6. On a Determination of Real Quadratic Fields of Class Number One and Related Continued Fraction Period Length Less than 25

By R. A. MOLLIN*) and H. C. WILLIAMS**)

(Communicated by Shokichi IYANAGA, M. J. A., Jan. 14, 1991)

§ 1. **Introduction.** The primary thrust of this paper is to investigate real quadratic fields $Q(\sqrt{d})$ of class number $h(d)$ equal to 1 when related to the period length, k of the continued fraction expansion of ω where $\omega=(\sigma-1+\sqrt{d})/\sigma$ with $\sigma=\begin{Bmatrix} 1 \text{ if } d\equiv 2,3 \pmod 4 \\ 2 \text{ if } d\equiv 1 \pmod 4 \end{Bmatrix}$. We actually determine, (with only one possible value remaining, whose very existence would be a counterexample to the Riemann hypothesis), all those positive square-free integers d with $h(d)=1$ and $k\leq 24$. Moreover our new approach allows us to reformulate the Gauss conjecture as to the infinitude of real quadratic fields $K=Q(\sqrt{d})$ with d positive square-free and $h(d)=1$, in terms of the theory of continued fractions.

§ 2. **Notations and preliminaries.** We let $\mathcal{O}_K$ denote the maximal order in $K=Q(\sqrt{d})$.

Throughout d will be assumed to be a positive square-free integer. For convenience sake we collect together basic facts involving continued fractions which we will be using throughout the paper.

For ω as above let the continued fraction expansion of ω be denoted by $\omega=\langle a, \overline{a_1, \cdots, a_k}\rangle$. Then $a_0=a=\lfloor\omega\rfloor$, $a_i=\lfloor(P_i+\sqrt{d})/Q_i\rfloor$ for $i\geq 1$ (here $\lfloor\ \rfloor$ denotes the greatest integer function), where $(P_0, Q_0)=(1, 2)$ if $d\equiv 1 \pmod 4$ and $(P_0, Q_0)=(0, 1)$ otherwise. Also,

(2.1) $P_{i+1}=a_iQ_i-P_i$ for $i\geq 0$,

(2.2) $Q_{i+1}Q_i=d-P_{i+1}^2$ for $i\geq 0$, and

(2.3) $a_i=a_{k-i}$ for $1\leq i\leq k-1$.

Moreover either,

(2.4) $P_i=P_{i+1}$ in which case $k=2i$ or

(2.5) $Q_i=Q_{i+1}$ in which case $k=2i+1$.

Now we give some background to the research involved herein. In [2] Kim and Leu showed that 2 conjectures (one of Chowla [1], and one of Yokoi [15]) are valid with one possible exceptional value remaining, and therefore that one of the 2 conjectures is valid with the remaining one failing for at most one value. In [7] we proved Chowla's conjecture under the assumption of the generalized Riemann hypothesis (GRH). Subsequently we extended

*) Department of Mathematics and Statistics, University of Calgary, Calgary, Alberta, Canada, T2N 1N4.

**) Department of Computer Science, University of Manitoba, Winnipeg, Manitoba, Canada, R3T 2N2.

our techniques in [8]–[9] to determine all $h(d)=1$, under the GRH, when $d=m^2+r$ where $4m\equiv 0 \pmod r$; i.e., when d is of a form we call *extended Richaud-Degert* (ERD)-type. In [11] we were able to remove the GRH assumption and determined all ERD-types d where $h(d)=1$, with one possible value remaining. Moreover, the above provided applications to conjectures in the literature; viz., the aforementioned ones of Chowla and Yokoi as well as one of Mollin in [3], and three of Mollin-Williams in [9]. The results of [8]–[9] and [11] therefore show that five of the six aforementioned conjectures are valid with the remaining one failing for at most one value, the existence of which would be a counterexample to the Riemann hypothesis, (see [5] for details as well as a general survey). Therefore we have generalized the work of Kim-Leu in [2] since they were only interested in very special ERD-types; viz, $d=m^2+1$ or $d=m^2+4$. Furthermore from the results of Mollin in [3]–[4] we know that if $h(d)=1$ and d is of ERD-type then d is one of the forms in the aforementioned six conjectures, and that $k\leq 4$. Thus we began investigation of the class number one problem from the perspective of continued fraction theory in [10]. The work herein continues that approach.

We now turn our attention to extending our algebraic and computational techniques on this continued fraction approach in the next section.

§3. Continued fractions and class number one. We now provide a description of those $h(d)=1$ for k as large as possible. For reasons which will become clear later, we look at $k\leq 24$. The following table lists all square-free d with $h(d)=1$ for $k\leq 24$ and $\Delta<50{,}000$ where

$$\Delta=\begin{Bmatrix} d \text{ if } d\equiv 1 \pmod 4 \\ 4d \text{ if } d\equiv 2,3 \pmod 4 \end{Bmatrix}.$$

Table 3.1

k	d
1	2, 5, 13, 29, 53, 173, 293
2	3, 6, 11, 21, 38, 77, 83, 93, 227, 237, 437, 453, 1133, 1253
3	17, 37, 61, 101, 197, 317, 461, 557, 677, 773, 1877
4	7, 14, 23, 33, 47, 62, 69, 133, 141, 167, 213, 398, 413, 573, 717, 1077, 1293, 1397, 1757, 3053
5	41, 149, 157, 181, 269, 397, 941, 1013, 2477, 2693, 3533, 4253
6	19, 22, 57, 59, 107, 131, 253, 278, 309, 341, 381, 749, 813, 893, 1893, 2453, 2757, 3317
7	89, 109, 113, 137, 373, 389, 509, 653, 797, 853, 997, 1493, 1997, 2309, 2621, 3797, 4973
8	31, 71, 158, 206, 383, 501, 503, 581, 743, 789, 869, 917, 983, 989, 1333, 1349, 1437, 2573, 3093, 6677, 14693
9	73, 97, 233, 277, 349, 353, 613, 821, 877, 1181, 1277, 1613, 1637, 1693, 2357, 3557, 3989, 4157, 4517, 7213, 11213
10	43, 67, 86, 118, 129, 161, 301, 517, 563, 597, 669, 827, 1238, 1357, 1389, 2253, 2901, 3101, 3437, 4413, 4613, 7061, 7653

k	d
11	541, 593, 661, 701, 857, 1061, 1109, 1217, 1237, 1709, 1733, 1949, 2333, 2957, 3677, 3701, 4373, 5237, 5309, 7013, 8693, 9533, 10853, 12437
12	46, 103, 127, 177, 209, 239, 263, 479, 734, 887, 933, 973, 1149, 1541, 1589, 1661, 1797, 1837, 2229, 2933, 3269, 3309, 3453, 4829, 6261, 6333, 6797, 7637, 10757, 12381
13	421, 757, 1021, 1097, 1117, 1301, 1553, 1973, 2069, 2237, 2273, 2789, 2861, 3373, 3461, 3517, 3917, 4133, 4397, 5573, 5717, 6221, 6317, 7253, 7517, 8741, 9173, 9437, 10181, 11597, 15797
14	134, 179, 201, 251, 262, 307, 347, 422, 467, 497, 502, 587, 683, 713, 838, 1317, 1382, 1477, 2077, 2189, 2317, 3197, 3837, 4037, 4197, 4661, 4997, 5093, 5277, 5357, 5493, 5997, 7493, 7613, 7997, 9237, 17237
15	193, 281, 1861, 1933, 2141, 2437, 2741, 2837, 3037, 3413, 4637, 4877, 6653, 8117, 11549, 13037, 15077, 23117
16	94,191,217,249,302,311,329,393,431,446,537,542,589, 647, 878, 1319, 1487, 1909, 2157, 2351, 2413, 2517, 2733, 3149, 4109, 6013, 6117, 6533, 7629, 7773, 8717, 9037, 9917, 11693, 13853, 14253, 15221, 16397, 16557
17	521, 617, 709, 1433, 1597, 2549, 2909, 3581, 3821, 4013, 5501, 5693, 5813, 6197, 7853, 8093, 8573, 9677, 10597, 10973, 13109, 13613, 15413, 17093, 20261, 22637, 26717
18	139, 163, 283, 417, 419, 566, 633, 737, 758, 781, 787, 998, 1141, 1142, 1163, 1286, 1307, 1337, 1461, 1718, 1829, 1931, 2243, 2537, 2653, 2966, 2973, 3013, 3117, 3629, 3713, 4061, 4269, 4541, 4781, 6629, 6717, 7037, 7133, 7181, 8013, 8157, 8197, 8301, 8777, 9957, 10277, 10493, 11429, 11957, 12293, 13373, 13917, 16373, 18653, 18813, 18893, 20597, 23597, 24173, 26837, 30917
19	241, 313, 449, 829, 953, 1069, 1193, 1213, 1697, 2381, 3853, 4733, 5077, 5189, 5381, 5669, 5981, 6173, 6277, 6389, 6397, 6917, 7717, 7757, 7877, 8237, 9973, 10037, 11093, 11933, 12893, 13397, 19997, 27917
20	151, 199, 367, 622, 863, 1151, 1454, 1501, 1502, 1941, 2033, 3902, 4101, 4317,4677,4821,5549, 6077, 7277, 8133, 8453, 8813, 9253, 9357, 11381, 11733, 14237, 15837, 17933, 18293, 21653, 23453, 25157, 36077, 49013
21	337, 569, 977, 1453, 1669, 1741, 2053, 2293, 4093, 4349, 5437, 5557, 8861, 9341, 10133, 10709, 11117, 12917, 14549, 15053, 16253, 18413, 18917, 19013, 19973, 20117, 20333, 25373, 38493, 29333
22	166, 489, 491, 523, 643, 662, 947, 971, 1137, 1187, 1427, 1571, 1667, 1713, 1821, 2181, 2217, 2469, 3493, 3693, 3749, 3909, 3947, 4213, 4787, 4989, 5789, 5893, 5909, 6933, 6941, 7509, 7941, 10157, 10533, 10821, 11189, 11469, 12477, 12533, 13733, 14333, 14853, 15069, 15637, 15893, 17813, 19613, 20429, 21117, 23093, 30533, 35237, 36893
23	433,457,641,881, 1381, 1913, 2393, 2749, 3389, 3733, 4421, 5653, 6701, 7349, 7949, 8669, 10253, 11813, 12413, 13709, 13757, 14717, 14813, 14957, 15749, 16229, 16453, 19037, 19421, 22613, 22853, 24317, 27653, 28517, 30197, 31253, 33893, 37397
24	271, 382, 607, 753, 911, 1103, 1262, 1438, 1473, 1838, 1982, 2063, 2078, 2558, 2661, 2687, 2893, 2903, 3986, 3113, 3167, 3377, 3669, 4237, 4333, 4533, 5293, 5533, 5753, 6509, 6621, 7197, 7269, 8153, 8189, 8213, 8413, 10637, 11157, 11573, 11589, 11893, 12677, 12797, 13453, 13541, 14117, 15693, 15917, 17133, 17309, 18677, 18933, 19797, 20053, 20373, 20837, 22757, 25709, 25973, 26213, 27317, 34997, 39077

Conjecture 3.1. The values of d in Table 3.1 are all values with $h(d)=1$ and $k\leq 24$.

We have come close to proving Conjecture 3.1. In fact we have

Theorem 3.1. *If $k\leq 24$ then with possibly only one more value remaining $h(d)=1$ if and only if d is an entry in Table* 3.1.

Proof. Let Δ be as above and let χ_Δ be a real, non-principal primitive character modulo Δ. If R denotes the regulator of $Q(\sqrt{d})$ and $L(s,\chi_\Delta)$ is the associated L-function, then from the well-known analytic class number formulae we have

$$2h(d)R=\sqrt{\Delta}\,L(1,\chi_\Delta) \quad \text{and} \quad R<k\log\sqrt{\Delta}$$

(see for example [6]), as well as result of Tatuzawa [13] we get, if $h(d)=1$ then it is easily verified that $k>(.655\varepsilon\Delta^{(1/2)-\varepsilon})/(\log\Delta)$ when $\Delta>\max(e^{1/\varepsilon}, e^{11\cdot 2})$ with possibly only one exception. Thus, if $\Delta>B>e^{11\cdot 2}$, $\varepsilon=1/\log B$ and $f(B)=[.655B^{1/2-(1/\log B)}]/(\log B)^2$ then, $h(d)=1$ implies that $k>f(B)$ with one possible exception.

We choose $B=2^{31}-1$ for convenience on the machine level because of word size; i.e., any larger B would force us to use double precision. With this B we get $f(B)>24.1$. Therefore, for $k\leq 24$ then $h(d)>1$ if $\Delta>B$. We now deal with the case where $1\leq\Delta\leq B$.

In the continued fraction expansion of ω we must have exactly one of (2.4) or (2.5) holding. Thus we need only search the continued fraction expansion of ω up to $i=12$. We first check whether (2.4) or (2.5) occurs for Δ and discard those Δ with $k\leq 24$. We also store the values of Q_i/Q_0. Now, if $p<(\sqrt{\Delta})/2$ and $(\Delta/p)=1$, (where $(/)$ is the Legendre symbol), then the ideal (p) splits into the product of the prime ideals $\mathcal{P}$ and Q in $Q(\sqrt{d})$ with $\mathcal{P}, Q$ being reduced ideals (see [6] for details and definitions). Since the continued fraction expansion of ω produces *all* the reduced ideals in the principal class (see for example [14], pp. [414–416]), we see that if $h(d)=1$ then $N(\mathcal{P})=Q_i/Q_0$ for some $i\leq k/2$. Thus we need only search for a prime $p<(\sqrt{\Delta})/2$ such that $p\neq Q_i/Q_0$ for $i\leq n=k/2$ and with $(\Delta/p)=1$ in order to be assured that $h(d)>1$. When this simple exclusion method was used for all numbers in excess of 50,000 for which (2.4) or (2.5) held with $n\leq 12$, we found that there were no possible values of $\Delta\geq 50{,}000$ such that $k\leq 24$ and $h(d)=1$. This entire computational process took about 2 hours and 10 minutes on an Amdahl 5870 computer. The values of $\Delta<50{,}000$ such that $k\leq 24$ and $h(d)=1$ were then identified using standard class number evaluation techniques (see [6]), and turned out to be exactly those listed in Table 3.1.

Remark 3.1. Although the number of d with $h(d)=1$ tends to increase (in some general way but not monotocally however) as k increases, we have not been able to prove that this is so. If we could, then of course we would have proved the Gauss conjecture, which can now be reformulated in our terminology as $\#k\mapsto\infty$ as $k\mapsto\infty$ where $\#k$ is the number of d with $h(d)=1$ when ω has period length k.

Remark 3.2. As noted in Section 2, if d is of ERD-type and $h(d)=1$ then $k\leq 4$. Theorem 3.1 shows that if we do not restrict ourselves to ERD-types then, with one possible exception, $h(d)=1$ and $k\leq 4$ if and only if d is an entry in Table 2.1 together with the values 61, 317, 461, 557, 773 and 1877 for $k=3$; and 133, 1397 and 3053 for $k=4$.

Remark 3.3. In [12] we solved a problem of Yokoi in which all ERD-types with $h(d)=1$ were included.

Remark 3.4. The case $d\equiv 1 \pmod 8$ appears to be very special. In what follows we are able to show that those $d\equiv 1 \pmod 8$ in Table 3.1 are precisely those with $h(d)=1$; i.e., if the exceptional d exists then $d\not\equiv 1$ (mod 8).

The following table lists those $d\equiv 1 \pmod 8$ from Table 3.1.

Table 3.2

k	d
3	17
4	33
5	41
6	57
7	89, 113, 137
9	73, 97, 233, 353
10	129, 161
11	593, 857, 1217
12	177, 209
13	1097, 1553, 2273
14	201, 497, 713
15	193, 281
16	217, 249, 329, 393, 537
17	521, 617, 1433
18	417, 633, 737, 1337, 2537, 3713, 8777
19	241, 313, 449, 953, 1193, 1697
20	2033
21	337, 569, 977
22	489, 1137, 1713, 2217
23	433, 457, 641, 881, 1913, 2393
24	753, 1473, 3113, 3377, 5753, 8153

Theorem 3.2. *Let Δ and k be as above and let p be a prime which splits in $Q(\sqrt{d})$. If $\Delta>4p^{k+1}$ then $h(d)>1$.*

Proof. Suppose $h(d)=1$. By hypothesis $\Delta>4p^{k+1}$, whence, $p^{(k+1)/2}<(\sqrt{\Delta})/2$. Let $m=\lfloor(k+1)/2\rfloor$ then $p^i<(\sqrt{\Delta})/2$ for $i=1,2,\cdots,m$. Since the ideal $(p)=\mathcal{P}\bar{\mathcal{P}}$ in $Q(\sqrt{d})$ then $N(\mathcal{P})=N(\bar{\mathcal{P}})=p$ so the set of ideals $S=\{\mathcal{P}^i,\bar{\mathcal{P}}^i\}_{i=1}^m$ satisfies $N(I)<(\sqrt{\Delta})/2$ for all $I\in S$. Thus S consists of distinct reduced ideals, (see for example [14], op. cit.). Therefore, together with the trivial ideal $(1)=\mathcal{O}_K$ we have $2m+1$ reduced ideals. Since it is a fact that application of the continued fraction algorithm to any given reduced ideal will produce all of the reduced ideals equivalent to it, ([14], op. cit.), then $k \geq 2m+1$. However $m = \lfloor (k+1)/2 \rfloor > (k-1)/2$; whence $2m+1 > k$, a contradiction.

Corollary 3.1. *If* $d \equiv 1 \pmod 8$ *and* $k \leq 24$ *then* $h(d)=1$ *if and only if* d *is an entry in Table* 3.2.

Proof. From Theorem 3.2, $h(d)>1$ when $d>2^{k+3}$, (since 2 splits in $Q(\sqrt{d})$). Since we have already checked on a computer all d's up to $2^{31}-1$ as noted in the proof of Theorem 3.1, then the result follows since we are only concerned with $d>2^{27}$, a smaller bound.

We conclude by observing that the $d \equiv 1 \pmod 8$ case is the easiest to address. For example, Corollary 3.1 illustrates that we can get unconditional results. Further progress on this case will be published at a later date since there is much work yet to be done.

Acknowledgements. The first author's research is supported by NSERC Canada grant number A8484 and the second author's research is supported by NSERC Canada grant number A7649. Moreover this research was also supported by the first author's Killam award held at the University of Calgary in 1990. Finally the authors wish to thank Gilbert Fung, a graduate student of the second author, for doing the computing involved in tabulating the above values.

References

[1] S. Chowla and J. Friedlander: Class numbers and quadratic residues. Glasgow Math. J., **17**, 47–52 (1976).
[2] H. K. Kim and M. G. Leu: On two conjectures on real quadratic fields. Proc. Japan Acad., **63**A, 222–224 (1987).
[3] R. A. Mollin: Class number one criteria for real quadratic fields. I. ibid., **63**A, 121–125 (1987).
[4] ——: Class number one criteria for real quadratic fields. II. ibid., **63**A, 162–164 (1987).
[5] R. A. Mollin and H. C. Williams: Class number problems for real quadratic fields. Number Theory and Cryptography (ed. J. H. Loxton). London Math. Soc. Lecture Note Series, **154**, 177–195 (1990).
[6] ——: Computation of the class number of a real quadratic field (to appear in Advances in the theory of computation and computational mathematics).
[7] ——: A conjecture of S. Chowla via the generalized Riemann hypothesis. Proc. A.M.S., **102**, 794–796 (1988).
[8] ——: On prime-valued polynomials and class numbers or real quadratic fields. Nagoya Math. J., **112**, 143–151 (1988).
[9] ——: Prime-producing quadratic polynomials and real quadratic fields of class number one. Number Theory (ed. C. Levesque and J. M. DeKoninck). Walter de Gruyter, Berlin, New York, pp. 654–663 (1988).
[10] ——: Class number one for real quadratic fields, continued fractions, and reduced ideals. Number Theory and Applications (ed. R. A. Mollin) (NATO ASI series), vol. C265, Kluwer Academic Publishers, pp. 481–496 (1989).
[11] ——: Solution of the class number one problem for real quadratic fields of extended Richaud-Degert type (with one possible exception). Number Theory (ed. R. A. Mollin). Walter de Gruyter, Berlin, New York, pp. 417–425 (1990).
[12] ——: Solution of a problem of Yokoi. Proc. Japan Acad., **66**A, 141–145 (1990).
[13] T. Tatuzawa: On a theorem of Siegel. Japan J. Math., **21**, 163–178 (1951).
[14] H. C. Williams and M. C. Wunderlich: On the parallel generation of the residues for the continued fraction factoring algorithm. Math. Comp., **177**, 405–423 (1987).
[15] H. Yokoi: Class number one problems for certain kinds of real quadratic fields. Proc. Internat. Conf. in Class Numbers and Fundamental Units, Katata, Japan (1986).