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 \( k_{\infty}/k \) be the cyclotomic \( \mathbb{Z}_p \)-extension over \( k \) with its \( n \)th layer \( k_n \) \((k_0 = k)\). Let \( A_n \) be the Sylow \( p \)-subgroup of the ideal class group of \( k_n \) and \( A_{\infty} = \lim \leftarrow A_n \) 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 \( \lambda \)-invariant and the \( \mu \)-invariant associated to \( A_{\infty} \), 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 \( k_{\infty} \) 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 \( \varepsilon \) \((> 0)\) and any finite set \( S \) of prime ideals of \( K \), there exists a constant \( C \) \((> 0)\) depending only...
on $K, \varepsilon$ and $S$ such that

$$(1) \quad \prod_v \max(||a||_v, ||b||_v, ||c||_v) \leq C \left( \prod_p' N_p \right)^{1+\varepsilon}$$

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

Now, let $k/Q$ be a real abelian extension with $k \neq Q$, and $\Delta = \text{Gal}(k/Q)$. For a prime number $p$ with $p \nmid [k: Q]$ and a $Q_p$-character $\Psi$ of $\Delta$, let $\lambda_p(\Psi)$ and $\mu_p(\Psi)$ be the $\lambda$-invariant and the $\mu$-invariant associated to the $\Psi$-component $e_\Psi A_\infty$, respectively. Here, a $Q_p$-character means a $Q_p$-valued character of $\Delta$ defined and irreducible over $Q_p$, and $e_\Psi$ is the idempotent of $Q_p[\Delta]$ corresponding to $\Psi$, which is an element of $Z_p[\Delta]$ as $p \nmid [k: Q]$. By [FW], $\mu_p(\Psi) = 0$. We have $\lambda_p = \sum \lambda_p(\Psi)$, $\Psi$ running over all $Q_p$-characters of $\Delta$. Further, for the trivial character $\Psi_0$ of $\Delta$, we have $\lambda_p(\Psi_0) = 0$ since $\lambda_p(\Psi_0) = \lambda_p(Q)$.

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

**Theorem 2.** Let $k/Q$ 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) $k/Q$ is noncyclic or (ii) $k/Q$ is cyclic and $[k: Q]$ 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 $k/Q$ be a real abelian extension with $k \neq Q$, $p$ an odd prime number with $p \nmid [k: Q]$ and $\Psi$ a $Q_p$-character of $\Delta = \text{Gal}(k/Q)$. We fix $p$ and $\Psi$ in this section. Let $\psi$ be a fixed irreducible component of $\Psi$ over an algebraic closure $\overline{Q}_p$ of $Q_p$, and let $O = O_\psi$ be the subring of $\overline{Q}_p$ generated by the values of $\psi$ over $Z_p$. We identify the subring $e_\Psi Z_p[\Delta]$ of $Z_p[\Delta]$ with $O$ by $e_\Psi \sigma \mapsto \psi(\sigma)$ ($\sigma \in \Delta$). Then, for a $Z_p[\Delta]$-module $X$ (e.g. $A_n, A_\infty$), its $\Psi$-component $X(\psi) = e_\Psi X$ (or $X^{e_\Psi}$) is considered as an $O$-module. Therefore, $A_\infty(\Psi)$ is regarded as a module over the completed group ring $\Lambda_p, \psi = O[[\text{Gal}(k/k)]]$. 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 $Q_p$. The invariant $\lambda_p(\Psi)$ (resp. $\mu_p(\Psi)$) mentioned in §1 is $r$ times the $\lambda$-invariant (resp. $\mu$-invariant) of the torsion $\Lambda_p, \psi$-module $A_\infty(\Psi)$.

For a prime ideal $p$ of $k$ over $p$, let $k_p$ be the completion of $k$ at $p$ and $U_p$ the group of principal units of $k_p$. We denote by $U$ the group of semi-local units of $k$ at $p$, namely, $U := \prod \overline{U}_p$, $p$ running over all prime ideals of $k$ with $p|p$. The group $E$ of global units of $k$ is considered as a subgroup of $\prod_{p|p} k_p^\times$. Denote by $E$ the closure of $E \cap U$ in $U$. The groups $U$ and $E$ can be regarded as $Z_p[\Delta]$-modules in a natural way, and hence $U(\Psi)$ and $E(\Psi)$ are $O$-modules.
We regard $\psi$ as a primitive Dirichlet character, and we denote its “dual” character by $\psi^*$. Namely, $\psi^*$ is the primitive Dirichlet character associated to $\omega \psi^{-1}$, where $\omega$ 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 $\Psi$ is nontrivial. If $A_0(\Psi) = \{1\}$ and $U(\Psi) = \mathcal{E}(\Psi)$, 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 $M/k_\infty$ be the maximal pro-$p$ abelian extension unramified outside $p$ and $L/k_\infty$ 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 $\text{Gal}(M/k_\infty)$, $\text{Gal}(L/k_\infty)$, etc. are regarded as modules over $\mathbb{Z}_p[\Delta]$ in a natural way. By class field theory, $\text{Gal}(L/k_\infty)$ is canonically isomorphic to $A_\infty$. Therefore, as $M \supset L$, it suffices to show that $\text{Gal}(M/k_\infty)(\Psi) = \{1\}$. We have a canonical isomorphism $\text{Gal}(M_0/K_0) \simeq U/E$ by class field theory (cf. [C], Theorem 1). From this, we see that $\text{Gal}(M_0/K_0k_\infty)(\Psi)$ is isomorphic to $U(\Psi)/E(\Psi)$ since $\text{Gal}(M_0/K_0k_\infty)(\Psi) = \text{Gal}(M_0/K_0)(\Psi)$ as $\Psi \neq \Psi_0$. On the other hand, $\text{Gal}(K_0k_\infty/k_\infty)(\Psi)$ is naturally isomorphic to $A_0(\Psi)$. Therefore, under the assumptions of Lemma 2, we obtain $\text{Gal}(M_0/k_\infty)(\Psi) = \{1\}$ and hence $\text{Gal}(M/k_\infty)(\Psi) = \{1\}$ by Nakayama’s lemma.

**Lemma 3.** Assume $\psi^*(p) \neq 1$. Let $X$ be a closed Galois submodule of $U(\Psi)$ such that $u_q \neq 1 \mod q^2$ for some element $u = (u_p)p|p$ in $X$ and some prime ideal $q$ with $q|p$. Then, we have $X = U(\Psi)$.

**Proof.** We have $U(\Psi) \simeq O$ because of $\psi^*(p) \neq 1$ (cf. [Gi], §2). Therefore, $X = U(\Psi)^A$ for some ideal $A$ of $O$ since $X$ is an $O$-submodule of $U(\Psi)$. We have $A = p^aO$ for some integer $a$ ($\geq 0$) since the quotient field of $O$ is unramified over $\mathbb{Q}_p$ as $p \not| [k: \mathbb{Q}]$. If $a \geq 1$, then we must have $u_p \equiv 1 \mod p^2$ for all $u = (u_p)$ in $X$ and all $p|p$. Therefore, we obtain $A = O$ and $X = U(\Psi)$.

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

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

### 3. PROOF OF THE THEOREMS

Let $k/\mathbb{Q}$ be (A) a real cyclic extension with $[k: \mathbb{Q}]$ 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 $\varepsilon$ of $k$ with $\varepsilon \neq -1$. Then, $N\varepsilon = -1$ as $[k: \mathbb{Q}]$ is odd. Here, $N$ denotes the norm map from $k$ to $\mathbb{Q}$. In the case (B), let $\varepsilon$ be a fundamental unit of $k$, for which we have $N\varepsilon = -1$ by assumption. Let $\| \cdot \|_i$ ($1 \leq i \leq [k: \mathbb{Q}]$) be the real absolute values of $k$. Replacing $\varepsilon$ by $\varepsilon^x$ 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

\begin{equation}
|N(1 - \varepsilon^n)| > |N(1 - \varepsilon^m)| \quad \text{when } m > n \geq 1.
\end{equation}
Claim 1. Let \( \mathfrak{p} \) be a prime ideal of \( k \) with \( \mathfrak{p} \not| 2 \). If \( \varepsilon^n \equiv 1 \mod \mathfrak{p} \) for some odd integer \( n \), then \( \mathfrak{p} = \mathfrak{p} \cap \mathbb{Q} \) 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 \( [k: \mathbb{Q}] \) is a prime number. So, \( (\varepsilon^n)^n \equiv 1 \mod \mathfrak{p} \) for all \( \sigma \in \Delta \). Therefore, as \( n \) is odd, \(-1 = (N\varepsilon)^n \equiv 1 \mod \mathfrak{p} \). This contradicts \( p \not| 2 \).

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 \( C_1 \),

\[
|N(1 - \varepsilon^n)| \leq C_1 \left( \prod_{\mathfrak{p}|(1 - \varepsilon^n)} N\mathfrak{p} \right)^{3/2}
\]

for all integers \( n \). Here, \( \mathfrak{p} \) runs over all prime ideals of \( k \) with \( \mathfrak{p}|(1 - \varepsilon^n) \) and \( \mathfrak{p} \not| 2(1 - \varepsilon) \). Using this inequality, we show

Claim 2. Under the \( abc \) conjecture for \( k \), for all sufficiently large \( n \) satisfying

\[
(n, 2(1 - \varepsilon)) = 1,
\]

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

\[
(5)_n \quad \mathfrak{p} \not| 2(1 - \varepsilon), \quad \varepsilon^n \equiv 1 \mod \mathfrak{p} \quad \text{and} \quad \varepsilon^n \not\equiv 1 \mod \mathfrak{p}^2.
\]

Actually: For an integer \( n \) with (4) and a prime ideal \( \mathfrak{p} \) of \( k \) satisfying \( \mathfrak{p}|(1 - \varepsilon^n) \) and \( \mathfrak{p} \not| 2(1 - \varepsilon) \), we see that \( \text{ord}_\mathfrak{p}(1 - \varepsilon^n) \leq C_2 \) for some constant \( C_2 \) independent of \( n \) and \( \mathfrak{p} \), where \( \text{ord}_\mathfrak{p}(\varepsilon) \) 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 \( 2 \not| n \) 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 \( \mathfrak{p} \not| 2(1 - \varepsilon) \). 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 \( \mathfrak{p} \not| 2(1 - \varepsilon) \). For these \( n \), we have

\[
\prod_{\mathfrak{p}|(1 - \varepsilon^n)} N\mathfrak{p} \leq |N(1 - \varepsilon^n)|^{1/2}.
\]

Combining this inequality with (3), we obtain

\[
|N(1 - \varepsilon^n)| \leq C_1|N(1 - \varepsilon^n)|^{3/4}.
\]

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) with \( n = n_i \) \((i = 1, 2)\). Assume \( \mathfrak{p}_1 = \mathfrak{p}_2 \) \((= \mathfrak{p})\). Then, from \( \varepsilon^{n_1} \equiv 1 \mod \mathfrak{p} \) and \((n_1, n_2) = 1 \), we have \( \varepsilon \equiv 1 \mod \mathfrak{p} \), contradicting (5). Thus, we must have \( \mathfrak{p}_1 \neq \mathfrak{p}_2 \). 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

\[
\varepsilon^{N\mathfrak{p}^{-1}} = \varepsilon^{p^{-1}} \not\equiv 1 \mod \mathfrak{p}^2.
\]

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

\[
p \not| [k: \mathbb{Q}] \cdot d_k \cdot h_k,
\]

where \( d_k \) (resp. \( h_k \)) is the discriminant (resp. the class number) of \( k \). By (6) and \( p \not| [k: \mathbb{Q}] \), there exists a nontrivial \( \mathbb{Q}_p \)-character \( \Psi \) of \( \Delta \) such that \((\varepsilon^{p^{-1}})^{\Psi} \not\equiv 1 \mod \mathfrak{m}^2\).
Let $\psi$ be, as before, an irreducible component of $\Psi$ over $\overline{\mathbb{Q}}_p$. Then, by $p \nmid d_k$, the conductor of the dual character $\psi^*$ of $\psi$ is divisible by $p$, and hence $\psi^*(p) \neq 1$. Therefore, we have $U(\Psi) = E(\Psi)$ 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 $2p^{-1} \equiv 1 \mod p^2$ 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 $\varepsilon$ 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 $\psi$ a fixed nontrivial homomorphism from $\Delta = \text{Gal}(k/\mathbb{Q})$ to $\mathbb{Q}^\times$, where $\overline{\mathbb{Q}}$ is an algebraic closure of $\mathbb{Q}$. Fixing an embedding of $\mathbb{Q}$ into $\overline{\mathbb{Q}}_p$ for each prime $p$, we denote by $\Psi_p$ the $\mathbb{Q}_p$-character of $\Delta$ for which $\psi$ is an irreducible component over $\overline{\mathbb{Q}}_p$. We also denote by $k_\psi$ 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 $[k: \mathbb{Q}]$ 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 $k_\psi$ 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 $p \nmid [k: \mathbb{Q}]$ 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


[L] S. Lang, Old and new conjectured diophantine inequalities, Bull. AMS, 23 (1990), 37–75. MR 90k:11082


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

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