Then, we have

$$C_{N,a} := e_{\omega^a} \cdot \mathcal{L}_N \cdot y'_N \in H^1(\mathbf{Q}, \Lambda_N(1))^{\omega^a} = H^1_{Iw}(\mathbf{Q}(\zeta_N), \mathbf{Z}_p(1))^{\omega^a}$$

Sketch of the construction III

Using some local-global compatibility with p-adic Landlands correspondence, we can replace $Q_N \otimes \Lambda_N$ by a suitable quotient such that the exact sequence still holds and the corresponding co-kernel is killed by $\mathcal{L}_N$.

Let us call y'_N the projection of y_N the Galois cohomology of this quotient. Then, we have

$$C_{N,a} := e_{\omega^a} \cdot \mathcal{L}_N \cdot y'_N \in H^1(\mathbf{Q}, \Lambda_N(1))^{\omega^a} = H^1_{Iw}(\mathbf{Q}(\zeta_N), \mathbf{Z}_p(1))^{\omega^a}$$

The classes are integral and the norm relation will follow from the one satisfied by $\mathcal{L}_N$:

$$\pi_{N,\ell}(\mathcal{L}_{N\ell}) = (1- < \ell >_N^{-1}) \cdot \mathcal{L}_N$$

where $\pi_{N,\ell}$ is the projection $\Lambda_{N\ell} \to \Lambda_N$.

THANK YOU !