MATHEMATICS OF COMPUTATION
Volume 65, Number 214
April 1996, Pages 779–784

COMPUTATION OF $\mathbb{Z}_3$-INVARIANTS OF REAL QUADRATIC FIELDS

HISAO TAYA

ABSTRACT. Let k be a real quadratic field and p an odd prime number which splits in k. In a previous work, the author gave a sufficient condition for the Iwasawa invariant $\lambda_p(k)$ of the cyclotomic $\mathbb{Z}_p$-extension of k to be zero. The purpose of this paper is to study the case $p = 3$ of this result and give new examples of k with $\lambda_3(k) = 0$, by using information on the initial layer of the cyclotomic $\mathbb{Z}_3$-extension of k.

1. INTRODUCTION

Let k be a finite totally real extension of the field of rational numbers $\mathbb{Q}$. Let p be a fixed prime number and $\mathbb{Z}_p$ the ring of p-adic integers. We denote by $\lambda_p(k)$, $\mu_p(k)$ and $\nu_p(k)$ the Iwasawa invariants of the cyclotomic $\mathbb{Z}_p$-extension of k for p (cf. [8]). In Greenberg's paper [7], both $\lambda_p(k)$ and $\mu_p(k)$ were conjectured to be zero. However, Greenberg's conjecture is not yet proven, even for real quadratic fields, although we know by the Ferrero-Washington theorem that $\mu_p(k)$ is always zero when k is an abelian extension of $\mathbb{Q}$ (cf. [1]).

Let k be a real quadratic field and p an odd prime number which splits in k. In a previous paper [10], we gave a sufficient condition for $\lambda_p(k)$ to be zero. In the present paper, we first define two invariants $n_0^{(r)}$ and $n_2^{(r)}$ for k and p, and rewrite our previous result in terms of these invariants. Next, using this result for $p = 3$, we will give some examples of k with $\lambda_3(k) = 0$, which are of a new type. For this purpose, we will compute $n_0^{(1)}$ and $n_2^{(1)}$ for $p = 3$ by determining the unit group of the initial layer of the cyclotomic $\mathbb{Z}_3$-extension of k by the method of Mäki (cf. [3, 9]).

2. A SUFFICIENT CONDITION FOR $\lambda_p(k) = 0$

Let k be a real quadratic field with class number h and fundamental unit ε, and p an odd prime number which splits in k, namely, $(p) = \mathfrak{p}\mathfrak{p}'$ in k where $\mathfrak{p} \neq \mathfrak{p}'$. Then we can choose $\alpha \in k$ such that ${\mathfrak{p}'}^h = (\alpha)$. Fukuda and Komatsu [5] defined two invariants $n_1, n_2 \in \mathbb{N}$ for k and p, by

$$\mathfrak{p}^{n_1} \parallel (\alpha^{p-1} - 1), \quad \mathfrak{p}^{n_2} \parallel (\varepsilon^{p-1} - 1).$$

Here $\mathfrak{p}^n \| \mathfrak{a}$ means that $\mathfrak{p}^n | \mathfrak{a}$ and $\mathfrak{p}^{n+1} \nmid \mathfrak{a}$ for an ideal $\mathfrak{a}$ of k. Though the choice of α is not unique, n_1 is uniquely determined under the condition $n_1 \leq n_2$.

Received by the editor October 12, 1993 and, in revised form, August 2, 1994.
1991 *Mathematics Subject Classification.* Primary 11R23, 11R11, 11R27, 11Y40.
Key words and phrases. Iwasawa invariants, real quadratic fields, unit groups, computation.

For the cyclotomic $\mathbb{Z}_p$-extension

$$k = k_0 \subset k_1 \subset k_2 \subset \cdots \subset k_n \subset \cdots \subset k_\infty,$$

let $\mathfrak{p}'_n$ be the unique prime ideal of k_n lying above $\mathfrak{p}'$, d_n the order of $\mathfrak{p}'_n$ in the ideal class group of k_n and E_n the unit group of k_n. For $m \geq n \geq 0$, we denote by $N_{m,n}$ the norm map from k_m to k_n. Now we fix an integer $r \geq 0$. Then we can choose $\beta_r \in k_r$ such that ${\mathfrak{p}'_r}^{d_r} = (\beta_r)$. We define two other invariants $n_0^{(r)}, n_2^{(r)} \in \mathbb{N}$ for k and p, by

$$\mathfrak{p}^{n_0^{(r)}} \parallel (N_{r,0}(\beta_r)^{p-1} - 1), \quad p^{n_2^{(r)}} = p^{n_2}(E_0 : N_{r,0}(E_r)).$$

As in the case of n_1, $n_0^{(r)}$ is uniquely determined under the condition $n_0^{(r)} \leq n_2^{(r)}$, though the choice of β_r is not unique. Put $n_0 = n_0^{(0)}$, noting that $n_2 = n_2^{(0)}$. It is easily seen that $n_0 \leq n_1 \leq n_2$.

Remark 1. The invariant $n_0^{(r)}$ is a generalization of m_r, which was defined in [10] under the assumptions that $p \nmid h$ and $n_2 \geq 2$.

Let A_n be the p-primary part of the ideal class group of k_n and ζ_p a primitive pth root of unity. For the CM-field $k^* = k(\zeta_p)$, we put $\lambda_p^-(k^*) = \lambda_p(k^*) - \lambda_p((k^*)^+)$, where $(k^*)^+$ is the maximal real subfield of k^*. Noting Theorem 1 of [5] and Lemma 3 of [10], we may rewrite Theorem 2 of [10] as follows, which is a generalization of the results of Fukuda and Komatsu in [2] and [5].

Theorem 1. *Let k be a real quadratic field and p an odd prime number which splits in k. Fix an integer $r \geq 0$. Assume that*

1. $A_0 = 1$,
2. $\lambda_p^-(k^*) = 1$.

If $n_0^{(r)} \neq n_2^{(r)}$, then we have $\lambda_p(k) = 0$.

Greenberg, Fukuda, Komatsu and Wada gave a number of examples of k with $\lambda_p(k) = 0$ in three cases where $n_1 = 1$, $2 \leq n_1 \neq n_2$ and $n_1 = n_2 = 2$ (cf. [2, 5, 6, 7]). However, in the case where $n_1 = n_2 \geq 3$, no examples of such k's have been given until now. In the rest of this paper, we will give some examples of k with $\lambda_3(k) = 0$ in the cases where $n_1 = n_2 = 3$, 4 and 5, using Theorem 1 for $p = 3$ and $r = 1$. Note that $\lambda_3^-(k^*) = \lambda_3(\mathbb{Q}(\sqrt{-3d}))$, where d is the discriminant of k (cf. the proof of Theorem 10.10 in [11]). Therefore, we will compute $n_0^{(1)}$ and $n_2^{(1)}$ for $p = 3$ to achieve our purpose.

3. Computation of the invariants $n_0^{(1)}$ and $n_2^{(1)}$ for $p = 3$

Let m be a positive square-free integer and $k = \mathbb{Q}(\sqrt{m})$. In this section, we will explain how to compute $n_0^{(1)}$ and $n_2^{(1)}$ for $p = 3$. Let k_1 be the initial layer of the cyclotomic $\mathbb{Z}_3$-extension of k and $\mathbb{Q}_1 = \mathbb{Q}(\theta)$, where $\theta = 2\cos(2\pi/9)$. Then $k_1 = \mathbb{Q}(\sqrt{m}, \theta)$. We put $\omega = (1 + \sqrt{m})/2$ or $\sqrt{m}$ according as $m \equiv 1 \pmod 4$ or $2, 3 \pmod 4$, and $\theta' = 2\cos(4\pi/9)$. The following facts are well known:

(a) $\{1, \theta, \theta'\}$ is an integral basis for $\mathbb{Q}_1$,
(b) $\{1, \omega\}$ is an integral basis for k.

We further assume that m is prime to 3. Since k and $\mathbb{Q}_1$ are linearly disjoint over $\mathbb{Q}$ and their discriminants are relatively prime, we obtain the following:

(c) $\{1, \theta, \theta', \omega, \theta\omega, \theta'\omega\}$ is an integral basis for k_1.

Since k_1 is a real cyclic extension of degree 6 over $\mathbb{Q}$, we can determine the unit group E_1 by Mäki's algorithm (cf. [3, 9]). We now let

$$E_1 = \langle -1, \eta_1, \eta_2, \eta_3, \eta_4, \eta_5 \rangle,$$

where the generators η_i are obtained by this algorithm and represented as linear combinations of the integral basis (c) for k_1. Then we can compute $n_2^{(1)}$ for $p = 3$ because this algorithm enables us to determine either $N_{1,0}(E_1) = E_0$ or E_0^3 (cf. §3 in [9], also [3]).

Now we assume that $m \equiv 1 \pmod 3$. In order to compute $n_0^{(1)}$ for $p = 3$, we need to know the $\mathfrak{p}$-adic valuation of $N_{1,0}(\beta_1)^2 - 1$. Thus we have to find a generator β_1 of ${\mathfrak{p}'_1}^{d_1}$. Note that $d_1 = d_0$ or $3d_0$.

In the case where $d_1 = 3d_0$, we have $(\beta_0) = {\mathfrak{p}'_1}^{3d_1} = (\beta_1)$. Hence, we may take $\beta_0 \in k_1$ as a generator of ${\mathfrak{p}'_1}^{d_1}$ and can obtain β_0 explicitly by a continued fraction expansion as in solving the Pell equations.

In another case where $d_1 = d_0$, we have $(\beta_0) = {\mathfrak{p}'_1}^{3d_1} = (\beta_1^3)$. Therefore we obtain

$$\beta_1^3 = \pm \eta_1^{r_1} \eta_2^{r_2} \eta_3^{r_3} \eta_4^{r_4} \eta_5^{r_5} \beta_0 \qquad \text{for some } r_i \in \mathbb{Z}.$$

Since $(\beta_0) = (\beta_1^3)$, there exists an *appropriate* system $(r_1, r_2, r_3, r_4, r_5)$, where $0 \le r_i \le 2$, with the property that $\eta_1^{r_1} \eta_2^{r_2} \eta_3^{r_3} \eta_4^{r_4} \eta_5^{r_5} \beta_0$ is a cube in k_1. Then its unique real cubic root in k_1 is a generator of ${\mathfrak{p}'_1}^{d_1}$. To find this *appropriate* system, we check whether a given $\eta_1^{r_1} \eta_2^{r_2} \eta_3^{r_3} \eta_4^{r_4} \eta_5^{r_5} \beta_0$ is a cube in k_1, using approximate values of its unique real cubic root and its conjugates, and this is verified rigorously afterwards (see Example 1).

Our programs have been executed on a Sun SPARC-station 2 using the C-language and on a NEC PC-9801RA using Y. Kida's UBASIC86.

Remark 2. We do not need to know the entire unit group of k_1 for our purpose. It is sufficient to know only the unit group *modulo cubic*.

4. New examples of k with $\lambda_3(k) = 0$

By executing our procedure mentioned in the previous section, we will give some examples of k with $\lambda_3(k) = 0$ in the cases where $n_1 = n_2 = 3$, 4 and 5, respectively. First, we describe the following explicit example of such a k in detail.

Example 1. Let $k = \mathbb{Q}(\sqrt{8965})$ and $p = 3$. Then we can easily verify that $h = 2$ $(A_0 = 1)$, $d_0 = 2$, $\varepsilon = 402390206 + 8590401\omega$, $\mathfrak{p}^2 = (890 + 19\omega)$ and $\mathfrak{p}'^2 = (890 - 19\omega)$, so $\beta_0 = 890 - 19\omega$, where ω is as in §3. It follows from the $\mathfrak{p}$-adic expansions of ε^2 and β_0^2 that $n_0 = n_1 = n_2 = 3$. Since $\lambda_3^-(k^*) = \lambda_3(\mathbb{Q}(\sqrt{-3 \cdot 8965}))$, it also follows from Fukuda's table [4] that $\lambda_3^-(k^*) = 1$.

On the other hand, by the method of Mäki, we obtain a system $\{\eta_1, \eta_2, \eta_3, \eta_4, \eta_5\}$ of fundamental units of k_1 as follows:

$$\begin{aligned}
\eta_1 &= \varepsilon = 402390206 + 8590401\omega, \\
\eta_2 &= \theta, \\
\eta_3 &= \theta', \\
\eta_4 &= 48894 - 364640\theta + 191520\theta' + 1045\omega - 7720\theta\omega + 4160\theta'\omega, \\
\eta_5 &= 49939 - 195680\theta - 568040\theta' - 1045\omega + 4160\theta\omega + 11880\theta'\omega,
\end{aligned}$$

where θ and θ' are as in §3. We note that $\{\theta, \theta'\}$ is a system of fundamental units of $\mathbb{Q}_1$, and that η_4 and η_5 are relative units of k_1. Hence it follows that $N_{1,0}(E_1) = E_0^3$, so we obtain $n_2^{(1)} = 4$.

In this case, we have $d_1 = d_0 = 2$ by Theorem 1 for $r = 0$ of [10]. Now let us put $\gamma = \eta_1 \eta_2^2 \eta_3 \eta_4 \eta_5 \beta_0$, i.e., choose the system $(1, 2, 1, 1, 1)$ (see Remark 3). Then we can get approximate values γ_i of the unique real cubic roots of the six conjugates of γ as follows:

$$\begin{aligned}
\gamma_1 &\doteqdot -9577.87443954844258997143906495554959 43\cdots, \\
\gamma_2 &\doteqdot -0.0578252538221422012093779803554794569\cdots, \\
\gamma_3 &\doteqdot -11423747.6941770457646474962532507834 15\cdots, \\
\gamma_4 &\doteqdot -0.0001895209088981839062474670241349699\cdots, \\
\gamma_5 &\doteqdot -13.3733680698208492348943934432438859 52\cdots, \\
\gamma_6 &\doteqdot -0.0000005612408729122976653704111340309\cdots.
\end{aligned}$$

Taking the trace from k_1 to $\mathbb{Q}$, we have

$$\sum_{i=1}^{6} \gamma_i \doteqdot -11433339.000000000000000000000000000000\cdots,$$

which is close to an integer (if it is not, then this system is not *appropriate*). By solving the system of equations

$$\begin{cases}
\gamma_1 = x_0 + x_1\theta + x_2\theta' + (y_0 + y_1\theta + y_2\theta')\omega, \\
\gamma_2 = x_0 + x_1\theta' + x_2\theta'' + (y_0 + y_1\theta' + y_2\theta'')\omega', \\
\gamma_3 = x_0 + x_1\theta'' + x_2\theta + (y_0 + y_1\theta'' + y_2\theta)\omega, \\
\gamma_4 = x_0 + x_1\theta + x_2\theta' + (y_0 + y_1\theta + y_2\theta')\omega', \\
\gamma_5 = x_0 + x_1\theta' + x_2\theta'' + (y_0 + y_1\theta' + y_2\theta'')\omega, \\
\gamma_6 = x_0 + x_1\theta'' + x_2\theta + (y_0 + y_1\theta'' + y_2\theta)\omega',
\end{cases}$$

where $\theta'' = 2\cos(8\pi/9)$ and $\omega' = (1 - \sqrt{8965})/2$, we obtain the following root approximately:

$$(x_0, x_1, x_2, y_0, y_1, y_2) \doteqdot (-1885431, 1396449, -745160, -40251, 29812, -15908),$$

which is also close to an integer (if it is not, then this system is not *appropriate*). We then put

$$\beta_1 = -1885431 + 13964449\theta - 7451160\theta' - 40251\omega + 298812\theta\omega - 159908\theta'\omega.$$

It is easy to verify that $\gamma = \beta_1^3$, so the system $(1, 2, 1, 1, 1)$ is really *appropriate*. Hence β_1 is a generator of ${\mathfrak{p}'_1}^2$. Taking the norm from k_1 to k, we have $N_{1,0}(\beta_1) = -723897967519 - 15454088423\omega$. It follows from the $\mathfrak{p}$-adic expansion of $N_{1,0}(\beta_1)^2$ that $n_0^{(1)} = 3 \neq n_2^{(1)}$.

Therefore we see by Theorem 1 for $r = 1$ that $\lambda_3(\mathbb{Q}(\sqrt{8965})) = 0$.

Remark 3. In Example 1, if $(r_1, r_2, r_3, r_4, r_5)$ is an *appropriate* system, then $3^2\theta^{2r_2}{\theta'}^{2r_3}$ is a cube in $\mathbb{Q}_1$. On the other hand, it is easy to see that $3\theta^2\theta'$ is a cube in $\mathbb{Q}_1$. Hence we obtain $r_2 = 2$ and $r_3 = 1$, so that it suffices for all practical purposes to search among only r_1, r_4 and r_5, where $0 \leq r_i \leq 2$. This is often efficient in finding an *appropriate* system for other examples.

Let m be a positive square-free integer such that $m \equiv 1 \pmod 3$. We executed the above procedure for the following all real quadratic fields $k = \mathbb{Q}(\sqrt{m})$ and $p = 3$:

(i) $n_1 = n_2 = 3$ for $1 \leq m \leq 20000$ (The number of such k's is exactly 31).
(ii) $n_1 = n_2 = 4$ for $1 \leq m \leq 30000$ (The number of such k's is exactly 10).
(iii) $n_1 = n_2 = 5$ for $1 \leq m \leq 50000$ (The number of such k's is exactly 2).

The results are summarized in Tables 1, 2 and 3. In these tables, h, A_0, d_n and $\lambda_3^-(k^*)$ are as in §2, and $D_n = \langle Cl(\mathfrak{p}'_n)\rangle \cap A_n$, where $Cl(\mathfrak{p}'_n)$ denotes the ideal class of $\mathfrak{p}'_n$. The mark $*$ indicates that the assumptions (1) and (2) of Theorem 1 are satisfied for $r = 1$, but we do not know whether $\lambda_3(k) = 0$ or not, and the mark $**$ indicates that we cannot apply Theorem 1, so we do not know whether $\lambda_3(k) = 0$ or not. For the 17 remaining k's, i.e., exactly 11, 4 and 2 k's in the cases where $n_1 = n_2 = 3$, 4 and 5, respectively, we can verify that Greenberg's conjecture is true by Theorem 1 for $r = 1$.

TABLE 1. The case where $n_1 = n_2 = 3$ for $p = 3$

m	h	$\lvert A_0\rvert$	d_0	$\lvert D_0\rvert$	d_1	$\lvert D_1\rvert$	$\lambda_3^-(k^*)$	$(n_0^{(1)}, n_2^{(1)})$	$\lambda_3(k)$
2059	2	1	2	1	2	1	1	(4,4)	$*$
2917	3	3	3	3	3	3	3	(4,4)	$**$
4081	4	1	4	1	4	1	1	(4,4)	$*$
4279	6	3	6	3	18	9	2	(3,3)	$**$
5062	1	1	1	1	1	1	1	(3,4)	0
5611	10	1	5	1	15	3	3	(3,3)	$**$
7006	12	3	12	3	12	3	3	(3,4)	$**$
7465	18	9	18	9	18	9	2	(3,4)	$**$
7969	2	1	1	1	1	1	1	(3,4)	0
8965	2	1	2	1	2	1	1	(3,4)	0
9895	10	1	10	1	10	1	1	(3,4)	0
12007	3	3	3	3	3	3	2	(3,4)	$**$
12313	1	1	1	1	1	1	1	(4,4)	$*$
12421	1	1	1	1	1	1	1	(4,4)	$*$
12553	1	1	1	1	1	1	1	(4,4)	$*$
13939	2	1	2	1	2	1	1	(3,4)	0
14113	13	1	13	1	39	3	2	(3,3)	$**$
15802	2	1	2	1	2	1	1	(3,4)	0
16081	2	1	1	1	1	1	1	(4,4)	$*$
16519	1	1	1	1	1	1	1	(3,4)	0
17431	1	1	1	1	3	3	2	(3,3)	$**$
17443	1	1	1	1	3	3	3	(3,3)	$**$
17686	2	1	1	1	3	3	2	(3,3)	$**$
18022	1	1	1	1	1	1	1	(4,4)	$*$
18085	2	1	2	1	6	3	2	(3,3)	$**$
18091	2	1	1	1	1	1	1	(3,4)	0
18721	10	1	5	1	5	1	1	(4,4)	$*$
18766	2	1	1	1	1	1	1	(3,4)	0
18787	1	1	1	1	1	1	1	(3,4)	0
18826	6	3	6	3	6	3	2	(4,4)	$**$
19309	1	1	1	1	1	1	1	(3,4)	0

TABLE 2. The case where $n_1 = n_2 = 4$ for $p = 3$

m	h	$\|A_0\|$	d_0	$\|D_0\|$	d_1	$\|D_1\|$	$\lambda_3^-(k^*)$	$(n_0^{(1)}, n_2^{(1)})$	$\lambda_3(k)$
2149	1	1	1	1	1	1	1	(5,5)	$*$
9814	2	1	2	1	2	1	1	(5,5)	$*$
10849	1	1	1	1	1	1	1	(5,5)	$*$
16861	4	1	2	1	2	1	1	(4,5)	0
17707	1	1	1	1	1	1	1	(5,5)	$*$
24007	1	1	1	1	1	1	1	(4,5)	0
24985	2	1	2	1	6	3	3	(4,4)	$**$
25597	2	1	1	1	1	1	1	(4,5)	0
26245	16	1	4	1	4	1	1	(4,5)	0
26893	3	3	1	1	1	1	1	(4,5)	$**$

TABLE 3. The case where $n_1 = n_2 = 5$ for $p = 3$

m	h	$\|A_0\|$	d_0	$\|D_0\|$	d_1	$\|D_1\|$	$\lambda_3^-(k^*)$	$(n_0^{(1)}, n_2^{(1)})$	$\lambda_3(k)$
22333	1	1	1	1	1	1	1	(5,6)	0
42205	2	1	2	1	2	1	1	(5,6)	0

Acknowledgment

The author wishes to express his thanks to Professor T. Fukuda for helpful suggestions during his computational work, and to Professors N. Adachi, S. Iyanaga and S. Nakajima for their kind advice and encouragement.

References

1. B. Ferrero and L. C. Washington, *The Iwasawa invariant μ_p vanishes for abelian number fields*, Ann. of Math., **109** (1979), pp. 377–395. MR **81a:**12005
2. T. Fukuda, *Iwasawa λ-invariants of certain real quadratic fields*, Proc. Japan Acad., **65**A (1989), pp. 260–262. MR **91b:**11115
3. ______, *Computation of unit group for $\mathbb{Z}_3$-extensions of real quadratic fields*, Bull. of Yamagata Univ., Nat. Sci., **13**, no.1 (1992), pp. 27–33. MR **93g:**11108
4. ______, *Iwasawa λ-invariants of imaginary quadratic fields*, J. of the College of Industrial Technology, Nihon Univ. 27 (1994), 35–88.
5. T. Fukuda and K. Komatsu, *On $\mathbb{Z}_p$-extensions of real quadratic fields*, J. Math. Soc. Japan, **38** (1986), pp. 95–102. MR **87d:**11081
6. T. Fukuda, K. Komatsu, and H. Wada, *A remark on the λ-invariants of real quadratic fields*, Proc. Japan Acad., **62**A (1986), pp. 318–319. MR **88a:**11113
7. R. Greenberg, *On the Iwasawa invariants of totally real number fields*, Amer. J. Math., **98** (1976), pp. 263–284. MR **53:**5529
8. K. Iwasawa, *On $\mathbb{Z}_l$-extensions of algebraic number fields*, Ann. of Math., **98** (1973), pp. 246–326. MR **50:**2120
9. S. Mäki, *The determination of units in real cyclic sextic fields*, in Lecture Notes in Math. 797. Springer–Verlag, Berlin, Heidelberg, New York (1980). MR **82a:**12004
10. H. Taya, *On the Iwasawa λ-invariants of real quadratic fields*, Tokyo J. Math., **16** (1993), pp. 121–130. MR **94f:**11113
11. L. C. Washington, *Introduction to Cyclotomic Fields*, in Graduate Texts in Math. vol. 83. Springer-Verlag, New York, Heidelberg, Berlin (1982). MR **85g:**11001

DEPARTMENT OF MATHEMATICS, SCHOOL OF SCIENCE AND ENGINEERING, WASEDA UNIVERSITY 3-4-1, OKUBO SHINJUKU-KU, TOKYO 169, JAPAN

E-mail address: taya@cfi.waseda.ac.jp