ACTA ARITHMETICA
LXV.3 (1993)

On the non-triviality of the basic Iwasawa λ-invariant for an infinitude of imaginary quadratic fields

by

Jonathan W. Sands (Burlington, Vt.)

1. Introduction. We fix an odd prime p and let K vary throughout the family of all imaginary quadratic fields in which p splits. The basic p-adic Iwasawa λ-invariant of K will be denoted by $\lambda_p(K)$. This is our principal object of consideration.

In our special situation, the theorem of Ferrero and Washington [3] implies that the basic p-adic Iwasawa μ-invariant $\mu_p(K)$ vanishes, and $\lambda_p(K)$ has two especially simple interpretations. Analytically, it is the Weierstrass degree of the power series connected with a p-adic L-function associated with K. Algebraically, it arises in connection with the basic unramified p-adic Iwasawa module for K. Under our assumption, this module is free over the ring $\mathbb{Z}_p$ of p-adic integers and $\lambda_p(K)$ is simply its rank.

When we focus on the case where p splits in the field K, one can see from either point of view that $\lambda_p(K) \geq 1$. Analytically, the splitting of p creates a trivial zero at the origin in the p-adic L-function and hence in the related power series. Thus the power series has no constant term and is of Weierstrass degree at least one. Algebraically, class field theory guarantees that for each of the two divisors of p there is a $\mathbb{Z}_p$-extension of K which does not ramify outside of that prime. The composite of these two extensions is unramified above the basic $\mathbb{Z}_p$-extension of K and thus contributes 1 to the rank of the basic unramified p-adic Iwasawa module for K. Genus theory can also be used to provide another algebraic interpretation.

Because $\lambda_p(K) \geq 1$ in the case of interest to us, we consider it to be trivial when $\lambda_p(K) = 1$ and non-trivial when $\lambda_p(K) > 1$. Heuristics and computations [1] suggest that among imaginary quadratic fields K in which p splits, the trivial case is significantly more common, while both cases should have a positive natural density. Horie [5] has proved the infinitude

Research supported by National Security Agency Grant MDA904-89-H-2012 and the Deutsche Forschungsgemeinschaft.

of non-trivial cases, while Jochnowitz [6] can now prove the infinitude of trivial cases. Our method is tailored towards actually counting the number of non-trivial cases among imaginary quadratic fields whose discriminant has absolute value below a given bound X. We are not able to prove positive density, but for $X = 4p^{2n}$ we obtain more than $\sqrt{X}/2p$ non-trivial cases, thus strengthening Horie's result.

Our proof consists of first obtaining a criterion which avoids the consideration of class numbers, and then actually constructing fields which satisfy this criterion. This explains why our method improves on Horie's result and at the same time fails to apply to the trivial case. For in order that $\lambda_p(K) = 1$ when p splits in K, it is necessary that p not divide the class number of K, as we will see (Proposition 2.1). Jochnowitz's work on the Fourier coefficients of modular forms allows her to control the class number and obtain the infinitude of trivial cases. On the other hand, Horie [5] noted that the infinitude of non-trivial cases follows immediately from Yamamoto's [7] construction of infinitely many imaginary quadratic fields in which p splits and the class group has p-rank at least 2. Horie's main result in that work is the infinitude of imaginary quadratic fields K with $\lambda_p(K) = 0$, which also requires controlling the class number. These results involving class numbers do not lend themselves to the derivation of useful asymptotic estimates. By the avoidance of class number questions, we are able to construct a different sort of family of fields whose discriminants are relatively small.

We thank Ralph Greenberg for bringing Jochnowitz's work to our attention. We also thank the staff, students, and faculty of the Fachbereich Informatik, Universität des Saarlandes, for their support and hospitality during the period in which this note was written.

2. A variant of Gold's criterion.

The necessary and sufficient condition of Gold [4] for $\lambda_p(K) > 1$ in our situation requires that K have class number $h(K)$ not divisible by p. However, we can see the effect of a factor of p in the class number via a special case of the theorem of Federer, Gross and Sinnott [2]. This leads to the following.

2.1. Proposition. *Assume that p is an odd prime and that p splits in the imaginary quadratic field K. Thus $(p) = \mathcal{P}\overline{\mathcal{P}}$, the product of a first degree prime ideal of K and its complex conjugate. Then*

1. $\lambda_p(K) \geq 1$.

2. *Suppose that r is a positive integer not divisible by p such that $\mathcal{P}^r = (\alpha)$, a principal ideal of K. Then $\lambda_p > 1$ if and only if either $\alpha^{p-1} \equiv 1 \pmod{\overline{\mathcal{P}}^2}$ or p divides the class number $h(K)$.*

2.2. Remark. Gold's criterion [4] is exactly this proposition in the case when $h(K)$ is not divisible by p.

Proof of Proposition 2.1. Under our assumptions, the theorem of Federer, Gross and Sinnott [2] says that the leading term of the characteristic polynomial in the variable T for the basic unramified p-adic Iwasawa module of K is (up to multiplication by a factor which is relatively prime to p)

$$\frac{h(K)\log_p(\alpha)}{rp}T = \frac{h(K)\log_p(\alpha^{p-1})}{rp(p-1)}T\,.$$

The function $\log_p$ is the p-adic logarithm, with the usual normalization. The element α is viewed as lying in the completion $K_{\overline{\mathcal{P}}}$ of K at $\overline{\mathcal{P}}$, which one identifies with the field of p-adic numbers $\mathbb{Q}_p$. Then $\alpha^{p-1} \equiv 1 \pmod{\overline{\mathcal{P}}}$, so $\alpha^{p-1} = 1 + x$ with $x \in p\mathbb{Z}_p$, and $\log_p(\alpha^{p-1})$ may be computed by means of the power series $\log_p(1+x) = x - x^2/2 + \ldots$ The Iwasawa invariant $\lambda_p(K)$ is the Weierstrass degree of the characteristic polynomial. The formula above shows (without any assumption on r) that this degree is at least one, thus establishing the first statement of the proposition.

The formula also implies that $\lambda_p(K)$ is greater than 1 if and only if p divides $h(K)(x/p)$ in $\mathbb{Z}_p$. This follows from the fact that p is odd and $r(p-1)$ is not divisible by p. Thus $\lambda_p(K) > 1$ if and only if p divides $h(K)$ or p^2 divides $x = \alpha^{p-1} - 1$ in $\mathbb{Z}_p$. But p^2 divides $\alpha^{p-1} - 1$ in $\mathbb{Z}_p$ if and only if $\alpha^{p-1} - 1 \in \overline{\mathcal{P}}^2$ in K. ∎

2.3. Corollary. *Assume that p is an odd prime and that p splits as $(p) = \mathcal{P}\overline{\mathcal{P}}$ in the imaginary quadratic field K. Suppose that $r > 1$ is an integer not divisible by p such that $\mathcal{P}^r = (\alpha)$, and let $\operatorname{Tr}(\alpha) \in \mathbb{Z}$ be the trace of α. Then $\lambda_p(K) > 1$ if and only if either p divides $h(K)$ or $(\operatorname{Tr}(\alpha))^{p-1} \equiv 1 \pmod{p^2}$.*

Proof. Since $(\alpha) = \mathcal{P}^r$, we have $(\overline{\alpha}) = \overline{\mathcal{P}}^r$, and since $r > 1$, we conclude that $\overline{\alpha} \equiv 0 \pmod{\overline{\mathcal{P}}^2}$. Hence $\operatorname{Tr}(\alpha) = \alpha + \overline{\alpha} \equiv \alpha \pmod{\overline{\mathcal{P}}^2}$ and $(\operatorname{Tr}(\alpha))^{p-1} \equiv \alpha^{p-1} \pmod{\overline{\mathcal{P}}^2}$. By combining this with the proposition, we now see that

$$\begin{aligned}\alpha^{p-1} \equiv 1 \pmod{\overline{\mathcal{P}}^2} &\Leftrightarrow (\operatorname{Tr}(\alpha))^{p-1} \equiv 1 \pmod{\overline{\mathcal{P}}^2}\\ &\Leftrightarrow (\operatorname{Tr}(\alpha))^{p-1} \equiv 1 \pmod{p^2}\,.\end{aligned}$$

The last equivalence holds because $\operatorname{Tr}(\alpha) \in \mathbb{Z}$, and $\overline{\mathcal{P}}^2 \cap \mathbb{Z} = (p^2)$. ∎

3. Construction of fields to meet the criterion.

We now construct imaginary quadratic fields K in which p splits and which satisfy $\lambda_p(K) > 1$. This is done by constructing discriminants $-D$ with an appropriate property and putting $K = \mathbb{Q}(\sqrt{-D})$. The infinitude of such fields will follow easily from the construction.

Recall that p is a fixed odd prime. We now also fix an arbitrary integer $n \geq 2$, *which is not divisible by* p. It is interesting to note that Horie's fields with $\lambda_p(K) > 1$ come from Yamamoto's construction of ideal classes of order p, while our construction of fields with $\lambda_p(K) > 1$ parallels Yamamoto's construction of ideal classes of order n. Indeed, we could impose further conditions to ensure that the primes above p generate such classes. We define a function f_n from the set

$$C_n = \{a \in \mathbb{Z} : 0 < a < 2p^n \text{ and } a \not\equiv 0 \pmod{p}\}$$

to the set of integers greater than $-4p^{2n}$ and not divisible by p which are the discriminants of imaginary quadratic fields.

If $a \in C_n$, then $0 < 4p^{2n} - a^2$. The latter quantity may be written uniquely as $b^2 D$, with b a positive integer and $-D$ a discriminant of an imaginary quadratic field. Of course we then know that $0 < D < 4p^{2n}$ and $p \nmid D$ since $p \nmid a$. Thus we can define $f_n(a) = -D$.

3.1. Lemma. *Let $-D$ be in the image of f_n. Then*

1. *The prime p splits in $K = \mathbb{Q}(\sqrt{-D})$.*

2. *The cardinality of $f_n^{-1}(-D)$ is at most half the number of units in K. Hence if $-D < -4$, then it corresponds to a unique a. If $-D = -4$, there are at most* 2 *corresponding a's, and if $-D = -3$, there are at most* 3.

Proof. Suppose $a \in f_n^{-1}(-D)$, so that $f_n(a) = -D$. By the definition of f_n, there exists a positive integer b such that $4p^{2n} - a^2 = b^2 D$. Thus

$$p^{2n} = \frac{a^2 + b^2 D}{4} = N\left(\frac{a + b\sqrt{-D}}{2}\right),$$

with N denoting the norm from K to $\mathbb{Q}$. So p divides $N\big(\frac{a+b\sqrt{-D}}{2}\big)$, but $p \nmid \frac{a+b\sqrt{-D}}{2}$ because $p \nmid a$. This shows that p splits in K.

Now $(p) = \mathcal{P}\overline{\mathcal{P}}$ in K, and we have observed that this product does not divide $\frac{a+b\sqrt{-D}}{2}$. Since the norm of the latter is p^{2n}, the only factorization possibilities are $\big(\frac{a+b\sqrt{-D}}{2}\big) = \mathcal{P}^{2n}$ or $\overline{\mathcal{P}}^{2n}$. Now we see that the positive integer a is twice the real part of a generator of $\mathcal{P}^{2n}$. However, the number of choices for this generator equals the number of units in K, and only half of these choices yield $a > 0$. ∎

The discriminants in the image of f_n will determine fields of the desired type once we restrict to an appropriate subset of C_n.

Define

$$A_n = \{a \in C_n : a^{p-1} \equiv 1 \pmod{p^2}\}.$$

3.2. Lemma. *Suppose that $a \in A_n$ and $f_n(a) = -D$. Then the field $K = \mathbb{Q}(\sqrt{-D})$ has $\lambda_p(K) > 1$.*

Proof. The preceeding lemma shows that $p = \mathcal{P}\overline{\mathcal{P}}$ in K and that $\mathcal{P}^{2n} = (\alpha)$ with $\alpha = \frac{a+b\sqrt{-D}}{2}$, for some integer b. Since $\mathrm{Tr}(\alpha) = a \in A_n$ and the definition of A_n specifies that $a^{p-1} \equiv 1 \pmod{p^2}$, we can conclude from the corollary above that $\lambda_p(K) > 1$. We have assumed that $p \nmid n$ precisely so that this corollary can be applied with $r = 2n \not\equiv 0 \pmod{p}$. ■

Our main result will follow upon counting the number of elements in A_n.

3.3. Theorem. *Among the imaginary quadratic fields in which p splits, there exist at least $2(p-1)p^{n-2} - 3$ fields K for which $\lambda_p(K) > 1$ and whose discriminant $-D$ satisfies $-D > -4p^{2n}$.*

Proof. The condition for $a \in C_n$ to lie in A_n depends only on $a \pmod{p^2}$. Thus to determine the cardinality of A_n, we count the number of elements $a \in C_n$ in the range $0 \le a < p^2$ which satisfy this condition, and multiply by the number $2p^n/p^2 = 2p^{n-2}$ of translates of this range by p^2 which are contained in C_n. This count yields the $p-1$ solutions of $a^{p-1} \equiv 1 \pmod{p^2}$. Thus the cardinality of A_n is $2(p-1)p^{n-2}$.

By the preceding lemma, each $a \in A_n$ determines a discriminant $-D = f_n(a)$ of an imaginary quadratic field K with the desired properties $-D > -4p^{2n}$ and $\lambda_p(K) > 1$. The first lemma implies that taking the image of a subset of C_n under f_n decreases the cardinality by at most 3. This yields the result. ■

As a corollary, we have a new proof of Horie's observation.

3.4. Corollary. *For each fixed odd prime p, there exist infinitely many imaginary quadratic fields K such that p splits in K and $\lambda_p(K) > 1$.*

Proof. Let $n \to \infty$ in the theorem. ■

References

[1] D. S. Dummit, D. Ford, H. Kisilevsky and J. W. Sands, *Computation of Iwasawa lambda invariants for imaginary quadratic fields*, J. Number Theory 37 (1991), 100–121.

[2] L. J. Federer and B. H. Gross (Appendix by W. Sinnott), *Regulators and Iwasawa modules*, Invent. Math. 62 (1981), 443–457.

[3] B. Ferrero and L. Washington, *The Iwasawa invariant μ_p vanishes for abelian number fields*, Ann. of Math. 109 (1979), 377–395.

[4] R. Gold, *The nontriviality of certain $\mathbb{Z}_l$-extensions*, J. Number Theory 6 (1974), 269–273 .

[5] K. Horie, *A note on basic Iwasawa λ-invariants of imaginary quadratic fields*, Invent. Math. 88 (1987), 31–38.

[6] N. Jochnowitz, *A p-adic conjecture about derivatives of L-series attached to modular forms*, to appear.

[7] Y. Yamamoto, *On unramified Galois extensions of quadratic number fields*, Osaka J. Math. 7 (1970), 57–76.

DEPARTMENT OF MATHEMATICS AND STATISTICS
UNIVERSITY OF VERMONT
BURLINGTON, VERMONT 05405
U.S.A.

Received on 25.11.1992 (2343)