PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 126, Number 5, May 1998, Pages 1315–1320
S 0002-9939(98)04196-3

A NOTE ON GREENBERG'S CONJECTURE AND THE ABC CONJECTURE

HUMIO ICHIMURA

(Communicated by William W. Adams)

ABSTRACT. For any totally real number field k and any prime number p, Greenberg's conjecture for (k,p) asserts that the Iwasawa invariants $\lambda_p(k)$ and $\mu_p(k)$ are both zero. For a fixed real abelian field k, we prove that the conjecture is "affirmative" for infinitely many p (which split in k) if we assume the *abc* conjecture for k.

1. INTRODUCTION

For a number field k and a prime number p, let k_∞/k be the cyclotomic $\mathbb{Z}_p$-extension over k with its nth layer k_n ($k_0 = k$). Let A_n be the Sylow p-subgroup of the ideal class group of k_n and $A_\infty = \varprojlim A_n$ the projective limit w.r.t. the relative norms. We denote by $\lambda_p = \lambda_p(k)$ and $\mu_p = \mu_p(k)$ the Iwasawa λ-invariant and the μ-invariant associated to A_∞, respectively. Greenberg's conjecture for k and p asserts that $\lambda_p = \mu_p = 0$ for any totally real number field k and any p (cf. [Iw], p. 316, [Gr]). It is well known that the conjecture is valid if (1) there is only one prime ideal of k over p and it is totally ramified in k_∞ and further (2) $A_0 = \{1\}$ (cf. [W], Proposition 13.22). In particular, $\lambda_p(\mathbb{Q}) = \mu_p(\mathbb{Q}) = 0$ for all p. Further, it is known that $\mu_p = 0$ when k is abelian over $\mathbb{Q}$ (cf. [FW]). But, the conjecture for general k and p is far from being settled in spite of the efforts of several authors (see [IS] and its references).

In this note, we consider the following subproblem: "*For a fixed totally real number field k ($\neq \mathbb{Q}$), do there exist infinitely many prime numbers p for which $\lambda_p = \mu_p = 0$?*" In view of the proposition in [W] cited above, we should confine ourselves to those p which *split* in k. We prove that for a certain real abelian field k, the problem is "affirmative" if we assume the *abc* conjecture for k. Here, the *abc* conjecture is formulated as follows:

Conjecture (cf. [V], p. 84)**.** Let K be a number field. For any ε (> 0) and any finite set S of prime ideals of K, there exists a constant C (> 0) depending only

Received by the editors June 23, 1996 and, in revised form, October 30, 1996.
1991 *Mathematics Subject Classification.* Primary 11R23.
The author was partially supported by the Grants-in-Aid for Scientific Research, The Ministry of Education, Science and Culture, Japan.

on K, ε and S such that

$$\prod_v \max(\|a\|_v, \|b\|_v, \|c\|_v) \le C \left({\prod_{\mathfrak{p}|abc}}' N\mathfrak{p} \right)^{1+\varepsilon} \tag{1}$$

for all integers a, b, c of K with $a + b = c$. Here, v runs over all absolute values of K, $\| * \|_v$ denotes the normalized valuation and $\mathfrak{p}$ runs over all prime ideals of K with $\mathfrak{p}|abc$ and $\mathfrak{p} \notin S$.

Now, let $k/\mathbb{Q}$ be a real abelian extension with $k \neq \mathbb{Q}$, and $\Delta = \mathrm{Gal}(k/\mathbb{Q})$. For a prime number p with $p \nmid [k\colon \mathbb{Q}]$ and a $\mathbb{Q}_p$-character Ψ of Δ, let $\lambda_p(\Psi)$ and $\mu_p(\Psi)$ be the λ-invariant and the μ-invariant associated to the Ψ-component $e_\Psi A_\infty$, respectively. Here, a $\mathbb{Q}_p$-character means a $\mathbb{Q}_p$-valued character of Δ defined and irreducible over $\mathbb{Q}_p$, and e_Ψ is the idempotent of $\mathbb{Q}_p[\Delta]$ corresponding to Ψ, which is an element of $\mathbb{Z}_p[\Delta]$ as $p \nmid [k\colon \mathbb{Q}]$. By [FW], $\mu_p(\Psi) = 0$. We have $\lambda_p = \sum_\Psi \lambda_p(\Psi)$, Ψ running over all $\mathbb{Q}_p$-characters of Δ. Further, for the trivial character Ψ_0 of Δ, we have $\lambda_p(\Psi_0) = 0$ since $\lambda_p(\Psi_0) = \lambda_p(\mathbb{Q})$.

Theorem 1. *Let $k/\mathbb{Q}$ be a real cyclic extension with $[k\colon \mathbb{Q}]$ an odd prime number. If the abc conjecture for k is valid, then there exist infinitely many pairs (p, Ψ) of a prime number p (with $p \nmid [k\colon \mathbb{Q}]$) and a nontrivial $\mathbb{Q}_p$-character Ψ of Δ satisfying* (I) *p splits in k and* (II) *$\lambda_p(\Psi) = 0$.*

Theorem 2. *Let $k/\mathbb{Q}$ be a real quadratic extension for which the norm of a fundamental unit is -1. If the abc conjecture for k is valid, then there exist infinitely many prime numbers p satisfying* (I) *p splits in k and* (II) *$\lambda_p = 0$.*

When (i) $k/\mathbb{Q}$ is noncyclic or (ii) $k/\mathbb{Q}$ is cyclic and $[k\colon \mathbb{Q}]$ is a composite, an assertion similar to the above theorems holds *without* assuming the *abc* conjecture (see §4).

2. Some lemmas

First, we introduce some notation. Let $k/\mathbb{Q}$ be a real abelian extension with $k \neq \mathbb{Q}$, p an odd prime number with $p \nmid [k\colon \mathbb{Q}]$ and Ψ a $\mathbb{Q}_p$-character of $\Delta = \mathrm{Gal}(k/\mathbb{Q})$. We *fix* p and Ψ in this section. Let ψ be a fixed irreducible component of Ψ over an algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$, and let $O = O_\psi$ be the subring of $\overline{\mathbb{Q}}_p$ generated by the values of ψ over $\mathbb{Z}_p$. We identify the subring $e_\Psi \mathbb{Z}_p[\Delta]$ of $\mathbb{Z}_p[\Delta]$ with O by $e_\Psi \sigma \leftrightarrow \psi(\sigma)$ ($\sigma \in \Delta$). Then, for a $\mathbb{Z}_p[\Delta]$-module X (e.g. A_n, A_∞), its Ψ-component $X(\Psi) = e_\Psi X$ (or X^{e_Ψ}) is considered as an O-module. Therefore, $A_\infty(\Psi)$ is regarded as a module over the completed group ring $\Lambda_{p,\Psi} = O[[\mathrm{Gal}(k_\infty/k)]]$. It is known to be torsion over $\Lambda_{p,\Psi}$ by [Iw], Theorem 5. Let r be the degree of the quotient field of O over $\mathbb{Q}_p$. The invariant $\lambda_p(\Psi)$ (resp. $\mu_p(\Psi)$) mentioned in §1 is r times the λ-invariant (resp. μ-invariant) of the torsion $\Lambda_{p,\Psi}$-module $A_\infty(\Psi)$.

For a prime ideal $\mathfrak{p}$ of k over p, let $k_\mathfrak{p}$ be the completion of k at $\mathfrak{p}$ and $\mathcal{U}_\mathfrak{p}$ the group of principal units of $k_\mathfrak{p}$. We denote by $\mathcal{U}$ the group of semi-local units of k at p, namely, $\mathcal{U} := \prod_{\mathfrak{p}|p} \mathcal{U}_\mathfrak{p}$, $\mathfrak{p}$ running over all prime ideals of k with $\mathfrak{p}|p$. The group E of global units of k is considered as a subgroup of $\prod_{\mathfrak{p}|p} k_\mathfrak{p}^\times$. Denote by $\mathcal{E}$ the closure of $E \cap \mathcal{U}$ in $\mathcal{U}$. The groups $\mathcal{U}$ and $\mathcal{E}$ can be regarded as $\mathbb{Z}_p[\Delta]$-modules in a natural way, and hence $\mathcal{U}(\Psi)$ and $\mathcal{E}(\Psi)$ are O-modules.

We regard ψ as a primitive Dirichlet character, and we denote its "dual" character by ψ^*. Namely, ψ^* is the primitive Dirichlet character associated to $\omega\psi^{-1}$, where ω is the Teichmüller character $\mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}_p$.

Lemma 1 (cf. [IS], Remark 4)**.** *If* $\psi(p) \neq 1$ *and* $A_0(\Psi) = \{1\}$*, then we have* $\lambda_p(\Psi) = \mu_p(\Psi) = 0$.

Lemma 2. *Assume that* Ψ *is nontrivial. If* $A_0(\Psi) = \{1\}$ *and* $\mathcal{U}(\Psi) = \mathcal{E}(\Psi)$*, then we have* $\lambda_p(\Psi) = \mu_p(\Psi) = 0$.

Lemma 1 is a refinement of the proposition in [W] cited in §1. Lemma 2 is already known when k is a real quadratic field by [FK]. The assertion for the general case and its proof were communicated to the author by Hiroki Sumida.

Proof of Lemma 2. Let M/k_∞ be the maximal pro-p abelian extension unramified outside p and L/k_∞ the maximal unramified pro-p abelian extension. Further, let M_0 be the maximal abelian extension of k contained in M and K_0 the Hilbert p-class field of k. The Galois groups $\mathrm{Gal}(M/k_\infty)$, $\mathrm{Gal}(L/k_\infty)$, etc. are regarded as modules over $\mathbb{Z}_p[\Delta]$ in a natural way. By class field theory, $\mathrm{Gal}(L/k_\infty)$ is canonically isomorphic to A_∞. Therefore, as $M \supset L$, it suffices to show that $\mathrm{Gal}(M/k_\infty)(\Psi) = \{1\}$. We have a canonical isomorphism $\mathrm{Gal}(M_0/K_0) \simeq \mathcal{U}/\mathcal{E}$ by class field theory (cf. [C], Theorem 1). From this, we see that $\mathrm{Gal}(M_0/K_0k_\infty)(\Psi)$ is isomorphic to $\mathcal{U}(\Psi)/\mathcal{E}(\Psi)$ since $\mathrm{Gal}(M_0/K_0k_\infty)(\Psi) = \mathrm{Gal}(M_0/K_0)(\Psi)$ as $\Psi \neq \Psi_0$. On the other hand, $\mathrm{Gal}(K_0k_\infty/k_\infty)(\Psi)$ is naturally isomorphic to $A_0(\Psi)$. Therefore, under the assumptions of Lemma 2, we obtain $\mathrm{Gal}(M_0/k_\infty)(\Psi) = \{1\}$ and hence $\mathrm{Gal}(M/k_\infty)(\Psi) = \{1\}$ by Nakayama's lemma. □

Lemma 3. *Assume* $\psi^*(p) \neq 1$*. Let* X *be a closed Galois submodule of* $\mathcal{U}(\Psi)$ *such that* $u_\mathfrak{q} \not\equiv 1 \mod \mathfrak{q}^2$ *for some element* $u = (u_\mathfrak{p})_{\mathfrak{p}|p}$ *in* X *and some prime ideal* $\mathfrak{q}$ *with* $\mathfrak{q}|p$*. Then, we have* $X = \mathcal{U}(\Psi)$.

Proof. We have $\mathcal{U}(\Psi) \simeq O$ because of $\psi^*(p) \neq 1$ (cf. [Gi], §2). Therefore, $X = \mathcal{U}(\Psi)^A$ for some ideal A of O since X is an O-submodule of $\mathcal{U}(\Psi)$. We have $A = p^aO$ for some integer a (≥ 0) since the quotient field of O is unramified over $\mathbb{Q}_p$ as $p \nmid [k\colon \mathbb{Q}]$. If $a \geq 1$, then we must have $u_\mathfrak{p} \equiv 1 \mod \mathfrak{p}^2$ for all $u = (u_\mathfrak{p})$ in X and all $\mathfrak{p}|p$. Therefore, we obtain $A = O$ and $X = \mathcal{U}(\Psi)$. □

The following lemma is easily proved and we do not give its proof.

Lemma 4. *Let* K *be a number field,* $\mathfrak{p}$ *a prime ideal of* K *and* α *an element of* K *relatively prime to* $\mathfrak{p}$*. If* $\alpha^n \equiv 1 \mod \mathfrak{p}$ *but* $\alpha^n \not\equiv 1 \mod \mathfrak{p}^2$ *for some integer* n*, then we have* $\alpha^{N\mathfrak{p}-1} \not\equiv 1 \mod \mathfrak{p}^2$.

3. Proof of the theorems

Let $k/\mathbb{Q}$ be (A) a real cyclic extension with $[k\colon \mathbb{Q}]$ an odd prime number or (B) a real quadratic extension for which the norm of a fundamental unit is -1. In the case (A), take a totally negative unit ε of k with $\varepsilon \neq -1$. Then, $N\varepsilon = -1$ as $[k\colon \mathbb{Q}]$ is odd. Here, N denotes the norm map from k to $\mathbb{Q}$. In the case (B), let ε be a fundamental unit of k, for which we have $N\varepsilon = -1$ by assumption. Let $\|*\|_i$ ($1 \leq i \leq [k\colon \mathbb{Q}]$) be the real absolute values of k. Replacing ε by ε^x for some large *odd* integer x if necessary, we may well assume that $\|\varepsilon\|_i$ is so large (resp. so small) for all i with $\|\varepsilon\|_i > 1$ (resp. $\|\varepsilon\|_i < 1$) that

$$|N(1-\varepsilon^m)| > |N(1-\varepsilon^n)| \quad \text{when } m > n \geq 1. \tag{2}$$

Claim 1. Let $\mathfrak{p}$ be a prime ideal of k with $\mathfrak{p} \nmid 2$. If $\varepsilon^n \equiv 1 \mod \mathfrak{p}$ for some *odd* integer n, then $p = \mathfrak{p} \cap \mathbb{Q}$ splits completely in k.

Actually: Assume that p does not split completely in k. Then, $\mathfrak{p}$ is the unique prime ideal of k over p since $[k\colon \mathbb{Q}]$ is a prime number. So, $(\varepsilon^\sigma)^n \equiv 1 \mod \mathfrak{p}$ for all $\sigma \in \Delta$. Therefore, as n is odd, $-1 = (N\varepsilon)^n \equiv 1 \mod \mathfrak{p}$. This contradicts $\mathfrak{p} \nmid 2$.

Now, we assume that the *abc* conjecture holds for k. Then, applying the inequality (1) for $\varepsilon^n + (1-\varepsilon^n) = 1$, we see that for some constant C_1,

$$|N(1-\varepsilon^n)| \le C_1 \left(\prod_{\mathfrak{p}|(1-\varepsilon^n)}{}' N\mathfrak{p} \right)^{3/2} \tag{3}$$

for all integers n. Here, $\mathfrak{p}$ runs over all prime ideals of k with $\mathfrak{p}|(1-\varepsilon^n)$ and $\mathfrak{p} \nmid 2(1-\varepsilon)$. Using this inequality, we show

Claim 2. Under the *abc* conjecture for k, for all sufficiently large n satisfying

$$(n, 2(1-\varepsilon)) = 1, \tag{4}$$

there exists a prime ideal $\mathfrak{p}$ of k such that

$$\mathfrak{p} \nmid 2(1-\varepsilon), \quad \varepsilon^n \equiv 1 \mod \mathfrak{p} \quad \text{and} \quad \varepsilon^n \not\equiv 1 \mod \mathfrak{p}^2. \tag*{$(5)_n$}$$

Actually: For an integer n with (4) and a prime ideal $\mathfrak{p}$ of k satisfying $\mathfrak{p}|(1-\varepsilon^n)$ and $\mathfrak{p}|2(1-\varepsilon)$, we see that $\mathrm{ord}_{\mathfrak{p}}(1-\varepsilon^n) \le C_2$ for some constant C_2 independent of n and $\mathfrak{p}$, where $\mathrm{ord}_{\mathfrak{p}}(*)$ is the normalized additive valuation at $\mathfrak{p}$. This follows from $(1-\varepsilon^n)/(1-\varepsilon) \equiv n \mod (1-\varepsilon)$ and $(n, 1-\varepsilon) = 1$ for $\mathfrak{p}$ with $\mathfrak{p}|(1-\varepsilon)$ and from $2 \nmid n$ for $\mathfrak{p}$ with $\mathfrak{p}|2$. Therefore, by (2), for all sufficiently large n with (4), there exists a prime ideal $\mathfrak{p}$ such that $\varepsilon^n \equiv 1 \mod \mathfrak{p}$ and $\mathfrak{p} \nmid 2(1-\varepsilon)$. Assume that there are infinitely many n with (4) such that $\varepsilon^n \equiv 1 \mod \mathfrak{p}^2$ for all $\mathfrak{p}$ satisfying $\varepsilon^n \equiv 1 \mod \mathfrak{p}$ and $\mathfrak{p} \nmid 2(1-\varepsilon)$. For these n, we have

$$\prod_{\mathfrak{p}|(1-\varepsilon^n)}{}' N\mathfrak{p} \le |N(1-\varepsilon^n)|^{1/2}.$$

Combining this inequality with (3), we obtain

$$|N(1-\varepsilon^n)| \le C_1 |N(1-\varepsilon^n)|^{3/4}.$$

This is a contradiction since the last inequality holds only for a finite number of n because of (2), and hence, Claim 2 is proved.

Let n_1 and n_2 be (sufficiently large) integers satisfying (4) and $(n_1, n_2) = 1$, and let $\mathfrak{p}_i$ be a prime ideal of k satisfying $(5)_n$ with $n = n_i$ $(i = 1, 2)$. Assume $\mathfrak{p}_1 = \mathfrak{p}_2$ $(:= \mathfrak{p})$. Then, from $\varepsilon^{n_i} \equiv 1 \mod \mathfrak{p}$ and $(n_1, n_2) = 1$, we have $\varepsilon \equiv 1 \mod \mathfrak{p}$, contradicting $(5)_n$. Thus, we must have $\mathfrak{p}_1 \ne \mathfrak{p}_2$. Therefore, by Claims 1, 2 and Lemma 4, we see that there exist *infinitely many* prime ideals $\mathfrak{p}$ of k for which $p = \mathfrak{p} \cap \mathbb{Q}$ splits completely in k and

$$\varepsilon^{N\mathfrak{p}-1} = \varepsilon^{p-1} \not\equiv 1 \mod \mathfrak{p}^2. \tag{6}$$

Let $\mathfrak{p}$ be a prime ideal of k satisfying the above two conditions. We may well assume that $p = \mathfrak{p} \cap \mathbb{Q}$ is so large that

$$p \nmid [k\colon \mathbb{Q}] \cdot d_k \cdot h_k,$$

where d_k (resp. h_k) is the discriminant (resp. the class number) of k. By (6) (and $p \nmid [k\colon \mathbb{Q}]$), there exists a nontrivial $\mathbb{Q}_p$-character Ψ of Δ such that $(\varepsilon^{p-1})^{e_\Psi} \not\equiv 1$

mod $\mathfrak{p}^2$. Let ψ be, as before, an irreducible component of Ψ over $\overline{\mathbb{Q}}_p$. Then, by $p \nmid d_k$, the conductor of the dual character ψ^* of ψ is divisible by p, and hence $\psi^*(p) \neq 1$. Therefore, we have $\mathcal{U}(\Psi) = \mathcal{E}(\Psi)$ by Lemma 3. Now, we obtain $\lambda_p(\Psi) = \mu_p(\Psi) = 0$ from Lemma 2 and $p \nmid h_k$. Further, in the case (B) (= the real quadratic case), we have $\lambda_p = \lambda_p(\Psi) + \lambda_p(\Psi_0) = 0$. Thus, we have proved Theorems 1 and 2. □

Remark 1. Lang [L], p. 41, presents an argument which derives the existence of infinitely many primes p with $2^{p-1} \not\equiv 1 \mod p^2$ from the *abc* conjecture for $\mathbb{Q}$. In the above proof of Theorems 1 and 2, we have used this classical argument.

Remark 2. In the above proof of Theorems 1 and 2, the existence of a unit ε with $N\varepsilon = -1$ is quite essential. The author could not handle a real quadratic field whose fundamental unit has norm 1 by the method in this note.

4. Remark

Let $k/\mathbb{Q}$ be a real abelian extension with $k \neq \mathbb{Q}$ and ψ a fixed nontrivial homomorphism from $\Delta = \mathrm{Gal}(k/\mathbb{Q})$ to $\overline{\mathbb{Q}}^\times$, where $\overline{\mathbb{Q}}$ is an algebraic closure of $\mathbb{Q}$. Fixing an embedding of $\overline{\mathbb{Q}}$ into $\overline{\mathbb{Q}}_p$ for each prime p, we denote by Ψ_p the $\mathbb{Q}_p$-character of Δ for which ψ is an irreducible component over $\overline{\mathbb{Q}}_p$. We also denote by k_ψ the subfield of k corresponding to $\ker\psi$ by Galois theory.

Assume that (C) $k/\mathbb{Q}$ is non-cyclic or (D) $k/\mathbb{Q}$ is cyclic with $[k\colon \mathbb{Q}]$ a composite. In the case (D), we further assume that $k_\psi = k$. Then, there exist infinitely many primes p satisfying (I) p splits in k and (II) $\lambda_p(\Psi_p) = 0$.

Actually: As is easily seen, there exist infinitely many p which remain prime in k_ψ but split in k (resp. which split but not completely in k) in the case (C) (resp. (D)). For these p, we have $\psi(p) \neq 1$, and hence $\lambda_p(\Psi_p) = 0$ if $p \nmid [k\colon \mathbb{Q}]$ and $p \nmid h_k$ by Lemma 1.

Acknowledgement

The author is very grateful to Hiroki Sumida for communicating Lemma 2 and its proof to him and for kindly permitting him to include them in this note.

References

[C] J. Coates, *p-adic L-functions and Iwasawa's theory*, Algebraic Number Fields (Durham Symposium, 1975; ed. by A. Fröhlich), 269–353, Academic Press, London (1977). MR **57:**276

[FW] B. Ferrero and L. Washington, *The Iwasawa invariant μ_p vanishes for abelian number fields*, Ann. Math., **109** (1979), 377–395. MR **81a:**12005

[FK] T. Fukuda and K. Komatsu, *On $\mathbb{Z}_p$-extensions of real quadratic fields*, J. Math. Soc. Japan, **38** (1986), 95–102. MR **87d:**11081

[Gi] R. Gillard, *Unités cyclotomiques, unités semi-locales et $\mathbb{Z}_l$-extensions* II, Ann. Inst. Fourier, **29** (1979), 1–15. MR **81e:**12005b

[Gr] R. Greenberg, *On the Iwasawa invariants of totally real number fields*, Amer. J. Math., **98** (1976), 263–284. MR **53:**5529

[IS] H. Ichimura and H. Sumida, *On the Iwasawa invariants of certain real abelian fields* II, International J. Math., **7** (1996), 721–744. CMP 97:03

[Iw] K. Iwasawa, *On $\mathbb{Z}_l$-extensions of algebraic number fields*, Ann. Math., **98** (1973), 246–326. MR **50:**2120

[L] S. Lang, *Old and new conjectured diophantine inequalities*, Bull. AMS, **23** (1990), 37–75. MR **90k:**11032

[V] P. Vojta, *Diophantine Approximations and Value Distribution Theory*, Lecture Notes in Math., vol. 1239, Springer-Verlag, Berlin and New York, 1987. MR **91k:**11049

[W] L. Washington, *Introduction to Cyclotomic Fields*, Grad. Texts in Math. no. 83, Springer-Verlag, Berlin and New York, 1982. MR **85g:**11001

Department of Mathematics, Yokohama City University, 22-2, Seto, Kanazawa-ku, Yokohama, 236 Japan

E-mail address: ichimura@yokohama-cu.ac.jp