

## ON THE COMPUTATION OF A TABLE OF COMPLEX CUBIC FIELDS WITH DISCRIMINANT $D > -10^6$

GILBERT W. FUNG AND H. C. WILLIAMS

**ABSTRACT.** A method for finding all the nonisomorphic complex cubic fields with discriminant  $D > -10^6$  is described. Three different methods were used to find the class number of each of these fields. The speed of these techniques is discussed and several tables illustrating the computational results are presented. These include tables of the distribution of the fields and the class numbers and the class group structures of these fields.

### 1. INTRODUCTION

Recently Ennola and Turunen [8] and Llorente and Quer [10] have produced large tables of totally real cubic fields. However, since the work of Angell [1] little work seems to have been done on the tabulation of complex cubic fields. The purpose of this paper is to describe an algorithm which was used to produce all the nonisomorphic complex cubic fields with discriminant  $D > -10^6$ . The previously mentioned table of Angell (see also [12]) only dealt with fields with  $D > -20000$ .

We also discuss three different techniques for evaluating the class number of each of these fields. Two of these methods involve the use of the Euler product to estimate the Artin  $L$ -function at 1, and the third makes use of a transformation of the Dirichlet series. These techniques were implemented and run on a computer. Each obtained the same results, but with rather different timings. Finally, we provide several tables illustrating some of the results of these computations. These tables describe the distribution of the various fields, their class numbers, and their class group structures.

### 2. CONSTRUCTION OF THE COMPLEX CUBIC FIELDS

Any cubic field  $\mathcal{K}$  can be generated by the zero of an irreducible (over the rationals  $\mathbf{Q}$ ) polynomial

$$(2.1) \quad f(a, b, c; x) = x^3 - ax^2 + bx - c,$$

where  $a, b, c \in \mathbf{Z}$ . The discriminant of the polynomial  $f(a, b, c; x)$  is given

---

Received November 30, 1988; revised June 8, 1989, August 14, 1989, August 29, 1989.  
1980 *Mathematics Subject Classification* (1985 Revision). Primary 11R16, 11Y40, 11R29.  
The second author's research was supported by NSERC of Canada Grant #A7649.

by

$$(2.2) \quad D(a, b, c) = a^2b^2 + 18abc - 4b^3 - 4a^3c - 27c^2.$$

Further, the discriminant  $D$  of the field  $\mathcal{K}$  is given by

$$(2.3) \quad D(a, b, c) = DI^2,$$

where  $I = I(a, b, c)$  is the index of the polynomial  $f(a, b, c; x)$ . We further point out that a field generated by the polynomial  $f(a, b, c; x)$  is also generated by the polynomial

$$f(a', b'; x) = x^3 - a'x + b',$$

where  $a' = 3a^2 - 9b$  and  $b' = 9ab - 2a^3 - 27ac$ . The discriminant  $D(a', b')$  of this polynomial is given by

$$D(a', b') = 4a'^3 - 27b'^2 = DI'^2 = D(27I)^2$$

for  $I$  given by (2.3).

It should also be mentioned (see [10]) that

$$(2.4) \quad D = dT^2,$$

where  $d$  is the fundamental discriminant of the quadratic field  $Q(\sqrt{D})$ ,  $T = 3^m T_0$  ( $0 \leq m \leq 2$ ), and  $T_0$  is a square-free integer such that  $\gcd(T_0, 3d) = 1$ .

The basis of our construction of the complex cubic fields is the following theorem of Angell [1] (misprint corrected).

**Theorem 2.1.** *Let  $\mathcal{K}$  be a cubic number field with discriminant  $D < 0$ . There is at least one polynomial which generates  $\mathcal{K}$  such that if the zeros of the polynomial are  $\alpha, \beta \pm i\gamma$  ( $\alpha, \beta, \gamma$  real), then  $0 < \alpha < 1, \beta > 0$  and*

$$S = S(\alpha, \beta, \gamma) = (\alpha - \beta)^2 + 3\gamma^2 \leq \sqrt{|D|}.$$

Since  $a, b, c$  are given by

$$a = \alpha + 2\beta, \quad b = 2\alpha\beta + \beta^2 + \gamma^2, \quad c = \alpha(\beta^2 + \gamma^2),$$

it is easy to deduce the following lemma from Theorem 2.1, (2.2), and (2.3).

**Lemma 2.1.** *Let  $\mathcal{K}$  be any cubic field with discriminant  $D < 0$ . Then  $\mathcal{K}$  is generated by some polynomial  $f(a, b, c; x)$  such that for  $a, b, c \in \mathbf{Z}$ ,*

$$0 < a < 3 + 2|D|^{1/4}, \quad 0 < b < (a^2 + \sqrt{|D|})/3, \\ 0 < c < (a^2 - 3 + 2\sqrt{|D|})/6.$$

Also, the index  $I = I(a, b, c)$  must satisfy

$$3\sqrt{3}I < \sqrt{124a^2 + 432a + 4\sqrt{|D|} + 729}.$$

As a consequence of this lemma we see that if we wish to determine all the possible complex cubic fields with discriminant  $D$  satisfying  $|D| \leq B$ , where

$B$  is some bound, we need to examine only a finite number of triplets  $(a, b, c)$  as possible coefficients of the generating polynomials of the form (2.1). The integers in these triplets must satisfy

$$(2.5) \quad \begin{cases} 0 < a < 3 + 2B^{1/4}, \\ 0 < b < (a^2 + \sqrt{B})/3, \\ 0 < c < (a^2 - 3 + 2\sqrt{B})/6, \end{cases}$$

and the index  $I(a, b, c)$  must satisfy

$$(2.6) \quad I(a, b, c) < I_B = \left( \sqrt{124a^2 + 432a + 4\sqrt{B} + 729} \right) / 3\sqrt{3}.$$

We are now able to present Algorithm 2.1 for determining all the complex cubic fields with discriminant  $D$  satisfying  $|D| \leq B$ . This algorithm is, with minor modifications, very similar to that employed in §3 of [10].

**Algorithm 2.1.** For each triplet  $(a, b, c)$  satisfying (2.5) perform the following steps:

(i) Compute  $a' = 3a^2 - 9b$ ,  $b' = 9ab - 2a^3 - 27ac$ , and  $S(a', b') = 27I_B$ , where  $27I_B$  is given by (2.6), as the bound on the index of  $f(a', b'; x)$ .

(ii) In the case of  $a' = 0$ , determine whether or not the pure cubic field  $\mathcal{K} = \mathbf{Q}(\sqrt[3]{b'})$  has its discriminant in the correct range.

(iii) If  $a' \neq 0$ , execute steps 1–7 of the algorithm given in [10], incorporating the following changes.

(a) Change step 1(a) so that, instead of eliminating the pair  $(a', b')$  when there is a prime  $p$  with  $v_p(a') \geq 2$  and  $v_p(b') \geq 3$ , we replace  $a'$  by  $a'/p^2$ , and  $b'$  by  $b'/p^3$  and then return to the beginning of step 1 of [10]. In the case considered by [10], the pair  $(a'/p^2, b'/p^3)$  will already be among the finite number of pairs being considered; hence,  $(a'/p^2, b'/p^3)$  would be duplication. In our case, however, we do not have the same situation, as  $(a', b')$  is obtained via the transformation in step (i).

(b) In step 2, when determining the irreducibility of  $f(a', b'; x)$  over  $\mathbf{Z}$ , if none of (11), (12) or (13) in part A of [10, §2] holds, then if  $f(a', b'; x)$  is reducible it must have a zero  $m \in \mathbf{Z}$  such that  $m|b'$  and  $|m| < \sqrt{|a'| + |b'|}$ . This change must be made because  $a'$  and/or  $b'$  here can be negative. This is not the case in [10].

(iv) If the pair  $(a', b')$  has not been eliminated by the preceding steps, then  $f(a', b'; x)$  is a generating polynomial of a complex cubic field with discriminant  $D$  satisfying  $|D| < B$ .

After this algorithm has been performed, we will have all the fields with  $|D| < B$ ; however, for any given  $D$  we may have several fields which are isomorphic. To eliminate these isomorphisms, we used the algorithm given in §13 of Delone and Faddeev [7].

This entire procedure was programmed in FORTRAN with some assembly language subroutines and run on the Amdahl 5870 computer in the University of Manitoba Computer Centre. Indeed, all the computations described here and in the sequel were performed on this machine. We first tested our programs by putting  $B = 20000$ . In about 30 CPU seconds we produced a table of fields which agreed with that of [1]. When we put  $B = 10^6$ , it required 4 hours and 11 minutes of CPU time to find all the nonisomorphic complex cubic fields with discriminant  $D > -10^6$ . Of this time, about 63 seconds was needed to eliminate the isomorphisms. In §5 we give a more detailed description of our results.

### 3. COMPUTATION OF THE CLASS NUMBER VIA THE EULER PRODUCT

The next step in the creation of our table of complex cubic fields was the evaluation of the class number for each of the fields. In order to do this, we made use of the analytic class number formula

$$(3.1) \quad 2\pi hR = \sqrt{|D|}\Phi(1),$$

where  $h$  is the class number,  $R$  is the regulator, and  $D$  is the discriminant of  $\mathcal{K}$ . Further,

$$\Phi(1) = \lim_{s \rightarrow 1} \zeta_{\mathcal{K}}(s)/\zeta(s),$$

where  $\zeta_{\mathcal{K}}(s)$  is the Dedekind zeta function and  $\zeta(s)$  the Riemann zeta function.

We adapted the algorithm of Voronoi as modified in Williams, Cormack, and Seah [15] to the general (negative  $D$ ) cubic case. Since  $|D|$  is small ( $< 10^6$ ), we found that a double-precision FORTRAN program was sufficient for the evaluation of a very good approximation to  $R$ . All of the regulators were evaluated in about 89 minutes of CPU time. In the case where a particular discriminant had more than one associated field, we compared the corresponding regulators as a check that these fields were indeed nonisomorphic.

From (3.1) we see that in order to evaluate  $h$ , we need to find an approximation to  $\Phi(1)$  which is sufficiently good that we can evaluate  $h$  (an integer) unequivocally. There are two basic approaches that can be used:  $\Phi(1)$  can be estimated by using the Euler product formula, or it can be estimated by using the Dirichlet series. In this section we will briefly discuss the Euler product techniques.

We first remark that we can write  $\Phi(1)$  as the Euler product

$$(3.2) \quad \Phi(1) = \prod_p f(p),$$

where the product is taken over all the rational primes, and for each such prime  $p$  the value of  $f(p)$  depends upon how the principal ideal  $(p)$  splits in  $\mathcal{K}$ . These values are given in Table 3.1.

TABLE 3.1

Type	Factorization of $(p)$	$f(p)$
A	$\mathfrak{p}\mathfrak{p}'\mathfrak{p}''$	$p^2/(p^2 - 2p + 1)$
B	$(p)$	$p^2/(p^2 + p + 1)$
C	$\mathfrak{p}q$	$p^2/(p^2 - 1)$
D	$\mathfrak{p}^2q$	$p/(p - 1)$
E	$\mathfrak{p}^3$	1

Here we use  $\mathfrak{p}, \mathfrak{p}', \mathfrak{p}'', q$  to denote distinct prime ideals in  $\mathcal{K}$ .

In order to determine the splitting type of  $p$ , we used the method of Llorente and Nart [9]. However, in the case where it was necessary to distinguish whether or not the factorization of  $(p)$  was of type A or B, we used the Lucas function technique mentioned in Williams and Zarnke [16], the algorithm for determining the value of the appropriate Lucas function (mod  $p$ ) being that of Williams [14]. This routine was written in assembly language.

Set

$$F(Q, D) = \prod_{q \leq Q} f(q),$$

where the product is evaluated over the rational primes. Since  $\Phi(1)$  in (3.2) is given as an infinite product, we must determine how large to make  $Q$  such that

$$H(Q, D) = \sqrt{|D|}F(Q, D)/(2\pi R)$$

is within  $1/2$  of  $h$ . When this occurs,  $h = \text{Ne}(H(Q, D))$ , where by  $\text{Ne}(x)$  we denote the nearest integer to  $x$ . One way to do this is to use the heuristics of Shanks mentioned in [3]. We evaluate  $H(Q, D)$  by using the first 500, then 1000, 1500, 2000, etc. primes until  $H(Q, D)$  is within .1 of the same integer  $H$  for six successive evaluations. When this occurs we declare  $h = H$ . This heuristic is easy to implement and executes fairly rapidly; but, unfortunately, it is not a mathematically rigorous method of computing  $h$ .

Another method which can be used is that of Buchmann and Williams [4]. The details of the method are discussed in [4]; we only mention here that in our case we have  $D_{\mathcal{L}} = |d|^3 T^4$  for  $D$  given by (2.4),  $n_{\mathcal{L}} = 6$ ,  $C(t) = 2\tilde{C}(t)/3$ , and  $c_1 + 2c_2^2 = 3$ . Given a known divisor  $h^*$  of  $h$ , this technique makes use of the Euler product to determine  $h$  in  $O(|D|^{1+\epsilon}/(h^* R)^2)$  elementary operations for any  $\epsilon > 0$ . However, we need to assume the truth of the Riemann Hypothesis on  $\zeta_{\mathcal{L}}$ , where  $\mathcal{L}$  is the normal closure of  $\mathcal{K}$ , in order to be able to assert that our class number is correct.

Further, in cases for which  $R$  is small, we must find a value for  $h^*$  which is large enough that our technique does not take too much time in executing. To do this, we simply produce (by trial) a nonprincipal ideal  $\mathfrak{a}$  in  $\mathcal{K}$  such that the least value of  $m (> 0)$  for which

$$(3.3) \quad \mathfrak{a}^m \sim (1)$$

is sufficiently large. We then put  $h^* = m$ . In order to do this, we started  $m$  at 1 and increased it until we found that value for which (3.3) holds. This process was not very time-consuming because the fairly small value of  $|D|$  guarantees us that  $h$  will not be large. We used the algorithm of Voronoi to find all the reduced principal ideals in  $\mathcal{K}$  and the reduction technique described in Williams [13] to determine whether or not (3.3) holds for a particular  $m$ -value. In our application we found that a value of  $h^*$  could be found such that  $h^* > \tilde{h}/6$ , where  $\tilde{h}$  is our first approximation to  $h$  (using 500 primes in the Euler product, say).

Both of these methods of utilizing the Euler product to compute  $h$  were implemented in FORTRAN (again with some assembly language subroutines) and run. The Shanks heuristic method required 8 hours and 16 minutes of CPU time to find all the class numbers, whereas the Riemann Hypothesis technique required 14 hours and 10 minutes. The large difference in these times is a result of the fact that the Shanks heuristics usually (80% of the time) required that no more than 3000 primes were needed for the evaluation of  $H$ , and only rarely required that more than 5000 primes be used. On the other hand, the use of the Riemann Hypothesis demanded that 5000 or more primes be used in most cases.

#### 4. DETERMINATION OF $h$ FROM THE DIRICHLET SERIES

As noted in [3], we can write

$$(4.1) \quad \Phi(1) = \sum_{j=1}^{\infty} \alpha(j)j^{-1},$$

where  $\alpha(j)$  is a multiplicative function,  $\alpha(1) = 1$ , and  $\alpha(p^n)$ , where  $p$  is any rational prime, is given in the Table 4.1 (see Barrucand, Loxton, and Williams [2]).

TABLE 4.1

Type	$n$	$\alpha(p^n)$
A	any	$n + 1$
B	$n \equiv 0 \pmod{3}$	1
B	$n \equiv 1 \pmod{3}$	-1
B	$n \equiv 2 \pmod{3}$	0
C	$n \equiv 0 \pmod{2}$	1
C	$n \equiv 1 \pmod{2}$	0
D	any	1
E	any	0

Notice that  $\alpha(p^n) \leq d(p^n)$ , where by  $d(k)$  we represent the number of divisors of  $k$ . It follows that  $\alpha(k) \leq d(k)$ .

Also, formula (4.1) can be transformed into

$$\Phi(1) = \sum_{j=1}^{\infty} \alpha(j)j^{-1}e^{-jC} + C \sum_{j=1}^{\infty} \alpha(j)E(jC),$$

where  $C = 2\pi/\sqrt{|D|}$  and  $E(y) = \int_y^{\infty} e^{-x}x^{-1}dx$ . Thus, if we put

$$A(m) = \sum_{j=1}^m \alpha(j)j^{-1}e^{-jC} + C \sum_{j=1}^m \alpha(j)E(jC),$$

then by using the reasoning of [3] we get

$$(4.2) \quad \left| \frac{\Phi(1)}{C} - \frac{A(m)}{C} \right| < \frac{2M(m)e^{-mC}}{C(e^C - 1)},$$

where

$$(4.3) \quad M(m) = \max\{d(j)j^{-1} \mid j > m\}.$$

Thus, by (4.2) and (3.1) we get

$$(4.4) \quad \left| h - \frac{A(m)}{CR} \right| < \frac{2M(m)e^{-mC}}{C(e^C - 1)R}.$$

It follows that if  $m$  is sufficiently large that

$$(4.5) \quad 2M(m)e^{-mC} < C(e^C - 1)R/2,$$

then

$$(4.6) \quad h = \text{Ne}(A(m)/CR).$$

In order to ensure that (4.5) holds, we must find a bound on  $M(m)$ . To do this, we first prove

**Lemma 4.1.** *Given any integer  $n \geq 2$ , there exists an integer  $m$  such that  $n/3 < m \leq n/2$  and  $d(m)/m \geq d(n)/n$ .*

*Proof.* If  $p$  is the least prime which divides  $n$ , and  $k = [p/2]$ , then it is an easy matter to show that our result holds for  $m = kn/p$ .  $\square$

From this result it is a simple matter to deduce

**Theorem 4.1.** *For  $M(m)$  defined as in (4.3) we have*

$$M(m) = \max\{d(j)j^{-1} \mid m < j \leq 3m\}.$$

Under the assumption (later verified) that we would never require a value for  $m$  in (4.5) that exceeds 2000 (for values of  $|D| < 10^6$ ) we found, by using Theorem 4.1 to tabulate  $M(m)$ , that

$$M(m) < 7.4(\log m)/m \quad (m < 2000).$$

Thus, in order to determine  $h$ , we can use any value of  $m$  in (4.6) such that

$$(4.7) \quad e^{-mC}m^{-1} \log m \leq .0338CR(e^C - 1),$$

provided that such a value of  $m$  is  $\leq 2000$ . In fact, for the range of  $D$ -values that we considered we never needed a value for  $m$  which exceeded 1109 in order to have (4.7) hold.

This technique is not only mathematically rigorous but, surprisingly, is very much faster than either technique based on the Euler product. To find all the class numbers by this method required only 60.8 minutes of CPU time, once our program was written in FORTRAN and supplemented by assembly language routines for evaluating  $\alpha(k)$  and  $E(y)$ . In view of the complexity of the Dirichlet series method ( $O(D^{1/2+\epsilon})$ ) one would expect the methods of §3 to be faster; however, these complexity measures have more relevance when  $|D|$  is large rather than the small values of  $|D|$  which we were considering. It turned out that for these values the asymptotically faster method was actually considerably slower than the Dirichlet series method. For much larger values of  $|D|$ , of course, this situation would be reversed.

### 5. COMPUTATIONAL RESULTS AND TABLES

A large table, giving the values of  $D$ ,  $a$ ,  $b$ ,  $T$ ,  $R$ ,  $h$  for each of the 181748 nonisomorphic cubic fields with negative discriminant  $> -10^6$ , has been deposited in the UMT file. In this table we use the symbols  $a$ ,  $b$  to represent the coefficients of a generating polynomial of the form  $x^3 - ax + b$  for the field  $\mathcal{K}$ . Also,  $T^2$  is the value of the largest square which divides the discriminant  $D$  of  $\mathcal{K}$  (note that this is not the same  $T^2$  as in (2.4)),  $R$  is the regulator, and  $h$  is the class number of  $\mathcal{K}$ . In this section we will give a brief discussion of some of the information provided by these computations.

In Table 5.1 we give the number of fields that were constructed for values of  $|D|$  within certain intervals and the number of these that were nonisomorphic. In Table 5.2 we present the number of the discriminants in our range for which there are exactly  $k$  nonisomorphic fields having that discriminant.

TABLE 5.1

Interval for $ D $	Number of Fields	Number of Nonisomorphic Fields
1-100489	67735	17137
100490-200704	45563	17927
200705-300304	41373	17964
300305-400689	40846	18268
400690-501264	40111	18425
501265-600625	38429	18237
600626-700569	37963	18346
700570-801025	38104	18521
801026-900601	37259	18367
900602-1000000	37620	<u>18556</u>
		181748



TABLE 5.2

$k$	Number of Discriminants
1	148709
2	1762
3	5438
4	3189
5	7
6	49
7	0
8	1
9	12
> 9	0

TABLE 5.3

$L$	Density	$L$	Density
100489	.170536	600625	.179743
200704	.174705	700564	.180288
300304	.176581	801025	.180780
400689	.177934	900601	.181203
501264	.178989	1000000	.181748

TABLE 5.4

Range of $h$	Number of Fields
1-10	172152
11-20	6355
21-30	1894
31-40	688
41-50	324
51-60	148
61-70	90
71-80	36
81-90	29
91-100	14
101-110	8
111-120	1
121-130	3
131-140	1
141-150	3
151-160	1
161-162	1

In Table 5.3 we exhibit the density of the nonisomorphic cubic fields for which  $-L < D < 0$ .

TABLE 5.5

$h$	Number of Fields	$h$	Number of Fields
1	97069	11	843
2	26273	12	1644
3	22491	13	600
4	7730	14	514
5	4461	15	841
6	5919	16	477
7	2122	17	312
8	2096	18	633
9	2913	19	270
10	<u>1078</u>	20	<u>221</u>
	172152		6355

TABLE 5.6

$L \setminus h_0$	1	2	4	5	7	8	10
100000	0.73495	0.16052	0.03838	0.02770	0.01209	0.00833	0.00423
200000	0.71319	0.16951	0.04398	0.02738	0.01253	0.01019	0.00532
300000	0.70303	0.17211	0.04582	0.02803	0.01323	0.01059	0.00572
400000	0.69636	0.17325	0.04845	0.02863	0.01359	0.01141	0.00590
500000	0.69046	0.17507	0.04961	0.02917	0.01390	0.01178	0.00607
600000	0.68578	0.17718	0.05035	0.02914	0.01372	0.01248	0.00634
700000	0.68250	0.17788	0.05105	0.02943	0.01398	0.01282	0.00642
800000	0.67954	0.17929	0.05165	0.02943	0.01395	0.01306	0.00648
900000	0.67701	0.18006	0.05204	0.02942	0.01394	0.01337	0.00651
1000000	0.67518	0.18073	0.05229	0.02945	0.01381	0.01341	0.00675

TABLE 5.7

$n$	$n$ -Rank	Number of Occurrences
2	2	3043
2	3	12
3	2	861
3	3	3
4	2	16
5	2	4
6	2	<u>5</u>
		3944

Davenport and Heilbronn [6] have proved a theorem which says that this density should approach the asymptotic limit of  $(4\zeta(3))^{-1} \approx .20798$ . If, however, the reader were to plot the density versus  $L$ , he would be somewhat astonished to see that this density is increasing so slowly that his first impression would be that it will not make it to the Davenport-Heilbronn (D-H) limit. Thus, it

TABLE 5.8

$D$	$a$	$b$	Class Group Structure
-300551	49	-169	$c_2 \times c_2 \times c_2$
-421423	453	-5015	$c_2 \times c_2 \times c_2$
-542251	-276	-3395	$c_2 \times c_2 \times c_2$
-588191	19	151	$c_2 \times c_2 \times c_2$
-841304	741	-9110	$c_2 \times c_2 \times c_2$
-864023	91	-379	$c_2 \times c_2 \times c_2$
-344411	139	1914	$c_2 \times c_2 \times c_4$
-379591	-159	3107	$c_2 \times c_2 \times c_4$
-433243	-229	1526	$c_2 \times c_2 \times c_4$
-612263	31	606	$c_2 \times c_2 \times c_4$
-562123	228	4115	$c_2 \times c_2 \times c_6$
-694543	473	-4272	$c_2 \times c_2 \times c_6$
-894348	0	182	$c_3 \times c_3 \times c_3$
-936684	84	-350	$c_3 \times c_3 \times c_3$
-936684	-42	154	$c_3 \times c_3 \times c_3$
-280468	795	-9056	$c_4 \times c_4$
-393828	-285	2684	$c_4 \times c_4$
-532463	37	-165	$c_4 \times c_4$
-555976	899	-10626	$c_4 \times c_4$
-655483	-28	145	$c_4 \times c_4$
-716131	-133	2538	$c_4 \times c_4$
-751819	98	-409	$c_4 \times c_4$
-787663	-267	-4295	$c_4 \times c_4$
-898175	175	1275	$c_4 \times c_4$
-989156	-149	310	$c_4 \times c_4$
-359131	44	-161	$c_4 \times c_8$
-375387	498	-10465	$c_4 \times c_8$
-653971	-46	99	$c_4 \times c_8$
-749723	40	-193	$c_4 \times c_8$
-804443	52	-225	$c_4 \times c_8$
-865851	516	-6613	$c_4 \times c_8$
-173287	-55	32	$c_5 \times c_5$
-304196	2307	-43508	$c_5 \times c_5$
-383827	-240	22489	$c_5 \times c_5$
-746287	1443	41650	$c_5 \times c_{15}$
-641196	-6	154	$c_6 \times c_6$
-782648	19	342	$c_6 \times c_6$
-864243	60	-253	$c_6 \times c_6$
-914683	-28	175	$c_6 \times c_6$
-939843	30	197	$c_6 \times c_6$

remains a challenging problem, assuming that the D-H limit is not in error, to explain the origin of this very slow convergence. This problem was indicated by Shanks in [11, 12], and on the real side in [11, 10], where the problem is further aggravated by even slower convergence. To date, and to our knowledge, no good quantitative explanation of this phenomenon has been given.

In Table 5.4 we present the number of nonisomorphic fields we found with class number  $h$  within a certain range. The largest class number found (162) was for discriminant  $-885871$ . Table 5.5 provides a more complete picture for values of  $h \leq 20$ . In Table 5.6 we give the density of fields with  $|D| < L$  and class number  $h = 3^\nu h_0$ , where  $3 \nmid h_0$  and  $h_0 \leq 10$ . According to the heuristics of Cohen and Martinet [5] we would expect the asymptotic densities to be .518642, .259321, .086440, .025932, and .012349 for  $h_0 = 1, 2, 4, 5, 7$  respectively. If, once again, the reader were to plot these densities given in Table 5.6, he would notice in the case of  $h_0 = 1, 2, 4$  an aggravated case of what occurred for the D-H theorem, and he might reasonably conjecture that the C-M heuristic limits are inaccurate. However, in view of the fact that we do not have an explanation of the similar situation with D-H, we do not consider it wise to invalidate the C-M heuristic limits. We do not know where they are going or how fast in the case  $h_0 = 1, 2, 4$ . We are pleased to put these facts before the reader and urge him to conduct his own investigation. However, note that the columns for  $h_0 = 5, 7$ , which seem to be increasing, have already passed the C-M prediction; this also is a problem which needs further investigation.

Once we had calculated the class numbers of our 181748 fields, it was a relatively simple matter to determine the structure of each class group. Only 3944 of these class groups are noncyclic. In Table 5.7 we give the number of these noncyclic class groups for a given  $n$ -rank.

Finally, in Table 5.8 we present those fields that have the most interesting class group structures. Here,  $c_n$  denotes the cyclic group of order  $n$ , and the values of  $a$  and  $b$  are those for which  $f(a, b; x)$  generates the corresponding cubic number field.

#### BIBLIOGRAPHY

1. I. O. Angell, *A table of complex cubic fields*, Bull. London Math. Soc. **51** (1973), 37–38.
2. P. Barrucand, J. Loxton, and H. C. Williams, *Some explicit upper bounds on the class number and regulator of a cubic field with negative discriminant*, Pacific J. Math. **128** (1987), 209–222.
3. P. Barrucand, H. C. Williams, and L. Baniuk, *A computational technique for determining the class number of a pure cubic field*, Math. Comp. **30** (1976), 312–323.
4. J. Buchmann and H. C. Williams, *On the computation of the class number of an algebraic number field*, Math. Comp. **53** (1989), 679–688.
5. H. Cohen and J. Martinet, *Class groups of number fields: numerical heuristics*, Math. Comp. **48** (1987), 123–138.
6. H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields. II*, Proc. Roy. Soc. London Ser. A **322** (1971), 405–420.

7. B. N. Delone and D. K. Faddeev, *The theory of irrationalities of the third degree*, Transl. Amer. Math. Soc., vol. 10, Amer. Math. Soc., Providence, R.I., 1964.
8. V. Ennola and R. Turunen, *On totally real cubic fields*, Math. Comp. **44** (1985), 495–518.
9. P. Llorente and E. Nart, *Effective determination of the decomposition of the rational primes in a pure cubic field*, Proc. Amer. Math. Soc. **87** (1983), 579–585.
10. P. Llorente and J. Quer, *On totally real cubic fields with discriminant  $D < 10^7$* , Math. Comp. **50** (1988), 581–594.
11. D. Shanks, *A survey of quadratic, cubic and quartic algebraic number fields (from a computational point of view)*, Cong. Numer. **17** (1976), 15–40.
12. ———, Review of [1], Math. Comp. **29** (1975), 661–665.
13. H. C. Williams, *Continued fractions and number-theoretic computations*, Rocky Mountain J. Math. **15** (1985), 621–655.
14. ———, *Effective primality tests for some integers of the form  $A5^n - 1$  and  $A7^n - 1$* , Math. Comp. **48** (1987), 385–403.
15. H. C. Williams, G. Cormack, and E. Seah, *Calculation of the regulator of a pure cubic field*, Math. Comp. **34** (1980), 567–611.
16. H. C. Williams and C. R. Zarnke, *Some algorithms for solving a cubic congruence modulo  $p$* , Utilitas Math. **6** (1974), 285–306.

DEPARTMENT OF COMPUTER SCIENCE, UNIVERSITY OF MANITOBA, WINNIPEG, MANITOBA,  
CANADA R3T 2N2