The Iwasawa invariants and the higher K-groups associated to real quadratic fields

Hiroki Sumida-Takahashi *

Abstract

Using fast algorithms, we computed the Iwasawa invariants of $\mathbf{Q}(\sqrt{f}, \zeta_p)$ in the range $1 < f < 200$ and $3 \leq p < 100\,000$. From these computational results, we obtained concrete information on the higher K-groups of the ring of integers of $\mathbf{Q}(\sqrt{f})$.

1 Introduction

Let χ be an *even* Dirichlet character of conductor $f = f_\chi$. The generalized Bernoulli numbers $B_{k,\chi}$ are defined by

$$\sum_{a=1}^{f} \frac{\chi(a)te^{at}}{e^{ft}-1} = \sum_{k=0}^{\infty} B_{k,\chi}\frac{t^k}{k!}.$$

First, let us look back over the case of $\chi = \chi^0$ the trivial character . For $k \neq 1$, B_{k,χ^0} is the k-th Bernoulli number B_k, and $B_{1,\chi^0} = B_1 + 1 = 1/2$. A pair of integers (p, k) is said to be an irregular pair if p is a prime, k is an even integer satisfying $2 \leq k \leq p-3$, and p divides the numerator of $B_k = B_{k,\chi^0}$. Irregular pairs have been computed by Kummer, Vandiver, D.H. Lehmer, E. Lehmer, Selfridge, Nicol, Pollack, Johnson, Wada, Wagstaff, Tanner, Ernvall, Metsänkylä, Buhler, Crandall, Sompolski and Shokrollahi. These computations were originally used to verify "Fermat's Last Theorem". However, even after the proof was completed by Wiles, they are still important because they give us concrete knowledge of the ideal class group of cyclotomic fields.

*Partially supported by the Grants-in-Aid for Encouragement of Young Scientists (No.16740019) from Japan Society for the Promotion of Science.
Mathematics Subject Classification (2000): 11R23, 11R70
key words and phrases: Iwasawa invariant, K-group, Vandiver's conjecture, Greenberg's conjecture

Let p be an odd prime number and A_n the p-part of the ideal class group of $K_n = \mathbf{Q}(\zeta_{p^{n+1}})$. Let $\omega = \omega_p$ be the Teichmüller character $\mathbf{Z}/p\mathbf{Z} \to \mathbf{Z}_p$ such that $\omega(a) \equiv a \bmod p$. We identify $\Delta = \mathrm{Gal}(K_\infty/\mathbf{Q}_\infty)$ with $(\mathbf{Z}/p\mathbf{Z})^\times$. Put

$$e_{\omega^k} = \frac{1}{\sharp\Delta} \sum_{\delta \in \Delta} \omega^k(\delta)\delta^{-1}$$

the idempotent of the group ring $\mathbf{Q}_p[\Delta]$. Then we have

$$A_n = \bigoplus_{k:even} e_{\omega^k} A_n \oplus \bigoplus_{p-k:odd} e_{\omega^{p-k}} A_n,$$

where k is an even integer with $2 \le k \le p-1$. We denote the even part (resp. odd part) by A_n^+ (resp. A_n^-). Let r_p be the irregularity index, i.e., the number of irregular pairs (p, k). For any prime number $p < 12\ 000\ 000$, it has been verified that

$$A_n^+ = \{0\} \text{ and } A_n^- \simeq (\mathbf{Z}/p^{n+1}\mathbf{Z})^{r_p} \text{ for all } n \ge 0$$

(cf. [Buhler et al. 1993] and [Buhler et al. 2001]). The former statement is called Vandiver's conjecture. We have a naive explanation of the fact that we have not been able to find any counter-example. If we follow the argument of [Washington 1997, pp.158–159], we can expect that the number of exceptions to Vandiver's conjecture for $x_0 < p \le x_1$ is approximately $(\log\log x_1 - \log\log x_0)/2$. Then, $(\log\log 12\ 000\ 000 - \log\log 37)/2 = 0.7536143467\cdots$ is perhaps too small to find one counter-example. However, many number theorists may doubt the above expected number. As a matter of fact, we have to consider some effects on ideal class groups from an upper bound for the numerators of Bernoulli numbers, and from a lower bound for discriminants (cf. [Washington 1997, pp.221–230]). If there is another strong bound, the actual number can be much less than the above number.

In this paper, following [Sumida-Takahashi 2004], we consider the $\chi\omega^k$-part instead of the ω^k-part, where χ is an even quadratic Dirichlet character. The reason why we consider quadratic characters is that their values are included in $\mathbf{Q}$ as well as the trivial character. The first main purpose of this paper is to effectively find "exceptional pairs" $(p, \chi\omega^k)$ in order to argue about the expected number. Here we call $(p, \chi\omega^k)$ an exceptional pair if and only if $\chi\omega^k(p) \ne 1$, $\chi\omega^{1-k}(p) \ne 1$, and one of the following conditions is satisfied: $\nu_p(\chi\omega^k) > 0$, $v_p(L_p(1, \chi\omega^k)) > 1$, $v_p(L_p(0, \chi\omega^k)) > 1$, or $\tilde{\lambda}_p(\chi\omega^k) > 1$, where $\nu_p(\chi\omega^k)$ is the $\chi\omega^k$-part of ν_p-invariant and v_p is the p-adic valuation such that $v_p(p) = 1$ (see section 3 for the details). We actually computed the Iwasawa invariants of $\mathbf{Q}(\sqrt{f_\chi}, \zeta_p)$ in the range $1 < f_\chi < 200$ and $3 \le p < 100\ 000$. From our data, the actual number of exceptional pairs seems to be near to the expected number in the range. On the other hand, we could not find any exceptional pair for $f_\chi = 5$ and $p < 2\ 000\ 000$ as well as for the trivial character.

Let $F = F_\chi$ be the real quadratic field associated to χ, and $\mathcal{O}_F$ the ring of integers of F. By [Dwyer and Friedlander 1985] and [Kolster et al. 1996], there are relations between Quillen's K-groups $K_n(\mathcal{O}_F)$ and the Iwasawa modules for unramified abelian p-extensions of $\cup_{n\geq 0}F(\zeta_{p^n})$. The second main purpose of this paper is to give concrete information on the higher K-groups of $\mathcal{O}_F$ by using the computational results. For example, we found that for $3 \leq p < 100\,000$, p divides the order of $K_{68372}(\mathcal{O}_{\mathbf{Q}(\sqrt{8})})$ if and only if $p = 34301$ under the Quillen-Lichtenbaum conjecture.

2 Notation and conjectures

In this section, we introduce some conjectures on higher K-groups and Iwasawa modules, which will appear in the following sections.

Let F be a finite extension of $\mathbf{Q}$. The following theorems and conjecture are well known.

Theorem 1. (*Quillen*) *For all $n \geq 0$, $K_n(\mathcal{O}_F)$ is a finitely generated $\mathbf{Z}$-module.*

Theorem 2. (*Borel*) *For $m \geq 1$,*

$$\mathrm{rank}_{\mathbf{Z}}(K_{2m-1}(\mathcal{O}_F)) = \begin{cases} r_1(F) + r_2(F) & \text{if } m \text{ is odd,} \\ r_2(F) & \text{if } m \text{ is even,} \end{cases}$$

where $r_1(F)$ is the number of real embeddings of F, and $r_2(F)$ is the number of pairs of complex embeddings of F. Further,

$$K_{2m-2}(\mathcal{O}_F) \text{ is finite.}$$

Conjecture 1. (*The Quillen-Lichtenbaum conjecture*) *The natural map* (*via p-adic Chern characters*)

$$K_{2m-i}(\mathcal{O}_F) \otimes \mathbf{Z}_p \to H^i_{\acute{e}t}(Spec(\mathcal{O}_F[1/p]), \mathbf{Z}_p(m))$$

is an isomorphism for all $m \geq 2$, $i = 1, 2$ and any odd prime number p, where $A(m)$ is the m-th Tate twist of a Galois module A.

The surjectivity of p-adic Chern characters was proved by [Dwyer and Friedlander 1985]. We simply denote $H^i_{\acute{e}t}(Spec(\mathcal{O}_F[1/p]), A)$ by $H^i(\mathcal{O}_F, A)$. Put $K = F(\zeta_p)$ and denote by K_∞ the cyclotomic $\mathbf{Z}_p$-extension of K. Put $G_\infty = \mathrm{Gal}(K_\infty/F)$, $\Delta = \mathrm{Gal}(K_\infty/F_\infty)$ and $\Gamma = \mathrm{Gal}(K_\infty/K)$. Then we have $G_\infty = \Delta \times \Gamma$. Let L_∞ be the maximal unramified abelian p-extension of K_∞ and L'_∞ the maximal unramified abelian p-extension of K_∞ in which every prime divisor lying above p splits completely. Put $X_\infty = \mathrm{Gal}(L_\infty/K_\infty)$ and $X'_\infty = \mathrm{Gal}(L'_\infty/K_\infty)$. Let E'_n be the group of p-units of K_n and $\overline{E}'_\infty = \lim_{\leftarrow}(E'_n \otimes \mathbf{Z}_p)$, where the inverse limits are taken with respect to norm maps. The above étale cohomology groups are expressed as follows.

Theorem 3. ([Schneider 1979, §6.1] and [Kolster et al. 1996, §3, §4]) *For $m \neq 0, 1$, we have an exact sequence*

$$0 \to (\overline{E}'_\infty(m-1))_{G_\infty} \to H^1(\mathcal{O}_F, \mathbf{Z}_p(m)) \to X'_\infty(m-1)^{G_\infty} \to 0.$$

Further we have $H^1(\mathcal{O}_F, \mathbf{Z}_p(m))_{tors} \simeq H^0(\mathcal{O}_F, \mathbf{Q}_p/\mathbf{Z}_p(m))$.
For $m \neq 1$, we have an exact sequence

$$\begin{aligned} 0 \to X'_\infty(m-1)_{G_\infty} &\to H^2(\mathcal{O}_F, \mathbf{Z}_p(m)) \\ &\to \prod_{v|p} H^2(F_v, \mathbf{Z}_p(m)) \to H^0(\mathcal{O}_F, \mathbf{Q}_p/\mathbf{Z}_p(1-m))^\vee \to 0, \end{aligned}$$

where $A^\vee = \mathrm{Hom}_{\mathbf{Z}_p}(A, \mathbf{Q}_p/\mathbf{Z}_p)$.

It is not difficult to compute $H^0(\mathcal{O}_F, \mathbf{Q}_p/\mathbf{Z}_p(m))$ and $H^2(F_v, \mathbf{Z}_p(m))$ (cf. section 4). Therefore, if the Quillen-Lichtenbaum conjecture is true, it is not difficult to determine the structure of $K_{2m-1}(\mathcal{O}_F)$ as an abelian group. Further, we can obtain the order of $K_{2m-2}(\mathcal{O}_F)$ by using the order of $X'_\infty(m-1)_{G_\infty}$. Let us consider the following case

$$F \text{ is totally real and } F \cap \mathbf{Q}(\zeta_p) = \mathbf{Q}.$$

For a $\mathbf{Z}_p[\Delta]$-module A and a character ω^m of $\Delta \simeq \mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})$, we denote $e_{\omega^m}A$ by $A^{(m)}$. Since

$$X'_\infty(m-1)_{G_\infty} \simeq (X'^{(1-m)}_\infty \otimes \mathbf{Z}_p(m-1))_\Gamma,$$

it is important to study the structure of $X'^{(1-m)}_\infty$ as an Iwasawa module. If m is even, $X'^{(1-m)}_\infty$ has no nontrivial finite submodule (cf. [Washington 1997, p. 290]). Therefore, the order of the Γ-coinvariant quotient can be obtained from the Iwasawa polynomial for $X'^{(1-m)}_\infty$. By the Iwasawa main conjecture proved by [Mazur and Wiles 1984] and [Wiles 1990], the polynomial is essentially the p-adic L-function. Therefore, if F is abelian, it suffices to compute the Kubota-Leopoldt p-adic L-function. On the other hand, if m is odd, it seems to be more difficult to study the structure of $X'^{(1-m)}_\infty$. In fact, the following classical conjectures are still open.

Conjecture 2. (*Vandiver's conjecture*) *For $F = \mathbf{Q}$ and any odd integer m, $X'^{(1-m)}_\infty$ is trivial.*

Conjecture 3. (*Greenberg's conjecture*) *For any totally real number field F and any odd integer m, $X'^{(1-m)}_\infty$ is finite.*

So far we have not been able to find any counter-example to the conjectures. Conjecture 2 has been verified for all $p < 12\ 000\ 000$. Conjecture 3 has been mainly verified for real abelian fields with small discriminants and some prime numbers $p = 3, 5, 7, \cdots$ by using cyclotomic units and auxiliary prime numbers (cf. [Ichimura and Sumida 1996] and [Kraft and Schoof 1995]). In [Sumida-Takahashi 2004], the author exploited a method to effectively check the exact value of the p-part of the class number by using Gauss sums and auxiliary prime numbers. We will give some numerical examples of the Iwasawa invariants and the higher K-groups in the following sections.

3 Iwasawa invariants of $\mathbf{Q}(\sqrt{f_\chi}, \zeta_p)$

Let χ be an *even quadratic* Dirichlet character and p an odd prime number. Put $F = F_\chi = \mathbf{Q}(\sqrt{f_\chi})$ and $K = \mathbf{Q}(\sqrt{f_\chi}, \zeta_p)$. We use the notation in the previous sections. We put $\Delta' = \mathrm{Gal}(K_\infty/\mathbf{Q}_\infty)$ and $e'_\psi = \frac{1}{\sharp\Delta'}\sum_{\delta\in\Delta'}\psi(\delta)\delta^{-1}$ for a Dirichlet character ψ of Δ'. For a $\mathbf{Z}_p[\Delta']$-module A, we denote $e'_\psi A$ by A^ψ. Let $\lambda_p(\psi)$, $\mu_p(\psi)$ and $\nu_p(\psi)$ (resp. $\lambda'_p(\psi)$, $\mu'_p(\psi)$ and $\nu'_p(\psi)$) be the Iwasawa invariants associated to X^ψ_∞ (resp. X'^ψ_∞), i.e.,

$$\sharp A^\psi_n = p^{\lambda_p(\psi)n+\mu_p(\psi)p^n+\nu_p(\psi)} \quad (\text{resp. } \sharp A'^\psi_n = p^{\lambda'_p(\psi)n+\mu'_p(\psi)p^n+\nu'_p(\psi)})$$

for sufficiently large n. By Ferrero-Washington's theorem, we have $\mu_p(\psi) = \mu'_p(\psi) = 0$ for all p and ψ.

Assume that ψ is even. The Iwasawa polynomial $g_\psi(T) \in \mathbf{Z}_p[T]$ for the p-adic L-function is defined as follows. Let $L_p(s,\psi)$ be the p-adic L-function constructed by [Kubota and Leopoldt 1964]. Let f_0 be the least common multiple of f_ψ and p. By [Iwasawa 1972, §6], there uniquely exists $G_\psi(T) \in \mathbf{Z}_p[[T]]$ satisfying $G_\psi((1+f_0)^{1-s}-1) = L_p(s,\psi)$ for all $s \in \mathbf{Z}_p$ if $\psi \neq \chi^0$. By [Ferrero and Washington 1979], it was proved that p does not divide $G_\psi(T)$. Therefore, by the p-adic Weierstrass preparation theorem, we can uniquely write $G_\psi(T) = g_\psi(T)u_\psi(T)$, where $g_\psi(T)$ is a distinguished polynomial of $\mathbf{Z}_p[T]$ and $u_\psi(T)$ is an invertible element of $\mathbf{Z}_p[[T]]$. Put $\tilde{\lambda}_p(\psi) = \deg g_\psi(T)$.

Let k be an even integer with $2 \le k \le p-3$. Then $\chi\omega^k$ is an even character. For a pair $(p, \chi\omega^k)$, we set the following condition

$$\text{(C)} \qquad \chi\omega^k(p) \neq 1 \text{ and } \chi\omega^{1-k}(p) \neq 1.$$

If $\chi\omega^k(p) \neq 1$, we have $\lambda_p(\chi\omega^k) = \lambda'_p(\chi\omega^k)$ and $\nu_p(\chi\omega^k) = \nu'_p(\chi\omega^k)$. In the range $1 < f_\chi < 200$, $3 \le p < 100\,000$ and even integers k with $2 \le k \le p-3$, there are 13 631 032 822 pairs of $(p, \chi\omega^k)$ satisfying (C). Among them, 288 086 pairs satisfy $\tilde{\lambda}_p(\chi\omega^k) = 1$, 53 pairs $\tilde{\lambda}_p(\chi\omega^k) = 2$, and two pairs $\tilde{\lambda}_p(\chi\omega^k) = 3$. By the method of [Ichimura and Sumida 1996], we verified Greenberg's conjecture, i.e., $\lambda_p(\chi\omega^k) = 0$ for each of them. Moreover, we checked that $\nu_p(\chi\omega^k) \le 2$. In the above range, 38 pairs do not satisfy (C). For these cases, we checked that $\tilde{\lambda}_p(\chi\omega^k) = 0$ if $\chi\omega^k(p) = 1$, and that $\tilde{\lambda}_p(\chi\omega^k) = 1$ if $\chi\omega^{1-k}(p) = 1$, which implies that $\nu_p(\chi\omega^k) = 0$. Further, by computation of the p-units of real quadratic fields $\mathbf{Q}(\sqrt{f_\chi})$, we verified that $\lambda_p(\chi) = \lambda'_p(\chi) = \nu'_p(\chi) = 0$ for all f_χ and p in the above range (cf. [Fukuda and Komatsu 1986] and [Fukuda and Taya 1995]).

Proposition 1. $\lambda_p(\mathbf{Q}(\sqrt{f_\chi}, \zeta_p + \zeta_p^{-1})) = 0$ *for all* $1 < f_\chi < 200$ *and* $3 \le p < 100\,000$.

The ν-invariants of real quadratic fields

$\nu_p(\chi)$	(f_χ, p)
1	(8,31)(24,523)(33,29)(33,37)(37,7)(40,191)(40,643)(41,7211)(57,59) (57,28927)(60,181)(65,8831)(69,5)(73,41)(76,79)(85,3)(92,7)(97,3331) (104,2683)(109,3)(109,5)(109,809)(113,53)(113,20219)(124,157) (129,5419)(136,37)(136,547)(136,4733)(140,23)(140,577)(145,17) (145,37)(149,7)(156,5)(156,7)(157,9613)(161,5)(165,199)(172,3) (173,227)(181,3)(185,139)(185,2389)
2	(89,5)(69,17)

Let us call a pair of integers (p,k) a χ-irregular pair if p is a prime, k is an even integer satisfying $2 \leq k \leq p-3$, p divides $a_0(\chi\omega^k) = L_p(1,\chi\omega^k)$ (or $b_0(\chi\omega^k) = L_p(0,\chi\omega^k)$), and $(p,\chi\omega^k)$ satisfies (C). Further we define the χ-irregularity index $r_p(\chi)$ by

$$r_p(\chi) = \sharp\{(p,k) | (p,k) \text{ is a } \chi\text{-irregular pair}\}.$$

We call a prime number p χ-irregular if $r_p(\chi) > 0$. Let $m_p(\chi)$ be the number of even integers k with $2 \leq k \leq p-3$ such that $(p,\chi\omega^k)$ satisfies (C). We define

$$n_r = \sum_{(\chi,p) \text{ s.t. } r_p(\chi)=r} 1$$

and

$$n'_r = \sum_{\chi,p} {}_{m_p(\chi)}C_r \left(\frac{1}{p}\right)^r \left(\frac{p-1}{p}\right)^{m_p(\chi)-r},$$

where χ runs over all even quadratic characters with $1 < f_\chi < 200$, and p runs all prime numbers with $3 \leq p < 100\ 000$. The distribution of the indices of χ-irregularity is given in the following table. The actual numbers n_r seem to be near to the expected numbers n'_r (cf. [Washington 1997, p.63]).

The χ-irregularity index density

r	n_r	n'_r	the density	the density'
0	348574	349090.14	0.60579423	0.60669125
1	174919	174464.73	0.30399548	0.30320601
2	43596	43583.01	0.07576642	0.07574384
3	7293	7257.27	0.01267466	0.01261257
4	942	906.2	0.00163712	0.00157492
5	73	90.51	0.00012686	0.00015730
6	3	7.53	0.00000521	0.00001309
7	0	0.53	0.00000000	0.00000093

We extended the tables of [Sumida-Takahashi 2004] to all primes below 100 000.

$\nu_p(\chi\omega^k) = 1$ (2 for the $*$-marked case)

f_χ	p	k	f_χ	p	k	f_χ	p	k	f_χ	p	k
8	34301	114	12	701	542	21	199	150	33	53	30
37	43	32	53	1033	564	56	55621	9294	69	19	14
85	3697	3086	88	71	26	101	5333	2770	104	19	14
113	43	32	113	3373	1602	124	197	126	124	239	48
129	67	28	140	4751	120	141	5431	4826	149	43	32
149	71	16	149	229	182	156	50051	4582	157	401	56
161	101	22	168	37	22	172	73	10	173	7	4
173	43	32	173	101	42	177	17	$6*$	181	71	52
181	6991	1628	185	827	354	188	1621	168	193	62791	57100
197	521	372									

$v_p(a_0(\chi\omega^k)) = 2$

f_χ	p	k	f_χ	p	k	f_χ	p	k	f_χ	p	k
8	59	36	17	61	32	21	149	128	21	10169	7388
28	977	828	33	59	42	37	1091	812	40	12101	318
41	7	4	41	283	102	44	787	148	53	7	2
53	1879	1158	57	2161	758	61	17	4	61	1747	1270
76	191	84	88	35099	24446	89	41	10	92	181	124
97	17	4	105	769	524	105	1453	162	120	2749	2196
124	41	30	124	26227	13770	140	107	74	149	797	140
149	2767	2178	152	17	12	152	25453	15704	156	66877	48258
168	43	10	173	13	4	177	31	24	184	373	72
193	7873	1886									

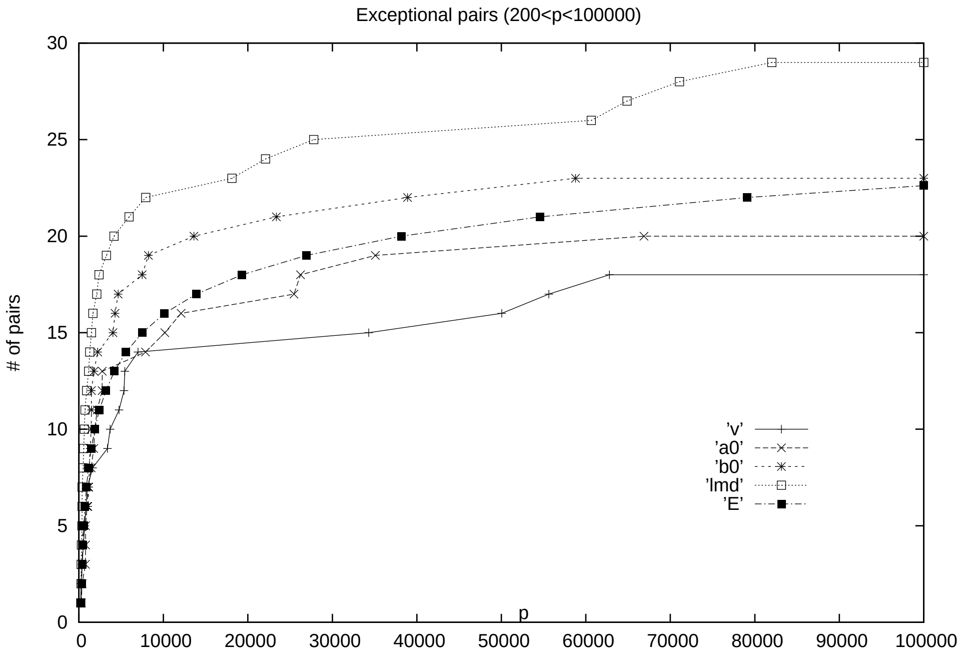
$v_p(b_0(\chi\omega^k)) = 2$

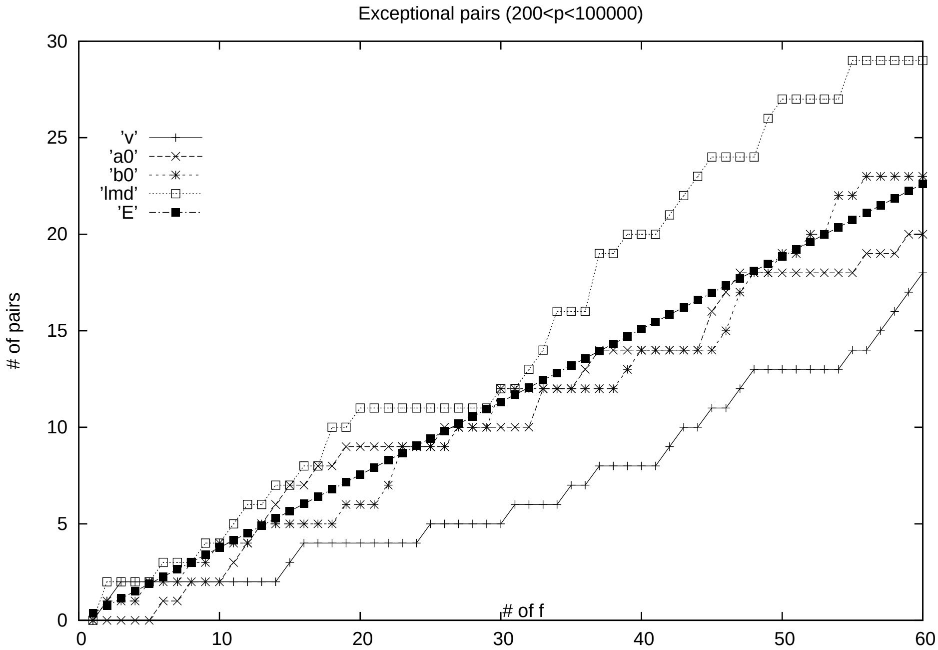
f_χ	p	k	f_χ	p	k	f_χ	p	k	f_χ	p	k
8	2221	1600	13	109	6	17	1319	88	28	223	126
33	31	24	33	1777	1184	41	19	12	41	421	126
60	19	14	61	7481	3516	73	11	2	73	1487	808
76	1451	418	76	4283	3484	89	23369	9986	97	367	26
97	13613	13022	109	41	32	133	1061	446	136	449	284
152	41	2	152	4027	3108	156	4637	2280	156	38891	9454
157	8221	582	165	29	26	165	89	66	165	1229	48
172	11	4	172	1487	900	177	337	74	177	58787	20838
184	1171	464	185	167	68	188	89	76			

$\underline{\tilde{\lambda}(\chi\omega^k) = 2 \text{ (3 for the } *\text{-marked cases)}}$

f_χ	p	k	f_χ	p	k	f_χ	p	k	f_χ	p	k
8	1151	842	8	27791	11840	21	11	4	21	60637	16528
24	29	4	24	181	84	29	569	64	37	5	2
37	89	66	37	3251	1094	40	257	232	44	653	448
53	193	14	56	1663	616	60	1277	582	60	1481	986
65	18121	3044	92	5	2	97	271	94	104	19	14
104	7919	4386	105	373	340	109	131	100	109	293	132
109	373	128	124	733	58	124	2111	1480	124	22091	15370
129	23	4	133	911	196	136	71	20	137	17	8
140	23	10	140	367	292	141	113	108	141	5939	2938
145	43	28	145	61	58	145	167	128	145	4157	3528
149	5	2	149	509	426	161	2389	646	161	64879	57186
165	11	2	165	23	6*	165	71089	24840	172	13	10
172	47	38	173	7	4	177	157	48	181	223	26
181	82007	51630	185	17	10*	185	17	6			

In the following graphs, we compare the actual number of exceptional pairs with the expected number in the range $200 < p < 100\ 000$.





On the other hand, we found the following fact.

Proposition 2. *For $f_\chi = 5$ and $p < 2\ 000\ 000$, there is no exceptional pair, that is, for any pair $(p, \chi\omega^k)$ which satisfies* (C),

$$\nu_p(\chi\omega^k) = 0,\ v_p(a_0(\chi\omega^k)) = v_p(b_0(\chi\omega^k)) = \tilde{\lambda}_p(\chi\omega^k) \leq 1.$$

From our data, the actual number seems to be near to the expected number. Even for large p, it might be possible that the actual number is near to the expected number. Therefore it is not very strange that we have not been able to find any exceptional pair for $\chi = \chi^0$, especially any counter-example to Vandiver's conjecture.

4 Higher K-groups of the ring of integers of $\mathbf{Q}(\sqrt{f_\chi})$

In order to compute étale cohomology groups, we prepare some notation. For an odd integer m, we write the Iwasawa polynomial $g_{\chi\omega^{1-m}}(T)$ for the p-adic L-function $L_p(s, \chi\omega^{1-m})$ in the form

$$g_{\chi\omega^{1-m}}(T) = \prod_{i=1}^{\tilde{\lambda}(\chi\omega^{1-m})} (T - \alpha_{\chi\omega^{1-m},i}), \quad \alpha_{\chi\omega^{1-m},i} \in \overline{\mathbf{Q}}_p.$$

We put

$$x(p, \chi, m-1) = \min\left\{\nu_p(\chi\omega^{1-m}),\ v_p\left(\prod_{i=1}^{\tilde{\lambda}(\chi\omega^{1-m})} \left(1 - (1+f_0)^{m-1}(\alpha_{\chi\omega^{1-m},i}+1)\right)\right)\right\}.$$

For an even integer m, put $\alpha^*_{\chi\omega^m,i} = \frac{f_0 - \alpha_{\chi\omega^m,i}}{1+\alpha_{\chi\omega^m,i}}$, $g^*_{\chi\omega^m}(T) = \prod_{i=1}^{\tilde{\lambda}(\chi\omega^m)}(T - \alpha^*_{\chi\omega^m,i})$ and

$$x^*(p,\chi,m-1) = v_p\left(\prod_{i=1}^{\tilde{\lambda}(\chi\omega^m)}\left(1-(1+f_0)^{m-1}(\alpha^*_{\chi\omega^m,i}+1)\right)\right).$$

Further, for an integer m, we define the following sets of prime numbers

$$\begin{aligned} S_1(\chi,m-1) = \ & \{p : \tfrac{p-1}{2} | (m-1),\ (p-1) \nmid (m-1),\ \chi\omega^{\frac{p-1}{2}}(p) = 1 \text{ and } \chi\omega^{\frac{p-1}{2}} \neq \chi^0\}, \\ S_2(\chi,m-1) = \ & \{p : (p-1)|(m-1) \text{ and } \chi(p) = 1\}. \end{aligned}$$

We put

$$y(p,\chi,m-1) = \begin{cases} v_p(m-1)+1 & \text{if } p \in S_1(\chi,m-1) \cup S_2(\chi,m-1), \\ 0 & \text{otherwise.} \end{cases}$$

Proposition 3. *Let χ be an even quadratic Dirichlet character, p an odd prime number and $F = F_\chi$. For an even integer m, if $(p,\chi\omega^m)$ satisfies* (C)*, then*

$$\sharp X'_\infty(m-1)^\chi_{G_\infty} = p^{x^*(p,\chi,m-1)}.$$

For an odd integer m, assume that $X'^{\chi\omega^{1-m}}_\infty$ is finite. If $(p,\chi\omega^{1-m})$ satisfies (C) *and if $g_{\chi\omega^{1-m}}(T)$ is an Eisenstein polynomial or of degree one, then*

$$\sharp X'_\infty(m-1)^\chi_{G_\infty} = p^{x(p,\chi,m-1)}.$$

Further, for an integer m, we have

$$\frac{\sharp\prod_{v|p} H^2(F_v,\mathbf{Z}_p(m))^\chi}{\sharp H^0(\mathcal{O}_F,\mathbf{Q}_p/\mathbf{Z}_p(1-m))^\chi} = p^{y(p,\chi,m-1)}.$$

Proof. We first set some notation. Let γ be the topological generator of Γ such that $\zeta^\gamma_{f_0p^n} = \zeta^{1+f_0}_{f_0p^n}$ for all $n \geq 0$. As usual, we can identify the completed group ring $\mathbf{Z}_p[[\Gamma]]$ with the formal power series ring $\Lambda = \mathbf{Z}_p[[T]]$ by $\gamma = 1+T$. For a finitely generated torsion Λ-module A, we define the Iwasawa polynomial $\mathrm{char}_\Lambda(A)$ to be the characteristic polynomial of the action T on $A \otimes \mathbf{Q}_p$ (cf. [Washington 1997, §13]). By (C) and [Mazur and Wiles 1984], $\mathrm{char}_\Lambda(X'^{\chi\omega^{1-m}}) = g^*_{\chi\omega^m}(T)$, Since

$$X'_\infty(m-1)^\chi_\Delta \simeq X'^{\chi\omega^{1-m}}_\infty \otimes \mathbf{Z}_p(m-1),$$

we have

$$\mathrm{char}_\Lambda(X'_\infty(m-1)^\chi_\Delta) = \prod_{i=1}^{\tilde{\lambda}(\chi\omega^m)}(T+1-(1+f_0)^{m-1}(\alpha^*_{\chi\omega^m,i}+1)).$$

Since $X'_\infty(m-1)^\chi_\Delta$ has no nontrivial finite Λ-submodule, the order of the Γ-coinvariant quotient is obtained from the constant term of the characteristic polynomial: $v_p(\sharp A/A^{\gamma-1}) = v_p(\sharp A/TA) = v_p(\mathrm{char}_\Lambda(A)|_{T=0})$. Hence we obtain the first equation.

Let M_∞ be the maximal abelian p-extension of K_∞ unramified outside p. Put $Y_\infty = \mathrm{Gal}(M_\infty/K_\infty)$ and $D_\infty = \mathrm{Gal}(M_\infty/L'_\infty)$. By definition, $X'_\infty = Y_\infty/D_\infty$. By (C) and [Mazur and Wiles 1984], we have $\mathrm{char}_\Lambda(Y_\infty^{\chi\omega^{1-m}}) = g_{\chi\omega^{1-m}}(T)$. Hence

$$\mathrm{char}_\Lambda(Y_\infty(m-1)^\chi_\Delta) = \prod_{i=1}^{\tilde{\lambda}(\chi\omega^{1-m})} (T+1-(1+f_0)^{m-1}(\alpha_{\chi\omega^{1-m},i}+1)).$$

Since $Y_\infty(m-1)^\chi_\Delta$ has no nontrivial finite Λ-submodule, by the assumption on $g_{\chi\omega^{1-m}}(T)$, we can completely distinguish any Λ-submodules of $Y_\infty(m-1)^\chi_\Delta$ by their indices. Hence $D_\infty^{\chi\omega^{1-m}}$ is the submodule of $Y_\infty^{\chi\omega^{1-m}}$ of index $p^{\nu_p(\chi\omega^{1-m})}$. Therefore the second equation follows.

Put $z = \sqrt{(-1)^{\frac{p-1}{2}}p}$. Then, $\mathbf{Q}(z)$ (resp. $\mathbf{Q}(z\sqrt{f})$) is associated to $\eta = \omega^{\frac{p-1}{2}}$ (resp. $\chi\eta$). In order to prove the third equation, we first calculate $h_{2,v} = \sharp H^2(F_v, \mathbf{Z}_p(m))$. By local duality, we have $h_{2,v} = \sharp H^0(F_v, \mathbf{Q}_p/\mathbf{Z}_p(1-m)) = \sharp H^0(F_v, \mathbf{Q}_p/\mathbf{Z}_p(m-1))$. If $z \notin F_v$, that is, $\chi\eta(p) \neq 1$, we have

$$h_{2,v} = \begin{cases} p^{v_p(m-1)+1} & \text{if } (p-1)|(m-1), \\ 1 & \text{otherwise.} \end{cases}$$

If $z \in F_v$, that is, $\chi\eta(p) = 1$, we have

$$h_{2,v} = \begin{cases} p^{v_p(m-1)+1} & \text{if } \frac{p-1}{2}|(m-1), \\ 1 & \text{otherwise.} \end{cases}$$

Similarly, we can calculate $h_0 = \sharp H^0(\mathcal{O}_F, \mathbf{Q}_p/\mathbf{Z}_p(1-m)) = \sharp H^0(\mathcal{O}_F, \mathbf{Q}_p/\mathbf{Z}_p(m-1))$. If $z \notin F$, that is, $\chi\eta \neq \chi^0$, we have

$$h_0 = \begin{cases} p^{v_p(m-1)+1} & \text{if } (p-1)|(m-1), \\ 1 & \text{otherwise.} \end{cases}$$

If $z \in F$, that is, $\chi\eta = \chi^0$, we have

$$h_0 = \begin{cases} p^{v_p(m-1)+1} & \text{if } \frac{p-1}{2}|(m-1), \\ 1 & \text{otherwise.} \end{cases}$$

(I) If $\chi\eta = \chi^0$, then $\chi(p) = 0 \neq 1$ and $\chi\eta(p) = 1$. Hence, we have $h_{2,v} = h_0$.
(II) If $\chi\eta \neq \chi^0$ and $\chi(p) = 1$, then $\chi\eta(p) = 0 \neq 1$. Hence, we have $h_{2,v_1}h_{2,v_2} = 1^2$ and $h_0 = 1$ if $(p-1) \nmid (m-1)$. If $(p-1)|(m-1)$, we have $h_{2,v_1}h_{2,v_2} = (p^{v_p(m-1)+1})^2$ and $h_0 = p^{v_p(m-1)+1}$. Since $\chi(p) = 1$ implies $\chi\eta \neq \chi^0$, such a prime number p is included in $S_2(\chi, m-1)$.

(III) If $\chi\eta \neq \chi^0$, $\chi(p) \neq 1$ and $\chi\eta(p) \neq 1$, then we have $h_{2,v} = h_0$.
(IV) If $\chi\eta \neq \chi^0$, $\chi(p) \neq 1$ and $\chi\eta(p) = 1$, then we have $h_{2,v} = h_0$ unless $\frac{p-1}{2} | (m-1)$ and $(p-1) \nmid (m-1)$. If $\frac{p-1}{2} | (m-1)$ and $(p-1) \nmid (m-1)$, we have $h_{2,v} = p^{v_p(m-1)+1}$ and $h_0 = 1$. Since $\chi\eta(p) = 1$ implies $\chi(p) = 0 \neq 1$, such a prime number p is included in $S_1(\chi, m-1)$. Hence, we obtain the third equation. $\square$

For a positive integer m and a prime number p, we denote by $K_{2m-2}(\mathcal{O}_F)(p)$ the p-Sylow subgroup of $K_{2m-2}(\mathcal{O}_F)$. Here we put

$$K'_{2m-2}(\mathcal{O}_F) = \bigoplus_{3 \leq p < 100\,000} K_{2m-2}(\mathcal{O}_F)(p),$$

$$X'(\chi, m-1) = \prod_{3 \leq p < 100\,000} \sharp X'_\infty(m-1)^\chi_{G_\infty} \text{ and}$$

$$Y'_i(\chi, m-1) = \prod_{p \in S_i(\chi, m),\ 3 \leq p < 100\,000} \frac{\sharp \prod_{v|p} H^2(F_v, \mathbf{Z}_p(m))^\chi}{\sharp H^0(\mathcal{O}_F, \mathbf{Q}_p/\mathbf{Z}_p(1-m))^\chi}.$$

Then, by Theorem 3 and the surjectivity of p-adic Chern characters, we have

$$\sharp K'_{2m-2}(\mathcal{O}_F)^\chi \text{ is divided by } X'(\chi, m-1) \cdot Y'_1(\chi, m-1) \cdot Y'_2(\chi, m-1).$$

For an even integer m and a prime number p which divides the numerator of $B_{m,\chi}$, we can compute $v_p(X'(\chi, m-1))$ from the zeros of the Iwasawa polynomial by Proposition 3. In fact, we can easily obtain a lot of examples of (χ, m) with $X'(\chi, m-1) > 1$. On the other hand, for an odd integer m, it is more difficult to obtain examples of (χ, m) with $X'(\chi, m-1) > 1$. Since Vandiver's conjecture is true for all $p < 12\,000\,000$, $X'_\infty(m-1)^{\chi^0}_{G_\infty}$ is trivial for any odd integer m. Further we have $\sharp H^2(\mathbf{Q}_p, \mathbf{Z}_p(m)) = \sharp H^0(\mathbf{Q}_p, \mathbf{Q}_p/\mathbf{Z}_p(1-m)) = \sharp H^0(\mathbf{Z}, \mathbf{Q}_p/\mathbf{Z}_p(1-m))$. By Theorem 3, Proposition 3 and our computational result, we obtain such examples in the following table.

Factors of $\sharp K'_{4m'}(\mathcal{O}_{\mathbf{Q}(\sqrt{f_\chi})})$

$4m'$	f_χ	$X'(\chi,2m')$	$Y'_2(\chi,2m')$	$4m'$	f_χ	$X'(\chi,2m')$	$Y'_2(\chi,2m')$
68372	8	34301		316	12	701	
96	21	199	5·17	44	33	53	
20	37	43	3·11	936	53	1033	$7{\cdot}13^2{\cdot}37$
92652	56	55621	43·6619·15443	8	69	19	5
1220	85	3697	3	88	88	71	3
5124	101	5333	43·367	8	104	19	5
20	113	43	11	3540	113	3373	7·11·31
140	124	197	3·11	380	124	239	3·11
76	129	67		9260	140	4751	
1208	141	5431	5	20	149	43	
108	149	71	7·19	92	149	229	47
90936	156	50051	5·7·19	688	157	401	3·173
156	161	101		28	168	37	
124	172	73	3	4	173	7	
20	173	43		116	173	101	
20	177	17	11	36	181	71	3^3
10724	181	6991	3	944	185	827	
2904	188	1621	23·67·727	11380	193	62791	3
296	197	521					

We have $Y'_1(\chi,2m')=1$ for all the above cases. If the Quillen-Lichtenbaum conjecture is true, there is no other factor of $K'_{4m'}(\mathcal{O}_{\mathbf{Q}(\sqrt{f_\chi})})$: for example,

$$K'_{96}(\mathcal{O}_{\mathbf{Q}(\sqrt{21})}) \simeq \mathbf{Z}/(5\cdot 17\cdot 199\mathbf{Z}).$$

In [Soulé 2003], an explicit huge bound is given for the order of $K_{4m'}(\mathcal{O}_F)$. However, by our method, it would be impossible to compute $x(p,\chi,2m')$ up to the bound.

5 Algorithms for computing arithmetic elements

We compute the following arithmetic elements:
(I) the generalized Bernoulli numbers modulo p, i.e., $\sum_{k=0}^{p-3} B_{k,\chi}t^k/k! \bmod p$,
(II)$_n$ the Iwasawa polynomial $g_{\chi\omega^k}(T) \mod p^{n+1}$,
(III)$_n$ the special cyclotomic unit $c_n^{Y_n(T)}$ modulo a prime ideal $\mathfrak{L}_n$, and
(IV)$_n$ the Gauss sum $g_0(\mathfrak{L}_0)$ modulo a prime ideal $\mathfrak{L}_0^*$, where $\mathfrak{L}_0 = N_{K_n/K_0}\mathfrak{L}_n$.
Some effective algorithms are known for computing the above elements. Here we briefly explain them. For simplicity, we assume that p does not divide $f=f_\chi$.

(I) We first compute the inversion of power series $(e^{ft}-1)/t$ modulo (p,t^{p-2}) by the method of [Knuth 1981, §4.7], in which we use the "Fast Fourier Transform

(FFT)" algorithm (cf. [Knuth 1981, §4.3.3]). Next, we compute the approximated polynomial $\sum_{a=1}^{f} \chi(a)e^{at}$ modulo (p, t^{p-2}). Finally, we multiply the two polynomials by using the FFT algorithm again.

(II)$_n$ By [Washington 1997, Theorem 5.11], we have

$$\begin{aligned} -L_p(1, \chi\omega^k) &\equiv -L_p(1-k, \chi\omega^k) \\ &= (1 - \chi\omega^k\omega^{-k}(p)p^{k-1})\frac{B_{k,\chi\omega^k\omega^{-k}}}{k} \\ &= (1 - \chi(p)p^{k-1})\frac{B_{k,\chi}}{k} \\ &\equiv \frac{B_{k,\chi}}{k} \bmod p. \end{aligned}$$

Therefore, from the result of (I), we can obtain indices k such that p divides $L_p(1, \chi\omega^k) = g_{\chi\omega^k}(0)u_{\chi\omega^k}(0)$. In order to effectively compute $g_{\chi\omega^k}(T) \bmod p^{n+1}$, we use the following theorem (cf. [Washington 1997, §5.2]).

Theorem 4. (*Washington*) *We have the formula*

$$L_p(s, \chi\omega^k) = \frac{1}{f_0}\frac{1}{s-1}\sum_{a=1,\ p\nmid a}^{f_0} \chi\omega^k(a)\langle a\rangle^{1-s}\sum_{j=0}^{\infty}\binom{1-s}{j}(B_j)\left(\frac{f_0}{a}\right)^j,$$

where $\langle a\rangle = a\omega^{-1}(a)$.

(III)$_n$ By using the Iwasawa polynomial $g_{\chi\omega^k}(T) \bmod p^{n+1}$, we define a polynomial $Y_n(T) \in \mathbf{Z}[T]$ (cf. [Ichimura and Sumida 1996]). Then we can study the difference between the group of global units and that of cyclotomic units from the information on the special cyclotomic unit $c_n^{Y_n(T)} \bmod \mathfrak{L}_n$ for some prime ideals $\mathfrak{L}_n$ of K_n of degree one. From the information we can obtain an upper bound for the order of the p-part of the ideal class group by Mazur-Wiles' theorem.

(IV)$_n$ We can make certain that the computation (III)$_n$ gives the exact value of the order by studying the Gauss sums $g_0(\mathfrak{L}_0) \bmod \mathfrak{L}_0^*$ for some prime ideals $\mathfrak{L}_0^*$ of K_0. In order to effectively compute $g_0(\mathfrak{L}_0) \bmod \mathfrak{L}_0^*$, we use the FFT algorithm once again. Concerning the details for computation of the ideal class groups of real abelian fields, see [Schoof 2003] and [Sumida-Takahashi 2004].

The computations in section 3 were handled by 30 personal computers of the Division of Mathematical and Information Sciences, Faculty of Integrated Arts and Sciences, Hiroshima University. The programs were written in UBASIC and C-language, in which the GNU MP library was included in order to multiply polynomials of large degree. For example, for $p = 55\ 621$ and $f_\chi = 56$, it took about (I) 7, (II)$_1$ 30, (III)$_0$ 7, (III)$_1$ 7.4×10^5, (IV)$_0$ 4.8×10^2 seconds by one PC (CPU: Pentium IV, 2.6G Hz, RAM: 1G byte).

References

[Buhler et al. 1993] J. Buhler, R. Crandall, R. Ernvall, and Metsänkylä, *Irregular primes and cyclotomic invariants to four million*, Math. Comp. **61** (1993), 151–153.

[Buhler et al. 2001] J. Buhler, R. Crandall, R. Ernvall, T. Metsänkylä, and A. M. Shokrollahi, *Irregular primes and cyclotomic invariants to* 12 *million*, J. Symbolic Comput. **31** (2001), 89–96.

[Dwyer and Friedlander 1985] W. Dwyer and E. Friedlander, *Algebraic and étale K-theory*, Trans. Amer. Math. Soc. **292** (1985), 247–280.

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

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

[Fukuda and Taya 1995] T. Fukuda and H. Taya, *The Iwasawa λ-invariants of $\mathbf{Z}_p$-extensions of real quadratic fields*, Acta Arith. **69** (1995), 277–292.

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

[Iwasawa 1972] K. Iwasawa, *Lectures on p-adic L-functions*, Ann. of Math. Stud., vol. 74, Princeton Univ. Press: Princeton, N.J., 1972.

[Knuth 1981] E. Knuth, *The art of computer programming, vol.* 2*: Seminumerical algorithms.* 2*nd edition*, Addison-Wesley Publishing Co., Reading, Mass,, 1981.

[Kolster et al. 1996] M. Kolster, T. Nguyen Quang Do, and V. Fleckinger, *Twisted S-units, p-adic class number formulas, and the Lichtenbaum conjectures*, Duke Math. J. **84** (1996), 679–717.

[Kraft and Schoof 1995] J. S. Kraft and R. Schoof, *Computing Iwasawa modules of real quadratic number fields*, Compositio Math. **97** (1995), 135–155.

[Kubota and Leopoldt 1964] T. Kubota and H.W. Leopoldt, *Eine p-adische Theorie der Zetawerte, I. Einführung der p-adischen Dirichletschen L-Funktionen*, J. reine angew. Math. **214/215** (1964), 328–339.

[Mazur and Wiles 1984] B. Mazur and A. Wiles, *Class fields of abelian extensions of* $\mathbf{Q}$, Invent. Math. **76** (1984), 179–330.

[Schneider 1979] P. Schneider, *Über gewisse Galoiscohomologiegruppen*, Math. Z. **168** (1979), 181–205.

[Schoof 2003] R. Schoof, *Class numbers of real cyclotomic fields of prime conductor*, Math. Comp. **72** (2003), 913–937.

[Soulé 2003] C. Soulé, *A bound for the torsion in the K-theory of algebraic integers*, Doc. Math. **Extra Vol.** (2003), 761–788.

[Sumida-Takahashi 2004] H. Sumida-Takahashi, *Computation of Iwasawa invariants of certain real abelian fields*, J. Number Theory **105** (2004), 235–250.

[Washington 1997] L. Washington, *Introduction to cyclotomic fields. second edition*, Graduate Texts in Math., vol. 83, Springer-Verlag: New York, 1997.

[Wiles 1990] A. Wiles, *The Iwasawa conjecture for totally real fields*, Ann. of Math. **131** (1990), 493–540.

Address: Hiroki SUMIDA-TAKAHASHI
Faculty of Integrated Arts and Sciences, Hiroshima University
Kagamiyama, Higashi-Hiroshima 739-8521, Japan
TEL:(+81)-82-424-6482, FAX:(+81)-82-424-0756
hiroki@mis.hiroshima-u.ac.jp