MATHEMATICS OF COMPUTATION, VOLUME 28, NUMBER 128
OCTOBER 1974, PAGES 1137–1152

The Simplest Cubic Fields

By Daniel Shanks

Abstract. The cyclic cubic fields generated by $x^3 = ax^2 + (a+3)x + 1$ are studied in detail. The regulators are relatively small and are known at once. The class numbers are always of the form $A^2 + 3B^2$, are relatively large and easy to compute. The class groups are usually easy to determine since one has the theorem that if m is divisible only by primes $\equiv 2 \pmod 3$, then the m-rank of the class group is even. Fields with different 3-ranks are treated separately.

1. The Simplest Cubic Fields. Godwin and Samet [1] tabulated the 830 totally real cubic fields of discriminant $D < 2 \cdot 10^4$. Godwin [2] computed their class numbers h and found that 764 of these fields (92%) have $h = 1$. Borewicz and Šafarevič [3] reproduced Godwin's table and pointedly remarked that none of these class numbers exceed 4.

It is clear that among cubic fields with larger D, those having relatively small regulators will have larger h. In principle, we could exhibit some of these by extending Godwin's tables to $D < 4 \cdot 10^4$, or say $D < 10^5$, but that would require a great deal of intricate computation. An alternative project, much simpler computationally, and of interest in its own right, is based upon the selection of a subset of these fields that are especially easy to compute. With such a restriction, one may readily determine their fundamental units and class numbers to much larger limits, say $D < 10^{10}$.

The simplest cubic fields are the cyclic fields, those having square discriminants:

$$D = N^2. \tag{1}$$

Like the quadratic fields, but unlike other cubic fields, *all* roots of the generating polynomial are in the field, *all* primes q either split completely in the field or do not split at all, and the residue class of $q \pmod N$ determines whether q splits or does not. But, unlike quadratic fields, if N is not 9 or a prime, there will be more than one cubic field with this D, and the splitting criterion for a specific one of these fields becomes a little more complicated. Further, there are two fundamental units in need of computation. But these two complications may be eliminated if we restrict N

Received December 17, 1973.

AMS (MOS) subject classifications (1970). Primary 12A30, 12A35, 12A50, 12A70, 12A95, 12–04.

to certain primes P, namely, to primes of the form

$$P = P(a) = a^2 + 3a + 9 \tag{2}$$

such as $P(-1) = 7, P(1) = 13, P(2) = 19, \cdots, P(410) = 169339$. Since (2) gives nothing new for $a < -1$ we will restrict a to values $\geqslant -1$.

The cubic equation

$$x^3 = ax^2 + (a + 3)x + 1 \tag{3}$$

has the discriminant

$$D = (a^2 + 3a + 9)^2, \tag{4}$$

and if $a^2 + 3a + 9$ is prime, (4) is obviously also the discriminant of the field $Q(\rho)$ where ρ is a root of (3). One may easily verify that the other two roots of (3) are

$$\rho_2 = -1/(1 + \rho) \quad \text{and} \quad \rho_3 = -1/(1 + \rho_2). \tag{5}$$

Since $\rho(\rho^2 - a\rho - a - 3) = 1$, ρ is a unit of $Q(\rho)$, and since $\rho_2(\rho_2^2 - a\rho_2 - a - 3) = 1$, $1 + \rho = -1/\rho_2$ is also a unit. They are, in fact, independent fundamental units, as may be verified by Godwin's criterion [4]. One therefore knows the regulator

$$R = \log^2 |\rho| - \log |\rho| \log |(1 + \rho)| + \log^2 |(1 + \rho)| \tag{6}$$

a priori. The formula (6) is invariant if ρ is replaced by ρ_2 or ρ_3. We may compute R explicitly with the trigonometric solution of (3). Let

$$\theta = \frac{1}{3} \arctan \frac{\sqrt{27}}{2a + 3}. \tag{7}$$

Then

$$\rho = \frac{1}{3}(2\sqrt{P} \cos \theta + a), \tag{8}$$

and ρ is the positive root of (3) if the principal value is chosen in (7).

From (2), $P \equiv 1 \pmod 3$, and for all $q \neq P$, the polynomial

$$x^3 - ax^2 - (a + 3)x - 1$$

splits completely (mod q) or is irreducible (mod q) according as

$$q^{(P-1)/3} \equiv 1 \pmod P, \tag{9}$$

or not—that is, according as q is a cubic residue of P, or not. If $\zeta_K(s)$ is the

Dedekind Zeta function of $K = Q(\rho)$, it follows that

$$\lim_{s=1+} \zeta_K(s)/\zeta(s) = \prod_{q=2}^{\infty} f(q) \tag{10}$$

where

$$\begin{aligned} f(q) &= 1 && \text{for } q = P, \\ f(q) &= \left(\frac{q}{q-1}\right)^2 && \text{for } q^{(P-1)/3} \equiv 1 \pmod{P}, \\ f(q) &= \frac{q^2}{q^2+q+1} && \text{otherwise.} \end{aligned} \tag{11}$$

On the other hand,

$$\lim_{s=1+} \zeta_K(s)/\zeta(s) = \frac{4Rh}{P}. \tag{12}$$

Since we know R, we may therefore compute the class number h by calculating the product on the right side of (10) with sufficient accuracy.

Now, this product converges rather slowly (the first 15000 factors give an accuracy of about 1 part in 2000, cf. [5]), but a great deal of accuracy is not needed here since h is an integer, and not a very big one if $D < 10^{11}$. Formulas (10) and (11) are easily programmed on a computer. With a computer, we evaluated the first 100 cases of these fields–from $P(-1) = 7, D = 49$ to $P(410) = 169339, D = 28675696921$. Table 1 lists these 100 primes P and class numbers h.

2. Moderate Class Numbers. In Table 1 one notes: (a), the mean growth of h as a function of a; and (b), the arithmetic restrictions upon h in that all of these h are of the form $3k + 1$, and prime factors of the form $3k - 1$ always occur with even exponents. The first property is analytic, having reference to $\zeta_K(s)$; it is discussed briefly in this section. The second property is algebraic, having reference to the class group; it will be examined in Section 4.

Although the h in Table 1 are much larger than the $h \leqslant 4$ computed by Godwin that were referred to above, they are *not* exceptionally large considering the size of their own discriminants $D = (a^2 + 3a + 9)^2$. By (7) and (8),

$$\rho = a + 1 + \frac{4}{2a+3} + O\left(\frac{1}{a^3}\right). \tag{13}$$

Then, by (6),

$$R = \log^2 a + \frac{3 \log a}{a} + O\left(\frac{\log a}{a^2}\right), \tag{14}$$

and by (10) and (12) we have

$$h = \frac{a^2 + 3a + 9}{4 \log^2 a} \left\{1 - \frac{3}{a \log a} + o\left(\frac{1}{a^2}\right)\right\} \prod_{q=2}^{\infty} f(q). \tag{15}$$

TABLE 1

a	P	h	a	P	h	a	P	h
−1	7	1	112	12889	37	259	67867	217
1	13	1	121	15013	127	260	68389	127
2	19	1	122	15259	61	262	69439	172
4	37	1	127	16519	52	266	71563	343
7	79	1	130	17299	52	277	77569	148
8	97	1	133	18097	52	281	79813	349
10	139	1	134	18367	49	284	81517	124
11	163	4	136	18913	100	290	84979	208
16	313	7	140	20029	37	296	88513	511
17	349	4	142	20599	112	301	91513	364
23	607	4	143	20887	64	302	92119	133
25	709	4	155	24499	67	304	93337	229
28	877	7	158	25447	61	305	93949	208
29	937	4	163	27067	76	310	97039	364
31	1063	13	164	27397	61	317	101449	403
32	1129	7	169	29077	76	322	104659	139
37	1489	19	172	30109	61	331	110563	553
38	1567	7	175	31159	61	332	111229	244
43	1987	7	176	31513	112	343	118687	325
49	2557	7	179	32587	76	346	120763	421
50	2659	19	182	33679	73	359	129967	292
56	3313	19	197	39409	67	361	131413	553
58	3547	19	200	40609	133	364	133597	259
64	4297	16	205	42649	91	367	135799	277
70	5119	31	206	43063	223	368	136537	247
73	5557	19	212	45589	169	371	138763	400
85	7489	28	214	46447	73	380	145549	547
88	8017	19	218	48187	112	388	151717	325
91	8563	49	220	49069	100	392	154849	217
94	9127	31	224	50857	169	395	157219	316
95	9319	28	238	57367	91	403	163627	193
98	9907	31	239	57847	121	406	166063	304
101	10513	64	254	65287	175	410	169339	277
107	11779	43						

Since R is very small here, these h would be exceptionally large were it not for the fact that $q = 2$ and $q = 3$ are cubic nonresidues for all $P(a)$, and therefore the first two factors in the product are

$$f(2)f(3) = \frac{4}{7} \cdot \frac{9}{13}. \tag{16}$$

Further, $q = 5$ is a cubic residue for only $1/5$ of these $P(a)$, not $1/3$, and the same deficiency holds for $q = 7$.

Jacobi determined if q is a cubic residue of a prime $p \equiv 1 \pmod 3$ by writing

$$4p = L^2 + 27M^2. \tag{17}$$

Then, for $q = 2$ or 3, q is a cubic residue iff $M \equiv 0 \pmod q$, while for $q = 5$ or 7 the criterion is $LM \equiv 0 \pmod q$. We have

$$4P(a) = (2a + 3)^2 + 27; \tag{18}$$

(note the geometric meaning of θ in Eq. (7)). Thus, 2 and 3 are never cubic residues of $P(a)$, 5 is a cubic residue only if $a \equiv 1 \pmod 5$ while 7 is a cubic residue only if $a \equiv 2 \pmod 7$. Since $a^2 + 3a + 9 \equiv 0 \pmod q$ has no solution for $q = 5$ and two solutions for $q = 7$, for either of these q only $1/5$ of the $P(a)$ have q as a cubic residue. In general, for

$$q = 3N + 2 \quad \text{or} \quad q = 3N + 4,$$

it can be shown that $N/(3N + 2)$ of the $P(a)$ have q as a cubic residue. This fraction approaches $1/3$ from below, the bias being due to the fact that the coefficient M of (17) is never $\equiv 0 \pmod q$ for any of our $P(a)$.

A rough mean value for our h is given by

$$h \approx 3P(a)/35 \log^2 a. \tag{19}$$

The larger class numbers here occur for $a \equiv 1 \pmod 5$, $a \equiv 2 \pmod 7$, and especially

$$a \equiv 16 \pmod{35}.$$

Note the examples: $P = 313$, 15013, 88513, and 110563 in Table 1. But even these h must be considered moderate for D of this size; if 2 and 3 were both cubic residues instead of nonresidues the class number would increase by a factor of $91/4$.

3. The Analogous Quadratic Fields. It is of interest to compare our cubic fields with the following, closely analogous real quadratic fields:

$$Q(\sqrt{P}) = Q(\rho), \tag{20}$$

where ρ is a solution of

$$x^2 = ax + 1, \tag{21}$$

and P is a prime

$$P = P(a) = a^2 + 4. \tag{22}$$

Again,

$$\rho = \tfrac{1}{2}(\sqrt{P} + a) = a + \frac{1}{a} + O\left(\frac{1}{a^3}\right) \tag{23}$$

is a fundamental unit, and so this time we have

$$h = \frac{\sqrt{a^2+4}}{2\log a}\left\{1 - \frac{1}{a^2 \log a} + o\left(\frac{1}{a^4}\right)\right\} \prod_{q=2}^{\infty} f(q) \tag{24}$$

where

$$\begin{aligned} f(q) &= 1 \qquad \text{for } q = P, \\ f(q) &= q/(q-1) \quad \text{for } q^{(P-1)/2} \equiv 1 \pmod{P}, \\ f(q) &= q/(q+1) \quad \text{otherwise.} \end{aligned} \tag{25}$$

Again, $q = 2$ is always a quadratic nonresidue and so

$$f(2) = \frac{2}{3}. \tag{26}$$

Again, there is a deficiency of quadratic residues: $q = 3$ and 5 are quadratic residues for $1/3$ of the $P(a)$, not $\tfrac{1}{2}$, and similarly,

$$q = 4N + 3 \quad \text{or} \quad q = 4N + 5$$

are quadratic residues for $(2N + 1)/(4N + 3)$ of the $P(a)$. We now have a rough mean value of h that is approximately the square root of what it was in (19), namely,

$$h \approx 3\sqrt{P(a)}/10 \log a.$$

This time h is prime to 2, not 3, but there are *no other restrictions* on h. That is the big difference. It reflects a difference of structure in the class groups as we shall see in the next section.

In Table 2 we give the 61 of these $Q(\sqrt{P(a)})$ and their class numbers up to the same limit in a. This count, 61, is precisely what is called for by the Hardy-Littlewood Conjecture. The number of primes of the forms

$$P(a) = a^2 + 3a + 3^2 \quad \text{and} \quad P(a) = a^2 + 2^2,$$

for $a \leqslant A$, are asymptotic, respectively, to

$$1.12073\pi(A) \quad \text{and} \quad 0.68641\,\pi(A),$$

and $0.68641/1.12073 = 0.6124$. See [6].

TABLE 2

The Quadratic Analogue

a	P	h	a	P	h
1	5	1	167	27893	5
3	13	1	177	31333	19
5	29	1	183	33493	9
7	53	1	193	37253	5
13	173	1	203	41213	7
15	229	3	207	42853	15
17	293	1	215	46229	13
27	733	3	217	47093	9
33	1093	5	233	54293	9
35	1229	3	235	55229	15
37	1373	3	243	59053	25
45	2029	7	245	60029	13
47	2213	3	253	64013	9
57	3253	5	255	65029	27
65	4229	7	265	70229	19
67	4493	3	267	71293	15
73	5333	3	275	75629	21
85	7229	5	277	76733	7
87	7573	9	287	82373	13
95	9029	7	293	85853	11
97	9413	3	303	91813	23
103	10613	5	307	94253	9
115	13229	5	313	97973	13
117	13693	15	317	100493	13
125	15629	9	347	120413	11
135	18229	19	357	127453	33
137	18773	5	373	139133	15
147	21613	13	375	140629	25
155	24029	9	385	148229	23
163	26573	9	403	162413	15
			407	165653	13

4. Class Groups. In Table 2, all 61 class groups are cyclic even though there are some h there that are not square-free. However, not all such $Q(\sqrt{P(a)})$ have cyclic groups, since if we continued the table we would find

$$a = 4913, \qquad P = 24137573$$

which has the class group [7] $C(3) \times C(39)$. In contrast, we shall see that *none* of the many h in Table 1 divisible by 4, 25, or 121 correspond to cyclic groups.

In Table 1, $h = 2, 5, 8, 10$, and 22 never occur (besides all h divisible by 3). Cubic fields can have such h, however, since they are found [8] in $Q(N^{1/3})$ for $N = 11$, 263, 389, 303, and 281, respectively. But these are not cyclic fields.

The key question is this. Where do conjugate ideals lie in the class group of a cyclic field? In a quadratic field, if e is an element of the group of order m, then the conjugates of its ideals lie in e^{m-1} since the product of the two elements must be the identity $e^m = I$. Thus, in a quadratic field the conjugate is in the inverse in the group. In a cubic field, both conjugates of e must either be in the subgroup S of order m generated by e, or both conjugates must lie outside of S, since the product of the 3 elements must be I.

Consider the first option. If one conjugate of e lies in e^x, the second conjugate must lie in e^{x^2} and we have

$$1 + x + x^2 \equiv 0 \pmod{m} \tag{27}$$

since $e \cdot e^x \cdot e^{x^2} = e^0 = I$. Thus,

$$(2x + 1)^2 \equiv -3 \pmod{p} \tag{28}$$

for each prime divisor p of m. So, $p = 3$ or

$$p \equiv 1 \pmod{3}. \tag{29}$$

Therefore, all cases of $h = 4, 16, 28, 100, 121$, etc., must have noncyclic groups. One can make a stronger statement: Since conjugate elements have the same order, we have the following

THEOREM. *If m is divisible only by primes $\equiv 2 \pmod 3$, the m-rank of the class group of a cyclic cubic field must be even.*

Proof. Assume $p \equiv 2 \pmod 3$ and write the p-Sylow subgroup as the direct product:

$$\prod_{n=1}^{\infty} [C(p^n)]^{s_n}.$$

Here, $s_n = 0$ for all $n >$ some n_0. The p-rank r_p of the class group is therefore

$$r_p = \sum_{m=1}^{\infty} s_m$$

and the p^n-rank is

$$r_{p^n} = \sum_{m=n}^{\infty} s_m, \quad \text{which we abbreviate as } r(n).$$

Let

$$P_n = \prod_{m=1}^{n} p^{ms_m}.$$

The number of elements M_n of the subgroup of order $\leqslant p^n$ is

$$M_n = P_{n-1}p^{nr(n)} = P_n p^{nr(n+1)},$$

and therefore the number of order precisely p^n is

$$M_n - M_{n-1} = P_{n-1}p^{(n-1)r(n)}[p^{r(n)} - 1].$$

Since conjugates have the same order, this number is divisible by 3 and we must have

$$r_{p^n} \equiv 0 \pmod 2 \quad \text{and so} \quad s_n \equiv 0 \pmod 2$$

for all n. Let $m = \Pi_i p_i^{\alpha_i}$. Since the m-rank is given by $r_m = \min \{r_{p_i^{\alpha_i}}\}$ it is also even.

Therefore, we know the class groups of many of the cyclic fields in Table 1 immediately.

Examples in Table 1.

$D = 163^2$ has the group $C(2) \times C(2)$.

$D = 7489^2$ has the group $C(2) \times C(14)$.

$D = 18913^2$ has the group $C(10) \times C(10)$.

$D = 57847^2$ has the group $C(11) \times C(11)$.

But $D = 10513^2$ cannot be settled without further computation since $[C(8)]^2$, $[C(4) \times C(2)]^2$, or $[C(2)]^6$ are all allowed by the theorem.

On the other hand, the cyclic group of order 7 for $D = 313^2$ has conjugate elements in $\{e, e^2, e^4\}$ and in $\{e^3, e^6, e^5\}$ and in e^0, while for $D = 1063^2$ they lie in $\{e, e^3, e^9\}$, etc.

The self-conjugate elements e, those with $x = 1$ in Eq. (27), and the associated 3-Sylow subgroup has recently been studied very completely in the theses of Gerth [9] and Gras [10]. See also [11], [12].

It follows that the class numbers h of cyclic fields are always of the form

$$h = A^2 + 3B^2. \quad (30)$$ *

This is very restrictive since the number of such $h \leqslant H$ is [13] asymptotic to

$$0.63891\, H/\sqrt{\log H}, \quad (31)$$

*This was already known to Hasse [17] and others by considering the cubic field as a subfield of a cyclotomic field.

and therefore these numbers have zero density. That is not surprising since the N of (1) also have zero density. In our special case $N = P(a)$ we have the further restriction that $3 \nmid h$ and so $3 \nmid A$ in (30) and (31) becomes

$$0.42594\, H/\sqrt{\log H}. \tag{31a}$$

Clearly, the theorem can be generalized to cyclic fields of higher degree, but we do not do so here.

The cyclotomic field of the pth root of unity is cyclic of degree $p - 1$. In the table by Newman [14] of h^*, the first factor of the class number, one sees that *most* of the large prime factors of h^* are of the form $k(p-1) + 1$. In fact, D. H. Lehmer utilized this in greatly accelerating these factorizations. For example, a 24-digit factor of $h^*(199)$ was assumed to factor into $(198k_1 + 1)(198k_2 + 1)$, and thereby Lehmer found the prime divisors having

$$k_1 = 1046937112, \quad k_2 = 16000961681.$$

See [14].

5. Hasse's Question. In personal correspondence, Professor Hasse asked me for an example of a completely split prime p in an algebraic field whose divisors do not lie in a cyclic subgroup of the class group. Shortly thereafter I brought the question to the attention of Robert Gold and Richard Lakein. They put together the composite biquadratic field $Q(\sqrt{-23}, \sqrt{-31})$ wherein the four divisors of 2 are in $C(3) \times C(3)$.

The simplest answer to Hasse's question should have $h = 4$ in a field of degree 3—these are the smallest possible values. It is our $D = 163^2$. One can rewrite (3) as

$$(x - 1)(x + 2)(x - a - 1) = 2a + 3. \tag{32}$$

By (5), we have

$$\rho_2 - 1 = -(\rho + 2)/(\rho + 1), \quad \rho_3 - 1 = -(\rho - a - 1)(\rho + 1), \tag{33}$$

and so $2a + 3$ is the norm of $(\rho - 1)$. For $a = 11, P(a) = 163, 2a + 3 = 5^2$ one therefore finds the three conjugate, nonprincipal, and inequivalent ideals of norm 5 to be

$$(5, \rho - 1), \quad (5, \rho + 2), \quad (5, \rho - 12).$$

By further examination of the divisors of $f(x) = x^3 - 11x^2 - 14x - 1$, one finds the ramifying and principal prime $(1 + \rho + \rho^2)$ of norm 163, and that all splitting $p < 163$, namely, 5, 13, 17, 23, 31, 37, 53, 59, 61, 127, and 157 are nonprincipal and disposed in the class group as Hasse required, (and in the most elegant way possible). The first principal primes > 163 are

$$(\rho - 10), \quad (10\rho + 11), \quad (11\rho + 1)$$

of norm 241.

6. The Next Notch. Returning to (3) it seems desirable to examine briefly some of these fields where $N = a^2 + 3a + 9$ is not prime. If N is square-free or 9 times a square-free number, everything in Section 1 remains valid except for the splitting criterion (9) and (11). The next simplest possibility is this:

$$\begin{aligned} &a = 9b, && N = 9(9b^2 + 3b + 1) \text{ or} \\ &a = 9b - 3, && N = 9(9b^2 - 3b + 1) \end{aligned} \tag{34}$$

with $9b^2 \pm 3b + 1 = p(b) = p$ prime and $b \not\equiv 0 \pmod 3$. Such p have 3 as a cubic nonresidue and are $\not\equiv 1 \pmod 9$.

Then if

$$c = (2a + 3)/3, \quad e = (p - 1)/3, \tag{35}$$

and

$$d \equiv c^e \pmod{9p}, \tag{36}$$

it may be shown that (11) should be replaced by

$$\begin{aligned} &f(q) = 1 && \text{for } q = 3 \text{ and } p \\ &f(q) = \left(\frac{q}{q-1}\right)^2 && \text{for } q^e \equiv 1 \text{ or } d \text{ or } d^2 \pmod{9p}, \\ &f(a) = \frac{q^2}{q^2 + q + 1} && \text{otherwise.} \end{aligned} \tag{37}$$

This is equally easy to compute. One verifies that h is divisible by 3 but not by 9, cf. [9], [10]. In Table 3 we list a, $H = h/3$ and $p = N/9$ up to the same limit.

7. Maximal 3-Ranks. As is well known, if the $a^2 + 4$ of (22) is a square-free product of k distinct primes, the 2-rank of that $Q(\sqrt{a^2 + 4})$ is $k - 1$ and there are 2^{k-1} genera. Similarly, in the last section the $N = a^2 + 3a + 9$ of (3) is divisible by two distinct primes and the 3-rank equals 1. That is also true for other N we have skipped over, such as

$$\begin{aligned} &a = 13, N = 7 \cdot 31; \quad a = 14, N = 13 \cdot 19; \quad a = 19, N = 7 \cdot 61; \\ &a = 20, N = 7 \cdot 67; \quad a = 22, N = 13 \cdot 43; \quad a = 26, N = 7 \cdot 109. \end{aligned} \tag{38}$$

The first five cases in (38) have $h = 3$ and the sixth has $h = 12$.

TABLE 3

$N = a^2 + 3a + 9 = 9p, \quad h = 3H$

a	P	H	a	p	H
6	7	1	171	3307	100
9	13	1	177	3541	52
15	31	1	198	4423	91
18	43	1	207	4831	67
36	157	4	225	5701	52
42	211	4	231	6007	112
45	241	4	234	6163	49
60	421	7	303	10303	208
63	463	7	315	11131	76
72	601	16	330	12211	103
99	1123	13	333	12433	103
114	1483	37	357	14281	91
123	1723	19	393	17293	112
150	2551	28	414	19183	133

But now consider the $a = 9b - 3 = 24$ of (34) for $b = 3$ that we have also skipped over. Here, $N = 9 \cdot 73$, and unlike the previous section, we now have $73 \equiv 1 \pmod 9$ while 3 is a cubic residue of 73. One finds $h = 9$. But, by the same argumentation as in Section 4, the class group of a cyclic cubic field cannot be $C(9)$ and we must have $C(3) \times C(3)$ with a 3-rank equal to 2.

By Leopoldt's theory of genera in abelian fields [15], as developed in detail by Gerth and Gras, a cyclic cubic field with k ramifying primes has a 3-rank r_3 that satisfies

$$k - 1 \leqslant r_3 \leqslant 2(k - 1). \tag{39}$$

For $k = 2, r_3$ is 1 or 2 and $r_3 = 2$ iff both primes are cubic residues of each other. In Table 4, we list all such $N = 9p$ or p_1p_2 up to the same limit in a where we have the maximal $r_3 = 2$. Under $Q(\rho)$ we list the class groups except for $a = 329$ and four larger a where we merely list the class number thus: (h). In these five cases the 2-Sylow subgroup or the 3-Sylow subgroup is uncertain without further computation although we do know that $r_3 = 2$ and $r_2 =$ even.

We conclude this section with (a): specific data on the $C(3) \times C(3)$ for $N = 9 \cdot 73$ to illustrate a surprising phenomenon; (b): brief mention of the revised splitting rules needed to compute Table 4; and (c): brief mention of the case $a = 3418, N = 151 \cdot 211 \cdot 367$ which has $k = 3$ and the maximal $r_3 = 4$.

(a) In the abstract group $C(3) \times C(3)$ only the identity has a special role; the other eight elements behave identically and any two may be interchanged by an automorphism. The four subgroups of order 3 are likewise indistinguishable, abstractly

TABLE 4

$k = r_3 = 2$

a	N	$Q(\rho)$	a	N	$Q(\rho)$
24	9·73	3×3	213	9·5113	6×42
34	7·181	3×3	232	31·1759	3×39
35	13·103	3×3	233	43·1279	15×15
47	7·337	3×3	240	9·6481	3×63
51	9·307	3×21	247	151·409	3×57
52	19·151	3×3	248	13·4789	6×18
53	13·229	3×3	253	211·307	3×39
71	19·277	6×6	256	13·5101	15×15
79	13·499	3×21	267	9·8011	3×63
81	9·757	3×21	270	9·8191	15×15
83	7·1021	6×6	275	157·487	6×42
86	79·97	3×21	293	7·12391	15×15
106	31·373	3×21	297	9·9901	3×63
110	7·1777	3×9	328	7·15511	3×63
113	13·1009	6×6	329	313·349	(144)
137	31·619	6×6	338	73·1579	(243)
145	7·3067	3×21	341	7·16759	(324)
146	7·3109	6×18	350	157·787	6×42
148	79·283	3×21	351	9·13807	(567)
162	9·2971	3×21	353	109·1153	3×63
181	7·4759	6×42	358	307·421	6×42
185	19·1831	3×21	373	13·10789	3×117
186	9·3907	3×63	382	19·7741	(324)
208	7·6271	3×39	413	19·9043	3×93

speaking. If an abstract group is exemplified by a specific mathematical object, one expects the elements of that object to behave correspondingly.

Not so with the $C(3) \times C(3)$ for $D = (9 \cdot 73)^2$. Here is how the splitting primes lie in this group. (A) The ramified 3 and 73 are nonprincipal, equivalent, and of order 3 so the principal $(1 + \rho + \rho^2)$ has the norm $3^2 \cdot 73$. (B) One-ninth of the splitting primes are principal, such as $(\rho + 3)$ of norm 163. (C) One-ninth, such as 577, are equivalent to 3, 73, and its two conjugates. (D) One-ninth, such as 17, are equivalent to its conjugates but inverse to 3 so we find $(\rho - 1)$, $(\rho + 2)$, and $(\rho - 25)$ of norm $51 = 3 \cdot 17 = 2a + 3$. The primes in (B), (C) and (D) are all cubic residues of both 9 and 73, and together with (A) make up one unique subgroup of order 3.

(E) The one-third of the splitting primes q that satisfy $q^2 \equiv 4 \pmod 9$, $q^{24} \equiv 8 \pmod{73}$ are nonprincipal and the three inequivalent conjugates are found, one each, in the other three subgroups. An example is $q = 11$ and we find $(\rho + 7)$ of norm 1331. (F) Finally, those q with $q^2 \equiv 7 \pmod 9$ and $q^{24} \equiv 64 \pmod{73}$, such

as 13, are nonprincipal, inequivalent, and inverse to those in (E). One notes $(\rho - 2)$ of norm 143.

Thus, one of the four subgroups is exceptional; it is populated very differently than the other three. Perhaps the author lacks imagination. He could hardly believe that such a thing would be possible.

(b) Let $N = p_1p_2$, $e_1 = (p_1 - 1)/3$, $e_2 = (p_2 - 1)/3$, and let Q be any prime that is a cubic nonresidue of both p_1 and p_2. If Q splits and

$$Q^{e_1} \equiv A \pmod{p_1}, \qquad Q^{e_2} \equiv B \pmod{p_2}, \tag{40}$$

then all splitting q are characterized as follows: If

$$q^{e_1} \equiv A^i \pmod{p_1} \quad \text{then} \quad q^{e_2} \equiv B^i \pmod{p_2} \tag{41}$$

for $i = 0$, 1, or 2. If p_1 is 9 instead, then $e_1 = 2$ as in the $N = 9 \cdot 73$ discussed above. Whereas, if Q does not split and satisfies (40) the splitting q with $q^{e_1} \equiv A^i \pmod{p_1}$ have $q^{e_2} \equiv B^{3-i} \pmod{p_2}$ for $i = 0$, 1, or 2. Thus, the needed replacement for Eqs. (11) are not difficult to compute.

(c) For $a = 3418$, $N = 151 \cdot 211 \cdot 367$, each of the three ramifying primes is a cubic residue of the other two. By the theory [9], [10], (39) becomes $r_3 = 2(3 - 1) = 4$ and $C(3) \times C(3) \times C(3) \times C(3)$ is a subgroup of the class group. There are, of course, four different fields with $D = (151 \cdot 211 \cdot 367)^2$. The one of these for $a = 3418$ has $h = 16848 = 2^4 \cdot 3^4 \cdot 13$.

I would like to thank Carol Neild for assistance in computing the tables.

8. A Recent Paper and Others to Appear. As I completed the foregoing, I noticed in the current *Contents Contemporary Math. Jour.* the listing of a paper [16] by M. N. Gras, N. Moser, and J. J. Payan that was about to appear. The "de certains corps cubiques cycliques" in its title sounded extremely appropriate. These fields are, in fact, our fields above, and tables are given up to what we designate as $a = 47$, $N = 7 \cdot 337$. But the approach and method is entirely different in this paper and I believe that justifies the publication of our own version. They do not give our Eq. (3). Rather, for $D \equiv 0 \pmod 9$, they use what would be

$$x^3 + x^2 = \frac{1}{3}(N - 1)x + [N(3 + \sqrt{4N - 27}) - 1]/27 \tag{42}$$

in our notation, with the sign of the radical chosen so that $\sqrt{4N - 27} \equiv 1 \pmod 3$. For $D \equiv 0 \pmod 9$ a still different equation is used. Whereas our approach is based entirely upon the relatively small and already known regulator (6), their point of departure is the fact that $4N = L^2 + 27$ implies that $\{1, \rho, \rho^2\}$ is an integral basis.

Marie-Nicole Gras then kindly sent me copies of her [18], [19]. The first is her thesis. It includes the theorem in our Section 4 and a detailed treatment of the $C(2) \times C(2)$ for $D = 163^2$ in our Section 5. Her [19], which will appear, has an interesting method of computing the class numbers and units of cyclic cubic fields and extensive tables including all N in $(1) < 4000$ and all $N = a^2 + 3a + 9 < 20000$. Both papers treat the cubic field as a subfield of the cyclotomic field of the Nth roots of unity.

While there is therefore a considerable overlap of her papers and mine, there are also differences in method and content. We do not use the cyclotomic fields and our calculations for h are probably simpler and faster.

Computation and Mathematics Department
Naval Ship Research and Development Center
Bethesda, Maryland 20084

1. H. J. GODWIN & P. A. SAMET, "A table of real cubic fields," *J. London Math. Soc.*, v. 34, 1959, pp. 108–110. MR 20 #7009.

2. H. J. GODWIN, "The determination of the class-numbers of totally real cubic fields," *Proc. Cambridge Philos. Soc.*, v. 57, 1961, pp. 728–730. MR 23 #A3733.

3. Z. I. BOREVIČ & I. R. ŠAFAREVIČ, *Number Theory*, "Nauka", Moscow, 1964; German transl., *Zahlentheorie*, Birkhäuser, Basel, 1966, p. 462; English transl., Pure and Appl. Math., vol. 20, Academic Press, New York, 1966. MR 30 #1080; 33 #4000; #4001.

4. H. J. GODWIN, "The determination of units in totally real cubic fields," *Proc. Cambridge Philos. Soc.*, v. 56, 1960, pp. 318–321. MR 22 #7998.

5. CAROL NEILD & DANIEL SHANKS, "On the 3-rank of quadratic fields and the Euler product," *Math. Comp.*, v. 28, 1974, pp. 279–291.

6. DANIEL SHANKS, "On the conjecture of Hardy and Littlewood concerning the number of primes of the form $n^2 + a$," *Math. Comp.*, v. 14, 1960, pp. 320–332. MR 22 #10960.

7. DANIEL SHANKS & PETER WEINBERGER, "A quadratic field of prime discriminant requiring three generators for its class group, and related theory," *Acta Arith.*, v. 21, 1972, pp. 71–87. MR 46 #9003.

8. B. D. BEACH, H. C. WILLIAMS & C. R. ZARNKE, *Some Computer Results on Units in Quadratic and Cubic Fields*, Sci. Report No. 31, University of Manitoba, Winnipeg, Canada, 1971.

9. FRANK GERTH III, *Sylow 3-Subgroups of Ideal Class Groups of Certain Cubic Fields*, Thesis, Princeton University, Princeton, N. J., 1972.

10. GEORGE GRAS, *Sur les l-Classes d'Idéaux dans les Extensions Cycliques Relative de Degré Premier l*, Thesis, Grenoble, 1972.

11. P. BARRUCAND & H. COHN, "A rational genus, class number divisibility, and unit theory for pure cubic fields," *J. Number Theory*, v. 2, 1970, pp. 7–21. MR 40 #2643.

12. P. BARRUCAND & H. COHN, "Remarks on principal factors in a relative cubic field," *J. Number Theory*, v. 3, 1971, pp. 226–239. MR 43 #1945.

13. DANIEL SHANKS & LARRY P. SCHMID, "Variations on a theorem of Landau," *Math. Comp.*, v. 20, 1966, pp. 551–569. MR 35 #1564.

14. MORRIS NEWMAN, "A table of the first factor for prime cyclotomic fields," *Math. Comp.*, v. 24, 1970, pp. 215–219. MR 41 #1684.

15. H. W. LEOPOLDT, "Zur Geschlechtertheorie in abelschen Zahlkörpern," *Math. Nachr.*, v. 9, 1953, pp. 351–362. MR 15, 14.

16. M. N. GRAS, N. MOSER & J. J. PAYAN, "Approximation algorithmique de certains corps cubiques cycliques," *Acta Arith.*, v. 23, 1973, pp. 295–300.

17. H. HASSE, "Arithmetische Bestimmung von Grundeinheit und Klassenzahl in zyklischen kubischen und biquadratischen Zahlkörpern," *Abh. Deutsch. Akad. Wiss. Berlin. Math.-Nat. Kl.*, v. 1948, no. 2, 95 pp. MR 11, 503.

18. MARIE-NICOLE MONTOUCHET, *Sur le Nombre de Classes du Sous-Corps Cubique de* $Q^{(p)}(p \equiv 1(3))$, Thesis, Grenoble, 1971.

19. MARIE NICOLE GRAS, "Méthodes et algorithmes pour le calcul numérique du nombre de classes et des unités des extensions cubiques cycliques de Q," *Crelle's J.* (To appear.)