Introduction to Herbrand-Ribet theorem

唐一萌

2022/4/29

Main result

Let p be an odd prime number, and A the ideal class group of $\mathbb{Q}(\mu_p)$. C denotes the $\mathbb{F}_p$ vector space A/A^p, we know that dimension of C equals the p-rank of A.

Write Δ for $Gal(\mathbb{Q}(\mu_p)/\mathbb{Q})$. Denoted the cyclotomic character by $\chi : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to \Delta \to \mathbb{F}_p^*$. χ can be seen as the generator of the dual of Δ.

Δ acts on C naturally. Because Δ is cyclic, $\mathbb{F}_p[\Delta] \cong \mathbb{F}_p[x]/(x^{p-1} - 1)$ is semi simple, each simple module over $\mathbb{F}_p[\Delta]$ is 1-diemensional, and we have the following decomposition:

$$C = \bigoplus_i C(\chi^i)$$

where $C(\chi^i)$ is the maximal submodule of C, that Δ acts on it through χ^i.

Main result

The k-th Bernoulli number B_k is given by the expansion:

$$\frac{t}{e^t - 1} + \frac{t}{2} - 1 = \sum_{n \geqq 2} \frac{B_n}{n!} t^n$$

The main result of this article is the following theorem:

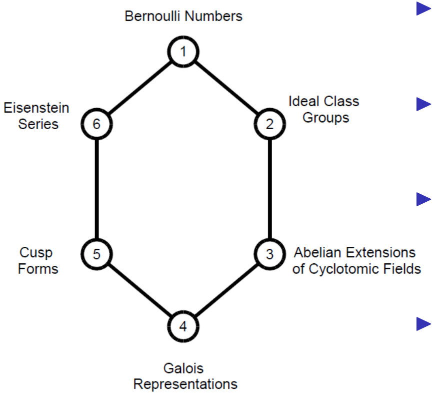
Theorem 1 (Ribet)

Let k be even, $2 \leqq k \leqq p - 3$. Then $p \mid B_k \iff C(\chi^{1-k}) \neq 0$

Corollary 1 (Kummer)

An odd prime number p is irregular $\iff$ there exists some even integer k with $2 \leqq k \leqq p - 3$, such that p divides (the numerator of) the k-th Bernoulli number B_k.

Scketch of the proof



- Note that B_k arises naturally in the constant term of q-expansion of Eisenstein series.
- Using the condition $p \mid B_k$, Ribet constructs a new form of weight 2 and level p, congruent to Eisenstein series.
- The Galois representation (reduction with suitable lattice) associated with this new form, cut out some unramified abelian extension of $\mathbb{Q}(\mu_p)$.
- By class field theory, this ensures the part of C we want is nontrivial.

$3 \to 2$: From class field to ideal class group

$$
\begin{tikzcd}
E \arrow[d, dash] \arrow[d, dash, bend right=60, "H"'] \arrow[dd, dash, bend left=60, "G"] \\
\mathbb{Q}(\mu_p) \arrow[d, dash] \\
\mathbb{Q}
\end{tikzcd}
$$

Theorem 2

Suppose $p \mid B_k$. Then there exists a Galois extension $E/\mathbb{Q}$ containing $\mathbb{Q}(\mu_p)$ with the following properties:

i: *The extension $E/\mathbb{Q}(\mu_p)$ is unramified.*

ii: *The group H is a non-zero abelian group of type $(p, \dots, p)$, i.e., killed by p.*

iii: *If $\sigma \in G$ and $\tau \in H$, then $\sigma\tau\sigma^{-1} = \chi(\sigma)^{1-k} \cdot \tau$.*

From class field to ideal class group: Theorem 2 $\to$ theorem 1

$$\begin{tikzcd} E \arrow[d, dash] \arrow[d, dash, bend right, "H"'] \arrow[dd, dash, bend left=60, "G"] \\ \mathbb{Q}(\mu_p) \arrow[d, dash] \\ \mathbb{Q} \end{tikzcd}$$

Proof

By i, E is contained in the Hilbert class field of $\mathbb{Q}(\mu_p)$. Combined with ii and iii, its Artin map ϕ can be formulated like:

$$\textit{idele class group} \to A \to A/A^p \to Gal(E/\mathbb{Q}(\mu_p)) = H$$

By "functoriality" of class field theory, given an idele α of $\mathbb{Q}(\mu_p)$ and $\sigma \in \Delta = Gal(\mathbb{Q}(\mu_p)/\mathbb{Q})$, $\phi(\sigma\alpha) = \tilde{\sigma}\phi(\alpha)\tilde{\sigma}^{-1}$ for any lift $\tilde{\sigma} \in G$ of σ.

In abstract language, if we define an action of Δ acts on H like: given $h \in H, \sigma \in \Delta$, then $\sigma h = \tilde{\sigma} h \tilde{\sigma}^{-1}$ for any lift $\tilde{\sigma} \in G$. Then the last paragraph is saying that, Artin map is a homomorphism of Δ-modules. Then using Schur lemma, we now know Artin map factor through $C(\chi^{1-k})$ like:

$$A \to A/A^p \to C(\chi^{1-k}) \to Gal(E/\mathbb{Q}(\mu_p)) = H$$

Since E is not a trivial extension, $C(\chi^{1-k})$ is not trivial.

Theorem 3

Suppose $p \mid B_k$. Then there exists a finite field $\mathbb{F} \supseteq \mathbb{F}_p$ and a continuous representation

$$\bar{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbf{GL}(2, \mathbb{F})$$

with the properties:

- i *$\bar{\rho}$ is unramified at all primes $l \neq p$.*
- ii *The representation $\bar{\rho}$ is reducible (over $\mathbb{F}$) in such a way that $\bar{\rho}$ is isomorphic to a representation of the form*

  $$\begin{pmatrix} 1 & * \\ 0 & \chi^{k-1} \end{pmatrix}$$

  That is, $\bar{\rho}$ is an extension of the 1-dimensional representation with character χ^{k-1} by the trivial 1-dimensional representation.
- iii *The image of $\bar{\rho}$ has order divisible by p. In other words, $\bar{\rho}$ is not diagonalizable.*
- iv *Let D be a decomposition group for p in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Then $\bar{\rho}(D)$ has order prime to p, i.e., $\bar{\rho} \mid D$ is diagonalizable.*

Proof

Denoted by L_k the subfield of $\mathbb{Q}(\mu_p)$ corresponding to the kernel in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ of χ^{1-k}.

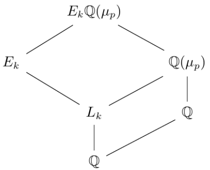
We first prove theorem 2 with $\mathbb{Q}(\mu_p)$ replaced by L_k, E replaced by E_k, then verify that the extension $\mathbb{Q}(\mu_p)E_k/\mathbb{Q}(\mu_p)$ satisfies properties in theorem 2.

Denoted by E_k the field cut out by $\bar{\rho}$. First note the map: $im(\bar{\rho}) \to \mathbb{F}^*$, $\begin{pmatrix} 1 & * \\ 0 & \chi^{k-1} \end{pmatrix} \mapsto \chi^{k-1}$ is a group homomorphism, with ker matrices like $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$. By Galois correspondence, E_k contains L_k and $Gal(E_k/L_k)$ is matrices like $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$ in $im(\bar{\rho})$, which is a group of $(p, \cdots, p)$ type. And we can verify iii of theorem 2 by the formula:
$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}^{-1} = \begin{pmatrix} 1 & ad^{-1}x \\ 0 & 1 \end{pmatrix}.$$

From Galois representation to class field: Theorem 3 $\rightarrow$ theorem 2

It remains to show E_k/L_k unramifies in place p (the only place of L_k over p). But every elements of $Gal(E_k/L_k)$ is of order p, thus by iv of theorem 3, the decomposition group over p (in $Gal(E_k/L_k)$) is trivial.

Now we passage to $\mathbb{Q}(\mu_p)E_k/\mathbb{Q}(\mu_p)$



$\mathbb{Q}(\mu_p)/L_k$ is unramified at any places over $l \neq p$, then so do $\mathbb{Q}(\mu_p)E_k/\mathbb{Q}(\mu_p)$. A decomposition group over place p of $Gal(\overline{\mathbb{Q}}/\mathbb{Q}(\mu_p))$ can be seen as subgroup of the decomposition group over p in $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$. Thus the previous analysis on the order of decomposition group remains valid.

ii of theorem 2 is obtained by observation on degree of field extension.

iii of theorem 2 follows from $E_k \cap \mathbb{Q}(\mu_p) = L_k$.

Theorem 4 (Ribet)

Suppose that $p \mid \mathrm{B}_k$. There exist a normalised cuspidal eigenform $f \in \mathbf{S}_2(p, \varepsilon), f = \sum_{n>0} a_n q^n$. ε is not trivial. And there is a prime $\mathfrak{p} \mid p$ of the number field K_f generated by all a_n, such that for every prime $l \neq p$, the number a_l is $\mathfrak{p}$-integral and

$$a_l \equiv 1 + l^{\,k-1} \equiv 1 + \varepsilon(l) l (\operatorname{mod} \mathfrak{p})$$

Note that K_f is a number field and that ε may be thought of as taking values in $\mathrm{K}_f^\times$, for K_f contains $\mathbb{Q}(\varepsilon)$, the number field generated by the values of ε.

Laterly we will show there is a Galois representation associated to this form, having the properties $(i) - (iv)$ of Theorem 3.

We have the following Eisenstein series of weight k and level 1 :

$$G_k = -\frac{B_k}{2k} + \sum_{n\geq 1}\sum_{d|n} d^{\,k-1} q^n \quad \text{for } k \geq 4$$

By the q-expansion principle, reduction of G_k *mod p* is a eigenform form in $S_k(1, \mathbb{F}_p)$. Now using the following lifting lemma, we find a cusp form of level 1 congruent to G_k *mod p*.

Theorem 5 (Deligne, Serre)

Let M be a free module of finite rank over a discrete valuation ring R with residue field k, fraction field K and maximal ideal $\mathfrak{m}$. Let S be a (possibly infinite) set of commuting R-endomorphisms of M. Let $0 \neq f \in M$ be an eigenvector modulo $\mathfrak{m}M$ for all operators in S, i.e., $Tf = a_T\, f\, mod \mathfrak{m} \forall T \in S$ $(a_T \in R)$. Then there exists a DVR $R\,'$ containing R with maximal ideal $\mathfrak{m}\,'$ containing $\mathfrak{m}$, whose field of fractions $K\,'$ is a finite extension of K and a non-zero vector $f\,' \in R' \otimes_R M$ such that $Tf\,' = a'_T f\,'$ for all $T \in S$ with eigenvalues a'_T satisfying $a'_T \equiv a_T \bmod \mathfrak{m}'$.

Key idea in Deligne and Serre's proof

$$\begin{array}{ccc}
\left\{\begin{array}{c}\text{normalized eigenforms in}\\ S_2(\Gamma,\bar{K})\text{ modulo }G_K\text{-conjugacy}\end{array}\right\} & \to & \left\{\begin{array}{c}\text{normalized eigenforms in}\\ S_2(\Gamma,\bar{k})\text{ modulo }G_k\text{-conjugacy}\end{array}\right\}\\
\downarrow & & \downarrow\\
\{\text{maximal ideals of } \mathbb{T}_K\} & & \{\text{maximal ideals of } \mathbb{T}_k\}\\
\updownarrow & & \updownarrow\\
\{\text{minimal primes of } \mathbb{T}_{\mathcal{O}}\} & \twoheadrightarrow & \{\text{maximal primes of } \mathbb{T}_{\mathcal{O}}\}
\end{array}$$

Example

Consider the case of level 1 and weight 12. In this case

$$\mathcal{M}_{12}(1) = \mathcal{E}_{12}(1) \oplus \mathcal{S}_{12}(1),$$

where $\mathcal{G}_{12}(1)$ is one-dimensional, spanned by

$$G_{12} = \frac{691}{32760} + \sum_{n=1}^{\infty}\left(\sum_{d|n} d^{11}\right) q^n = \frac{691}{32760} + q + 2049q^2 + 177148q^3 + \cdots ,$$

and $\mathcal{S}_{12}(1)$ is also one-dimensional, spanned by Ramanujan's famous cusp form

$$\Delta(\tau) = q\prod_{n=1}^{\infty}(1-q^n)^{24} = \sum_{n=1}^{\infty}\tau(n)q^n = q - 24q^2 + 252q^3 + \cdots .$$

Then these two forms are congruent mod 691, and not congruent mod any other prime number.

Remark

- Congruence of modular forms and Eisenstein series can be rephrased in language of Eisenstein ideals.
- Hida and Mazur considered congruence of modular forms under the more general framework of p-adic modualr forms, which leads to the deformation theory of Galois representation.

Defination 1

A λ-adic Galois representation is a continuous homomorphism $G_{\mathbb{Q}} \to \mathbf{GL}(d, K_\lambda)$, unramified at all but finitely many primes, where K_λ is a finite extension of $\mathbb{Q}_p$.

Denoted by $\mathscr{O}$ the rings of intergers of K_λ, and λ the maximal ideal of $\mathscr{O}$, residue field k.

Because the image of a λ-adic representation is compact, it's not hard to show that each matrix lying in the image is with det beloinging to $\mathscr{O}^*$. This implies we can do reduction to these representation.

Reduction of λ-adic Galois representation

Following previous notations. If $\rho : G_{\mathbb{Q}} \to \mathbf{GL}(d, K)$ is an λ-adic representation, then the image of ρ is compact, and there is at least one $G_{\mathbb{Q}}$-stable $\mathscr{O}$-lattice, i.e. ρ can be conjugated to a homomorphism $G_{\mathbb{Q}} \to GL_d(\mathcal{O})$.

Here by a $\mathscr{O}$-lattice we mean a sub free $\mathscr{O}$-module generated by some K-basis of K^n. If $\Lambda \subset \mathrm{V}$ is any $\mathscr{O}$-lattice, the subgroup $\mathrm{H} = \rho^{-1}(\mathrm{GL}(\Lambda))$ is open in $G_{\mathbb{Q}}$, hence the index $(G_{\mathbb{Q}} : \mathrm{H})$ is finite, and the $\mathscr{O}$-lattice $\sum_{\sigma \in G/H} \sigma(\Lambda)$ is$G_{\mathbb{Q}}$-stable.

Reducing modulo the maximal ideal λ gives a residual representation $\bar{\rho} : G_{\mathbb{Q}} \to \mathbf{GL}(d, k)$. This representation may depend on the particularly chosen $G_{\mathbb{Q}}$-stable lattice of ρ , but its semisimplification $\bar{\rho}^{ss}$ (i.e. the unique semi-simple representation with the same Jordan-Hölder factors) is uniquely determined by ρ by Brauer-Nesbitt theorem.

We'd like to rephrase the reduction of λ-adic representation in a more direct way. That is to find a matrix $\alpha \in \mathbf{GL}(d, K)$, such that $\alpha \rho \alpha^{-1}$ has image in $\mathbf{GL}(d, \mathscr{O})$. Then we can reduce those image matrixes in the natural way.

A useful lemma for reduction of λ-adic Galois representation

Lemma 1 (Ribet)

Suppose that the degree-2 λ-adic representation ρ of $G_{\mathbb{Q}}$ is simple but $\bar{\rho}$ is not simple. Then, for any ordering φ_1, φ_2 of the two characters of which $\bar{\rho}^{ss}$ is the direct sum, there is a $G_{\mathbb{Q}}$-stable $\mathscr{O}$-lattice $\Lambda \subset \mathrm{V}$ such that $\rho_\Lambda \sim \begin{pmatrix} \varphi_1 & * \\ 0 & \varphi_2 \end{pmatrix}$, as opposed to $\begin{pmatrix} \varphi_1 & 0 \\ * & \varphi_2 \end{pmatrix}$, and such that ρ_Λ is not semisimple, i.e., $\rho_\Lambda \not\cong \varphi_1 \oplus \varphi_2$.

Proof

From $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} d & c \\ 0 & a \end{pmatrix}$, *we can interchange the ordering of two characters. By the formula* $\begin{pmatrix} 1 & 0 \\ 0 & \pi \end{pmatrix} \begin{pmatrix} a & \pi b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & \pi \end{pmatrix}^{-1} = \begin{pmatrix} a & b \\ \pi c & d \end{pmatrix}$, *we can assume reduction matixes are upper triangular instead of lower, i.e. images of ρ lie in* $\begin{pmatrix} \mathscr{O}^* & \mathscr{O} \\ p\mathscr{O} & \mathscr{O}^* \end{pmatrix}$ *and 1-2 elements of them is not always zero. Now we can do conjugation by* $\begin{pmatrix} 1 & 0 \\ 0 & \pi \end{pmatrix}$ *enough many times , keeps images of representation still in* $\begin{pmatrix} \mathscr{O}^* & \mathscr{O} \\ p\mathscr{O} & \mathscr{O}^* \end{pmatrix}$, *but there are some matrix in this image with 1-2 elements in $\mathscr{O}^*$.*

$5 \to 4$: Construct Galois representation from new form

Let $N, k \geq 1$, and f be a weight k new form of $\Gamma_0(N)$. Let (c_p, ε) be its associated system of eigenvalues and Nebentypus. Let K_f be the subfield of C generated by the c_p and the values of ε, one can show K_f is a number field. Let K be any subfield of $\mathbb{C}$ containing K_f and is finite over $\mathbb{Q}$.

Let ℓ be a prime.

Theorem 6 (Deligne-Serre-Shimura)

There exists a (continuous) representation

$$\rho_\ell : G_{\mathbb{Q}} \to GL(2, K_f \otimes \mathbb{Q}_\ell)$$

with the following properties: If $p \nmid N\ell$ is a prime number, then ρ is unramified at p, and the image under ρ_ℓ of any Frobenius element for p is a matrix with trace c_p and determinant $\varepsilon(p)p^{k-1}$.

Note that $K_f \otimes \mathbb{Q}_\ell = \prod_{\lambda|\ell} K_{f,\lambda}$. Thus $\rho_\ell = \oplus_{\lambda|\ell}\rho_\lambda$

Theorem 7 (Ribet)

Representations constructed in last theorem are absolutely irreducible.

Proof

Following notations from last theorem.

$4 \to 3$: The representation from our new form

Recall that in theorem 4, from assumption $p \mid \mathrm{B}_k$, Ribet construct a new form f of weight 2 , level p, and character ε. And there exists a prime $\mathfrak{p} \mid p$ of field K_f such that for every prime number $\ell \neq p$, the number a_l is $\mathfrak{p}$-integral and

$$a_\ell \equiv 1 + \ell^{\,k-1} \equiv 1 + \varepsilon(\ell)\ell (\mathrm{mod} \mathfrak{p})$$

Now we considered the $\mathfrak{p}$-adic representation associated to this form.

Theorem 8

Their is some reduction of this Galois representation satisfys properties required in theorem 3.

Proof

By congruent property on q-coefficients of this form, under (any) reduction representation, Frobenius of ℓ acts with trace $\ell^{k-1} + 1$ and det $\ell^k - 1$. By Cebotarev density theorem, we know semi-simplification of any reduction representation is isomorphic to $\begin{pmatrix} 1 & 0 \\ 0 & \chi^{k-1} \end{pmatrix}$. Combined with Ribet's lemma, we only need to verify (iv) of theorem 3. Before that, we give 2 useful facts.

Two useful facts

Proposition 1 (Deligne-Rapoport)

Suppose that ε is not trivial. Then abelian variety A_f acquires good reduction at the unique prime dividing p in the maximal totally real subfield $\mathbb{Q}(\mu_p)^+ \subset \mathbb{Q}(\mu_p)$.

Proposition 2 (Raynaud)

Suppose that the ramification index of $K \mid \mathbb{Q}_p$ is $< p-1$. Let G be a finite flat commutative group scheme over K, killed by a power of p. There is at most one finite flat extension of G to $\mathscr{O}_K$.

Remark

- *Fontaine has some result on case of p=2.*
- *Tate wrote and English explanition of Raynaud's result in book <Modular forms and Fermat's last theorem>.*

Verify (iv) of theorem 3

Proof

Denoted by D_p a decomposition group of p in $G_{\mathbb{Q}}$. We denote the field $\mathbb{Q}(\mu_p)^+$ by K, and $\mathfrak{p}'$ its unique prime over p, and decomposition group over $\mathfrak{p}'$ by D, and its completion at place $\mathfrak{p}$ by L. It's not hard to see that $(D_p : D)$ is prime to p, thus we only need to prove the restriction of ρ on D is semisimple.

Recall that in Shimura's construction, The Tate module $\mathcal{T}_p(A_f) \otimes \mathbb{Q}_p$ is a rank2 free $K_f \otimes \mathbb{Q}_p$-module. Some quotient of the former is rank 2 free $K_{f,\mathfrak{p}}$-module. After substituting A_f with an abelian variety A isogenous to it, we can assume O_f lies in the endomorphism ring of A, and the kernel of $\mathcal{T}_p(A_f) \otimes K_{f,\mathfrak{p}}$ is canonically isomorphic to $A[\mathfrak{p}]$. We can suppose the lattice we choose to do reduction is $\mathcal{T}_p(A_f) \otimes O_{f,\mathfrak{p}}$. Then reduction representation is isomorphic to $A[\mathfrak{p}](\overline{\mathbb{Q}})$ as rank 2 free $O_{f,\mathfrak{p}}/\mathfrak{p}$-module (denoted this module by M, and the residue field by F).

Suppose $\mathscr{A}$ is the Neron model of A over $\mathscr{O}_L$. We use $\mathscr{A}[\mathfrak{p}]$ to get extra information about $A[\mathfrak{p}]$ (good reduction ensures the former is finite flat). Denoted by $\mathcal{M}$ the schematic closure of M in $\mathscr{A}[\mathfrak{p}]$. By Raynaud's result, we have 1-1 correspondence between submodules of M and sub group schemes of $\mathscr{A}[\mathfrak{p}]$.

Verify (iv) of theorem 3

We know that ρ, and hence $\rho|_{\mathrm{D}}$, is isomorphic to $\begin{pmatrix} 1 & * \\ 0 & \chi^{k-1} \end{pmatrix}$. Let $\mathrm{X} \subset A[p]$ be an F-line on which D acts trivially, so that D acts via χ^{k-1} on the F-line $\mathrm{Y} = \mathrm{M}/\mathrm{X}$; in particular, Y is ramified.

Let $\mathcal{X}$ be the schematic closure of X in $\mathcal{M}$. As the absolute ramification index $(p-1)/2$ of L is $< p-1$, the group scheme $\mathcal{X}$ is constant. It follows that $\mathcal{M}$ cannot be connected, for it has the étale subgroup scheme $\mathcal{X}$ (of order > 1).

Now, the group scheme $\mathcal{M}$ is an F-space scheme. Let M^0 be the sub F[D]-module of M coming from the identity component of $\mathcal{M}$, so that M/M^0 is unramified.

We have $\mathrm{M}^0 \neq \mathrm{M}$, because $\mathcal{M}$ is not connected, as we have seen. We have $M^0 \neq 0$ because M/M^0 is unramified whereas M is not (for it has the quotient Y which is ramified). For the same reason, $\mathrm{M}^0 \neq \mathrm{X}$, because M/M^0 is unramified whereas $\mathrm{Y} = \mathrm{M}/\mathrm{X}$ is ramified. Thus X and M^0 are two distinct D-stable F-lines in M, and hence the D-module M is semisimple, which was to be shown.

- Ribet considered method to raise level and decrease weight in his invent 100.
- It seems nowadays by Faltings' work on crystalline representation, it's possible to substitute the modular form we use by higher weight ones.