MATHEMATICS OF COMPUTATION
VOLUME 50, NUMBER 182
APRIL 1988, PAGES 581-594

On Totally Real Cubic Fields with Discriminant $D < 10^7$

By Pascual Llorente and Jordi Quer

Abstract. The authors have constructed a table of the 592923 nonconjugate totally real cubic number fields of discriminant $D < 10^7$, thereby extending the existing table of fields with $D < 5 \times 10^5$ constructed by Ennola and Turunen [4]. Each field is given by its discriminant and the coefficients of a generating polynomial. The method used is an improved version of the method developed in [8]. The article contains an exposition of the modified method, statistics and examples. The decomposition of the rational primes is studied and the relative frequency of each type of decomposition is compared with the corresponding density given by Davenport and Heilbronn [2].

1. Introduction. A table of totally real cubic fields with discriminant $D < D'$ has been constructed by Godwin and Samet [5] for $D' = 2 \times 10^4$. Angell [1] extended this table up to $D' = 10^5$ by using a similar method. These tables are not complete (see [4] and [9]). A complete table for $D' = 10^5$ is constructed in [8] by a different method. Finally, a third method is developed by Ennola and Turunen [4] to compute a table with $D' = 5 \times 10^5$. In this paper we shall describe an extended table for $D' = 10^7$. The method used is an improved version of that developed in [8]. Up to 5×10^5, this table agrees with Ennola and Turunen's.

The modified method and the new algorithm are described in Sections 2 and 3. Section 4 contains statistics and examples (Tables 1–6). The decomposition of the rational primes is studied using the congruential criteria given in [6] and [7]. In Section 5 we compare the relative frequency of each type of decomposition for different primes with the corresponding density given by Davenport and Heilbronn in [2] (Tables 7–11).

Computations were done on an IBM 3360 owned by the Universitat de Barcelona and a VAX-8600 owned by the Facultat d'Informàtica de Barcelona.

2. The Improved Method. The method used to compute our table of totally real noncyclic cubic fields is similar to the one described in [8] but improved in several ways. In this section we recall the main ideas in [8] and we explain the modifications introduced. For every prime $p \in \mathbf{Z}$ and integer m, $v_p(m)$ denotes the greatest integer k such that p^k divides m.

Each triple of conjugate noncyclic fields is defined by a polynomial of the type

$$f(a,b,X) = X^3 - aX + b, \tag{1}$$

Received September 22, 1986; revised February 17, 1987 and August 7, 1987.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11R16, 11-04.
Key words and phrases. Real cubic fields.

where a and b are positive integers such that

$$f(a,b,X) \text{ is irreducible in } \mathbf{Q}[X], \tag{2}$$

$$\text{there is not a prime } p \text{ with } v_p(a) \geq 2 \text{ and } v_p(b) \geq 3. \tag{3}$$

Then, each field on the triple is isomorphic to the cubic field $K = K(a,b) = \mathbf{Q}(\theta)$, where θ is a root of the polynomial $f(a,b,X)$. The descriminant of $f(a,b,X)$ is

$$D(a,b) = 4a^3 - 27b^2 = DS^2, \tag{4}$$

where $D = D(K)$ is the descriminant of the cubic field K and $S > 0$ is the index of θ. It is known (cf. [3] or [7]) that

$$D = D(K) = dT^2, \tag{5}$$

where d is the discriminant of $\mathbf{Q}(\sqrt{D})$ and $T = 3^m T_0$ with $0 \leq m \leq 2$ and $T_0 > 0$ is a square-free integer having no common factor with $3d$. Note that $d > 1$, since we are assuming that K is totally real and noncyclic.

Consider the congruences

$$a \equiv 3 \pmod 9, \qquad b \equiv \pm(a-1) \pmod{27}. \tag{6}$$

We have the following result (cf. [3, p.112]).

THEOREM 1 (VORONOI). (i) *If the congruences* (6) *are not satisfied, then S is the greatest positive integer whose square divides $D(a,b)$ for which there exist integers t, u and v such that*

$$-S/2 < t \leq S/2, \quad 3t^2 - a = uS, \quad t^3 - at + b = vS^2, \tag{7}$$

and $1, \theta, \beta$, with $\beta = (\theta^2 + t\theta + t^2 - a)/S$, is a basis for the integers of K.

(ii) *If the congruences* (6) *are satisfied, then $S = 27S'$, and S' is the greatest positive integer whose square divides $D(a,b)/729$ for which there exist integers t, u and v such that*

$$-3S'/2 < t \leq 3S'/2, \quad 3t^2 - a = 9uS', \quad t^3 - at + b = 27vS'^2, \tag{8}$$

and $1, \psi, \beta$, with $\psi = (\theta - t)/3$ and $\beta = (\theta^2 + t\theta + t^2 - a)/9S$, is a basis for the integers of K.

It follows that by choosing a minimal t in (7) or (8) there is a unique quadruple (S, t, u, v) of integers associated with each pair (a, b). The main idea in [8] is to associate a positive definite binary quadratic form $F(a,b)$ with each pair (a,b), whose coefficients are given in terms of a, S, t, u and v. We shall give an alternative definition for the quadratic form associated with the pair (a,b) (see D, below). We repeat here the definition and some of the properties of $F(a,b)$ given in [8], to make our exposition more self-contained.

If the congruences (6) are not satisfied, then $\mathrm{Tr}(1) = 3$, $\mathrm{Tr}(\theta) = 0$ and $\mathrm{Tr}(\beta) = u$ are the traces of the integers in a basis for the integers of K. So the integers $\gamma \in K$ with zero trace are given by

$$\gamma = (3x\theta^2 + 3(xt + Sy)\theta - 2ax)/3S; \qquad x, y \in \mathbf{Z}, \; 3 \mid ax. \tag{9}$$

Let $\gamma \neq 0$ be such an integer. Its minimum polynomial is $f(a', -N(\gamma), X)$, $N(\gamma)$ being the norm of γ and $a' = (3u^2 - 27tv)x^2/9 + (3ut - 9vS)xy/3 + ay^2$.

If $3 \nmid u$, since $\mathrm{Tr}(\theta) = 0$, we have $3 \mid x$. Let $z = x/3$; then

$$a' = (3u^2 - 27tv)z^2 + (3ut - 9vS)zy + ay^2.$$

If $3 \mid u$, let $u = 3w$; then

$$a' = (3w^2 - 27tv)x^2 + (ut - 3vS)xy + ay^2.$$

If the congruences (6) are satisfied, then

$$\begin{aligned} a &= 3a_1 && \text{with } a_1 = 3a_2 + 1 \text{ and } a_2 \in \mathbf{Z}, \\ u &= 3u_1 + \eta && \text{with } |\eta| < 2 \text{ and } u_1, \eta \in \mathbf{Z}, \\ t &= 3t_1 + \delta && \text{with } \delta = \pm 1 \text{ and } t_1 \in \mathbf{Z}. \end{aligned}$$

The integers $\gamma \in K$ with zero trace are given by

$$\gamma = (x\theta^2 + (tx + 3\mu Sx + 9Sy)\theta - 2a_1x)/9S; \qquad x, y \in \mathbf{Z},\ \mu = \eta\delta. \tag{10}$$

Let $\gamma \neq 0$ be such an integer. Its minimum polynomial is $f(a', -N(\gamma), X)$, $N(\gamma)$ being the norm of γ and

$$a' = (uu_1 + 2\eta u_1 - vt + \mu ut_1 - 3\mu vS' + \mu^2 a_2 + \mu^2)x^2 + (ut + 2\mu a_1 - 9vS')xy + ay^2.$$

With these notations, the quadratic form $F(a, b)$ associated with the pair (a, b) is defined in [8] as follows:

DEFINITION 1. (i) If the congruences (6) are not satisfied and $3 \nmid u$, we define

$$F(a, b) = (3u^2 - 27tv, 3ut - 9vS, a).$$

(ii) If the congruences (6) are not satisfied and $u = 3w$, we define

$$F(a, b) = (3w^2 - 3tv, ut - 3vS, a).$$

(iii) If the congruences (6) are satisfied we define

$$F(a, b) = (uu_1 + 2\eta u_1 - vt + \mu ut_1 - 3\mu vS + \mu^2 a_2 + \mu^2, ut + 2\mu a_1 - 9vS, a).$$

Then $F(a, b)$ represents precisely those integers $a' > 0$ for which there exists an integer b' such that $K(a', b')$ is isomorphic to $K(a, b)$. Then, if $K(a, b) \approx K(a', b')$, the corresponding associated forms $F(a, b)$ and $F(a', b')$ represent the same integers and, consequently, they are equivalent (cf. [8] or [10]).

THEOREM 2. *Let $F = F(a, b)$ be the form associated with the field $K = K(a, b)$ of discriminant $D = D(K)$. Then the discriminant $D(F)$ of the form F is*

$$\begin{aligned} D(F) &= -D/3 && \text{if } 27 \mid D, \\ D(F) &= -3D && \text{if } 27 \nmid D. \end{aligned}$$

Proof. One computes $D(F)$ from Definition 1. Then $D(F) = -D/3$ in case (ii), and $D(F) = -3D$ in cases (i) and (iii).

In case (ii) of Definition 1, we have $a = 3a_1$ (since $u = 3w$) and then $27 \mid DS^2$ in (4). If $3 \nmid S$ then $27 \mid D$; else, easy congruential considerations show that if $3 \mid u$ and $9 \mid S$, then the congruences (6) are satisfied, hence we must have $S = 3S_1$ with $3 \nmid S_1$ and $D = 3D_1$. From (7) it follows that $a_1 \equiv t^2 \pmod 3$ and $b \equiv 2t^3 \pmod 3$. Then $D_1S_1^2 = 4a_1^3 - b^2 \equiv 0 \pmod 3$, so $9 \mid D$ and from Theorem 2 of [7], 27 must divide D.

Conversely, from Theorem 2 of [7] and easy congruential considerations one can show that if $27 \mid D$ then case (ii) of Definition 1 holds. □

From this result and the elementary theory of reduced positive definite quadratic forms we obtain

THEOREM 3. *Let K be a totally real noncyclic cubic field of discriminant $D = D(K)$. Then $K \approx K(a, b)$ for some integer a with*

$$\begin{aligned} &a < \sqrt{D}/3 \quad &&\textit{if } 27 \mid D, \\ &a < \sqrt{D} &&\textit{if } 27 \nmid D. \end{aligned}$$

In this case, we have

$$\begin{aligned} &S < S(a) = 2\sqrt{a/3} \quad &&\textit{if } 27 \mid D, \\ &S < S(a) = 2\sqrt{a} &&\textit{if } 27 \nmid D. \end{aligned}$$

As a consequence, a table of all totally real noncyclic cubic fields of discriminant $D = D(K) < D'$ can be constructed from a finite number of pairs (a, b), carrying out the following steps:

- Elimination of all pairs not satisfying (2) or (3).
- Decomposition of $D(a, b)$ as in (4) for the remaining pairs.
- Elimination of all pairs not satisfying the bounds of Theorem 3.
- Elimination of isomorphic fields.

In this way, a table with $D' = 10^5$ was constructed (see [8] and [9]); but this algorithm is too inefficient (about 70 hours of computer time were needed to construct that table) to be applied to much greater D'. Moreover, the computation of $D(a, b)$ requires multiple-precision arithmetic. We explain below the improvements introduced in the method. With them, the method becomes much more efficient.

A. *Irreducibility of $f(a, b, X)$.* It is convenient to observe that each of the following conditions implies the irreducibility of $f(a, b, X)$ in $\mathbf{Q}[X]$:

(11) $$1 \leq v_p(b) \leq v_p(a) \quad \text{for some prime } p,$$

(12) $$a \equiv b \equiv 1 \pmod 2,$$

(13) $$a \equiv 1 \pmod 3 \quad \text{and} \quad 3 \nmid b.$$

In [8] one uses the fact that $f(a, b, X)$ is reducible if and only if it has a root $m \in \mathbf{Z}$. In this case, $m \mid b$, and an elementary study of $f(a, b, X)$ shows that such a root m must satisfy

$$0 < m < \sqrt{a} \quad \text{or} \quad \sqrt{a} < -m < \sqrt{a} + \sqrt{a/3}.$$

B. *Computation of $D(K)$ and S.* In [8], $D = D(K)$ and S were computed from $D(a, b)$ using Theorem 1. This was certainly the most laborious part of the method. The results in [7] simplify this computation. Indeed, if (11) is satisfied for a prime p, then $p \mid T$ and (11) is also a necessary condition for $p \mid T$ if $p \neq 3$; the factor 3^m of T can be determined from certain congruential conditions involving a and b (see [7, Theorems 1 and 2]). In this way, T is computed and, eventually, a divisor S_0 of S is also obtained. It is also easy to compute $v_2(D)$ and $v_2(S)$ from a and b in case $2 \nmid T$. Now, every new integer m whose square divides $D(a, b)$ will be a new factor of S, i.e., $m \mid S$ if and only if $D(a, b) \equiv 0 \pmod{m^2}$. Also, these computations sometimes give several prime factors of d; in fact, $p \mid d$ if any of the following conditions is satisfied:

$$1 = v_p(a) < v_p(b), \tag{14}$$

$$v_p(D(a,b)) \quad \text{is odd.} \tag{15}$$

These conditions are also necessary for $p \mid d$, except if $p = 3$. In this case, some additional congruential conditions must be considered (see [7, Theorem 1]). Using the bound $S < S(a)$ in Theorem 3, one can easily compute S (and then D) or eliminate the pair (a, b).

C. *Eliminating Superfluous Fields.* With the help of Theorem 3 we can eliminate all pairs (a, b) for which $S \geq S(a)$. We can eliminate also the pairs with $D \leq D(a)$, where

$$D(a) = 9a^2 \quad \text{or} \quad D(a) = a^2, \quad \text{according as } 27 \mid D \text{ or not,} \tag{16}$$

because in this case $K(a,b) \approx K(a', b')$ for some $a' < a$. The determination of the bounds $S(a)$ and $D(a)$ (i.e., if $27 \mid D$ or not) follows from the computations in B. In many cases, this elimination can be done by knowing only some factors of D and S, and it is not necessary to compute S and D completely as in [8].

D. *Eliminating Isomorphic Fields.* If we obtained two fields $K_1 = K(a_1, b_1)$ and $K_2 = K(a_2, b_2)$ with the same discriminant D, we have to test if $K_1 \approx K_2$ or not. As in [8], this can be done by studying their associated quadratic forms. The method has been improved at this point too. We start giving a new definition of the associated quadratic form:

DEFINITION 2. (i) In the first case of Voronoi's Theorem, let $B = (3b - 2at)/S$. Then we define

$$F^* = F^*(a,b) = (a, B, C) \quad \text{if } 27 \mid D,$$
$$F^* = F^*(a,b) = (a, 3B, C) \quad \text{if } 27 \nmid D,$$

where C is determined by the condition $D(F^*) = -D/3$ or $D(F^*) = -3D$, according as $27 \mid D$ or not.

(ii) In the second case of Voronoi's Theorem, let $a' = a/3$, let μ be the only integer with $|\mu| < 2$ and $\mu \equiv t(t^2 - a')/3S' \pmod 3$ and let $B = -2\mu a' + (b - 2a't)/3S'$. Then we define

$$F^* = F^*(a,b) = (a, B, C),$$

where C is determined by the condition $D(F^*) = -3D$.

It is immediate to see that the associated form $F^*(a,b)$ given in this definition is equivalent to the associated form $F(a,b)$ given in Definition 1. An advantage of this new definition is that it is not necessary to compute u and v in Voronoi's Theorem. Moreover, if a is minimum, the reduced equivalent quadratic form is easily obtained from a and B; it suffices to find $n \in \mathbf{Z}$ such that

$$B' = B + 2an \quad \text{and} \quad |B'| \leq a. \tag{17}$$

Then the reduced form will be $F' = (a, B', C')$, where C' is determined by the discriminant.

The following theorem permits us to eliminate a large number of isomorphic fields.

THEOREM 4. *Let $K_1 = K(a_1, b_1)$ satisfy the conditions of Theorem* 3, *and let $F' = (a_1, B', C')$ be the reduced form equivalent to its associated form. Then there exists a pair (a_2, b_2) with $a_2 \geq a_1$, and $b_2 \neq b_1$ in case $a_2 = a_1$, such that the field $K_2 = K(a_2, b_2)$ satisfies the conditions of Theorem* 3 *and is isomorphic to K_1 if and only if $D(C') < D(K_1)$. In this case, we must have $C' = a_2$, and there is only one such pair.*

Proof. We know that $a_2 = F'(x, y)$ must be an integer represented by F', and by (3) we have that $y \neq 0$. It is easy to see that $C' = F(0, 1)$ is the only integer a represented in that way by F' for which the condition $D(a) < D(K_1)$ can be satisfied. □

Theorem 4 is not sufficient to eliminate isomorphic fields if there exists a third field $K_3 = K(a_3, b_3)$ satisfying the conditions of Theorem 3, with the same discriminant as K_1 and K_2 and with $a_2 = a_3 = C'$ ($D = 77844$ is an instance of this case). Then we have to decide whether $K_1 \approx K_2$ or $K_1 \approx K_3$. For this we can proceed as in [8]: The representation of a_2 by $F(a_1, b_1)$ determines an integer γ in K_1 with zero trace, whose minimal polynomial is $f(a_2, -N(\gamma), X)$. Then $K_1 \approx K_2$ or $K_1 \approx K_3$ according as $|N(\gamma)|$ is equal to b_2 or b_3.

Using the definition of γ (see (9) and (10)) and the transformation taking $F(a_1, b_1)$ into its reduced associated form $F' = (a_1, B', a_2)$, and computing explicitly the norm $N(\gamma)$ of the integer γ, we obtain

THEOREM 5. *Let $K_1 = K(a_1, b_1)$ satisfy the conditions in Theorem* 3 *with $D(K_1) = D$. Let $F' = (a_1, B', a_2)$ be the reduced form equivalent to its associated form $F = F(a_1, b_1)$ with $D(a_2) < D$, and let γ be the null trace integer in K_1 determined by the representation of a_2 by F. Then:*

(i) *If $D = 27D'$ and $a_1 = 3a$, then*

$$N(\gamma) = ((2aa_2 - D')S^2 - 4a^3 + b_1(t - nS)(a_1 - (t - nS)^2))/S^3.$$

(ii) *If $27 \nmid D$ and the congruences* (6) *are not satisfied, then*

$$N(\gamma) = ((2a_1a_2 - D)S^2 - 4a_1^3 + b_1(3t - nS)(9a_1 - (3t - nS)^2))/S^3.$$

(iii) *If $a_1 = 3a$ and the congruences* (6) *are satisfied, then*

$$N(\gamma) = ((2a_1a_2 - D)27S'^2 - 4a^3 + b_1(t + 3\mu S' - 9nS')(a_1 - (t + 3\mu S' - 9nS')^2))/(9S')^3.$$

Here, S, S', t and μ are the integers used in Definition 2 *and n is the integer determined by* (17).

3. The New Algorithm. The method described in the previous section provides an easy computer-programmable algorithm to construct a table of the totally real cubic fields K with discriminant $D = D(K) < D'$ for a given D'. We shall now describe the algorithm used by the authors.

We take all integers a with $4 \leq a \leq \sqrt{D'}$ and, for each, we take the integers b with $1 \leq b \leq 2(a/3)^{3/2}$. For each pair (a, b) we proceed as follows:

Step 1. Compute $M = \text{g.c.d.}(a, b)$ and work with every prime factor p of M. During these computations:

(a) The pairs not satisfying (3) are eliminated.

(b) T_0 is always obtained and T is also obtained if $3 \mid M$ (as is explained in B of Section 2). In case $3 \mid M$, the bounds $S(a)$ and $D(a)$ are determined.

(c) $v_p(D)$ and $v_p(S)$ are computed using (b) and (14).

(d) In some cases, irreducibility of $f(a,b,X)$ is proved by (11).

Step 2. If irreducibility of $f(a,b,X)$ has not been proven in Step 1(d), use the other results in A of Section 2 to eliminate the pairs with $f(a,b,X)$ reducible.

Step 3. If $3 \nmid M$, compute $v_3(D)$ and $v_3(S)$, using the congruential conditions given in [7]. So, T is obtained and the bounds $S(a)$ and $D(a)$ are determined.

(*Remark*. During the computations, divisors S_0 of S and D_0 of D are obtained. If $S_0 \geq S(a)$ or $D_0 \geq D'$, the pair (a,b) is eliminated.)

Step 4. If $2 \nmid M$, compute $v_2(D)$ and $v_2(S)$, using the congruential criterion given in [7].

Step 5. Let $S_1 = S(a)/S_0$. For every prime p with $p \nmid 6M$ and $p < S_1$, examine $D(a,b)$ modulo p^2 (if $p^2 < S_1$ then examine $D(a,b)$ modulo p^4). In this way:

(a) $v_p(D)$ and $v_p(S)$ are computed using (15).

(b) Eventually, D_0, S_0 and S_1 are modified.

(c) The final S_0 is the greatest S in (4) with $S < S(a)$.

Step 6. Let $D_1 = D(a,b)/S_0^2$. If $D_1 \geq D'$, the pair (a,b) is eliminated. Indeed, in this case we have $D \geq D'$ or $S \geq S(a)$.

Step 7. Let $D_2 = D_1/D_0T^2$. The pair (a,b) is eliminated in the following cases:

(a) If D_2 is not square-free (in this case, $S \geq S(a)$).

(b) If $D_2 = D_0 = 1$ (in this case, $d = 1$).

(c) If $D_1 \leq D(a)$.

Step 8. If the pair (a,b) has not been eliminated in the preceding steps, $K = K(a,b)$ is a cubic field with discriminant $D = D_1 < D'$ satisfying the conditions of Theorem 3. During the process, $d = D_0D_2$, T and $S = S_0$ have been computed. Record these data in a file.

Step 9. Data in that file are ordered with increasing discriminant D *without altering the order* of their generation among the fields with the same discriminant.

Step 10. Eliminate isomorphic fields in the file by using the results of D in Section 2. To do this, proceed as follows: Let $K_i = K(a_i,b_i)$, $i = 1,\dots,N$, be all the fields in the file with the same discriminant D. According to Step 9, we have $a_1 \leq a_2 \leq \cdots \leq a_N$. Compute the reduced quadratic form (a_1,B,C) equivalent to the quadratic form associated with the pair (a_1,b_1). By Theorem 4, K_1 is isomorphic to some K_i with $i > 1$ (and only to one of them) if and only if $D(C) < D$, and in this case, $C = a_i$. If $C = a_i$ for only one $i > 1$, then eliminate the field K_i. If $C = a_i$ for more than one $i > 1$, then compute $N(\gamma)$ by using Theorem 5 and eliminate the field $K_i = K(a_i,b_i)$ for which $b_i = |N(\gamma)|$. Proceed in the same way with the next noneliminated field until the set of all fields with discriminant D is completely purged of isomorphic pairs.

This algorithm is very efficient. A table for $D' = 10^5$ can be constructed in less than a minute of computer time, and with $D' = 5 \times 10^5$ in about five minutes. We have used it with $D' = 10^7$, and the total computer time required was about 5 hours. Almost all time was spent in the generation of the fields $K(a,b)$ (Steps 1 to 8). The purge of isomorphic fields in Step 10 eliminated around 10% of the stored fields and required about 8 minutes.

4. Totally Real Cubic Fields with Discriminant $D < 10^7$. The table containing the 592422 nonconjugate totally real noncyclic cubic fields with discriminant less than 10^7 consists of 10 sectors, the kth containing the fields with discriminants between $10^6(k-1)$ and 10^6k. For each field $K = \mathbf{Q}(\theta)$, its discriminant D, the coefficients a and b of a polynomial $\mathrm{Irr}(\theta, \mathbf{Q}) = f(a, b, X)$ and the integers S and T are listed. Other data obtained during the computations were not stored for lack of space. Separately, we have constructed a table of the 501 cyclic cubic fields with discriminant less than 10^7.

TABLE 1
Number of cubic fields with discriminant $0 < D < 10^7$

Sector	Noncyclic	Cyclic	Total	Noncyclic (accum.)	Cyclic (accum.)	Total (accum.)
1	54441	159	54600	54441	159	54600
2	57777	67	57844	112218	226	112444
3	58787	47	58834	171005	273	171278
4	59266	44	59310	230271	317	230588
5	59738	36	59774	290009	353	290362
6	59994	36	60030	350003	389	350392
7	60376	27	60403	410379	416	410795
8	60507	35	60542	470886	451	471337
9	60705	25	60730	531591	476	532067
10	60831	25	60856	592422	501	592923

TABLE 2
Number of discriminants $0 < D < 10^7$ *with* 2 *associated nonconjugate cubic fields*

Sector	Noncyclic	Cyclic	Total	Noncyclic (accum.)	Cyclic (accum.)	Total (accum.)
1	166	37	203	166	37	203
2	223	18	241	389	55	444
3	206	10	216	595	65	660
4	218	11	229	813	76	889
5	231	9	240	1044	85	1129
6	221	9	230	1265	94	1359
7	241	9	250	1506	103	1609
8	224	6	230	1730	109	1839
9	262	9	271	1992	118	2110
10	239	8	247	2231	126	2357

Table 1 gives the number of cubic fields K by sectors. We give for each sector k the number of noncyclic cubic fields, cyclic cubic fields and cubic fields with discriminant $10^6(k-1) < D < 10^6k$ and with discriminant $1 < D < 10^6k$ (accumulated). Tables 2, 3 and 4 are similar for the number of discriminants with N associated nonconjugate fields, for $N = 2$, 3 and 4, respectively.

There are five discriminants $D < 10^7$ with N associated nonconjugate fields for $N > 4$. And we have $N = 6$ for all of them. In Table 5 we have listed these discriminants, their decomposition $D = d3^{2m}T_0^2$ and the coefficients a and b of the polynomials $f(a, b, X)$ defining the six corresponding fields. Among the discriminants corresponding to noncyclic fields in Table 4, there are nine with $T > 1$; these discriminants are listed in Table 6 in a way similar to those in Table 5.

TABLE 3

Number of discriminants $0 < D < 10^7$ *with* 3 *associated nonconjugate cubic fields*

Sector	Noncyclic	Noncyclic (accum.)
1	343	343
2	468	811
3	557	1368
4	552	1920
5	568	2488
6	601	3089
7	624	3713
8	622	4335
9	582	4917
10	626	5543

TABLE 4

Number of discriminants $0 < D < 10^7$ *with* 4 *associated nonconjugate cubic fields*

Sector	Noncyclic	Cyclic	Total	Noncyclic (accum.)	Cyclic (accum.)	Total (accum.)
1	161	1	162	161	1	162
2	233	1	234	394	2	396
3	255	1	256	649	3	652
4	284	1	285	933	4	937
5	283	1	284	1216	5	1221
6	293	1	294	1509	6	1515
7	311	0	311	1820	6	1826
8	348	2	350	2168	8	2176
9	364	0	364	2532	8	2540
10	347	0	347	2879	8	2887

From Tables 4 and 6 we observe that there are 2879 discriminants $D = d$, $1 < D < 10^7$, with four associated noncyclic fields. From class field theory we can conclude that there are 2879 real quadratic fields with discriminant $d < 10^7$ whose ideal class group $H(d)$ has 3-rank equal to 2. A complete study of the $H(d)$ having 3-rank ≥ 1 for $d < 10^7$ will be given in a later paper.

5. On Davenport and Heilbronn's Densities.

The total number of nonconjugate cubic fields with discriminant less than 10^7 is 592923, giving the empirical density 0.05929. Table 1 easily permits the computation of this empirical density in each sector. Davenport and Heilbronn prove in [2] that the asymptotic value is $(12\zeta(3))^{-1} \approx 0.06933$. Thus the convergence is very slow, as was noted in [11]. In [2], Davenport and Heilbronn obtain also the asymptotic value of the density of each type of decomposition of a rational prime p in cubic fields. The values obtained for them are:

$$\begin{aligned}
1/w &\quad \text{for } p = P^3,\\
p/w &\quad \text{for } p = PQ^2,\\
p^2/3w &\quad \text{for } p = P,\\
p^2/2w &\quad \text{for } p = PQ,\\
p^2/6w &\quad \text{for } p = PQR,
\end{aligned}$$

with $w = p^2 + p + 1$.

TABLE 5

Discriminants $0 < D < 10^7$ *with* 6 *associated cubic fields*

$D = 3^{2m}T_0d$	3^{2m}	T_0	d	Coefficients of the polynomial $f(a,b,X)$	
				a	b
3054132	9	2	84837	96	134
				102	210
				150	622
				210	1122
				336	1244
				366	2674
4735476	9	2	131541	108	106
				114	210
				168	726
				252	1292
				288	1834
				648	4772
5807700	81	10	717	180	60
				270	990
				360	2460
				450	2850
				540	4740
				720	6690
6367572	81	2	19653	126	246
				342	174
				396	2994
				450	3642
				540	3852
				720	3012
9796788	81	2	30237	144	282
				216	204
				540	3204
				648	5220
				756	7794
				918	5742

Using the results of [6] and [7], we have computed the decomposition type of the rational primes p for $2 \leq p \leq 181$ in each of the 592422 noncyclic cubic fields in the table. In particular, there are 46532 noncyclic cubic fields K with $D(K) < 10^7$ having 2 as its common index divisor, i.e., with the rational prime 2 decomposing completely. We give in Tables 7, 8, 9 and 10 the empirical density of each type of decomposition by sector and its asymptotic value for $p = 2, 3, 5$ and 7, respectively. In Table 11 we give the empirical density and its asymptotic value of each type of decomposition for the primes p with $2 \leq p < 100$ in all fields in the table.

TABLE 6

Discriminants $0 < D < 10^7$ *with* 4 *associated cubic fields and* $T = 3^{2m}T_0 > 1$

$D = 3^{2m}T_0d$	3^{2m}	T_0	d	Coefficients of the polynomial $f(a,b,X)$	
				a	b
1725300	81	10	213	90	210
				180	780
				270	1530
				360	2580
2238516	81	14	141	126	462
				252	546
				252	1428
				378	2814
2891700	81	10	357	90	30
				180	660
				180	870
				360	1290
4641300	81	10	573	180	420
				270	1170
				540	1590
				540	4140
6810804	81	14	429	126	210
				378	1302
				378	2394
				504	4326
7557300	81	10	933	270	630
				450	2550
				720	660
				810	8730
7953876	81	14	501	126	42
				252	1092
				378	798
				756	7308
8250228	9	14	4677	336	1694
				630	266
				756	7924
				840	8764
8723700	81	10	1077	270	90
				450	3630
				540	3420
				900	8700

TABLE 7

Type of decomposition of the prime 2 *in the noncyclic cubic fields with discriminant* $0 < D < 10^7$ *(%)*

Sector	P^3	PQ^2	P	PQ	PQR
1	15.797	27.540	21.458	28.335	6.870
2	15.378	27.800	20.860	28.385	7.577
3	15.173	27.996	20.612	28.510	7.709
4	15.167	27.824	20.590	28.504	7.915
5	15.211	28.004	20.459	28.412	7.913
6	15.048	28.014	20.467	28.443	8.027
7	15.115	28.028	20.412	28.429	8.016
8	15.038	28.023	20.379	28.471	8.088
9	14.900	28.153	20.331	28.446	8.171
10	15.163	27.951	20.210	28.532	8.144
All Table	15.192	27.938	20.567	28.448	7.855
Theoretical	14.286	28.571	19.048	28.571	9.524

TABLE 8

Type of decomposition of the prime 3 *in the noncyclic cubic fields with discriminant* $0 < D < 10^7$ *(%)*

Sector	P^3	PQ^2	P	PQ	PQR
1	8.416	22.257	25.988	34.718	8.620
2	8.154	22.447	25.271	34.694	9.435
3	8.162	22.493	25.038	34.683	9.625
4	8.060	22.546	24.943	34.683	9.768
5	8.151	22.661	24.842	34.584	9 763
6	8.082	22.612	24.746	34.710	9.849
7	8.109	22.658	24.710	34.469	10.054
8	8.055	22.538	24.663	34.768	9 976
9	7.881	22.652	24.659	34.816	9.993
10	8.162	22.628	24.458	34.670	10.082
All Table	8.120	22.553	24.919	34.679	9.729
Theoretical	7.692	23.077	23.077	34.615	11.538

TABLE 9

Type of decomposition of the prime 5 *in the noncyclic cubic fields with discriminant* $0 < D < 10^7$ *(%)*

Sector	P^3	PQ^2	P	PQ	PQR
1	3.477	15.373	30.148	40.558	10.444
2	3.415	15.650	29.230	40.533	11.172
3	3.375	15.702	29.103	40.478	11.341
4	3.390	15.665	28.821	40.487	11.637
5	3.296	15.797	28.851	40.552	11.504
6	3.434	15.752	28.676	40.387	11.751
7	3.379	15.793	28.728	40.402	11.698
8	3.342	15.785	28.641	40.384	11.848
9	3.311	15.673	28.587	40.552	11.877
10	3.362	15.869	28.558	40.307	11.905
All Table	3.377	15.709	28.920	40.463	11.531
Theoretical	3.226	16.129	26.882	40.323	13.441

TABLE 10

Type of decomposition of the prime 7 in the noncyclic cubic fields with discriminant $0 < D < 10^7$ *(%)*

Sector	P^3	PQ^2	P	PQ	PQR
1	1.859	11.712	31.992	43.148	11.289
2	1.784	11.873	30.967	43.341	12.034
3	1.829	11.955	30.869	42.992	12.355
4	1.794	11.863	30.675	43.366	12.302
5	1.863	11.868	30.587	43.053	12.628
6	1.784	12.010	30.656	42.984	12.566
7	1.847	11.953	30.555	43.035	12.609
8	1.778	12.051	30.134	43.393	12.643
9	1.817	11.931	30.503	43.071	12.678
10	1.863	11.843	30.513	42.942	12.840
All Table	1.822	11.908	30.731	43.131	12.408
Theoretical	1.754	12.281	28.655	42.982	14.327

TABLE 11

Type of decomposition of the rational primes $p < 100$ *in the noncyclic cubic fields with discriminant* $0 < D < 10^7$ *(%)*

Prime	P^3		PQ^2		P		PQ		PQR	
	Empirical	Theore-tical	Empirical	Theore-tical	Empirical	Theore-tical	Empirical	Theore-tical	Empirical	Theore-tical
2	15.192	14.286	27.938	28.571	20.567	19.048	28.448	28.571	7.855	9.524
3	8.120	7.692	22.553	23.077	24.919	23.077	34.679	34.615	9.729	11.538
5	3.377	3.226	15.709	16.129	28.920	26.882	40.463	40.323	11.531	13.441
7	1.822	1.754	11.908	12.281	30.731	28.655	43.131	42.982	12.408	14.327
11	0.776	0.752	8.015	8.271	32.300	30.326	45.628	45.489	13.280	15.163
13	0.559	0.546	6.893	7.104	32.705	30.783	46.286	46.175	13.558	15.392
17	0.332	0.326	5.359	5.537	33.218	31 379	47.158	47.068	13.933	15.689
19	0.265	0.262	4.822	4.987	33.391	31.584	47.473	47.375	14.049	15.792
23	0.188	0.181	4.017	4.159	33.614	31.887	47.900	47.830	14.281	15.943
29	0.120	0.115	3.216	3.330	33.811	32.185	48.340	48.278	14.512	16.093
31	0.102	0.101	2.996	3.122	33.893	32.259	48.429	48.389	14.580	16.130
37	0.069	0.071	2.536	2.630	34.017	32.433	48.686	48.650	14.693	16.217
41	0.063	0.058	2.310	2.380	34.022	32.521	48.824	48.781	14.783	16.260
43	0.051	0.053	2.209	2.272	34.057	32.559	48.863	48.838	14.819	16.279
47	0.043	0.044	2.008	2.082	34.119	32.624	48.926	48.937	14.904	16.312
53	0 037	0.035	1.798	1.851	34.104	32.705	49.078	49.057	14.984	16.352
59	0.028	0.028	1.627	1.666	34.229	32.769	49.065	49.153	15.051	16.384
61	0.025	0.026	1.580	1.612	34.161	32.787	49.158	49.181	15.077	16.394
67	0.021	0.022	1.433	1.470	34.211	32.836	49.203	49.254	15.132	16.418
71	0.021	0.020	1.335	1.389	34.108	32.864	49.403	49.296	15.132	16.432
73	0.018	0.019	1.308	1.351	34.181	32.877	49.313	49.315	15.179	16.438
79	0.015	0.016	1.196	1.250	34.227	32.911	49 338	49 367	15.224	16.456
83	0.015	0.014	1.148	1.190	34.212	32.932	49 390	49.398	15.234	16.466
89	0.013	0.012	1 080	1.111	34.202	32.959	49.416	49.438	15.289	16.479
97	0.013	0 011	0.989	1.020	34.257	32.990	49.400	49.485	15.340	16.495

Departamento de Matemática Aplicada
Edificio Matemáticas, Planta 1
Universitad de Zaragoza
50009 Zaragoza, Spain

Departament de Matemàtiques
Facultat d'Informàtica de Barcelona
Universitat Politècnica de Catalunya
Pau Gargallo,5
08028 Barcelona, Spain

1. I. O. ANGELL, "A table of totally real cubic fields," *Math. Comp.*, v. 30, 1976, pp. 184–187.

→ 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.

3. B. N. DELONE & D. K. FADDEEV, *The Theory of Irrationalities of the Third Degree*, Trudy Mat. Inst. Steklov., vol. 11, 1940; English transl., Transl. Math. Monographs, vol. 10, Amer. Math. Soc., Providence, R.I., Second Printing 1978.

4. V. ENNOLA & R. TURUNEN, "On totally real cubic fields," *Math. Comp.*, v. 44, 1985, pp. 495–518.

5. H. J. GOODWIN & P. A. SAMET, "A table of real cubic fields," *J. London Math. Soc.*, v. 34, 1959, pp. 108–110.

6. P. LLORENTE, "Cubic irreducible polynomials in $\mathbf{Z}_p[X]$ and the decomposition of rational primes in a cubic field," *Publ. Sec. Mat. Univ. Autònoma Barcelona*, v. 27, n. 3, 1983, pp. 5–17.

7. P. LLORENTE & E. NART, "Effective determination of the decomposition of the rational primes in a cubic field," *Proc. Amer. Math. Soc.*, v. 87, 1983, pp. 579–585.

8. P. LLORENTE & A. V. ONETO, "Cuerpos cubicos," *Cursos, Seminarios y Tesis del PEAM*, n. 5, Univ. Zulia, Maracaibo, Venezuela, 1980.

9. P. LLORENTE & A. V. ONETO, "On the real cubic fields," *Math. Comp.*, v. 39, 1982, pp. 689–692.

10. M. SCHERING, "Théorèmes relatifs aux formes binaires quadratiques qui représentent les mêmes nombres," *Jour. de Math.* (2), v. 4, 1859, pp. 253–270.

11. D. SHANKS, Review of I. O. Angell, "A table of totally real cubic fields," *Math. Comp.*, v. 30, 1976, pp. 670–673.