MATHEMATICS OF COMPUTATION, VOLUME 28, NUMBER 125, JANUARY, 1974

On the 3-Rank of Quadratic Fields and the Euler Product

By Carol Neild and Daniel Shanks

Abstract. This paper covers many (closely related) topics: the distribution of the 3-Sylow subgroups of imaginary quadratic fields; the possibility of finding 3-ranks greater than 4; some questions concerning $a^3 = b^2 + c^2D$; and the convergence of Euler products and its relation to the extended Riemann hypothesis. Two programs that were used in this investigation are described.

1. Introduction. The p-rank of an imaginary quadratic field $Q((-D)^{1/2})$ is designated as r_p and is the number of factors in the p-Sylow subgroup of its ideal class group. The discriminant d here equals $-D$, or $-4D$, according as $D \equiv 3 \pmod 4$, or not, and if d is divisible by exactly n distinct primes, one has, very simply,

$$r_2 = n - 1. \tag{1}$$

Thus, there is no problem in making r_2 as large as one wishes. Until recently, however, not a single case of $r_p > 2$ was known for any $p > 2$.

In [1] and [2] a number of examples of $r_3 = 3$ were developed and in [3] two cases of

$$r_3 = 4 \tag{2}$$

were displayed. Now, $r_3 \geqq 4$ has a profound algebraic implication [4]: *No* algebraic extension of such a $Q((-D)^{1/2})$ has class number 1. Therefore, no matter how many algebraic irrationalities are adjoined to $Q((-D)^{1/2})$, it is impossible to obtain unique factorization of the algebraic integers in the resulting, larger field.

One of the cases of $r_3 = 4$ in [3] is

$$D = 87386945207 = 167 \cdot 12409 \cdot 42169, \tag{3}$$

for which $Q((-D)^{1/2})$ has the class group

$$C(3) \times C(3) \times C(3) \times C(3) \times C(2^3) \times C(2) \times C(181). \tag{3a}$$

Here, $C(n)$ is the cyclic group of order n and one has

$$r_3 = 4, \quad r_2 = 2, \quad r_{181} = 1. \tag{3b}$$

The other case in [3] is

$$D = 83309629817 = \text{prime}, \tag{4}$$

for which we have

Received June 11, 1973.

AMS (MOS) subject classifications (1970). Primary 12A25, 12A65, 10C05, 12-04, 10H10.

$$C(3^2) \times C(3) \times C(3) \times C(3) \times C(2^2) \times C(181) \tag{4a}$$

and therefore

$$r_3 = 4, \quad r_2 = 1, \quad r_{181} = 1. \tag{4b}$$

Our point in departure here is the startling coincidence (?) wherein both examples have class numbers divisible by 181. A priori, it seems impossible to imagine why $r_{181} > 0$ has any relevance for $r_3 > 3$, and so the presumption was [3] that this common factor $C(181)$ was merely a coincidence. But no intuitive notion, no matter how fervently held, constitutes mathematics, and so it seemed desirable to find a third case of (2). If it now had $r_{181} = 0$, fine; but if one found $r_{181} > 0$ again, some hard thought would be called for!

The D in (4) is

$$D = D_3(-235) \tag{5}$$

where

$$D_3(y) = 27y^4 - 74y^3 + 84y^2 - 48y + 12. \tag{6}$$

By the theory in [2], one knows that $r_3 \geqq 2$ for all square-free $D_3(y)$ with $y \equiv -1 \pmod 6$.

We have recently programmed a more elaborate and versatile SPEEDY subroutine. Primarily, SPEEDY estimates the Dirichlet series of $Q(d^{1/2})$:

$$L(1, \chi) = \sum_{n=1}^{\infty} \left(\frac{d}{n}\right) \frac{1}{n} = \prod_{q=2}^{\infty} \frac{q}{q - (d/q)} \tag{7}$$

from a partial product of the Euler product on the right of (7). The additions to SPEEDY alluded to are described below. They enabled us to compute a class group analysis of $Q((-D_3(y))^{1/2})$ directly from the argument y in about 15 seconds computer time on a CDC 6700 for any y in the range $100 < |y| < 1000$.

Including those $Q((-D_3(y))^{1/2})$ calculated earlier, we have now examined the 250 smallest, square-free $D_3(y)$ with $y \equiv -1 \pmod 6$. These vary from $D_3(5) = 9497$ to $D_3(-919) = 19316154836081$ and include the sought-for

$$\begin{aligned} D = D_3(-739) &= 8082611041961 \\ &= 131 \cdot 61699320931 \end{aligned} \tag{8}$$

which has the class group

$$C(3) \times C(3) \times C(3) \times C(3) \times C(2) \times C(2) \times C(19) \times C(499) \tag{8a}$$

and therefore has

$$r_3 = 4, \quad r_2 = 2, \quad r_{181} = 0. \tag{8b}$$

So much for that.

To verify that $Q((-D_3(-739))^{1/2})$ contains $C(3) \times C(3) \times C(3) \times C(3)$ it suffices to examine four integral ideals in this field:

$$i = (a, (b + c(-D)^{1/2})/(b, c)) \tag{9}$$

that are of order 3:

$$a^3 = b^2 + c^2 D, \tag{10}$$

and none of which is equivalent to any product containing the other three. Four such generators of the 3-Sylow subgroup in (8a) are

$$\begin{aligned} j &= (2188922, \tfrac{1}{2}(3238506402 + 2(-D)^{1/2})), \\ k &= (40410, \tfrac{1}{2}(5801534 + 2(-D)^{1/2})), \\ l &= (82050, \tfrac{1}{2}(22804534 + 2(-D)^{1/2})), \\ m &= (96842, \tfrac{1}{2}(29595438 + 2(-D)^{1/2})). \end{aligned} \tag{11}$$

More on these ideals (9)–(10) later.

In the next section, we discuss the distribution of different 3-Sylow subgroups in our set of 250 class groups. Section 3 gives an heuristic estimate of the size of $|y|$ needed before we can reasonably expect to see $r_3 = 5$, 6, etc. (It has not yet been shown that such r_3 actually occur.) Section 4 indicates briefly some questions concerning the values of c that occur in (10).

Section 5 describes the new SPEEDY and gives data on two other distributions:

(a) For these discriminants $d = -4D_3(y)$, how are the Legendre symbols (d/q) distributed for the first 15000 odd primes q from $q_2 = 3$ to $q_{15001} = 163847$?

(b) For the same limit 163847, how are the relative errors distributed in the SPEEDY estimates:

$$\left(\prod_{q=2}^{163847} \frac{q}{q-(d/q)} - L(1,\chi)\right) \Big/ L(1,\chi)? \tag{12}$$

Both of these distributions relate to the question of whether the Dirichlet functions $L(s, \chi)$ obey the Riemann Hypothesis.

Finally, Appendix 2 describes CUROID which computes the ideal cube-roots of the identity (9)–(10), and Appendix 3 describes other new features of SPEEDY that may be used to speed up the factorization of large numbers.

2. The Distribution of the 3-Sylow Subgroups.

Our 250 cases of $Q((-D_3(y))^{1/2})$ have 3-Sylow subgroups that are distributed as follows.

$C(3) \times C(3)$:	115 cases	$C(3) \times C(3) \times C(3)$	: 30 cases
$C(3^2) \times C(3)$:	47 cases	$C(3^2) \times C(3) \times C(3)$	: 17 cases
$C(3^3) \times C(3)$:	21 cases	$C(3^3) \times C(3) \times C(3)$	: 6 cases
$C(3^4) \times C(3)$:	9 cases	$C(3^4) \times C(3) \times C(3)$	: 2 cases
$C(3^2) \times C(3^2)$:	1 case	$C(3) \times C(3) \times C(3) \times C(3)$:	1 case
		$C(3^2) \times C(3) \times C(3) \times C(3)$:	1 case

The proportion of cases with $C(3) \times C(3)$ drops slowly from about 5/9 to about 4/9: among the first 50, 100, 150, 200, and 250 cases, there are 27, 53, 73, 89, and 115 cases, respectively, of $C(3) \times C(3)$. This slow drop reflects the contrary trend wherein the proportion of cases having $r_3 > 2$ rises at about the same rate: There are correspondingly 7, 19, 28, 43, and 57 cases of $r_3 > 2$, respectively.

Although the evidence is not strong, one can conjecture that these proportions will have definite asymptotic limits as $|y| \to \infty$, and further, that each of the subgroups above will occur in its own limiting proportion; cf. [5], [6]. However, we do not have a convincing heuristic argument to support this conjecture or to predict the values of these purported limits.

Several comments on this conjectured distribution: Our discriminants $-4D_3(y)$ are, of course, very special. If one examined *all* imaginary quadratic fields, the proportions found would be very different; $r_3 = 0$ would predominate, and $r_3 > 2$ would be very rare.

If a limiting distribution does occur for our 3-Sylow subgroups, that would be in *marked distinction* to the expected distribution of the 2-Sylow subgroups. As $|y| \to \infty$, prime $D_3(y)$ should become rarer and rarer and, by (1), the proportion of cases with $r_2 = 1$ will therefore approach 0. And $r_2 = 2$ should approach 0 also, although much more slowly. In fact, for every n, the proportion of cases with $r_2 = n$ should peak at some value of $|y|$ and then very slowly approach zero density.

As we expected, we find no correlation between r_3 and r_2. We show below the number of our 250 cases that have values of r_2 from 1 to 6. The 57 cases having $r_3 > 2$ are seen to be distributed proportionally.

	r_2					
	1	2	3	4	5	6
all 250 cases	40	111	76	18	4	1
$r_3 > 2$	9	25	20	2	1	0

It would be of interest if one could predict r_3 for each $Q((-D_3(y))^{1/2})$ more directly from its argument y without computing the class group. At present, we know of no way, and perhaps no (substantially) faster computation is possible for large values of $|y|$. In the analogous problem for $p = 2$, r_2 may be determined from (1) by factoring $D_3(y)$. But as $|y| \to \infty$, the quickest way to do this, requiring only $O(|y|)$ operations, is via its 2-Sylow subgroup [7]. That is, one determines the n in (1) from r_2 instead of conversely.

If the reader wishes to pursue this problem of predicting r_3 from y, or the earlier problems concerning its distribution, he should find our Table 1, in Appendix 1, useful. We list there all 115 values of y which have $C(3) \times C(3)$, all 30 values for $C(3) \times C(3) \times C(3)$, etc.

3. The Norms a. Where are Cases with $r_3 > 4$? Our first field has $D = D_3(5) = 9497$. It has $r_3 = 2$. The first $r_3 = 3$ here is for $D_3(-61) = 390949805$. The first $r_3 = 4$ here is for $D_3(-235) = 83309629817$. Although we have not proven that $r_3 = 5, 6$, etc. occur in $Q((-D_3(y))^{1/2})$, we conjecture that they do. Lacking a better theory, we will give an heuristic estimate of the minimal $|y|$ required before we can expect such r_3 to appear.

The estimate is based upon the distribution of the integers a in (9)–(10). Here a is the minimal norm of all integral ideals in an equivalence class whose cube is the identity. Except for the identity itself, there are

$$\tfrac{1}{2}(3^{r_3} - 1) \tag{13}$$

pairs of such reduced, conjugate ideals:

$$(a, (b \pm c(-D)^{1/2})/(b, c)). \tag{14}$$

TABLE 2

$a^3 = b^2 + c^2$ 8082611041961

a	b	c	a	b	c
40410	5801534	2	1121789	1188124065	2
82050	22804534	2	1198921	1105537400	249
96842	29595438	2	1281850	1443152582	54
113837	37985097	2	1436922	893374922	518
130514	46806330	2	1574570	316450338	686
161754	58514342	10	1577186	345876390	686
269410	72777214	42	1635325	2061806966	123
398485	199265293	54	1711709	2123688927	250
448649	269169540	47	1776525	628526474	803
455394	251737430	62	1910805	32560082	929
523337	104436027	128	2153233	2225237284	789
618117	185442203	158	2159953	102478031	1116
629197	272827682	147	2188922	3238506402	2
735249	514823815	128	2212121	1532884995	1024
841713	716858956	101	2322933	3527573021	106
946089	913179787	40	2538573	4027499786	131
993018	752577214	226	2565669	3648915922	665
1043522	931988478	182	2607714	4150631438	250
1053345	161358767	376	2803714	4599920962	330
1068833	1104069711	16	2878917	4880354638	73

The $40 = \frac{1}{2}(3^4 - 1)$ equations (10) for the $D = D_3(-739)$ of (8) are listed in Table 2. The corresponding data for the $D_3(-235)$ of (4) were given in the similar Table 2 of [3].

Since the ideals (9) in both Tables 2 are reduced, a is bounded as follows:

$$0 < a < (4D/3)^{1/2}, \tag{15}$$

and since the 40 values of a in either Table 2 are squeezed into the interval (15) we expect, and find, that they are distributed fairly uniformly in (15) except at its upper end

$$D^{1/2} < a < (4D/3)^{1/2} \tag{16}$$

where the density falls off markedly. (Only the largest a in the Table 2 here falls into (16).)

The reason for this sharp falling off is that if we exclude ideals that are mere multiples of (9), namely

$$(na, (nb + nc(-D)^{1/2})/(b, c)),$$

the norm a_2 of the *second smallest norm* within each equivalence class satisfies

$$D^{1/2} < a_2 . \tag{17}$$

Thus, certain ideals of the smallest norm a, and of the second smallest norm a_2, will share the interval (16). For example, the five largest a in Table 2 here correspond, respectively, to equivalent ideals of norm $a_2 = 3214930, 3151465, 3099505, 3209553$, and 3028066, all of which are also in (16). This split in (16), one a to five a_2, is not typical; for the $D_3(-235)$ of [3] one finds, instead, three a and three a_2 in the interval (16).

Because of this approximate (but qualified) uniformity, we therefore expect, and find, that the smallest a in each Table 2 satisfies

$$a < \frac{1}{40}(4D/3)^{1/2}.$$

But this smallest a must also satisfy

$$a^3 > D \tag{18}$$

from (10) since (9) is of order 3. It follows that

$$(4D/3)^{1/2} > 48000 \quad \text{or} \quad D > 1728000000$$

if $r_3 = 4$. This is true for (4).

For larger r_3, we approximate (13) by $\frac{1}{2}\, 3^{r_3}$ and obtain

$$D > 3^3 \cdot 729^{r_3} \cdot 2^{-12}. \tag{19}$$

Taking $D \sim 27\, y^4$ from (6) therefore gives the heuristic bound

$$|y| > \tfrac{1}{8}((27)^{1/2})^{r_3} \tag{20}$$

for the fields $Q((-D_3(y))^{1/2})$ and larger values of r_3.

The smallest norm a in Table 2 corresponds to $c = 2$. While other reduced ideals there also have $c = 2$, $c = 1$ does not occur even once in Table 2. The same thing is true for the Table 2 of [3] for the first $r_3 = 4$, and also for the first $r_3 = 2$ and first $r_3 = 3$ mentioned at the start of this section. Now $c = 1$ *can* occur for the smallest a for some $Q((-D_3(y))^{1/2})$; for example, it occurs in

$$24801^3 = 3299062^2 + D_3(635).$$

But occurrences of $c = 1$ are very rare for any y, and in no known case does it occur in the first example of an r_3. We will resume a discussion of the various values of c in the next section.

Therefore, for most larger values of r_3, it is fairly safe to replace (18) by the stronger

$$a^3 > 4D. \tag{18a}$$

This implies

$$D > 3^3 \cdot 729^{r_3} \cdot 2^{-8} \tag{19a}$$

and therefore

$$|y| > \tfrac{1}{4}((27)^{1/2})^{r_3}. \tag{20a}$$

At best, (20a) is a necessary condition, not a sufficient one. Nonetheless, $r_3 = 3$ and $r_3 = 4$ did occur for $|y|$ less than twice the right side of (20a). The correct conclusion seems to be this: while it would be rash to predict that $r_3 = 5$ will occur before $|y| = 2000$, there is a moderate probability that it would do so.

Note added in proof. To verify that (20a) remains valid for $r_3 = 5$, we subsequently ran the next 10 cases of $Q((-D_3(y))^{1/2})$ beyond the $y = -919$ in Table 1. It is valid, and in the process we found $C(3^5) \times C(3)$ at $y = -937$ and $C(3^7) \times C(3)$ at $y = -949$.

4. Problems Concerning the Coefficients c. In Table 2 of [3] for $D = D_3(-235)$, one notes (and it was specifically called attention to there) that besides 9 cases of $c = 2$ there are 2 cases of $c = 2n^3$ for $n = 2, 3, 4$, and 5. In the present Table 2, $c = 2$ occurs 7 times, $c = 2n^3$ occurs twice for $n = 3, 4, 5$ and 7 and once for $n = 2$ and 8. Clearly, this is not merely coincidental; there must be a number-theoretic interpretation for the frequent occurrence of these $c = 2n^3$.

Here are some statistics. For the 25 largest cases of $r_3 = 3$ in Table 1, from $y = 575$ to $y = -919$, inclusive, there are $25 \times \frac{1}{2}(3^3 - 1) = 325$ reduced ideals of smallest norms a within their equivalence classes. In these 325 the following values of c occur with the indicated frequencies:

c	1	2	16	54	128	250	432	686
frequency	2	76	11	13	9	5	1	9

Thus, $c = 2n^3$ is very common (while $c = 1$ is very rare).

With the program CUROID of Appendix 2, we have not only computed these $13 = \frac{1}{2}(3^3 - 1)$ ideals of smallest norm a, but also the 13 of the second smallest norm a_2, of the third smallest norm a_3 and of the fourth smallest norm a_4. In this larger sample of $4 \times 325 = 1300$ ideals, the foregoing frequencies are somewhat increased:

c	1	2	16	54	128	250	432	686
frequency	2	105	13	14	11	14	1	11

In addition, one notes scattered values of $c = 2n^3$ for $n = 8, 9, 11$, and some larger values of n.

We must admit that we do not really understand this prevalence of these $c = 2n^3$ (or the rarity of the $c = 1$). The abundance of $n = 5$ and 7 above relative to $n = 6$ only adds to the mystery. The lone case of $n = 6$ in these 1300 ideals is

$$1279633^3 = 1243848007^2 + 432^2\, D_3(575).$$

And $n = 10$ does not appear here at all.

Perhaps an explanation of the prevalence of $c = 2n^3$ would follow from the theory of Mordell's equation [9]:

$$x^3 - y^2 = k.$$

But even if it did, one would still want an algebraic number theory interpretation.

The best clue now known to us is based upon that fact that the imaginary and real fields

$$Q((-D)^{1/2}) \quad \text{and} \quad Q((3D)^{1/2})$$

are related via class field theory [8]. It is known that the ideals satisfying

$$a^3 = b^2 + c^2D \quad \text{or} \quad a^3 = b^2 - c^2 3D \tag{21}$$

in either of these two fields may be used to compute the unramified cubic extensions of the other field (cf. [10]). It can be shown that if the coefficient c in (21) is divisible by a cube n^3, then the resulting cubic polynomial can be simplified by a transformation to yield a cubic polynomial with smaller coefficients. This is not itself an adequate explanation but it may indicate where one lies.

As for $c = 1$, it is easy to show that any case of $a^3 = b^2 + D_3(y)$ with $y \equiv -1 \pmod 6$ must satisfy

$$a \equiv 9 \pmod{12} \quad \text{and} \quad b \equiv \pm 4 \pmod{18}, \tag{22}$$

but whether these restrictions suffice to account for the observed rarity has not been examined. Many questions; few answers.

5. The New SPEEDY Features and its Statistics. The original SPEEDY was programmed [7, pp. 417, 433] by D. H. and Emma Lehmer. It estimates the Dirichlet series (7) by the partial product

$$L(Q) = \prod_{q=2}^{Q} \frac{q}{q - (d/q)}. \tag{23}$$

Except for $q = 2$, (d/q) is computed by a subroutine JACOBI that uses the Reciprocity Law. For $d < 0$, one therefore estimates the class number of $Q(d^{1/2})$ by

$$h(d) \approx \frac{(-d)^{1/2}}{\pi} L(Q). \tag{24}$$

Although we kept the same name, the new SPEEDY [11] is not particularly fast since it is written in Fortran. But it has a number of new features that we used here:

A. The odd primes q are on tape in blocks of 500 and the input parameter K sets the limit Q as the $500 \cdot K$th odd prime. In the present work we set $K = 30$ and therefore had

$$Q = q_{15001} = 163847.$$

B. All prime divisors of $d \leqq Q$, which are those q with $(d/q) = 0$, are recorded with their correct multiplicity. The cofactor of d (the quotient that remains after these divisions) is also recorded.

C. For each q having $(d/q) = +1$, there exists a quadratic form

$$F_q = (q, b_q, c_q) \tag{25}$$

of discriminant

$$d = b_q^2 - 4qc_q. \tag{26}$$

These forms are needed for the program CLASNO that computes the class group of $Q(d^{1/2})$ [7, Eq. (7)]. The input parameter L indicates the number of forms (25) that we wish. For each of the first L primes q having $(d/q) = +1$, we compute b_q by solving

$$b_q^2 \equiv d \pmod{q}, \qquad b_q \equiv d \pmod{2} \tag{27}$$

with the use of RESSOL, a subroutine described in [12], [13].

D. A record is also kept of $R(Q)$, the number of odd $q \leqq Q$ that have $(d/q) = +1$.

E. There are several variants of this new SPEEDY. The one used here computed $d = -4D_3(y)$ from y, computed (24) and (25) with $K = 30$, $L = 6$, and read this data directly into the input of CLASNO [7]. We thereby compute the class group of $Q((-D_3(y))^{1/2})$ directly from y. A second version computes (and plots) the sequence of partial products (23) for $K = 1, 2, 3, \cdots$. A third version is accessible on a remote teletype (time-sharing) terminal and has additional features described in Appendix 3.

The utility of SPEEDY is based upon the convergence of (23) as $Q \rightarrow \infty$. This convergence is slow, at best. It only occurs, at all, because the primes q with $(d/q) = +1$ (the "residues") and those with $(d/q) = -1$ (the "nonresidues") are equinumerous as $Q \rightarrow \infty$. Within this proven condition, however, there is much play possible: the rate of convergence of $L(Q)$ and the difference in the counts of the residues and nonresidues are dependent upon the complex zeros of the function $L(s, \chi)$. The fastest possible convergence and the smallest difference of counts can only occur if $L(s, \chi)$ obeys the Riemann Hypothesis.

The statistics that follow are based upon 200 of our 250 fields $Q((-D_3(y))^{1/2})$ since we did not wish to repeat those computed earlier. (If someone wishes to check our work, the 50 values of y omitted are the 22 values listed in [2, Table III], the 26 values referred to in [3, p. 185] that satisfy $137 \leqq |y| \leqq 595$ and have $r_2 = 1$ or $r_2 > 4$, and, finally, our last two new cases: $y = 917, -919$.)

With $K = 30$, and therefore 15000 odd primes q, one expects the number of residues $R(Q)$ to be about 7500. Here is how the 200 values of $R(Q)$ are distributed:

$R(Q)$

7325–7374	7375–7424	7425–7474	7475–7524	7525–7574	7575–7624	7625–7674
5	24	35	56	48	25	7

The extremes here are for $y = -865$ which has 7337 residues and for $y = -175$ which has 7666. The average $R(Q)$ is 7505, and the distribution is roughly Gaussian, but with a somewhat smaller spread.

For the optimum operation of CLASNO [7, p. 420], one wants to know the average accuracy of the estimate (24). The relative error, in parts per 1000, is

$$E(Q) = 1000\left(\prod_{q=2}^{Q} \frac{q}{q-(d/q)} - L(1,\chi)\right)\Big/ L(1,\chi). \tag{28}$$

Here is how the 200 cases are distributed for $Q = 163847$ $(K = 30)$.

E(Q)

-2 -1½ -1 -½ 0 +½ +1 +1½ +2

1	3	2	11	9	19	31	24	29	20	20	13	9	6	1	2

In brief, one can say that one-half of the cases are better than 1 part in 2000, one-sixth are worse than 1 part in 1000, but none (in this limited sample) are as bad as 2 parts in 1000. The worst estimates were for $y = -901$: $E = -1.751$, $y = -625$: $E = +1.756$, and $y = -709$: $E = +1.916$. (With the second variant of SPEEDY mentioned in point E above, we are currently studying possibilities of eliminating or reducing these worst errors.)

On the Riemann Hypothesis one estimates

$$R(Q) - \tfrac{1}{2}\pi(Q) = O(Q^{1/2}), \qquad E(Q) = O(Q^{-1/2}). \tag{29}$$

In fact, the exponents here follow directly from the real part of the s having $L(s, \chi) = 0$. Without attempting a more detailed study, we conclude that the $R(Q)$ and the $E(Q)$ tabulated above are consistent with the Riemann Hypothesis. Since $L(s, \chi)$ has, in any case, infinitely many zeros with real part $\frac{1}{2}$, the convergence of $L(Q)$ cannot be better than that which we have observed here. Whether some summability process can improve this convergence remains an open question. We are trying several ideas and will publish later anything of value that is found.

Appendix 1. The 3-Sylow Subgroup of $Q((-D_3(y))^{1/2})$.

TABLE 1. *Values of y*

$C(3) \times C(3)$: 115 cases.

5	−7	11	−13	17	−25	35	−37	47	59
77	89	−91	95	−97	101	107	−109	−133	−139
143	−151	155	−157	161	173	185	203	215	−223
227	233	−241	257	−259	263	−265	−271	−277	−283
299	−301	311	−319	329	341	347	−349	353	−355
359	−361	365	371	−373	383	389	−415	−427	437
443	−445	−457	−487	−493	−523	527	−529	533	−535
539	551	−553	−571	581	−595	−601	−613	641	−643
−649	659	−667	677	−679	−691	−721	−727	737	−745
749	761	767	−769	−775	785	803	−805	815	833
845	−847	857	−859	863	−865	−871	875	−877	−895
899	905	911	−913	917					

$C(9) \times C(3)$: 47 cases.

29	−49	53	−79	−103	113	−115	−121	−175	197
−199	−229	245	−289	−385	395	−403	−409	413	425
−451	473	−475	479	491	497	−541	605	−607	−637
653	683	−685	695	−697	701	−703	707	−733	−751
773	779	−811	−817	−823	827	−853			

$C(27) \times C(3)$: 21 cases.

−19	−55	71	137	−163	191	−193	−205	305	−313
323	467	485	−499	509	−511	557	−577	593	−619
−763									

$C(81) \times C(3)$: 9 cases.

23 65 −217 −439 −583 623 689 −709 809

$C(9) \times C(9)$: 1 case.

−433

$C(3) \times C(3) \times C(3)$: 30 cases.

−61 −145 149 −187 221 239 −247 275 281 287
317 −325 −367 −391 431 −469 515 −517 521 563
599 611 617 635 −661 665 725 −829 851 893

$C(9) \times C(3) \times C(3)$: 17 cases.

−67 −73 179 449 −559 −565 −625 647 731 791
821 −835 887 −889 −901 −907 −919

$C(27) \times C(3) \times C(3)$: 6 cases.

131 −307 575 743 −787 −793

$C(81) \times C(3) \times C(3)$: 2 cases.

407 455

$C(3) \times C(3) \times C(3) \times C(3)$: 1 case.

−739

$C(9) \times C(3) \times C(3) \times C(3)$: 1 case.

−235

Appendix 2. CUROID. CUROID [14] is a program for computing the cube-roots of the identity (9): the $\frac{1}{2}(3^{r_3} - 1)$ solutions (10) having the smallest norms, an equal number having the second smallest norm a_2, etc. Briefly, this is how it works.

Let 3^n be the largest power of 3 that divides the class number $h(d)$. Then each form (25) has a power f_q under composition

$$f_q = F_q^{(h/3^n)3^s} = (A_q, B_q, C_q) \tag{30}$$

whose cube is the principal form I:

$$f_q^3 = I \qquad (s < n, s = \text{minimal}). \tag{31}$$

With SPEEDY and CLASNO, one computes a sufficient number of such quadratic form cube-roots (30) wherewith to generate *all* such cube-roots by composition. CUROID accepts these f_q, determines r_3 of them that are independent, and generates the $\frac{1}{2}(3^{r_3} - 1)$ inequivalent reduced forms

$$G_\iota = (A_\iota, B_\iota, C_\iota) = I^{1/3}, \tag{32}$$

which, with their inverses

$$G_\iota^{-1} = G_\iota^2 = (A_\iota, -B_\iota, C_\iota), \tag{33}$$

and I itself, comprise the 3^{r_3} cube-roots of I.

The smallest norm a in each equivalence class equals the A_i of the reduced form (32), and its three successors are given by

$$a_2 = C_i, \qquad a_3 = A_i - |B_i| + C_i, \qquad a_4 = A_i + |B_i| + C_i. \tag*{34)}$$

To compute the solutions (10) for the smallest norms a, CUROID first squares (32) by composition. *Prior* to reduction, this square is a specific form

$$H_i = (A_i', B_i', C_i'). \tag{35}$$

Here,

$$A_i' = (A_i/r_i)^2 \tag{36}$$

wherein the GCD

$$r_i = (A_i, B_i) \tag{37}$$

is the so-called *ramification factor* [15, p. 220] which includes all prime divisors of A_i that divide the discriminant. CUROID now reduces (35) to its equivalent reduced form (33) by the unimodular matrix

$$\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}. \tag{38}$$

This implies that

$$A_i' = A_i\delta^2 + B_i\gamma\delta + C_i\gamma^2$$

and therefore that $a^3 = b^2 + c^2D$ where

$$a = A_i, \qquad b = r_i\, |A_i\delta + \tfrac{1}{2}B_i\gamma|, \qquad c = r_i\, |\gamma| \tag{39}$$

if the discriminant $d = -4D$.

If the user indicated to CUROID that he wished the solutions (10) for the m smallest norms ($m = 1$ to 4), and if $m > 1$, the program now continues, sequentially, with the following forms that are either equivalent or conjugate to G_i:

$$(C_i, -B_i, A_i),$$

$$(A_i - |B_i| + C_i, |B_i| - 2C_i, C_i),$$

$$(A_i + |B_i| + C_i, |B_i| + 2C_i, C_i).$$

By squaring and reducing *these* forms, and with slight variations of the formulas (39), one thereby also obtains the solutions (10) for $a = a_2$, a_3, and a_4 if one sets $m = 4$.

Thus, our Table 2 above for $d = -4D_3(-739)$ could be followed by three others having these larger norms. Among these larger solutions, one finds another case of $c = 2n^3$ for $n = 1$, 4, and 7 and two more for $n = 5$.

Appendix 3. SPEEDY for Factorization. If one uses CLASNO [7] to compute the class group of $Q((-D)^{1/2})$ the discriminant $d = -D$ or $-4D$ must be accepted as is. But if one only wishes to *factor d* it is frequently advantageous [7, p. 438, p. 439] to take as the discriminant some multiple or submultiple of d:

$$d' = dn \quad \text{or} \quad d/n.$$

The version of SPEEDY accessible on teletype has other features to facilitate such a change.

If the parameter K of point A in Section 5 is *positive*, after everything in points A thru D there is computed, SPEEDY asks for a new discriminant and continues with this new problem with K and L unchanged. But if $K < 0$, $|K|$ blocks of primes are read in, and after everything in A thru D is computed, the teletype asks instead "Multiply or Divide?" If the operator now types N, the following occurs. If $|N| > 1$, the previous discriminant is multiplied or divided by $|N|$ according as N is positive or negative, and the teletype again asks "Multiply or Divide?" If $N = 1$, the computation proceeds with the new discriminant and the same values of K and L. If $N = -1$, the operator is first given the opportunity to change K and L and then the computation proceeds. If $N = 0$, the current discriminant is abandoned and a new d is requested.

Thus, with $K = -1$, one can, with very little machine time, eliminate all small divisors of d and then select the optimal multiple of its cofactor to give the smallest possible $L(1, \chi)$ and the largest possible known divisor b of $h(d)$. This speeds up the CLASNO algorithm. One now resets K to 30, say, to get a more accurate estimate (24).

For brevity, we will not discuss the operator's technique of finding this optimal multiple—it is primarily based upon observation of the current estimate of $L(1, \chi)$ and the current list of small residues and nonresidues q.

Computation and Mathematics Department
Naval Ship Research and Development Center
Bethesda, Maryland 20034

1. Daniel Shanks & Peter Weinberger, "A quadratic field of prime discriminant requiring three generators for its class group, and related theory," *Sierpiński Memorial Volume, Acta Arith.*, v. 21, 1972, pp. 71–87.

2. Daniel Shanks, "New types of quadratic fields having three invariants divisible by 3," *J. Number Theory,* v. 4, 1972, pp. 537–556.

3. Daniel Shanks & Richard Serafin, "Quadratic fields with four invariants divisible by 3," *Math. Comp.*, v. 27, 1973, pp. 183–187. Corrigendum, *ibid.*, p. 1012.

4. Peter Roquette, "On class field towers," *Algebraic Number Theory,* (Proc. Instructional Conf., Brighton, 1965), Thompson, Washington, D.C., 1967, pp. 231–249. MR **36** #1418.

5. H. Davenport & H. Heilbronn, "On the density of discriminants of cubic fields," *Bull. London Math. Soc.*, v. 1, 1969, pp. 345–348. MR **40** #7223.

6. H. Davenport & H. Heilbronn, "On the density of discriminants of cubic fields. II," *Proc. Roy. Soc. London Ser. A*, v. 322, 1971, pp. 405–420.

7. Daniel Shanks, "Class number, a theory of factorization, and genera," *Proc. Sympos. Pure Math.*, vol. 20, Amer. Math. Soc., Providence, R.I., 1971, pp. 415–440.

8. A. Scholz, "Über die Beziehung der Klassenzahlen quadratischer Körper zueinander," *Crelle's J.*, v. 166, 1932, pp. 201–203.

9. L. J. Mordell, *Diophantine Equations,* Pure and Appl. Math., vol. 30, Academic Press, New York and London, 1969, Chapter 26. MR **40** #2600.

10. G. Gras, "Extensions abéliennes non ramifiées de degré premier d'un corps quadratique," *Bull. Soc. Math. France*, v. 100, 1972, pp. 177–193.

11. Carol C. Neild, *SPEEDY, A Code for Estimating the Euler Product of a Dirichlet L Function*, CMD-8-73, 1973, Naval Ship R&D Center, Bethesda, Maryland.

12. Daniel Shanks, "Five number-theoretic algorithms," *Proceedings of the Manitoba Conference on Numerical Mathematics, 1972*, University of Manitoba, Winnipeg, Canada, 1973.

13. Richard H. Serafin, *Two Subroutines for the Solution of $R \equiv A^n$ (modulo N) and $R^2 \equiv A$ (modulo P) and their Applications*, CMD-7-73, 1973, Naval Ship R&D Center, Bethesda, Maryland.

14. Carol C. Neild, *CUROID, A Code for Computing the Cube Roots of the Identity of the Class Group of an Imaginary Quadratic Field,* CMD-9-73, 1973, Naval Ship R&D Center, Bethesda, Maryland.

15. Daniel Shanks, "The infrastructure of a real quadratic field and its applications," *Proceedings of the 1972 Number Theory Conference,* University of Colorado, Boulder, Colorado, 1973, pp. 217–224.