BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 48, Number 2, April 2011, Pages 281–284
S 0273-0979(2011)01330-1
Article electronically published on January 11, 2011

SELECTED MATHEMATICAL REVIEWS

related to the paper in the previous section by
BARRY MAZUR

MR0419403 (54 #7424) 12A35; 10D05

Ribet, Kenneth A.

A modular construction of unramified p-extensions of $Q(\mu_p)$.

Inventiones Mathematicae **34** (1976), *no.* 3, 151–162.

An odd prime p is said to be irregular if the class number of the field $Q(\mu_p)$ is divisible by p (μ_p being the group of pth roots of unity). The purpose of the present paper is to strengthen Kummer's criterion that p is irregular if and only if there exists an even integer k with $2 \leq k \leq p-3$ such that p divides (the numerator of) the kth Bernoulli number B_k. Let A be the ideal class group of $Q(\mu_p)$, and let C be the F_p-vector space A/A^p. The vector space C has a canonical decomposition $C = \bigoplus_{i \bmod (p-1)} C(\chi^i)$, where $C(\chi^i) = \{c \in C | \sigma c = \chi^i(\sigma)c$ for all $\sigma \in \mathrm{Gal}(Q(\mu_p)/Q)\}$ and $\chi\colon \mathrm{Gal}(Q(\mu_p)Q) \xrightarrow{\sim} {F_p}^*$ is the standard character. The author's main result is as follows: Let k be even, $2 \leq k \leq p-3$; then $p|B_k$ if and only if $C(\chi^{1-k}) \neq 0$. This is the familiar consequence of the conjecture that p is prime to the class number of the real subfield $Q(\mu_p)^+$ of $Q(\mu_p)$ [J. Herbrand, J. Math. Pures Appl. (9) **11** (1932), 417–441; Zbl. **6**, 8]. The significant achievement of the paper is in the fact that the main result is proved without making any supplementary hypothesis.

From MathSciNet, December 2010

V. V. Sokurov

MR0742853 (85m:11069) 11R23; 11G05

Mazur, B.; Wiles, A.

Class fields of abelian extensions of Q.

Inventiones Mathematicae **76** (1984), *no.* 2, 179–330.

The authors prove the Main Conjecture of Iwasawa theory for real abelian extensions of $\mathbf{Q}$ and odd primes p. Namely, let χ be an even, primitive, Dirichlet character, with values in $\overline{\mathbf{Q}}_p^*$. Let $\mathfrak{O}$ be the integer ring of the extension of $\mathbf{Q}_p$ which is generated by the values of χ. Assuming that χ is nontrivial and of conductor not divisible by p^2, the Leopoldt-Kubota p-adic L-function $L_p(s, \chi)$ defines a certain principal ideal $(G(T))$ of the power series ring $\mathfrak{O}[[T]]$. The Main Conjecture states that this ideal coincides with the ideal generated by the "characteristic polynomial" $F(T)$ of a suitable Iwasawa module made using the ideal class groups of abelian extensions of $\mathbf{Q}$.

To prove it, one has, in the end, to produce unramified extensions of abelian fields, given p-power divisibilities of numbers of the form $L(-1, \theta)$, where θ is a Dirichlet character related to χ: one considers characters θ of the form $\chi\omega^{-2}\varepsilon$,

where ω is the Teichmuller character and ε is a character of p-power order and p-power conductor. This was first done by the reviewer [same journal 34 (1976), no. 3, 151–162; MR0419403 (54 #7424)], who considered p-divisibilities of L-values, and characters θ which are powers of ω. He obtained his unramified extensions by regarding the action of $G = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on the group of p-power torsion points of the Jacobian $J_1(p)$ of the modular curve $X_1(p)$. Each divisibility $p|L(-1,\omega^t)$ was shown to imply a congruence between a cusp form and an Eisenstein series, which could be translated into information about the action of G.

Subsequently, Wiles considered divisibilities of these same L-values by higher powers of p [ibid. 58 (1980), no. 1, 1–35; MR0570872 (82j:12009)]. His article made use of many of the techniques employed by Mazur in his study of $J_0(p)$ [Inst. Hautes Etudes Sci. Publ. Math. No. 47 (1977), 33–186; MR0488287 (80c:14015)]. Especially, Wiles exploited systematically the cuspidal divisor class group in $J_1(p)$, thus obviating the necessity of considering Eisenstein series and congruences linking them with cusp forms. (The divisor class group had been analyzed by D. Kubert and S. Lang [cf. Modular units, Springer, New York, 1981; MR0648603 (84h:12009)].) Wiles's article introduced many of the key constructions which are refined and generalized in the present work.

Although it is impossible to summarize these constructions in a short review, this important article has already been the subject of longer expository accounts. (See the report by J. Coates [Bourbaki seminar, Vol. 1980/81 (French), 220–242, Lecture Notes in Math., 901, Springer, Berlin, 1981; MR0647499 (83i:12005)] and the exposition of Lang [Bull. Amer. Math. Soc. (N.S.) 6 (1982), no. 3, 253–316; MR0648522 (83m:12002)].) Furthermore, the authors have done a superb job in orienting the reader: their introduction explains very well the general strategy of the proof, while Chapter I contains precise statements of the results they obtain directly, together with a derivation of the Main Conjecture from these results. In addition, the authors include an appendix on Fitting ideals, the technical tool used to obtain information about the basic Iwasawa module they work with, given information about certain of its quotients.

It is perhaps worth mentioning that the authors' proof required detailed knowledge of the behavior of the modular curves $X_1(N)$ ($N \geq 1$) at primes dividing N. A complete study of such questions, using techniques of Drinfeld, was accordingly undertaken by Mazur, in collaboration with N. Katz [see Arithmetic moduli of elliptic curves, Ann. Math. Stud., 108, Princeton Univ. Press, Princeton, N.J., 1985].

Secondly, a forthcoming article by Wiles proves a result approximating the Main Conjecture with the base field $\mathbf{Q}$ replaced by a totally real field F of odd degree over $\mathbf{Q}$. This article shows, in particular, that the cuspidal divisor class group may be excised from the proof of the Main Conjecture, with congruences among modular forms again playing their initial role. The point is that the modular curves used in the case $F = \mathbf{Q}$ are generalized by certain Shimura curves, which have no cusps for $F \neq \mathbf{Q}$.

From MathSciNet, December 2010

Kenneth A. Ribet

MR1802388 (2002e:11143) 11R18; 11F80

Khare, Chandrashekhar

Notes on Ribet's converse to Herbrand.

Cyclotomic fields and related topics (Pune, 1999), 273–284, *Bhaskaracharya Pratishthana, Pune*, 2000.

Let p be an odd prime and ζ_p a primitive pth root of unity. Kummer's criterion states that there is a non-principal ideal in $\mathbb{Z}[\zeta_p]$ whose pth power is principal if and only if p divides the numerator of a Bernoulli number B_k for some even $2 \leq k \leq p-3$. Let A be the ideal class group of $\mathbb{Z}[\zeta_p]$ and let $C = A/A^p$. It is a module for the action of $G = \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \simeq (\mathbb{Z}/p)^\times$ and so can be decomposed into eigenspaces

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

indexed by the characters of G. Here χ is the mod p cyclotomic character defined by $g \cdot \zeta_p = \zeta_p^{\chi(g)}$. Herbrand showed that if $C(\chi^{1-k}) \neq 0$, then $p \mid B_k$. About 25 years ago, K. A. Ribet [Invent. Math. **34** (1976), no. 3, 151–162; MR0419403 (54 #7424)] proved the converse of this result by a beautiful use of the geometry of modular curves and congruences between modular forms. Ribet's theorem led to many further developments and eventually to a proof of the "Main Conjecture" of Iwasawa theory by B. C. Mazur and A. J. Wiles [Invent. Math. **76** (1984), no. 2, 179–330; MR0742853 (85m:11069)]. The technology of congruences and the knowledge of the Galois representations attached to modular forms has advanced considerably since then and it eventually culminated in the astounding work of Wiles and Taylor-Wiles.

In this expository note, the author outlines a proof of Ribet's theorem using results on algebraic Hecke characters, an observation of K. Joshi [see also J.-P. Serre, in *Séminaire Delange-Pisot-Poitou: 1967/68, Théorie des Nombres, Fasc. 1, Exp. 14*, 17 pp, Secrétariat Math., Paris, 1969; MR0244147 (39 #5464)] to get the crucial congruence between a cusp form and an Eisenstein series, and results of G. Faltings and B. W. Jordan [Israel J. Math. **90** (1995), no. 1-3, 1–66; MR1336315 (96g:11055)] and of J.-M. Fontaine and G. Laffaille [Ann. Sci. École Norm. Sup. (4) **15** (1982), no. 4, 547–608 (1983); MR0707328 (85c:14028)]. The style of the paper makes for pleasant reading.

From MathSciNet, December 2010

V. Kumar Murty

MR1997986 (2004h:20064) 20G25

Bellaïche, Joël

À propos d'un lemme de Ribet.

Rendiconti del Seminario Matematico della Universita di Padova. **109** (2003), 45–62.

In this paper, the following situation is considered. We denote by G a group, by R a discrete valuation ring with fraction field K and residue field k, by ρ a finite-dimensional representation of G over K admitting a stable R-lattice. The character of ρ takes values in R, and the set $\{\overline{\rho}_1, \ldots, \overline{\rho}_r\}$ of isomorphism classes of Jordan-Hölder factors of the k-representation $\overline{\rho}_\Lambda$ of G over $\Lambda \otimes k$ induced by ρ

is independent of the choice of the stable lattice Λ. The question is the following: which nontrivial extensions among the representations $\overline{\rho}_1, \ldots, \overline{\rho}_r$ can arise as a subquotient of $\overline{\rho}_\Lambda$ for a stable lattice Λ?

To prove the converse of Herbrand's theorem, K. A. Ribet [Invent. Math. **34** (1976), no. 3, 151–162; MR0419403 (54 #7424)] considered the case when ρ is a two-dimensional irreducible representation and the factors $\overline{\rho}_1$ and $\overline{\rho}_2$ of $\overline{\rho}_\Lambda$ are characters. Then he showed the existence of a lattice Λ such that ρ_Λ is a nontrivial extension of $\overline{\rho}_1$ by $\overline{\rho}_2$ (resp. $\overline{\rho}_2$ by $\overline{\rho}_1$).

Let us now state the main result of the paper, which generalizes Ribet's statement above. We define an oriented graph Γ whose set of vertices is $\{\overline{\rho}_1, \ldots, \overline{\rho}_r\}$, with an edge from $\overline{\rho}_i$ to $\overline{\rho}_j$ if there exists a lattice Λ stable under ρ such that $\overline{\rho}_\Lambda$ admits a subquotient isomorphic to a nontrivial extension of $\overline{\rho}_j$ by $\overline{\rho}_i$.

Theorem. If ρ is irreducible then Γ is connected as an oriented graph.

The author ["Congruences endoscopiques et representations galoisiennes", thse, Univ. Paris Sud, Orsay, 2002] proved this theorem under the multiplicity-one assumption on $\overline{\rho}_\Lambda$ in order to establish the existence of nontrivial extensions of Galois characters as predicted by the Bloch-Kato conjectures. The proof of the theorem involves more precisely the structure of the nonempty set of all lattices stable under ρ (up to the action of K^*) as a subset of the building of the linear group over K as constructed by F. Bruhat and J. Tits [Inst. Hautes Études Sci. Publ. Math. No. 41 (1972), 5–251; MR0327923 (48 #6265)]. To this extent, part 3 of the paper is a useful dictionary of geometric interpretations of algebraic properties of ρ.

From MathSciNet, December 2010

Philippe Graftieaux