MATHEMATICS OF COMPUTATION,.VOLUME 32, NUMBER 142
APRIL 1978, PAGES 637–650

On Some Families of Imaginary Quadratic Fields

By F. Diaz y Diaz

Abstract. This paper gives a method of obtaining imaginary quadratic fields whose class groups have at least three invariants divisible by 3. Complementary calculations have yielded a large number of imaginary quadratic fields having class groups with four invariants divisible by 3. Some numerical examples, previously unknown, are included.

Introduction. In this paper we are presenting a method of calculating a large number of imaginary quadratic fields having a 3-rank of the class group which is equal to 3 or more. Very simple complementary calculations furnish some quadratic fields whose 3-rank of the class group is 4.

The first section summarizes the results of [3]. We subsequently learned that the essential content of Lemma B had already been established by Kuroda [4].

The second section deals with the properties upon which this method is based (Lemmas 3, 4 and 5), corresponding to a particular case of the method developed in [3]. Independently of our research, the properties established in these three lemmas were discovered and studied recently by Buell [1]. Although Buell imposes more restrictive hypotheses than those adopted here, the essential part of our second section is covered by Buell's paper. This permits us to state some results without proof, except for Lemma 5 for which we give our original proof based on the method of composition of ideals into a quadratic field. This proof is substantially different from the one given by Buell's geometric approach. His proof is based upon the fact that the composition of ideal classes (or forms) coincides with the group law of a certain elliptic curve associated with the quadratic field.

The third section describes our calculation procedure. Sufficient conditions for the 3-rank of an imaginary quadratic field to be at least 3 are stated in three different formulations (Theorems 2, 2′ and 2″). The conditions imposed in these theorems may be easily verified with a computer.

The fourth section gives numerical examples of interest previously unknown.

A final observation: In this paper we never deal with real quadratic fields. However, the manipulations made with Eq. (1) are also valid when the discriminant of the quadratic field is positive. Among the results obtained in the first and second sections, only the corollary to Lemma B is not valid in the real case. Lemmas A and B, as well as Lemmas 4 and 5, are true without any modification when the discriminant of the field is positive. In order that Lemmas 1, 2 and 3 be valid in the real case, it suffices, when stating these lemmas, to eliminate the hypothesis concerning the inequality between m and y.

Received February 25, 1977; revised September 6, 1977.

AMS (MOS) subject classifications (1970). Primary 12A25, 12A50, 12–04.

We especially thank Professor Poitou for his valuable advice and help, providing us with all the material means necessary for this paper. Dr. Shanks was kind enough to read this paper. I thank him for his remarks and his help concerning its publication.

1. Notations and Previous Procedure.

1.1. Let D be a positive squarefree integer and k the imaginary quadratic field $Q(\sqrt{-D})$. The discriminant of k is $-d$, where:

$$d = \begin{cases} D & \text{if } D \equiv 3 \pmod 4, \\ 4D & \text{otherwise.} \end{cases}$$

The 3-rank of the class group of k is designated as r and H denotes the subgroup of the class group generated by the classes whose cube is the principal class.

If $\mathfrak{M}$ is an ideal of k generated by the positive integer m and the algebraic integer $\tfrac{1}{2}(a + b\sqrt{-d})$ we write:

$$\mathfrak{M} = \langle m;\, a,\, b\rangle.$$

In the numerical examples, $b = 1$ will always be chosen; in this case, we simplify the notation and write:

$$\langle m;\, a\rangle \quad \text{for } \langle m;\, a,\, 1\rangle.$$

Let us assume that m, y and z are nonzero integers which, for a certain fundamental discriminant $-d$, satisfy:

$$4m^3 = y^2 + z^2 d.$$

The triple $s = (m; y, z)$ will be named *a solution* of the Diophantine equation:

$$(1) \qquad 4X^3 = Y^2 + Z^2 d.$$

We always chose the value of z in s to be positive. (The value of m must necessarily be positive if we deal with imaginary quadratic fields.)

1.2. The following lemmas give a relation between the ideals of k and the solutions of (1) [3], [4].

LEMMA A. *Let $\mathfrak{M}$ be an ideal of k of norm m whose cube is principal. Then, Eq.* (1) (*with $-d$ as the discriminant of k*) *has a solution.*

LEMMA B. *Let $s = (m; y, z)$ be a solution of Eq.* (1) *and let c be the greatest common divisor of m and z. If the following conditions are satisfied*:

(i) *c divides d,*

(ii) *c is squarefree,*

then

(a) *the ideal (m) decomposes in k in the form*:

$$(m) = \mathfrak{M} \cdot \overline{\mathfrak{M}}, \quad \textit{where } \mathfrak{M} = \langle m;\, y/c,\, z/c\rangle,$$

(b) *$\mathfrak{M}$ has no integral rational factors,*

(c) *$\mathfrak{M}^3$ is principal.*

When the conditions (i) and (ii) of Lemma B are satisfied we say that the ideal $\mathfrak{M} = \langle m; y/c, z/c\rangle$ is the *ideal corresponding to the solution* $s = (m; y, z)$ of Eq. (1).

COROLLARY. *If $s = (m; y, z)$ is a solution of* (1) *satisfying conditions* (i) *and* (ii) *of Lemma* B, *and if* $1 < m < \sqrt{d/4}$, *then the ideal* $\mathfrak{M}$ *of* k *corresponding to the solution* s *is of order* 3.

1.3. Following the same procedure as in [3], for the search for imaginary quadratic fields k having a 3-rank of the class group greater than 1, we look for solutions of (1).

From a numerical point of view, the search for two solutions $s = (m; y, z)$ and $s' = (m'; y', z')$ of Eq. (1) is easier if we insist that $z = z'$. (This is often the case in practice.) We then have

$$\begin{cases} 4m^3 = y^2 + z^2 d, \\ 4m'^3 = y'^2 + z^2 d, \end{cases}$$

and if we set

$$\begin{cases} m' - m = t, \\ y' - y = 2v, \end{cases}$$

we obtain

$$\begin{cases} 4m^3 = y^2 + z^2 d, \\ t(3m^2 + 3mt + t^2) = v(v + y). \end{cases} \tag{2}$$

Henceforth, we will assume that the integer value of m is fixed. Thus, concerning the first equation of (2) we may state the following:

LEMMA 1. *For each value of* y *which satisfies the inequality* $4m^3 > y^2$, *we can factor the integer* $y^2 - 4m^3$ *uniquely as a product of a square and a fundamental discriminant.*

It is sufficient to factor $4m^3 - y^2$ in primes.

The symbol $N(t)$ (or simply N if no ambiguity exists) will represent the value of the expression

$$N(t) = 3m^2 + 3mt + t^2$$

where the variable t takes only integer values.

Let us assume now that the value of t can be written as a product of two integers $t = t't''$ and that the same holds true for $N(t) = N'N''$. In this case the second equation of (2) becomes $t't''N'N'' = v(v + y)$; and if we insist that $v = t''N''$, it follows that $y = t'N' - t''N''$.

We may, therefore, state the following:

LEMMA 2. *Let us assume that integers* t *and* N *can both be factored in the form* $t = t't''$ *and* $N = N'N''$. *If the expression* $y = t'N' - t''N''$ *satisfies the inequality* $4m^3 > y^2$, *then Eq.* (1) *has the two following solutions*

$$s_1 = (m; y, z), \qquad s_2 = (m + t; y + 2t''N'', z).$$

The value of d *in Eq.* (1) *and the integer* z *which appears in* s_1 *and* s_2 *are the integers described in Lemma* 1.

2. The Case $t' = 1$. A particular case of interest is the one where we take for t' and t'' the values $t' = 1$ and $t'' = t$ (see also [1]). We then obtain the following lemma which is more precise than Lemma 2:

LEMMA 3. *Let us assume that the integer $N(t)$ can be decomposed as a product of two factors in the form $N = N'\, N''$. If the expression $y = N' - tN''$ satisfies the inequality $4m^3 > y^2$, then Eq.* (1) *has the three following solutions*:

$$s_1 = (m; y, z), \quad s_2 = (m + t; y + 2tN'', z), \quad s_3 = (m + \tilde{t}; y + 2\tilde{t}N'', z).$$

The values of d and z are the integers described in Lemma 1 *and the value of $\tilde{t}$ in s_3 is given by*

$$m + (m + t) + (m + \tilde{t}) = N''^2. \tag{3}$$

The proof of this lemma can be found in [1] for the case $z = 1$. The proof for the general case may be easily deduced. The solution s_3 can also be interpreted [1] as the third point of intersection of the straight line passing through the points (m, y) and $(m + t, y + 2tN'')$ in the x-y plane with the elliptic curve $Y^2 = 4X^3 - z^2d$.

LEMMA 4. *In order that the three solutions of Eq.* (1) *described in Lemma* 3 *satisfy the conditions of Lemma* B, *it is necessary for N'' to be the norm of an integer of $Q(\sqrt{-3})$.*

LEMMA 5. *Let us assume that the three solutions given by Lemma* 3 *satisfy the conditions of Lemma* B. *If $\mathfrak{M}_1$ (resp. $\mathfrak{M}_2, \mathfrak{M}_3$) is the ideal corresponding to the solution s_1 (resp. s_2, s_3), then the product $\mathfrak{M}_1\mathfrak{M}_2\mathfrak{M}_3$ is a principal ideal.*

Proof. Let us say that

$$y_1 = y = N' - tN'', \quad y_2 = y + 2tN'', \quad y_3 = y + 2\tilde{t}N'',$$

$$m_1 = m, \quad m_2 = m + t, \quad m_3 = m + \tilde{t},$$

nd note that the identities

$$\begin{aligned} 4m_1m_2m_3 &= 4m_1^3 + 4m_1^2(t + \tilde{t}) + 4m_1t\tilde{t} \\ &= 4m_1^3 + 4m_1^2(N''^2 - 3m_1) + 4m_1t(N''^2 - 3m_1 - t) \\ &= (4m_1^3 - y_1^2) + y_1^2 + 4m_1^2N''^2 + 4m_1(tN''^2 - 3m_1^2 - 3m_1t - t^2) \\ &= z^2d + y_1^2 + 4m_1^2N''^2 - 4m_1N''(N' - tN'') \end{aligned}$$

ive the formula

$$4m_1m_2m_3 = (y_1 - 2m_1N'')^2 + z^2d. \tag{4)}$$

The ideal corresponding to the solution s_i is the ideal $\mathfrak{M}_i = \langle m_i; y_i/c_i, z/c_i\rangle$, 'here c_i is the greatest common divisor of m_i and z, for $i = 1, 2, 3$.

Let us assume that the prime number p divides the product $\mathfrak{M}_1\mathfrak{M}_2\mathfrak{M}_3$ and that p oes not divide d. Because none of the ideals $\mathfrak{M}_i$ have integral rational factors, the leal (p) is not inert in the extension k/Q. Consequently, we have in k a factorization

$$(p) = \mathfrak{p}\bar{\mathfrak{p}}$$

and $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ never divide the same ideal at the same time. We can now assume that $\mathfrak{p}$ divides $\mathfrak{M}_1$ and $\bar{\mathfrak{p}}$ divides $\mathfrak{M}_2$ (the other possible cases can be verified in an analogous manner). The norms m_1 and m_2 of these ideals must be divisible by p. Thus, p divides t and we obtain the congruence $y_1 \equiv y_2 \pmod{2p}$. This implies that the ideal $\mathfrak{p}$ which divides the integer $\frac{1}{2}(y_1 + z\sqrt{-d})$ also divides the integer $\frac{1}{2}(y_2 + z\sqrt{-d})$ in contradiction with the fact that $\mathfrak{M}_2$ has no integral rational factors. Thus, if $\mathfrak{p}$ divides the product $\mathfrak{M}_1\mathfrak{M}_2\mathfrak{M}_3$, the same does not hold true for $\bar{\mathfrak{p}}$.

Let us now consider the case where q is a prime which divides d, and let us assume that the ideal $\mathfrak{q}$, which divides (q), divides at least one ideal in the product $\mathfrak{M}_1\mathfrak{M}_2\mathfrak{M}_3$. It is clear that q divides the norm of this ideal; consequently, q also divides the integer z. We now deduce, by using formula (4), that q^2 divides the product $m_1m_2m_3$. Now, according to condition (ii) of Lemma B, the ideal $\mathfrak{q}$ must necessarily divide at least two ideals among the three ideals $\mathfrak{M}_i$. In the particular case where the ideal $\mathfrak{q}$ divides each one of the three ideals $\mathfrak{M}_i$, we deduce from (3) that q also divides N''.

Let c be the greatest common divisor of the integers c_1, c_2 and c_3, and let $c_1 = cc'_1$. According to the above, the product $c'_1c_2c_3$ is a square which will be written as follows:

$$c''^2 = c'_1c_2c_3.$$

The product of the three ideals

$$(c_i)\mathfrak{M}_i = \langle c_im_i; y_i, z\rangle \qquad (i = 1, 2, 3)$$

is equivalent to the product $\mathfrak{M}_1\mathfrak{M}_2\mathfrak{M}_3$, as well as to the product $\mathfrak{M}'_1\mathfrak{M}'_2\mathfrak{M}'_3$ (the ideals $\mathfrak{M}'_i$ are defined by the formulae:

$$(c_1)\mathfrak{M}'_1 = \langle cm_1; y_1, z\rangle, \quad (c_2)\mathfrak{M}'_2 = \langle m_2; y_2, z\rangle, \quad (c_3)\mathfrak{M}'_3 = \langle m_3; y_3, z\rangle),$$

because the ideal $\mathfrak{M}_1\mathfrak{M}_2\mathfrak{M}_3$ only differs from the ideal $\mathfrak{M}'_1\mathfrak{M}'_2\mathfrak{M}'_3$ by the product of a square of a ramified ideal.

Since c has no square divisors, c therefore divides N'' and we have the following congruences:

$$y_1 \equiv y_1 - 2m_1N'' \pmod{2cm_1},$$

$$y_2 \equiv y_1 - 2m_1N'' \pmod{2m_2},$$

$$y_3 \equiv y_1 - 2m_1N'' \pmod{2m_3}.$$

We deduce that the integer

$$w = \tfrac{1}{2}[(y_1 - 2m_1N'') + z\sqrt{-d}\,],$$

whose norm is given by formula (4), is divisible by the ideal $\mathfrak{M}'_1\mathfrak{M}'_2\mathfrak{M}'_3$. If we compare the norm of the integer w/c'' and the norm of the ideal $\mathfrak{M}'_1\mathfrak{M}'_2\mathfrak{M}'_3$, we obtain:

$$\mathfrak{M}'_1\mathfrak{M}'_2\mathfrak{M}'_3 = (w/c'').$$

Consequently, the product $\mathfrak{M}_1\mathfrak{M}_2\mathfrak{M}_3$ is principal and the lemma is proven.

To obtain fields k with r greater than 2, we must find more solutions to Eq. (1).

3. Families of Imaginary Quadratic Fields. The notations used in the proof of Lemma 5 are maintained in this section.

3.1. We know that if N'' and t are two integers for which the conditions of Lemma 3 are satisfied, then Eq. (1) has three solutions.

If we wish to speak of ideals corresponding to these three solutions, it is necessary that these solutions also satisfy the conditions of Lemma B.

In this case, one necessary condition for the ideals $\mathfrak{M}_1$, $\mathfrak{M}_2$ and $\mathfrak{M}_3$ (whose respective norms are m_1, m_2 and m_3) to be reduced is that their norms satisfy the inequalities:

$$1 < m_i < \sqrt{d/3} \qquad (i = 1, 2, 3);$$

the relation (3) and the inequality $1 < d < 4m_1^3$ give

$$(5) \qquad \sqrt{m_1} < N'' < \sqrt{3}\,\sqrt[4]{4m_1^3/3} < 2\sqrt[4]{m_1^3}.$$

On the other hand (Lemma 4), N'' must be the norm of an integer of $Q(\sqrt{-3})$ and at the same time a divisor of the number

$$N = 3m_1^2 + 3m_1t + t^2.$$

Consequently, N'' is necessarily a number of the form

$$(6) \qquad N'' = 3^u a^2 b,$$

where the integers (positive) u, a and b are subject to the following conditions:

– u only takes the values 0 or 1;

– if p^α is the greatest power of the prime p which divides a, then p^α also divides m_1;

– if the prime p divides b, then p is a prime of the form $p \equiv 1 \pmod 6$.

We will call *norms suitable for* m_1 all integers which are of the form (6) and which also satisfy the inequalities (5).

It should be noted that if, for a certain value of N'' Eq. (1) has three solutions and the corresponding ideals are reduced, then N'' is necessarily a norm suitable for m_1.

Let us now assume that the value of m_1 was chosen in such a way so that the set of the suitable norms for m_1 not be empty (this is always possible for sufficiently large values of m_1).

Let N'' be a norm suitable for m_1, and then let us determine a complete system of residues mod N'' which will be designated by $R(N'')$.

The congruence

$$(7) \qquad 3m_1^2 + 3m_1t + t^2 \equiv 0 \pmod{N''},$$

therefore, has solutions. Let $t_0 \in R(N'')$ be a solution of (7). To this value of t_0, we associate the integer

$$y_0 = \frac{3m_1^2 + 3m_1t_0 + t_0^2}{N''} - t_0N'' = \frac{3m_1^2 - t_0\tilde{t}_0}{N''},$$

where $\tilde{t}_0 = N''^2 - 3m_1 - t_0$.

Every integer congruent to t_0 mod N'' may be put in the form $t_i = t_0 + iN''$ $(i \in Z)$; and we will associate to this value of t_i the integer

$$y_i = \frac{3m_1^2 + 3m_1t_i + t_i^2}{N''} - t_iN'',$$

which we will write in the form

$$y_i = y_0 + i(t_0 - \tilde{t}_0) + i^2N'' \qquad (i \in Z). \tag{8}$$

3.2. According to the symmetry between t_0 and $\tilde{t}_0$, it is clear that t_0 is a solution of the congruence (7) if and only if $\tilde{t}_0$ is a solution of (7).

Let $\tilde{t} \in R(N'')$ be the residue congruent to $\tilde{t}_0$ mod N'' and let us consider the family $\{\tilde{y}_i\}$ $(i \in Z)$, which may be associated to the pair $(N'', \tilde{t})$ in a way similar to that of formula (8). We immediately see that the family $\{\tilde{y}_i\}$ and the family $\{y_i\}$ associated to the pair (N'', t_0) only differ in the order of their terms. To avoid repetitions, we will only take into consideration the values of i for which $t_0 + iN'' = t_i < \tilde{t}_i = \tilde{t}_0 - iN''$, that is, whenever $t_0 < \tilde{t}_0 - 2iN''$.

Moreover, in the search for imaginary quadratic fields, we will only take into account the integer values of y_i in the family $\{y_i\}$ which satisfy the inequality

$$|y_i| < \sqrt{4m_1^3}. \tag{9}$$

We will associate to each pair (N'', t_0), where N'' is a norm suitable for m_1 and $t_0 \in R(N'')$ a solution of congruence (7), a subset of Z defined in the following manner:

$$I = I(N'', t_0) = \{i \in Z \,|\, |y_i| < \sqrt{4m_1^3};\ t_0 < \tilde{t}_0 - 2iN''\}.$$

If I is not empty, we obtain, for each integer $i \in I$:

– one integer y_i defined by formula (8) and satisfying inequality (9);

– two positive integers z_i and d_i, uniquely determined (Lemma 1), and defined by the equality $z_i^2d_i = 4m_1^3 - y_i^2$;

– three solutions of Eq. (1) (with d_i instead of d) explicitly given by Lemma 3.

With every set of indices I, we define the following subsets:

– $I' = I'(N'', t_0)$, subset of the set I containing all $i \in I$ for which the solutions of Eq. (1) satisfy the conditions of Lemma B.

– $I'' = I''(N'', t_0)$, subset of I' containing all $i \in I'$ for which at least two ideals among the three ideals corresponding to the three solutions of Eq. (1), are reduced and different.

– $I^* = I^*(N'', t_0)$, subset of I'' containing all the values $i \in I''$ for which the following conditions are satisfied:

(a) the three ideals corresponding to the solutions of Eq. (1) are reduced;

(b) the norms of the three ideals corresponding to the solutions of Eq. (1) are different from each other.

(Let us note that condition (b) above, can also be expressed in the form

(b′) $t_i \neq 0$, $t_i \neq N''^2 - 3m_1$.)

Whenever $I^* = I^*(N'', t_0)$ is not empty, we will name the family $\{y_i\}$ $(i \in I^*)$, *family of abscissas associated to the pair* (N'', t_0).

For each abscissa y_i belonging to the family of abscissas associated to the pair (N'', t_0), we obtain the field

$$k_i = Q(\sqrt{y_i^2 - 4m_1^3}) = Q(\sqrt{-z_i^2 d_i}) = Q(\sqrt{-d_i});$$

the family $\{k_i\}$ $(i \in I^*)$, will be called *family of fields associated to the pair* (N'', t_0).

We can now state:

THEOREM 1. *The 3-rank r for each field of the family associated to the pair* (N'', t_0) *satisfies* $r \geqslant 2$.

3.3. Let C (resp. C', C'', C^*) be the set of pairs of the form (N'', t_0) for which the set I (resp. I', I'', I^*) is not empty.

Let us now assume that C^* contains at least two different pairs: (N'', t_0) and $(\hat{N}'', \hat{t}_0)$. We will denote by I the set $I(N'', t_0)$ and by $\hat{I}$ the set $I(\hat{N}'', t_0)$. In an analogous manner we will designate by I', I'', I^* the subsets of I defined above and by $\hat{I}'$, $\hat{I}''$, $\hat{I}^*$ the corresponding subsets of I. The indices belonging to I will be designated by the letter i and the indices belonging to I, by the letter j. Thus, $\{y_i\}$ $(i \in I^*)$ will designate the family of abscissas associated to the pair (N'', t_0) and $\{y_j\}$ $(j \in \hat{I}^*)$, the family of abscissas associated to the pair $(\hat{N}'', \hat{t}_0)$. We will also note:

$$\begin{cases} t_i = t_0 + iN'', \\ \tilde{t}_i = \tilde{t}_0 - iN'' = N''^2 - 3m_1 - t_i \qquad (i \in I^*) \end{cases}$$

and

$$\begin{cases} t_j = t_0 + j\hat{N}'', \\ \tilde{t}_j = \hat{N}''^2 - 3m_1 - t_j \qquad (j \in \hat{I}^*). \end{cases}$$

We can now state:

THEOREM 2. *If there are indices* $i \in I^*$ *and* $j \in \hat{I}^*$ *such that*:

(i) $|y_i| = |y_j|$ *and*

(ii) *the integers* t_i, $\tilde{t}_i$, t_j, $\tilde{t}_j$ *are different from each other,*

hen the 3-rank of the field $Q(\sqrt{y_i^2 - 4m_1^3})$ *is* $r \geqslant 3$.

Proof. Equation (1) has the following solutions:

$$s_1 = (m_1; y_i, z_i), \quad s_2 = (m_1 + t_i; y_i + 2t_iN'', z_i),$$
$$s_3 = (m_1 + \tilde{t}_i; y_i + 2\tilde{t}_iN'', z_i), \quad s_4 = (m_1; y_j, z_i),$$
$$s_5 = (m_1 + t_j; y_j + 2t_j\hat{N}'', z_i), \quad s_6 = (m_1 + \tilde{t}_j; y_j + 2\tilde{t}_j\hat{N}'', z_i).$$

The ideals corresponding to these solutions are, respectively, $\mathfrak{M}_1$, $\mathfrak{M}_2$, $\mathfrak{M}_3$, $\mathfrak{M}_4$,

$\mathfrak{M}_5, \mathfrak{M}_6$. According to condition (i), the ideals $\mathfrak{M}_1$ and $\mathfrak{M}_4$ are either equal or conjugates.

From condition (ii) and from the definition of the sets I^* and $\hat{I}^*$, we deduce that in the set constructed with the ideals $\mathfrak{M}_1, \mathfrak{M}_2, \mathfrak{M}_3, \mathfrak{M}_5, \mathfrak{M}_6$ and their conjugates, all the ideals are different from each other. We deduce that the 3-rank of the field $Q(\sqrt{y_i^2 - 4m_1^3})$ is greater than 2.

3.4. We now make a few observations concerning the practical utilization of this method.

Remark 1. The most difficult verification to make is to ensure that an index i which belongs to the set I also belongs to the set I^*.

To simplify the calculation, we can use, instead of Theorem 2, the following theorem, the statement of which is equivalent to the one of Theorem 2, but in which we have established a different order for the verifications of the conditions imposed on the indices. This theorem is valid whenever C contains at least two different pairs.

THEOREM 2$'$. *If there are indices $i \in I$ and $j \in \hat{I}$ such that*

(i) $|y_i| = |y_j|$,

(ii) *the integers t_i, $\tilde{t}_i$, t_j, $\tilde{t}_j$ are different from each other,*

(iii) *$i \in I^*$ and $j \in \hat{I}^*$,*

then the 3*-rank of the field $Q(\sqrt{y_i^2 - 4m_1^3})$ is $r \geqslant 3$.*

Remark 2. Instead of considering the set C^*, we may use the set C''. In that case, we obtain a greater number of fields having a 3-rank $r = 3$ (cf. example in 4.1), but the calculation for obtaining sufficient conditions so that the 3-rank of the field be $r \geqslant 3$ is much more complicated.

The following theorem indicates the method to be used with C'':

THEOREM 2$''$. *Let us assume that C'' contains at least two different pairs (N'', t_0) and $(\hat{N}'', \hat{t}_0)$. If there are indices $i \in I$ and $j \in \hat{I}$ such that*

(i) $|y_i| = |y_j|$,

(ii) *$i \in I''$ and $j \in \hat{I}''$,*

(iii) *the class of ideals represented by $\mathfrak{M}_5$ does not belong to the subgroup of the class group generated by the classes represented by the ideals $\mathfrak{M}_1$ and $\mathfrak{M}_2$,*

then the 3*-rank of the field $Q(\sqrt{y_i^2 - 4m_1^3})$ is $r \geqslant 3$.*

3.5. The program for this calculation can, therefore, be established in two different ways, depending upon the choice of the theorem (Theorem 2$'$ or Theorem 2$''$).

The following procedure is common to both:

– we fix the desired value of m_1; then, we take for N'' all the norms suitable for this value of m_1;

– for each norm N'', we look for all the solutions of congruence (7) in $R(N'')$. We can then easily construct the set C;

– we determine (depending upon the available memory in the computer) a partition

$$Y_0 = 1, Y_1, \ldots, Y_n = E(\sqrt{4m_1^3}) + 1$$

in the interval $[1, E(\sqrt{4m_1^3})]$. (Here $E(x)$ denotes the integer part of x.) Every subinterval of the form $[Y_s, Y_{s+1} - 1]$ defines a subset, in each set I associated with each pair $(N'', t_0) \in C$, which we designate by I_s; this set I_s is defined as follows:

$$I_s = \{i \in I \mid Y_s \leqslant |y_i| < Y_{s+1}\}.$$

We may now use either Theorem 2′ or Theorem 2″, with the set I_s instead of the set I, for $s = 1, \dots, n$.

The results obtained through the utilization of Theorem 2′ are well-adapted for the construction of extensive tables of discriminants of imaginary quadratic fields having $r \geqslant 3$. Nonetheless, the utilization of Theorem 2″ seems to be better suited for the search for imaginary quadratic fields having $r \geqslant 4$ as well as for the search of small values of d corresponding to fields with $r = 3$.

4. Numerical Results.

4.1. We systematically analyzed all the values of m_1 in the interval $11 < m_1 \leqslant 2000$, and also certain values of m_1 in the interval $2000 < m_1 < 10000$ when using Theorem 2″ (these values of m_1 are, on the one hand, all the prime numbers and, on the other hand, all the square-free numbers having only prime divisors congruent to 2 mod 3). We thus obtain several thousand values of d for which the corresponding quadratic field has $r \geqslant 3$.

Certain values of d appear repeated either because they are obtained for two or more different values of m_1, or because there are for the same value of m_1, more than two pairs belonging to C'' satisfying the conditions of Theorem 2′ or 2″.

Whenever we have seven or more solutions for Eq. (1), it is easy to verify whether or not $r > 3$ for the corresponding value of d.

Concerning the difference between the utilization of Theorems 2′ and 2″, we may consider the example of the field $k_1 = Q(\sqrt{-63199139})$, discovered by Shanks [8], which served as the lower bound for the discriminants published in [3].

We found the field k_1 for the value $m_1 = 683$, for the pairs (37, 5) and (169, 1) and for the indices $-11 \in I^*(37, 5)$ and $-1 \in I''(169, 1)$. It is easy to verify that $-1 \notin I^*(169, 1)$, and this shows that the field k_1 cannot be obtained in the interval $11 < m_1 \leqslant 2000$ if we use only Theorems 2 and 2′.

4.2. We found 156 quadratic fields k having $r = 3$, unknown thus far [3], [10], for the values of d belonging to the interval

$$3321607 < d < 63199139.$$

Among these fields, there are five for which the value of d is less than 10^7. In Table 1, we give these values of d, the class number of the corresponding imaginary quadratic fields and three reduced ideals generating the group H comprised of the classes whose cube is the principal class. We also give the structure of the class group of these fields using the notation

$$n \times n' \times n'' \times \dots$$

to indicate that the group is a product of cyclic groups of orders $n, n', n'', \dots$.

Table 1

d	factors of d	class number	class group	basis for H	ideal of highest order
4447704	2^3.3.47.3943	864	3x3x3x8x2x2	<345; 6> <390; 96> <538;360>	<5;4> is of order 24
5769988	2^2.7.251.821	432	3x3x3x4x2x2	<658;210> <826;742> <917;406>	<13;6> is of order 12
7546164	2^2.3.17.71.521	1296	9x3x3x2x2x2x2	<1318;774> <645;204> <501; 30>	<5;4> is of order 18
8721735	3.5.11.52859	2160	3x3x3x4x2x2x5	<1464;837> <276;237> <1090;875>	<2;1> is of order 60
9379703	499.18797	1890	3x3x3x2x5x7	<626;207> <1412;995> <464;157>	<3;1> is of order 210

Table 2

d = 653329427 = 8867.73681
class number: 5670
class group: 3x3x3x3x2x5x7
the ideal <3;1> is of order 105

<639; 587>	(639; 19757, 1)	<6499; 1621>	(6499;1036568, 6)
<689; 589>	(689; 25593, 1)	<7213; 7083>	(7213;1203401, 9)
<843; 401>	(843; 41749, 1)	<7243; 1347>	(7243; 899125, 33)
<1139; 389>	(1139; 72507, 1)	<7367; 7161>	(7367; 839583, 37)
<1359; 965>	(1359; 96883, 1)	<7817; 6233>	(7817;1382025, 1)
<1649; 457>	(1649;131463, 1)	<8643; 2131>	(8643; 389281, 61)
<1807; 901>	(1807; 9020, 6)	<8663; 1101>	(8663;1612419, 1)
<2061; 691>	(2061;136693, 5)	<8753; 8089>	(8753; 80046, 64)
<2193; 325>	(2193; 19330, 8)	<10053; 5159>	(10053;2015759, 1)
<2217;1385>	(2217; 42118, 8)	<10721; 8397>	(10721; 864738, 80)
<2729; 161>	(2729;283977, 1)	<11031; 7475>	(11031; 988004, 82)
<2897;2635>	(2897;235458, 8)	<11271; 8927>	(11271;1793284, 62)
<3117;1999>	(3117;347105, 1)	<11653; 7071>	(11653;2410355, 27)
<3327; 923>	(3327;339547, 7)	<11867; 1651>	(11867;2585355, 1)
<3593;2015>	(3593;379110, 8)	<12321; 5645>	(12321;1556366, 88)
<4563;4489>	(4563;615931, 1)	<12513; 707>	(12513; 273301,109)
<5123;1287>	(5123;310104,26)	<13399;12771>	(13399;3055183, 21)
<6031;4239>	(6031;633391,27)	<13401;11689>	(13401;3095926, 8)
<6117;2243>	(6117;956405, 1)	<13773;12407>	(13773;2074495, 97)
<6157; 875>	(6157;676267,27)	<14279;13713>	(14279;1198791,125)

TABLE 3

d= 2520963512 = 2^3.311.1013249
class number: 14904
class group: 3x3x3x3x4x2x23
the ideal <3;2> is of order 276

<1361;1148>	(1361; 426, 2)	<11058; 9772>	(11058; 272584, 46)
<1433; 960>	(1433; 41070, 2)	<11241;10448>	(11241;2381506, 2)
<1662;1040>	(1662; 90992, 2)	<11799; 1970>	(11799;1866086, 35)
<2126; 848>	(2126; 168384, 2)	<12241; 7382>	(12241;2251222, 30)
<2802; 536>	(2802; 279128, 2)	<12322;10388>	(12322; 363800, 54)
<4127;1300>	(4127; 397038, 7)	<12777; 8720>	(12777; 661610, 56)
<4343;1328>	(4343; 150426,11)	<12879; 3698>	(12879;2763118, 19)
<5246;1080>	(5246; 753264, 2)	<14481;10324>	(14481;3483754, 2)
<5961;1510>	(5961; 914974, 2)	<14673; 2800>	(14673;2038550, 58)
<6066;3376>	(6066; 939544, 2)	<18206;11824>	(18206;4527456, 38)
<6801;1634>	(6801; 195286,22)	<20313;16244>	(20313;4071250, 82)
<6977;1520>	(6977;1161222, 2)	<20663;13074>	(20663;4422186, 79)
<7169; 416>	(7169; 682206,20)	<21071;18550>	(21071;6107166, 7)
<7433;7060>	(7433;1277730, 2)	<22129; 3736>	(22129;5999542, 54)
<7673;1182>	(7673;1077786,16)	<23214; 412>	(23214;6613376, 50)
<8786;3872>	(8786;1644024, 2)	<23223;17830>	(23223;2614406,131)
<9351;1378>	(9351;1594394,17)	<23433; 1486>	(23433;7173470, 2)
<10313;6720>	(10313;1934454,16)	<23481;13888>	(23481;6334726, 68)
<10393;9114>	(10393;2031590,12)	<23593; 4808>	(23593;2126270,138)
<10737;5518>	(10737;2222858, 2)	<25241;10272>	(25241;4798074,128)

Concerning the first two fields of Table 1, we would like to make a few supplementary remarks:

– $Q(\sqrt{-4447704}) = Q(\sqrt{-1111926})$. The integer $D = 1111926$ is the smallest known number for which the field $Q(\sqrt{-D})$ has a 3-rank $r = 3$. It should be easy, [1], to determine whether it is in fact the smallest number having this property.

– $Q(\sqrt{-5769988})$. The exponent of the class group of this field is 12. The smallest exponent previously known for the class group of an imaginary quadratic field having a 3-rank $r = 3$ was 18, occurring in the fields $Q(\sqrt{-3640387})$, $Q(\sqrt{-5048347})$ and $Q(\sqrt{-26156083})$ [3], [10].

4.3. All imaginary quadratic fields having $r = 4$, for which the discriminant is explicitly known [2], [9] were discovered by Shanks and Serafin [9] and by Neild and Shanks [5]; the discriminants of these fields are as follows:

$$\left.\begin{array}{l} -d_1 = -87386945207 \\ -d_2 = -333238519268 \end{array}\right\} \text{published in [9],}$$

$$-d_3 = -32330444167844 \quad \text{published in [5].}$$

We now know 52 values of d satisfying $d < d_1$ and 80 new values of d with $d > d_1$ (but d_1, d_2 and d_3 have not been found), for which the fields $Q(\sqrt{-d})$ have a 3-rank $r \geqslant 4$. (For all these fields, r very probably equals 4.) In Tables 2 and 3, we

Table 4

Values of d	Basis for H	Values of d	Basis for H
3146813128	⟨1489; 972⟩ ⟨1474; 1380⟩ ⟨1574; 896⟩ ⟨1958; 544⟩	7993105123	⟨1483; 99⟩ ⟨1517; 1423⟩ ⟨1337; 527⟩ ⟨14827; 8041⟩
4724490703	⟨2182; 103⟩ ⟨1126; 127⟩ ⟨1396; 295⟩ ⟨1466; 799⟩	8308370723	⟨1451; 1303⟩ ⟨1431; 1181⟩ ⟨20067;14455⟩ ⟨1301; 1059⟩
5252241199	⟨1250; 599⟩ ⟨1388; 1169⟩ ⟨4240; 3799⟩ ⟨1936; 695⟩	8418280523	⟨1787; 1483⟩ ⟨1917; 1285⟩ ⟨1383; 517⟩ ⟨1521; 839⟩
5288116947	⟨2887; 2315⟩ ⟨2283; 645⟩ ⟨5881; 1611⟩ ⟨2301; 2043⟩	9775810067	⟨1409; 959⟩ ⟨3093; 1661⟩ ⟨1713; 1141⟩ ⟨1347;. 475⟩
6905985272	⟨1913; 170⟩ ⟨4226; 160⟩ ⟨2306; 604⟩ ⟨1982; 1916⟩	9906365947	⟨1357; 1293⟩ ⟨2579; 129⟩ ⟨1943; 487⟩ ⟨1469; 217⟩
7311232679	⟨1250; 111⟩ ⟨1326; 199⟩ ⟨2690; 1991⟩ ⟨1670; 491⟩		

give a description of the two fields having the smallest values of d known to us. In these tables, we indicate the class number, the structure of the class group and the 40 reduced ideals of these fields, which, with their conjugates and the principal class, comprise the group H; alongside each reduced ideal, we indicate the corresponding solution of Eq. (1).

In Table 4 we present all the values of d, known to us, satisfying the inequality $d < 10^{10}$, for which the corresponding quadratic fields have a 3-rank $r = 4$. For each one of these fields, we give four reduced ideals representing classes which generate the complete group H.

4.4. All the numerical results in Tables 1, 2, 3 and 4, were obtained on the UNIVAC 1110 computer at the University of Paris XI (Orsay), with the exception of the class numbers and the structure of the class groups (given in Tables 1, 2 and 3), obtained with a programmable pocket calculator, following an intermediate method between Shanks' method [6], and the exhaustive calculation of the reduced ideals of the field.

Université de Paris-XI
Mathématiques, Batiment 425
91405 Orsay, France

1. D. A. BUELL, "Class groups of quadratic fields," *Math. Comp.*, v. 30, 1976, pp. 610–623.

2. M. CRAIG, "A type of class group for imaginary quadratic fields," *Acta Arith.*, v. 22, 1973, pp. 449–459.

3. F. DIAZ Y DIAZ, "Sur les corps quadratiques imaginaires dont le 3-rang du groupe des classes est supérieur à 1," *Séminaire Delange-Pisot-Poitou*, 1973/74, G-15.

4. S. KURODA, "On the class number of imaginary quadratic number fields," *Proc. Japan Acad.*, v. 40, 1964, pp. 365–367.

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

6. D. 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.

7. D. SHANKS & P. 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.

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

9. D. SHANKS & R. SERAFIN, "Quadratic fields with four invariants divisible by 3," *Math. Comp.*, v. 27, 1973, pp. 183–187.

10. D. SHANKS, "Class groups of the quadratic fields found by F. Diaz y Diaz," *Math. Comp.*, v. 30, 1976, pp. 173–178.