Greenberg's conjecture for real quadratic number fields.

by Pietro Mercuri, Maurizio Paoluzi and René Schoof.

1. Introduction.

Let F be a totally real number field and let p be a prime. Let

$$F = F_0 \subset F_1 \subset F_2 \subset \ldots$$

denote the cyclotomic $\mathbf{Z}_p$-extension of F. By A_n we denote the p-part of the ideal class group of the ring of integers of F_n. In his 1971 thesis Ralph Greenberg conjectured that $\#A_n$ remains bounded as $n \to \infty$. See [4] and [5, Conj (3.4)]. This is the "$\lambda = 0$"-conjecture of Iwasawa theory. In this note we report on a computation involving the 30394 real quadratic fields $\mathbf{Q}(\sqrt{f})$ of discriminant $f < 100,000$. As a consequence we obtain the following result.

Theorem 1.1. *Greenberg's conjecture is true for the prime $p = 3$ and the real quadratic fields of discriminant $f < 100,000$.*

For each of the real quadratic fields with discriminant f in the range of our compuation we have computed a certain Galois module $C(f)$, the finiteness of which is equivalent to Greenberg's conjecture. In this introduction we describe the module $C(f)$. In the rest of note we explain the computation and its results.

Let $F = \mathbf{Q}(\sqrt{f})$ be a real quadratic field of discriminant f. The Galois module $C(f)$ is defined in terms of cyclotomic units. For $k \geq 1$ let ζ_k denote a primitive k-th root of unity. For $F = \mathbf{Q}(\sqrt{f})$ and $n \geq 0$ the n-th layer in the cyclotomic $\mathbf{Z}_3$-extension of F is

$$F_n = \mathbf{Q}(\sqrt{f}, \zeta_{3^{n+1}} + \zeta_{3^{n+1}}^{-1}).$$

The field F_n is a subfield of the cyclotomic field $\mathbf{Q}(\zeta_{3^{n+1}f})$ and has degree 3^n over $\mathbf{Q}(\sqrt{f})$. Its ring of integers O_n contains cyclotomic units. See [9, 10]. The 3-part of the quotient of the unit group O_n^* by its subgroup of cyclotomic units is a finite group denoted by B_n. It is known that the groups A_n and B_n have the same cardinality. Therefore Greenberg's conjecture is true for the field F if and only if $\#B_n$ remains bounded as $n \to \infty$.

When the discriminant f is not congruent to 1 (mod 3), we let C_n denote the dual of the group B_n for $n = 0, 1, 2, \ldots$. When $f \equiv 1 \pmod 3$, we let C_n denote the dual of the group $\tilde{B}_n$. Here $\tilde{B}_n$ sits in the exact sequence

$$0 \longrightarrow \tilde{B}_n \longrightarrow B_n \xrightarrow{\phi_n} \mathbf{Z}_3/\log_3 \eta_0 \mathbf{Z}_3.$$

Here for $\epsilon \in O_n^*$ we put $\phi_n(\epsilon) = \frac{1}{3^n}\log_3(N_n(\epsilon))$, where $N_n : F_n^* \to \mathbf{Q}(\sqrt{f})^*$ is the norm map. Since the 3-adic logarithm of a generator η_0 of the group of cyclotomic units in $\mathbf{Q}(\sqrt{f})$ is not zero, the rightmost group is a finite cyclic group. It follows that $[B_n : \tilde{B}_n]$ and hence the quotient $\#B_n/\#C_n$ is bounded independently of n. Therefore Greenberg's conjecture is true if and only if $\#C_n$ remains bounded as $n \to \infty$.

For $n \geq m$ the natural maps $B_m \to B_n$ are injective and the natural maps $C_n \to C_m$ are surjective. Let $C(f)$ denote the projective limit of the C_n. Then $C(f)$ is a Galois module and hence in the usual way a module over the Iwasawa algebra $\Lambda = \mathbf{Z}_3[[T]]$. It follows from properties of cyclotomic units that it has rank 1. See [6, 7, 8]. In other words, we have

$$C(f) = \lim_{\leftarrow} C_n \cong \Lambda/J, \qquad \text{for some ideal } J \subset \Lambda.$$

The vanishing of the Iwasawa μ-invariant of $\mathbf{Q}(\sqrt{f})$ means that J contains a monic polynomial and hence that $C(f)$ is a finitely generated $\mathbf{Z}_3$-module [2]. Greenberg's conjecture affirms that $C(f)$ is actually *finite*.

We have computed the Galois module $C(f)$ and in the range of our computations we found the following. It is equivalent to Theorem 1.1.

Theorem 1.2. *For $p = 3$ and for all discriminants $f < 100,000$ the module $C(f)$ is finite.*

In most cases we have $C(f) = 0$. Indeed, for only 3359 out of the 30394 real quadratic fields considered, $C(f)$ is not zero or, equivalently, J is a proper Λ-ideal. This is about 11% of all cases. Of these, 2218 have J equal to the maximal ideal $(3, T)$ of Λ. In these cases $C(f)$ has order 3. For the remaining 1241 fields the module $C(f)$ is strictly larger. This is approximately 4% of all cases.

Rather than listing each ideal J, we indicate in section 3 how often ideals of a certain type appear in our computation. The full list of ideals may be of interest by itself and is available on github [12]. We also single out some discriminants for which the ideal J has a remarkable shape.

2. Upper bounds and lower bounds.

In this section we give a sketchy description of the algorithm. For the details see [6, 8]. Let $\mathbf{Q}(\sqrt{f})$ be a real quadratic field of discriminant f. Let J be the Λ-ideal described in the introduction for which $C(f) = \Lambda/J$. For $n \geq 0$ we put $\omega_n(T) = (1+T)^{p^n} - 1$ and we write (ω_n) for the ideal generated by it.

First we discuss the case where the discriminant f is *not* congruent to 1 (mod 3). In [6] it is explained that in this case we have

$$C_n = C(f)/\omega_n C(f) = \Lambda/(J + (\omega_n)), \qquad \text{for all } n \geq 0.$$

The Galois module $C(f)$ is finite if and only if $\omega_n C(f) = 0$ and hence $C(f) = C_n$ for some $n \geq 0$. By Nakayama's lemma this happens if and only if $J + (\omega_n) = J + (\omega_{n+1})$ for some $n \geq 0$. This observation leads to the following algorithm. For $n = 0, 1, 2, \ldots$ we compute the shrinking ideals $J + (\omega_n)$ until we find that $J + (\omega_n) = J + (\omega_{n+1})$.

Our method for computing the ideals $J + (\omega_n)$ runs as follows. For a given n we first calculate a lot of elements in the ideal. As is explained in [6], this involves calculations with cyclotomic units modulo certain primes and leads to an *upper bound* for $\Lambda/(J+(\omega_n))$. To obtain a *lower bound* we employ a method due to G. and M.-N. Gras [3]. This involves calculations with high precision approximations of the cyclotomic units in $F_n \otimes \mathbf{R}$. See also [6, section 4]. Clearly, when the upper and lower bounds agree, we have determined $J + (\omega_n)$ and hence $C_n = \Lambda/(J + (\omega_n))$.

The calculation of the lower bound becomes very time consuming and takes a lot of memory as n grows. This is caused by the high precision computations with units in cyclotomic fields of conductors several millions and degrees in the hundreds. In fact, for most discriminants f it becomes infeasible when n exceeds 2. Fortunately, for most f we find that $J + (\omega_n) = J + (\omega_{n+1})$ and hence $C(f) = C_n$ for $n \leq 2$.

In the rare cases where we need to consider $J + (\omega_n)$ for $n \geq 3$, it is still feasible to compute the upper bound. This means that we can calculate a lot of elements in $J+(\omega_n)$. An application of the Cebotarev density theorem suggests that these elements probably *generate* $J + (\omega_n)$, so that our upper bound is actually *equal* to the lower bound, but we have no rigorous proof of this.

Fortunately, we can still rigorously prove that $C(f) = \Lambda/J$ is finite and thus confirm Greenberg's conjecture even when we cannot use our algorithm to compute lower bounds for $\Lambda/(J + (\omega_n))$. It suffices to have an upper bound for n and a lower bound for *some* $m \leq n$ to which the following lemma applies. In the range of our computations this always works out with $n \geq m = 2$.

Lemma 2.1. *Let M be a finitely generated Λ-module. Suppose that for certain integers $n \geq m \geq 0$ and $b \geq a \geq 0$ we have*

$$\#M/\omega_m M \geq p^a \quad \textit{and} \quad \#M/\omega_n M \leq p^b.$$

If $b - a < n - m$, then $\omega_n M = 0$. In particular, if $M/\omega_n M$ is finite, so is M.

Proof. In the filtration

$$\omega_n M \quad \subset \quad \omega_{n-1} M \quad \subset \ldots \subset \quad \omega_{m+1} M \quad \subset \quad \omega_m M$$

there are $n - m$ inclusions. We have inequalities

$$\#(\omega_n M/\omega_m M) = \frac{\#M/\omega_n M}{\#M/\omega_m M} \leq p^{b-a} < p^{n-m}.$$

It follows that one of the inclusions must be an equality. So we have $\omega_{k+1} M = \omega_k M$ for some $k = m, \ldots, n-1$. Then $x = \omega_{k+1}/\omega_k$ is an element of the maximal ideal of Λ that has the property that $x\omega_k M = \omega_k M$. Nakayama's lemma implies then $\omega_k M = 0$. It follows that $\omega_n M$ is zero, as required.

When the discriminant f is congruent to 1 (mod 3), our method is the same, but the details are slightly different. See [7, 8] for the details. This time we have $C_n = C(f)/\omega'_n C(f) = \Lambda/(J + (\omega'_n))$ for all $n \geq 0$. Here $\omega'_n = \omega_n/T$. In particular we have $\omega'_0 = 1$ and $C_0 = 0$. For each $n = 1, 2, \ldots$ we compute the shrinking ideals $J + (\omega'_n)$ until we find $J + (\omega'_n) = J + (\omega'_{n+1})$, in which case Nakayama's lemma implies that $J = J + (\omega'_n)$ and hence $C(f) = C_n$ and we are done.

The issues with upper bounds and lower bounds are similar. We can still prove that $C(f) = \Lambda/J$ is finite in each case in the range of our computations. When the lower bound is not available for some $n \geq 3$, we invoke Lemma 2.1 with ω_m and ω_n replaced by ω'_m and ω'_n respectively.

3. Numerical data.

There are 30394 real quadratic fields of discriminant $f < 100,000$. In order to present our results, it is convenient to separate cases according to the residue class of f modulo 3.

Case $f \equiv 0 \pmod 3$.
There are 7606 real quadratic fields with discriminant $f \equiv 0 \pmod 3$ and $f < 100,000$. For precisely 769 of them the Galois module $C(f) = \Lambda/J$ is not zero. This is approximately 10%. For 513 discriminants J is equal to the maximal ideal $(3, T)$ of Λ. For the remaining 256 discriminants J is strictly smaller. Table 3.1 contains some data.

The rows of Table 3.1 correspond to the *level of stabilization* n. This means that n is the smallest integer for which the ideals $J + (\omega_n)$ and $J + (\omega_{n+1})$ are equal and hence $J = J + (\omega_n)$. In particular, we have $\Lambda/J = C(f) = C_n$. The number n is also the smallest for which $\omega_n = (1+T)^{3^n} - 1$ is in J. Equivalently, 3^n is the order of $1+T$ in the multiplicative group $(\Lambda/J)^*$. The columns are indexed by the symbols T^k for $k = 1, 2, \ldots$.

The entry in the n-th row and the T^k-column is the number of discriminants for which the level of stabilization is n, and the image of J in the ring $\mathbf{F}_3[[T]]$ is the ideal (T^k). Since ω_n is congruent to T^{3^n} modulo 3, the (n, T^k)-entry is zero whenever $k > 3^n$. In particular, in the row corresponding to $n = 0$, all entries with $k > 1$ are zero.

Table 3.1. The modules Λ/J for $f \equiv 0 \pmod 3$.

n	T	T^2	T^3	Total
0	536	0	0	536
1	112	50	2	164
2	35	7	2	44
3	15*	0	0	15
4	5*	1*	0	6
5	2*	0	0	2
6	2*	0	0	2
	707	58	4	769

In the first column we count the discriminants for which the ideal J is of the form $J = (T - a, b)$ for certain $a, b \in \mathbf{Z}$. For 536 discriminants there is stabilization at level $n = 0$ and we have $a = 0$. This means that $\#C_0 = \#C_1$ or, equivalently $\#A_0 = \#A_1$. The discriminants for which J is equal to the maximal ideal of Λ are included here. This entry was checked by computing the class numbers of the fields F_0 and F_1 of degrees 2 and 6 respecively. For the other entries in the first column, we have $a \notin b\mathbf{Z}_3$ and stabilization occurs at level $n = v_3(b/a)$. The calculations were done using a few lines of PARI/GP [11] code in these cases.

An asterisk indicates that we do not have a rigorous lower bound for $C(f)$ for some of the discriminants appearing in this entry. However, our upper bound is very likely to be sharp, so that almost certainly $C(f)$ is isomorphic to Λ/J. In each case Lemma 2.1 was applied to prove Greenberg's conjecture. The 62 cases appearing in the second and third columns were dealt with using the polynomial arithmetic of Magma [1]. We single out nine discriminants f for special mention.

Table 3.2. Exotic Galois modules for $f \equiv 0 \pmod 3$.

f	J	n	T^k
31989	$(T-996, 2187)$	6	T
38424	$(T+261, 2187)$	5	T
59061	$(T^2+3T-9, 81)$	4	T^2
60513	$(T^3+3, 3T, 9)$	2	T^3
61629	$(T^3, 3)$	1	T^3
69117	$(T+69, 729)$	5	T
71049	$(T^3, 3))$	1	T^3
76584	$(T^3+3, 3T, 9)$	2	T^3
95385	$(T-2988, 6561)$	6	T

Case $f \equiv 2 \pmod 3$.
There are 11394 real quadratic fields with discriminant $f \equiv 2 \pmod 3$ and $f < 100,000$. For precisely 1250 of them the Galois module $C(f) = \Lambda/J$ is not zero. This is approximately 11% of all discriminants. For 781 discriminants J is equal to the maximal ideal $(3, T)$ of Λ. For the remaining 469 discriminants J is strictly smaller. This is about 4% of all cases. Table 3.3 contains some data.

Table 3.3. The modules Λ/J for $f \equiv 2 \pmod 3$.

n	T	T^2	T^3	T^4	Total
0	827	0	0	0	827
1	158	87	8	0	253
2	101	7	4	1	113
3	36*	2*	0	0	38
4	13*	1*	0	0	14
5	4*	0	0	0	4
6	1*	0	0	0	1
	1140	97	12	1	1250

The interpretation of the data is the same as in the case $f \equiv 0 \pmod 3$. The 781 discriminants with $J = (3, T)$ are included in the entry with $n = 0$ of the first column. In this case we the discriminants in the first column were taking care of using a few lines of PARI/GP code. The other 110 cases were dealt with using the polynomial arithmetic of Magma. We single out a few discriminants for special mention.

Table 3.4. Exotic Galois modules for $f \equiv 2 \pmod 3$.

f	J	n	T^k
14165	$(T-255, 729)$	5	T
16673	$(T+462, 2187)$	6	T
29165	$(T-282, 729)$	5	T
47633	$(T^2-9, 3T-90, 243)$	4	T^2
51809	$(T^2+18, 3T-18, 81)$	3	T^2
71921	$(T^2+18, 3T+18, 81)$	3	T^2
76604	$(T+294, 729)$	5	T
90005	$(T+15, 729)$	5	T
98105	$(T^4+3, 3T, 9)$	2	T^4

Case $f \equiv 1 \pmod 3$.
There are 11394 real quadratic fields with discriminant $f \equiv 1 \pmod 3$ and $f < 100,000$. For precisely 1340 of them the module $C(f)$ is not zero. This is approximately 12% of all discriminants. For 824 discriminants J is equal to the maximal ideal $(3, T)$ of Λ. For the remaining 516 discriminants the ideal J is strictly smaller. This is 4.5% of all cases.

The mathematics is a bit different in this case. First of all, the groups A_0, B_0 are irrelevant for our computations and we have $C_0 = 0$. In addition, every module C_n is a cyclic module over the ring $\Lambda/(\omega_n)$ that is killed by ω'_n. In particular, C_1 is a cyclic module over the discrete valuation ring $\Lambda/(\omega'_1)$, where $\omega'_1 = \omega_1/T = T^2+3T+3$. Since T is a uniformizer of the ring $\Lambda/(\omega'_1)$, the module C_1 is isomorphic to $\Lambda/(T^2+3T+3, T^k)$ for some $k \geq 0$.

By Nakayama's lemma the ideal J contains a monic polynomial of degree 1 if and only if the ideal (T^2+3T+3, T^k) does. If J is a proper ideal, this happens precisely when $k = 1$, in which case C_1 is isomorphic to the order 3 module $\Lambda/(3, T)$. These cases appear in the first column and were computed using PARI/GP. Their ideals J are of the form $(T-a, b)$ with level of stabilization equal to $v_3(b)$. In particular, the first entry contains the 824 discriminants for which J is equal to the ideal $(3, T)$. The 119 entries in the remaining columns were taken care of using Magma's polynomial arithmetic.

Table 3.5. The modules Λ/J for $f \equiv 1 \pmod 3$.

n	T	T^2	T^3	T^4	T^5	Total
1	824	79	0	0	0	903
2	249	18	8	1	0	276
3	88	7	1	0	1	97
4	47*	3*	0	0	0	50
5	9*	0	1*	0	0	10
6	2*	0	0	0	0	2
7	2*	0	0	0	0	2
	1221	107	10	1	1	1340

We single out eleven discriminants for special mention.

Table 3.6. Exotic Galois modules for $f \equiv 1 \pmod 3$.

f	J	n	T^k
15217	$(T^4+3, 3T, 9)$	2	T^4
30904	$(T^3-27, 3T-63, 243)$	5	T^3
39256	$(T+621, 2187)$	7	T
40441	$(T^2, 9T-27, 81)$	4	T^2
44053	$(T+348, 729))$	6	T
57832	$(T^2+27, 3T-27, 81)$	4	T^2
71821	$(T^3+18, 3T+9, 27)$	3	T^3
78037	$(T-849, 2187)$	7	T
80056	$(T^5+9T+9, 3T^2+18, 27)$	3	T^5
81769	$(T^2+18, 3T+9, 81)$	4	T^2
96712	$(T-30, 729)$	6	T

Bibliography.

[1] Bosma, W., Cannon, J. and Playoust, C.: The Magma algebra system. I. The user language, *J. Symbolic Comput.* **24** (1997), 235–265.

[2] Ferrero, B. and Washington, L. C.: The Iwasawa invariant μ_p vanishes for abelian number fields, *Annals of Math.* **109** (1979), 77–395,

[3] Gras, G. and Gras, M.-N.: Calcul du nombre de classes et des unités des extensions abéliennes réelles de $\mathbf{Q}$, *Bulletin des Sciences Math.* **101** (1977), 97–129.

[4] Greenberg, R.: On some questions concerning the lwasawa invariants, Princeton University thesis 1971.

[5] Greenberg, R.: Iwasawa Theory Past and Present, *Advanced Studies in Pure Mathematics*, **30** (2001), 335–385

[6] Kraft, J.S. and Schoof, R.: Computing Iwasawa modules of real quadratic number fields, *Compositio Math.* **97** (1995),135–155. Erratum: Compositio Math. **103** (1996), 241.

[7] Nuccio, F.A.E.: Cyclotomic units and class groups in $\mathbf{Z}_p$-extensions of real abelian fields, *Math. Proc. Cambridge Phil. Soc.* **148** (2010), 93–106.

[8] Paoluzi, M.: *La congettura di Greenberg per campi quadratici reali.* Ph.D. thesis Università di Roma La Sapienza 2002.

[9] Sinnott, W.: On the Stickelberger ideal and the circular units of a cyclotomic field, *Annals of Math.* **108** (1978), 107–134.

[10] Sinnott, W.: On the Stickelberger ideal and the circular units of an abelian field, *Invent. Math.* **62** (1980), 181–234.

[11] The PARI Group, PARI/GP 2.13.0, Univ. Bordeaux (2020), `http://pari.math.u-bordeaux.fr`.

[12] `https://github.com/mercuri-pietro/Iwasawa-modules`

Pietro Mercuri
Università di Roma La Sapienza
Dipartimento SBAI,
00185 Roma
mercuri.ptr@gmail.com

Maurizio Paoluzi
Via Mariano Rampolla 24
00168 Roma
mauriziopaoluzi@gmail.com

René Schoof
Università di Roma Tor Vergata
Dipartimento di matematica,
00133 Roma
schoof.rene@gmail.com