A Note on Class-Number One in Pure Cubic Fields

By H. C. Williams and Daniel Shanks

Abstract. We examine a subset of the pure cubic fields wherein individual fields appear to have a probability of having class-number one approximately equal to 3/5. We also suggest more elaborate but more efficient algorithms that could be used to extend the data.

1. **Introduction.** It is known [1, p. 313] that if n distinct primes $p \equiv 1 \pmod 3$ divide N, the class-number h of $Q(\sqrt[3]{N})$ is divisible by 3^n. Since almost all N, i.e., all except for a set of measure zero, satisfy this condition, one weak consequence is that the density of $Q(\sqrt[3]{N})$ with $h = 1$ must equal zero. But if N is a prime $q \equiv 2 \pmod 3$, then 3 does not divide h, and if we restrict N to these prime radicands q it is plausible [2] that the $Q(\sqrt[3]{q})$ with $h = 1$ now have a positive asymptotic density in this smaller set of fields.

Of the 617 primes $q < 10^4$, the table computed for [1] lists 294 with $h = 1$, and in the review [2] of this table it was pointed out that this *mean density*: $294/617 = 0.476$ tends to remain quite stable as the upper limit for q increases towards 10^4. It was suggested [2] that the table be extended for $N = q > 10^4$ in order to examine the constancy of this mean density.

This was done in [3]. For the 1880 $q < 35,000$ the class-numbers of $Q(\sqrt[3]{q})$ are distributed as follows:

h	number of q	mean density
1	890	0.4734
2	486	0.2585
4	186	0.0989
5	49	0.0261
7	39	0.0207
8	72	0.0383
> 9	158	0.0840

Throughout the range $10^4 < q < Q = 35000$, the percentage having $h = 1$ is confined between -47.13% and -48.31%; see [3]. The computer run was terminated at $Q = 35000$ because the Voronoi algorithm for computing the fundamental unit u was becoming too time-consuming. This condition is much aggravated by this specific set

$Q(\sqrt[3]{q})$, since so many of these fields have $h = 1$ and, therefore, must have very large u. Since the discriminants are $O(q^2)$, the regulators $R = \ln u$ are $O(q^{1+\epsilon})$ if $h = 1$. The period of the Voronoi algorithm is nearly proportional to the regulator for these long periods.

2. **Two New Developments.** It is clear from the table that if we could further restrict our set of $Q(\sqrt[3]{q})$ to eliminate those with even class numbers, the mean density of those having $h = 1$ would rise even higher. In [4], Eisenbeis, Frey and Ommerborn study the 2-rank of pure cubic fields by the use of the Selmer group of appropriate elliptic curves, and they evaluate this 2-rank for the same 8122 fields $Q(\sqrt[3]{N})$ with $N < 10^4$ already tabulated [2]. Of these 8122 fields, 4612 or 56.8% have odd h. If one restricts N to the 1229 primes $< 10^4$, the percentage changes little: 676 fields or 55.0%. But when they confine the data to the 404 primes $\equiv \pm 1$ (mod 9), the ratio changes markedly: 289 fields or 71.5% have odd class numbers. In [4], a probabilistic, heuristic argument involving the Selmer group is included to explain this phenomenon. Whatever its explanation, the phenomenon is clearly pertinent for our $h = 1$ problem. If we restrict our fields to $Q(\sqrt[3]{r})$ where the r are primes $\equiv 17$ (mod 18), we have eliminated $3 \mid h$ and "discouraged", but not eliminated, $2 \mid h$. Thus, the mean density of $h = 1$ must rise.

We should state that this set $Q(\sqrt[3]{r})$ is not at all artificial. The r primes do have a natural role in the theory of pure cubic fields. The known inequalities for the 3-rank of such fields [1, p. 313] involve two types of primes that divide the discriminant, ω_0 and ω_1. But the r primes are the only primes besides 3 that are not counted in ω_0 or in ω_1. Further, the discriminant always equals $-3r^2$. The q primes that are not r primes have discriminants $d = -27q^2$ instead, and therefore the ordering of the $Q(\sqrt[3]{q})$ by q is different than their ordering by d. The r primes have an asymptotic density of $1/3$ in the first ordering, and a density of $3/5$ in the second. With this second ordering the mean density of the $Q(\sqrt[3]{q})$ with $h = 1$ would obviously be larger than the 0.4734 listed above. In the set $Q(\sqrt[3]{r})$ there is no such ambiguity. (In the $Q(\sqrt[3]{N})$ set, where some N are not square-free, the two orderings differ even more.) Since the $Q(\sqrt[3]{r})$ set has great homogeneity, it may be presumed that its theory, and its computation, would both be simplified.

The second new development that led to the present note was the considerable improvement that was made in the programming for the Voronoi algorithm. This is reported elsewhere [5], together with other tables computed with its use. With the faster algorithm, the smaller discriminants in the $K = Q(\sqrt[3]{r})$, and their more restricted population, we have now computed these fields for all $r < 200,000$.

As before, h was computed by combining the regulator R with an Euler product estimate for $\lim_{s=1+} \zeta_k(s)/\zeta(s)$.

3. **The Apparent Density.** In the table that follows we list $N(R)$, the number of primes $r \leqslant R$, and $C(R)$, the number of such $Q(\sqrt[3]{r})$ having class-number 1. We show increments in R of 2000 until $R = 40,000$ and increments of 10,000 thereafter.

R	C(R)	N(R)	C/N	R	C(R)	N(R)	C/N
2000	33	50	0.66000	38000	405	672	0.60268
4000	59	90	0.65556	40000	423	699	0.60515
6000	87	132	0.65909	50000	524	855	0.61287
8000	113	172	0.65698	60000	634	1014	0.62525
10000	126	201	0.62687	70000	727	1160	0.62672
12000	151	241	0.62656	80000	817	1309	0.62414
14000	177	277	0.63899	90000	896	1452	0.61708
16000	193	309	0.62460	100000	969	1594	0.60790
18000	213	344	0.61919	110000	1061	1738	0.61047
20000	233	375	0.62133	120000	1150	1883	0.61073
22000	251	408	0.61520	130000	1244	2038	0.61040
24000	274	446	0.61435	140000	1323	2168	0.61024
26000	292	478	0.61088	150000	1399	2299	0.60853
28000	313	514	0.60895	160000	1482	2440	0.60738
30000	330	543	0.60773	170000	1569	2576	0.60908
32000	344	572	0.60140	180000	1657	2719	0.60942
34000	369	608	0.60691	190000	1740	2854	0.60967
36000	388	642	0.60436	200000	1827	2993	0.61042

We observe the following behavior of the mean density $C(R)/N(R)$:

a. Moderate fluctuations and a moderate decline until about $R = 20,000$. Both of these features were expected.

b. A long, smooth, shallow wave with a local minimum of about 0.603 near $R = 38,000$ and a local maximum of about 0.627 near $R = 70,000$. No known explanation.

c. Very small oscillations for $100,000 < r < 150,000$.

d. A surprisingly flat behavior from 150,000 to 200,000.

Of course, nothing conclusive can be deduced from such empirical data. Nonetheless, the data look sufficiently good to suggest the following conjectures:

A. Class-number 1 has an asymptotic density in $Q(\sqrt[3]{r})$. With less assurance, we think it possible for the alleged limit to be close to the mean density at the end of our table.

B. If, contrary to the second sentence in A, the mean density continues to decrease, it is certainly plausible that the decrease will be very slow; e.g., $C(R)/N(R) < 1/2$ can hardly be expected until R is very large.

C. In any case, it is highly probable that there are infinitely many $Q(\sqrt[3]{r})$ with class-number 1.

The data do not justify more explicit language: "close to" in A, and "very large" in B we must leave undefined.

The problem of proving the existence of infinitely many algebraic number fields with $h = 1$ is a long-standing one; it is unlikely that it will be settled in the near future. The prevalence of $h = 1$ in certain sets of quadratic, cubic and quartic fields remains a most mysterious phenomenon. This is aggravated in $Q(\sqrt[3]{N})$ since these

fields are nonabelian. In abelian fields, it is conceivable that a deep study of cyclotomic units might throw some light on the problem.

4. Algorithmic Possibilities. There are, however, interesting algorithmic possibilities for extending the computation beyond $R = 200,000$. If one wished to examine samples of 100 fields, say, around $R = 500,000$ or $R = 10^6$, or larger, but did not want to rely on brute force or faster computers, the following algorithmic possibilities could be examined.

1. First, eliminate all $Q(\sqrt[3]{r})$ with even h by using the method in [4]. This would be substantially abbreviated in our cases since *we do not need to know the exact 2-rank,* merely that it exceeds zero. Our restriction to $r \equiv 17 \pmod{18}$ should also simplify the calculation.

2. There is a real possibility that the algorithm in [4] can be replaced with a much more elementary algorithm. This would be of mathematical interest in its own right.

3. With the even h thus culled out, the main competitors for $h = 1$ would be $h = 5$ and $h = 7$. It would be unnecessary to run the Voronoi algorithm to completion; as soon as its period becomes sufficiently long to assure that h is less than 5, it could be terminated. Thus, the Voronoi computation would be reduced to about one-fifth.

4. It is not improbable that the Voronoi algorithm itself can be radically abbreviated. This would require extensive study and development, but, if attained, it would also be of mathematical interest in its own right.

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

Department of Mathematics
University of Maryland
College Park, Maryland 20742

1. PIERRE BARRUCAND, H. C. WILLIAMS & L. BANIUK, "A computational technique for determining the class number of a pure cubic field," *Math. Comp.*, v. 30, 1976, pp. 312–323.

2. DANIEL SHANKS, Review of UMT file: "Table of pure cubic fields $Q(\sqrt[3]{D})$ for $D < 10^4$," *Math. Comp.*, v. 30, 1976, pp. 377–379.

3. H. C. WILLIAMS, "Certain pure cubic fields with class number one," *Math. Comp.*, v. 31, 1977, pp. 578–580; "Corrigendum," *Math. Comp.*, v. 33, 1979, pp. 847–848.

4. H. EISENBEIS, G. FREY & B. OMMERBORN, "Computation of the 2-rank of pure cubic fields," *Math. Comp.*, v. 32, 1978, pp. 559–569.

5. H. C. WILLIAMS, G. CORMACK & E. SEAH, "Computation of the regulator of a pure cubic field," *Math. Comp.* (To appear.)