

## A FAST ALGORITHM TO COMPUTE CUBIC FIELDS

K. BELABAS

ABSTRACT. We present a very fast algorithm to build up tables of cubic fields. Real cubic fields with discriminant up to  $10^{11}$  and complex cubic fields down to  $-10^{11}$  have been computed.

The classification of quadratic fields up to isomorphism is trivial: they are uniquely characterized by their discriminant, and we can compute tables as soon as we know how to test if an integer is squarefree and how to check some simple congruence modulo 16. We intend to show that *cubic* fields are essentially as easy to deal with, and we will get a canonical representation for them. Contrary to the quadratic case, the treatment depends on the signature but, the fundamental ideas being the same, we shall expose as much as we can before splitting cases.

Almost all results in this paper are either ancient or elementary. I would like to thank Professor H. Cohen for his interest when I first mentioned what I thought was a trivial application of some well known results. Moreover, his careful reading of successive drafts of this work and the many questions he had about it were most helpful in giving it its present shape.

### 1. PRELIMINARIES

Let  $(a, b, c, d)$  denote the integral binary cubic form  $F(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ . We call as usual  $\text{disc}(F)$  its discriminant:

$$\text{disc}(a, b, c, d) = b^2c^2 - 27a^2d^2 + 18abcd - 4ac^3 - 4b^3d .$$

We shall say a form  $F$  is *complex* whenever  $\text{disc } F < 0$ , and *real* otherwise. We call *roots* of  $F$ , the complex roots of  $F(X, 1) = 0$ .

A form is said to be primitive if  $\text{gcd}(a, b, c, d) = 1$ , and irreducible if it is so in  $\mathbb{Q}[x, y]$ . The usual change of variables gives an action of  $\text{GL}_2(\mathbb{Z})$  on the set of binary cubic forms, which preserves discriminants, irreducibility and primitivity. We call  $\Phi$  the set of classes of integral, binary cubic forms under this action. Please note that, contrary to the quadratic case, we do not restrict to  $\text{SL}_2(\mathbb{Z})$ .

Let  $V_p$  be the subset of  $\Phi$  given by the following congruence conditions:

- If  $p = 2$ :  $\text{disc } F \equiv 1 \pmod{4}$  or  $\text{disc } F \equiv 8, 12 \pmod{16}$ .
- If  $p \neq 2$ :  $p^2 \nmid \text{disc } F$ .

So that forms in  $V = \bigcap V_p$  have fundamental discriminants (we call an integer  $\Delta$  a fundamental discriminant either if  $\Delta = 1$  or if it is the discriminant of a quadratic field). Now we put  $U = \bigcap U_p$ , where  $U_p \subset \Phi$  is given by:  $F \in U_p$  if

---

Received by the editor February 2, 1996 and, in revised form, June 5, 1996.  
1991 *Mathematics Subject Classification*. Primary 11R16, 11Y40.  
*Key words and phrases*. Cubic fields, computations.

- it belongs to  $V_p$ , or
- it factors as  $\lambda(\alpha x + \beta y)^3$  modulo  $p$ , with  $\lambda \in \mathbb{F}_p^*$ , and  $\alpha, \beta$  in  $\mathbb{F}_p$  not both zero. Furthermore, there exists an  $e \in \mathbb{F}_p^*$  such that the equation

$$F(x, y) \equiv ep \pmod{p^2}$$

has a solution in  $x, y \in \mathbb{Z}/p^2\mathbb{Z}$ .

Let  $C$  denote the set of non-isomorphic cubic extensions of  $\mathbb{Q}$ . Given  $K \in C$  and  $x \in K$ , we call  $\mathfrak{d}(x)$  the discriminant of the minimal polynomial of  $x$ , and denote by  $x, x', x''$  the three conjugates of  $x$  in  $\overline{K}$ . Now put

$$F_K(x, y) = \frac{\text{Norm}[(\alpha - \alpha')x - (\beta - \beta')y]}{\sqrt{\mathfrak{d}_K}} = \sqrt{\frac{\mathfrak{d}(\alpha x - \beta y)}{\mathfrak{d}_K}},$$

where  $[1, \alpha, \beta]$  is any  $\mathbb{Z}$ -basis of the maximal order of  $K$  whose first element is 1, and  $\mathfrak{d}_K$  is its absolute discriminant.

The key ingredient is the following result establishing the link between cubic forms and fields:

**Theorem 1.1** (Davenport-Heilbronn [6]). *Consider the following maps:*

$$\begin{aligned} \varphi_{CU} &: \text{conjugacy class of } K &\longrightarrow & \text{class of } F_K(x, y) \\ \varphi_{UC} &: \{\mathbb{Q}(\theta_1), \mathbb{Q}(\theta_2), \mathbb{Q}(\theta_3)\} &\longleftarrow & \text{class of } F(x, y) \end{aligned}$$

where the  $\theta_i$  are the zeros of  $F(\theta, 1) = 0$ . These are well defined inverse maps, and induce a discriminant preserving bijection between the sets  $U$  and  $C$ .

This rather abstract statement has a very nice algorithmic translation. First, reduction theory enables us to efficiently single out a *canonical* representative in each equivalence class of irreducible cubic forms. We shall discuss this in great detail in §3 (positive discriminants) and §4 (negative discriminants). We will call such forms *reduced* in the sequel. For the time being, we only need to know that if  $F = (a, b, c, d)$  is reduced, then any reduced form equivalent to  $F$  is equal to  $F$  (see Corollary 3.3 and Lemma 4.3). Hence, to a given field, we can associate a unique companion form. And second, we shall see that, as their names imply, the reduced forms have rather small coefficients, bounded in terms of their discriminant.

Denote by  $H_F$  the Hessian form associated to  $F$ :

$$H_F = -\frac{1}{4} \begin{vmatrix} \frac{\partial^2 F}{\partial x \partial x} & \frac{\partial^2 F}{\partial x \partial y} \\ \frac{\partial^2 F}{\partial x \partial y} & \frac{\partial^2 F}{\partial y \partial y} \end{vmatrix} = Px^2 + Qxy + Ry^2,$$

where

$$P = b^2 - 3ac, \quad Q = bc - 9ad, \quad \text{and} \quad R = c^2 - 3bd.$$

One can easily see that the Hessian is covariant with respect to  $\text{GL}_2(\mathbb{Z})$ : we have  $H_{F \circ M} = H_F \circ M$  for all  $M \in \text{GL}_2(\mathbb{Z})$ . Moreover, a simple calculation shows that  $\text{disc } H_F = -3 \text{ disc } F$ .

We summarize in the next lemma the elementary properties of the set  $U$ , which enable us to test easily whether a given form is associated to a cubic field or not.

**Lemma 1.2.** *Let  $F = (a, b, c, d)$  be a cubic primitive form, and  $(P, Q, R)$  its Hessian. We write  $(F, p) = (1^3)$  whenever, up to a scalar factor,  $F$  is a cube modulo  $p$ .*

1.  $(F, p) = (1^3)$  if and only if  $p \mid \gcd(P, Q, R)$ .
2. If  $(F, p) = (1^3)$  and  $p \neq 3$ , then  $F \in U_p$  if and only if  $p^3 \nmid \text{disc}(F)$ .
3. If  $F \in U_3$ , then  $3^6 \nmid \text{disc}(F)$ .
4. If  $(F, 3) = (1^3)$ , the analogue of part 2. is completely described by the following algorithm :

$$\begin{aligned} & \text{if } 3 \mid a, & F \in U_3 & \iff 9 \nmid a \text{ and } 3 \nmid d, \\ & \text{else if } 3 \mid d, & F \in U_3 & \iff 9 \nmid d, \\ & \text{else if } 3 \mid (a - d), & F \in U_3 & \iff a - b + c - d \equiv 0 \pmod{9}, \\ & \text{else if } 3 \mid (a + d), & F \in U_3 & \iff a + b + c + d \equiv 0 \pmod{9}. \end{aligned}$$

5. If a reduced form  $F$  belongs to  $U$ , then it is irreducible.

*Proof.*

- 1. One first notes that  $p$  divides  $\text{disc}(F)$  if and only if  $(F, p) = (1^2 1)$  or  $(1^3)$ , with evident notations. This is clear when the point at infinity is one of the roots, i.e.  $F(x, 1)$  has degree at most two, so we suppose this is not the case. As the finite field  $\mathbb{F}_p$  is perfect,  $\text{disc } F \equiv 0 \pmod{p}$  implies that  $F$  is reducible modulo  $p$ , two of the roots in  $\overline{\mathbb{F}}_p$  being equal. As the sum of the roots is in  $\mathbb{F}_p$ , they all are (if  $p = 2$ , one uses their product instead).

If  $F$  splits as

$$F(x, y) \equiv (\alpha x + \beta y)^2(\gamma x + \delta y) \pmod{p},$$

one finds that  $H(x, y) \equiv (\alpha x + \beta y)^2(\alpha\delta - \beta\gamma)^2 \pmod{p}$ . As  $F$  is primitive,  $\alpha$  and  $\beta$  are not both zero modulo  $p$ , thus

$$H(x, y) \equiv 0 \pmod{p} \iff \alpha\delta - \beta\gamma \equiv 0 \pmod{p} \iff (F, p) = (1^3).$$

- 2. and 3. are exactly [6, Lemma 6]. Replacing  $F$  by an equivalent form, we can write  $F = (a, b, c, d)$ , with  $F \equiv ax^3 \pmod{p}$ . So  $\text{disc } F = -27a^2d^2$  modulo  $p^3$ . The form  $F$  is primitive, thus  $p \nmid a$ , and as  $p \neq 3$ ,  $p^3 \mid \text{disc } F$  is equivalent to  $p^2 \mid d$ . Now  $F(x, y) \equiv ep \pmod{p^2}$  implies that  $p$  divides  $x$ , thus  $F(x, y) \equiv dy^3 \pmod{p^2}$  and our claim follows. The case  $p = 3$  is left to the reader.
- 4. is trivial once one remarks that 3 must divide  $b$  and  $c$  and thus  $F(x, y)$  only depends on  $(x, y)$  modulo 3.
- 5. This last assertion will be proven later (Corollary 3.3 and Lemma 4.3).  $\square$

We can now propose an efficient algorithm to test if a given cubic form is in the image of the Davenport-Heilbronn map:

**Algorithm 1.3.**

Input: a cubic form  $F = (a, b, c, d)$ .

Output: **true** if and only if  $F$  corresponds to a cubic field.

1. If  $F$  is not reduced, **false**.
2. If  $F$  is not primitive, **false**.
3. Compute  $(P, Q, R)$ , the Hessian of  $F$ . Set  $D = 4PR - Q^2 = 3 \text{disc}(F)$  and  $f_H = \gcd(P, Q, R)$ . Check whether  $F$  belongs to  $U_2$  and  $U_3$ , else **false**.
4. If  $p^2 \mid f_H$  with  $p > 3$ , **false**.
5. Set  $t = D/f_H^2$ . Remove all powers of 2 and 3 from  $t$ : at most  $2^3$  and  $3^2$ . If  $\gcd(t, f_H) > 1$ , **false**.
6. If  $t$  is squarefree, **true**, else **false**.

*Proof.* We have to check that  $F$  is primitive, reduced, and belongs to  $U_p$  for all  $p$ , which implies it is irreducible. Steps 1 to 3 are straightforward, and we only have to check that a form satisfying steps 4 to 6 belongs to  $U_p$ , for all  $p \geq 5$ .

The prime divisors of  $f_H$  are exactly the ones for which  $(F, p) = (1^3)$ . For all of them we check in steps 4 and 5 whether  $p^3$  divides  $\text{disc } F$  or not. Finally, in step 6, we check the other prime divisors of  $\text{disc } F$ ,  $p \geq 5$ :  $F$  must belong to  $V_p$  for all of them, which is the case if and only if  $t$  is squarefree.  $\square$

*Remark 1.4.* Step 2 is only necessary, as an “early-abort” strategy: if a prime  $p$  divides all the coefficients of  $F$ , then  $p^2 | f_H$  and step 3 (if  $p = 2, 3$ ) or 4 (if  $p > 3$ ) would **false** just as well. *On average*, if one uses the techniques described hereafter, this step *slows down* the algorithm.

*Remark 1.5.* There is a real problem lying in steps 4 and 6. Squarefree factorization of integers is presently as difficult as complete factorization, so we need to factor  $f_H$  and  $t$  and check all prime divisors for greater than one valuation. But our aim here is to compute *tables* of fields and, calling  $X$  the discriminant bound, we will need to factor  $X$  discriminants of size about  $X$ , which is not acceptable. We shall see in §5 that simple hashing techniques reduce this to a sensible amount.

The discriminant of a cubic field  $K$  can be uniquely factored as  $f^2\Delta$ , where  $\Delta$  is a fundamental discriminant. The  $f_H$  appearing in step 3 of the algorithm is closely related to this one: it is known that a prime  $p$  is totally ramified in  $K$  if and only if  $p$  divides  $f$  (see [8]). Lemma 1.2 and Proposition 2.2 imply that this is equivalent to  $p | f_H$ . Thus  $f$  and  $f_H$  have the same prime divisors, but they may differ by a factor 3, if  $3 | \Delta$ . The precise result is as follows:

**Lemma 1.6.** *Let  $K$  be a cubic field,  $F_K$  its companion reduced cubic form, and  $\Delta f^2$  their common discriminant. Let  $(P, Q, R)$  be the Hessian of  $F_K$ , call  $f_H$  its content and put  $(P, Q, R) = f_H(P_1, Q_1, R_1)$ , where  $(P_1, Q_1, R_1)$  is primitive. We have  $f_H = f$  if and only if  $-\frac{1}{3}(Q_1^2 - 4P_1R_1)$  is fundamental, and  $f_H = 3f$  otherwise. The latter only happens when 3 divides both  $f$  and  $\Delta$ . It always happens when  $v_3(f) = 1$ .*

*Proof.* Straightforward given the preceding discussion, except for the prime 3. Lemma 1.2 tells us that  $3^3 \nmid f$ , and an easy computation shows that  $3 | f_H$  if and only if  $9 | f_H$ . Now write that

$$f_H^2(Q_1^2 - 4P_1R_1) = -3\Delta f^2 \quad ,$$

and compare the valuations at 3.  $\square$

## 2. PROPERTIES OF THE DAVENPORT-HEILBRONN CUBIC FORM

First and foremost, adjoining a root of  $F(X, 1)$  to  $\mathbb{Q}$  yields a representative of the class of cubic fields associated to  $F$ , in the sense of Theorem 1.1. But what we want to stress here is the ease with which one recovers the simple invariants associated to  $K$  from  $F_K$ .

**Proposition 2.1.** *Let  $F_K = (a, b, c, d)$  be a representative of the class of cubic forms associated to the cubic field  $K$  by the Davenport-Heilbronn bijection. For instance, the reduced one.*

1. *We have  $\text{disc } K = \text{disc } F_K$ .*

2. If  $\theta$  is a root of  $F_K$  belonging to  $K$ , then  $[1, a\theta, a\theta^2 + b\theta]$  is a basis of the maximal order  $\mathbb{Z}_K$ .

*Proof.* 1. is part of the Davenport-Heilbronn theorem, and can be easily checked from the definition of  $F_K$  anyway.

As for 2, we use an idea attributed to H. Lenstra by H. Cohen [3, Exercise 15, p. 216]. Let  $\theta$  be an algebraic number, and  $P(X) = a_0X^n + a_1X^{n-1} + \dots + a_n$  be its minimal primitive polynomial, with integral coefficients. One defines

$$\mathbb{Z}_\theta = \mathbb{Z}[a_0\theta, a_0\theta^2 + a_1\theta, \dots, a_0\theta^{n-1} + \dots + a_{n-2}\theta] .$$

Then  $\mathbb{Z}_\theta$  is easily seen to be an algebra of finite type over  $\mathbb{Z}$ , and thus is an order in  $\mathbb{Z}_K$ . Now, if we denote the roots of  $P$  by  $\theta_1, \dots, \theta_n$ , then a Vandermonde-type calculation gives

$$\text{disc } \mathbb{Z}_\theta = a_0^{2n-2} \prod_{i \neq j} (\theta_i - \theta_j) = \text{disc } P .$$

Here, we have  $\text{disc } F_K = \text{disc } K$ , so  $\mathbb{Z}_\theta = \mathbb{Z}_K$ . □

The next proposition is an algorithmic restatement of [6, Lemma 11]:

**Proposition 2.2.** *Call  $\theta$  a root of  $F_K$  belonging to  $K$ . A prime  $p \in \mathbb{Z}$  decomposes in  $K$  as  $F_K = (a, b, c, d)$  factors in  $\mathbb{F}_p[X, Y]$ . More precisely, if we take an irreducible decomposition*

$$F_K(X, Y) \equiv \prod_i T_i^{e_i}(X, Y) \pmod{p} ,$$

we have

$$p\mathbb{Z}_K = \prod_i \mathfrak{p}_i^{e_i}, \quad \text{with } \mathfrak{p}_i \text{ prime in } \mathbb{Z}_K .$$

Moreover, we can take:

- If  $p \nmid a$ , then

$$\mathfrak{p}_i = p\mathbb{Z} + T_i(\theta, 1)\mathbb{Z}_K .$$

- If  $p|a$  but  $p \nmid d$ , then

$$\mathfrak{p}_i = p\mathbb{Z} + T_i(\theta, 1)/\theta^{\deg T_i} \mathbb{Z}_K .$$

- If  $p|a$  and  $p|d$ , but  $p \neq 2$  or  $F(X, Y) \not\equiv XY(X + Y) \pmod{2}$ , there exists  $u \in \mathbb{Z}$  such that  $u \not\equiv 0 \pmod{p}$ , and, in the case  $p \nmid c$ ,  $u \not\equiv -b/c \pmod{p}$ . Then we take:

$$\mathfrak{p}_i = p\mathbb{Z} + T_i(\theta, 1)/(1 - u\theta)^{\deg T_i} \mathbb{Z}_K .$$

- Finally, if  $p = 2$  and  $F(X, Y) \equiv XY(X + Y) \pmod{2}$ , then  $2\mathbb{Z}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ , with

$$\mathfrak{p}_1 = 2\mathbb{Z}_K + a\theta\mathbb{Z}_K, \quad \mathfrak{p}_2 = 2\mathbb{Z}_K + (a\theta^2 + b\theta + 1)\mathbb{Z}_K \quad \text{and}$$

$$\mathfrak{p}_3 = 2\mathbb{Z}_K + (a\theta^2 + (a + b)\theta)\mathbb{Z}_K .$$

*Proof.*

1. We suppose first that  $p \nmid a$  and consider

$$f(X) = a^2 F(X/a, 1) = (1, b, ac, a^2 d) .$$

It is a monic irreducible integral polynomial with a root  $\alpha$  in  $K$ . Localizing at  $\mathfrak{p}$  above  $p$  in  $\mathbb{Z}_K$ , we find that  $\alpha$  generates  $\mathbb{Z}_{K,\mathfrak{p}}$  over  $\mathbb{Z}_{(p)}$ . Indeed  $\mathbb{Z}[\alpha] \subset \mathbb{Z}_K$  and

$$\text{disc}(\mathbb{Z}[\alpha]/\mathbb{Z}) = a^2 \text{disc}(\mathbb{Z}_K/\mathbb{Z})$$

with  $\text{gcd}(a, p) = 1$ . Thus, if  $f(X) = \prod U_i^{e_i}(X)$ , we get

$$p\mathbb{Z}_K = \prod \mathfrak{p}_i^{e_i}, \quad \text{with } \mathfrak{p}_i = p\mathbb{Z}_K + U_i(\alpha)\mathbb{Z}_K .$$

Now, we can take  $\alpha = a\theta$  and  $T_i(X, Y) = \varepsilon Y^{\deg U_i} U_i(aX/Y)$ , with  $\varepsilon \in \mathbb{F}_p^*$ . Hence, we have

$$\mathfrak{p}_i = p\mathbb{Z}_K + T_i(\theta, 1)\mathbb{Z}_K .$$

2. When this is not the case, we look for an  $M \in \text{GL}_2(\mathbb{Z})$  such that we can apply 1. to  $F \circ M$ . If  $p \nmid d$ , we take

$$M = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} ,$$

else  $F$  has at most one non-zero root  $\alpha$  in  $\mathbb{F}_p$ . If we are not in the last special case of the theorem, there exists  $u \in \mathbb{F}_p^*$ ,  $u^{-1} \neq \alpha$ , so that  $F(1, u)$  is not  $0 \pmod p$ . Then we take

$$M = \begin{pmatrix} 1 & 0 \\ u & 1 \end{pmatrix} .$$

As  $F(1, u)$  is exactly the coefficient of  $x^3$  in  $G = F \circ M$ , we are back to the preceding case. Of course,  $G$  is not reduced anymore, but still generates the field  $K$ .

3. In the last case,  $p$  divides the coefficient of  $x^3$  in all forms equivalent to  $F_K$ . Thus, from the definition of  $F_K$ ,  $p^2 \mathfrak{d}_K | \mathfrak{d}(x)$  for all  $x \in \mathbb{Z}_K$ . This makes of  $p$  a “non-essential divisor” which, in our cubic setting, happens if and only if  $p$  equals 2 and is totally split in  $K/\mathbb{Q}$  (see [9]). As 2 is unramified,  $\text{disc } F_K = \text{disc } K$  is odd. We know as well that  $2|a$  and  $2|d$ , so finally, we get  $a \equiv d \equiv 0 \pmod 2$ ,  $b \equiv c \equiv 1 \pmod 2$ , and  $F_K$  still factors as  $p$ .

To find an explicit decomposition, one has to split the étale algebra

$$\mathbb{A} = \mathbb{Z}_K/2\mathbb{Z}_K \approx (\mathbb{Z}/2\mathbb{Z})^3$$

whose elements are all idempotents. Now, if we put  $e_1 = 1$ ,  $e_2 = a\theta$ ,  $e_3 = a\theta^2 + b\theta$ , we find  $e_2 e_3 = a^2 \theta^3 + ab\theta^2 = -ac\theta - ad = a\theta = e_2$  in  $\mathbb{A}$ , as  $a\theta \in \mathbb{Z}_K$  and  $c \equiv 1 \pmod 2$ ,  $ad \equiv 0 \pmod 2$ .

So  $e_2, e_1 + e_3$ , and  $e_2 + e_3$  are the orthogonal idempotents giving the three factors. □

### 3. REAL CUBIC FIELDS

If  $F$  is a class of positive discriminant, then  $\text{disc}(H_F)$  is negative. It is well known that there is a nice reduction theory for definite binary quadratic forms. Recall that the Hessian is covariant with respect to the action of  $\text{GL}_2(\mathbb{Z})$ . We shall get a canonical representative for  $F$  by specifying that its Hessian should be a

reduced quadratic form, with some extra care for those forms lying on the boundary of the fundamental domain. This approach was initiated by Hermite, see [10, 11].

We call a quadratic form with real coefficients  $(P, Q, R)$  reduced if

$$|Q| \leq P \leq R,$$

and  $R > 0$  to exclude the trivial form. Beware that this is not exactly the standard notion. For instance our definition implies that  $(1, -1, 1)$  is reduced, as well as  $(0, 0, 1)$ ! If  $H = (P, Q, R)$  is a definite binary quadratic form, we call  $H^{-1}$  the quadratic form  $(P, -Q, R)$  and  $\text{Aut}(H)$  the set of matrix in  $\text{GL}_2(\mathbb{Z})$  stabilizing  $H$ . Furthermore, we set

$$\sigma = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

**Lemma 3.1.** *Let  $H = (P, Q, R)$  and  $H' = (P', Q', R')$  be two reduced definite binary quadratic forms, such that there exists  $M \in \text{GL}_2(\mathbb{Z})$  with  $H \circ M = H'$ . Then, either  $H' = H$  and  $M \in \text{Aut}(H)$ , or  $H' = H^{-1}$  and  $M$  belongs to  $\text{Aut}(H)\sigma$ . Moreover, the only elements of  $\text{Aut}(H)$  are  $\pm \text{Id}$ , except in the following special cases, which can occur simultaneously:*

- If  $P = R$ ,  $\text{add } \pm \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ .
- If  $Q = 0$ ,  $\text{add } \pm \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ .
- If  $P = R$  and  $Q = 0$ ,  $\text{add } \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ .
- If  $P = \varepsilon Q$ ,  $\text{add } \pm \begin{pmatrix} 1 & \varepsilon \\ 0 & -1 \end{pmatrix}$ .
- If  $P = \varepsilon Q = R$ ,  $\text{add } \pm \begin{pmatrix} -1 & 0 \\ \varepsilon & 1 \end{pmatrix}, \pm \begin{pmatrix} 0 & -1 \\ 1 & \varepsilon \end{pmatrix}, \pm \begin{pmatrix} \varepsilon & 1 \\ -1 & 0 \end{pmatrix}$ ,

where, in the last two cases,  $\varepsilon$  is either 1 or  $-1$ .

*Proof.* Being equivalent,  $H$  and  $H'$  represent the same numbers and share the same discriminant. As they are reduced, their first and last coefficients respectively correspond to their minimum over  $\mathbb{Z}^2 - \{(0, 0)\}$  and their next minimal value. Thus they are equal. Equality of discriminants then yield  $Q^2 = Q'^2$ . Hence  $H' = H$  or  $H' = H^{-1} = H \circ \sigma$ , and we only need to compute  $\text{Aut}(H)$ .

We call as usual  $S$  and  $T$  the following two generators of the modular group:

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

and let

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

be an automorphism of  $(P, Q, R)$ . We call  $\mathcal{F}$  the usual fundamental domain for  $\text{SL}_2(\mathbb{Z})$  in Poincaré's half-plane. If  $M \in \text{PSL}_2(\mathbb{Z})$ , it fixes a point in  $\mathcal{F}$ , and so is either  $\text{Id}$ ,  $S$  if  $H = (P, 0, P)$ ,  $ST$  or  $(ST)^2$  if  $H = (P, P, P)$ ,  $TS$  or  $(TS)^2$  if  $H = (P, -P, P)$ .

If  $\det M = -1$ , then  $M$  swaps the two complex roots  $\tau$  and  $\bar{\tau}$  of  $H$ . That is

$$\frac{a\tau + b}{c\tau + d} = \bar{\tau} \Rightarrow a\tau + b = c\tau\bar{\tau} + d\bar{\tau}.$$

Taking imaginary parts, we get  $a = -d$  and then  $bP = aQ + cR$ , the determinant value giving  $a^2 + bc = 1$ . Putting things together we get:  $H(a, c) = P$ . On the other hand,  $H(a, c) \geq (P - |Q| + R) \min(a^2, c^2)$ , and, as  $H$  is reduced, we have  $|Q| \leq P \leq R$ . It follows:

- If  $ac \neq 0$ , then  $a^2 = c^2 = 1$  and  $P = |Q| = R$ . We have  $a = -d = \pm 1$  and  $b = 0$ . If  $P = \varepsilon Q$ , we have  $a = -\varepsilon c$ , where  $\varepsilon = \pm 1$ .
- If  $c = 0$ , then  $a^2 = 1$ , and  $bP = aQ$ . This implies either  $b = 0$ ,  $Q = 0$ , or  $b = \varepsilon a$ ,  $P = \varepsilon Q$ , with  $\varepsilon = \pm 1$ .
- If  $a = 0$ , then  $Rc^2 = P$ , so  $R = P$ ,  $c^2 = 1$ . We deduce  $b = c = \pm 1$ ,  $a = d = 0$ , which concludes our proof.  $\square$

**Definition 3.2.** A binary integral cubic form  $F = (a, b, c, d)$  of *positive* discriminant is called *reduced* whenever its Hessian  $(P, Q, R)$  is so and

- $a > 0$ ,  $b \geq 0$ , where  $d < 0$  whenever  $b = 0$ .
- If  $Q = 0$ ,  $d < 0$ .
- If  $P = Q$ ,  $b < |3a - b|$ .
- If  $P = R$ ,  $a \leq |d|$ , and  $b < |c|$  whenever  $|d| = a$ .

It then comes as no surprise that:

**Corollary 3.3.**

1. *Two equivalent reduced real cubic forms are equal.*
2. *A reduced real cubic form belonging to  $U$  is irreducible.*
3. *Any irreducible real cubic form is equivalent to a unique reduced one.*

*Proof.*

1. Tedious but straightforward: as their Hessians are equal, or inverse of one another, one only needs to check the possible automorphisms as listed in Lemma 3.1. Some side notes though: it is well known that the automorphisms of positive determinant of a quadratic form correspond to units in the quadratic field defined by its discriminant. These in turn act on the cubic form according to the *cube* of the unit. Thus  $TS$  and  $(TS)^2$ , which correspond to cube roots of unity, act trivially on any cubic form. A brute force calculation readily confirms this anyway. Also,  $P = Q = R$ , resp.  $P = -Q = R$ , if and only if  $F$  is of the form  $(a, b, b - 3a, -a)$ , resp.  $(a, b, -b - 3a, a)$ .
2. Suppose  $F$  is reducible. Then there exists a form  $G = (a, b, c, d)$  equivalent to  $F$ , with  $a = 0$ ,  $b \geq 0$ , and  $0 \leq c \leq b$ , which of course belongs also to  $U$ . We are going to show that the Hessian of this last form is reduced; checking its automorphisms will then lead us to a contradiction. We compute the discriminant of  $G$ ,  $\Delta = b^2c^2 - 4b^3d$ , and its Hessian

$$(P, Q, R) = (b^2, bc, c^2 - 3bd) .$$

We see that  $b^2|\Delta$ , thus for all odd primes  $p$  dividing  $b$ , we have  $p|\gcd(P, Q, R)$  by Lemma 1.2/1. So  $p$  divides  $(c^2 - 3bd)$  and  $b$ , hence  $p|c$ , and  $p^3|\Delta$ . We must then have  $p = 3$  by Lemma 1.2/2. But  $9|a$  so  $G$  cannot belong to  $U_3 \setminus V_3$ , thus  $3 \nmid b$ .

Now, if  $2|b$ , then  $\Delta \equiv b^2c^2 \pmod{16}$  thus  $G$  does not belong to  $V_2$ . We must then have  $2|c$ , hence  $16|\Delta$ , which is absurd. Moreover,  $b \neq 0$  else  $\Delta = 0$  and  $G$  does not belong to  $U_p$ , for all  $p$ . Thus  $b = 1$ , and  $c = 0$  or  $c = 1$ . It follows that the Hessian of  $(a, b, c, d)$  is either  $(1, 1, 1 - 3d)$  or  $(1, 0, -3d)$ . But  $\Delta = c^2 - 4d > 0$ , so  $d \leq -1$  and thus both  $1 - 3d$  and  $-3d$  are greater than 1. Thus both our possible Hessians are reduced, and whichever is the correct one is equal to the Hessian  $H_F$  of  $F$  or to its inverse. This implies that  $G$  is obtained from  $F$  by an automorphism of  $H_F$ , modulo  $\sigma$ . As the only automorphisms of  $H_F$ , as well as  $\sigma$ , fix  $a$  which is 0, we see that the first coefficient of  $F$  is 0, which is forbidden for a reduced form. Here is our contradiction.

3. Any real cubic form is equivalent to a form  $F$  whose Hessian  $H$  is reduced. Now, if this Hessian has one of the aforementioned special forms, the patient reader will check that either  $F$  or  $F \circ M$  is reduced, where  $M$  is an automorphism of  $H$ . Note that it is vital that  $F$  be irreducible here. More precisely, we need the trivial fact that  $F$  is reducible whenever  $a$  or  $d$  equals 0,  $Q = b = 0$ ,  $P = Q$  and  $b = |3a - b|$ , or  $P = R$ ,  $a = |d|$  and  $b = |c|$ .  $\square$

*Remark 3.4.* In those cases where the Hessian has some non-trivial automorphisms, we needed to fix a representative in the corresponding orbits of cubic forms. There, all the possible choices are equivalent. Furthermore, Lemma 3.5 will imply that these special cases, as listed in Lemma 3.1, occur at most  $O(X^{3/4})$  times. But there is another choice we had to make, taking into account that we needed  $\text{GL}_2(\mathbb{Z})$  and not  $\text{SL}_2(\mathbb{Z})$  to operate on our set of forms. There are two natural ideas:  $b \geq 0$  as we have just seen, or  $Q \geq 0$ . The latter one was aesthetically more pleasing because we did not have to bother with  $\varepsilon$  or  $\sigma$ , and things were a little more “canonical”. They still are, but not in a very natural way.

In both cases, the algorithm would run roughly as follows: execute four enclosed loops for the four coefficients of the form, taking advantage of every possible inequality, testing each time if we had a field or not. And the choice  $Q \geq 0$  now became awkward. For instance the condition  $Q \geq 0$  could not be exploited before at least three of the four defining coefficients had been set. In fact, the general algorithm was much more complicated in this case, because the sign of  $b$  had to be considered at times, and disregarded at others. The most obvious example would be the computation of  $b^2$  which should only be done once. Thus, the  $b$ -loop had to actually be on the absolute value of  $b$ , sometimes executing two instructions, sometimes one, depending on whether the sign of  $b$  had any importance. This led to a rather obscure and slightly less efficient program. Thus, the opposite choice was made, but it should not be considered as the “right” one. In fact, the normalization  $Q \geq 0$  being best-suited for theoretical purpose, we shall use it in Proposition 3.9.

We can in a very explicit way find bounds for the coefficients of a reduced form:

**Lemma 3.5.** *Let  $F = (a, b, c, d)$  be a reduced form whose discriminant lies in  $]0, X]$ . We have:*

$$(1) \quad |a| \leq \frac{2X^{1/4}}{3\sqrt{3}} ,$$

$$(2) \quad 0 \leq b \leq \frac{3a}{2} + \sqrt{\sqrt{X} - \frac{27a^2}{4}} .$$

Call  $P_2$  the unique positive real solution of the equation

$$-4P_2^3 + (3a + 2b)^2P_2^2 + 27a^2X = 0 \quad ,$$

then

$$(3) \quad \frac{b^2 - P_2}{3a} \leq c \leq b - 3a \quad .$$

*Proof.* Let  $H = (P, Q, R)$  be the Hessian of  $F$ ,  $3\Delta = 4PR - Q^2$ . Recall that

$$|Q| \leq P \leq R \quad .$$

As in the classical quadratic case, we remark:

$$(4) \quad P^2 \leq PR \leq \Delta \leq X \quad .$$

On the other hand, the formulas defining  $H$  yield:

$$P^2 = Pb^2 - 3Qab + 9Ra^2 \quad .$$

This quadratic equation in  $b$  has discriminant

$$9a^2(Q^2 - 4PR) + 4P^3 = 4P^3 - 27a^2D \quad .$$

Thus it has a solution if and only if

$$a^2 \leq \frac{4P^3}{27D} \leq \frac{4P}{27} \leq \frac{4\sqrt{X}}{27} \quad ,$$

and (1) is proved.

The largest of these two solutions is :

$$b = \frac{3Qa + \sqrt{4P^3 - 27a^2D}}{2P} = \frac{3aQ}{2P} + \sqrt{P - \frac{27a^2D}{4P^2}} \leq \frac{3a}{2} + \sqrt{P - \frac{27a^2D}{4P^2}} \quad .$$

This is an increasing function of  $P$ , which is thus maximal when  $P^2 = D$ . As the resulting expression increases with  $D$ , we finally obtain

$$b \leq \frac{3a}{2} + \sqrt{\sqrt{X} - \frac{27a^2}{4}} \quad ,$$

which is (2). Note that these two bounds are actually sharp, as they are reached whenever  $P = Q = R$ .

The last one is a little more intricate: given  $a, b, P$  and  $D$ , we need to know at what condition there exists  $Q$  such that:

$$(5) \quad f(Q) = Pb^2 - 3Qab + 9a^2 \left( \frac{3D + Q^2}{4P} \right) - P^2 = 0 \quad ,$$

$$(6) \quad -P \leq Q \leq P \leq \frac{3D + Q^2}{4P} \quad .$$

Of course,  $(3D + Q^2)/4P$  is equal to  $R$ , but we do not want too many variables in there. Given (5), and if we recall that both  $a$  and  $b$  are non-negative, the rightmost inequality in (6) becomes

$$Q \geq \frac{P}{3ab}(b^2 + 9a^2 - P) =: U \quad .$$

Let's study (5) as a quadratic equation in  $Q$ : its discriminant is

$$\Delta = 4P^3 - 27a^2D \quad ,$$

and we have

$$\begin{aligned} f(-P) &= P^2(3a + 2b)^2 - \Delta , \\ f(P) &= P^2(3a - 2b)^2 - \Delta , \\ f(U) &= \frac{P^2}{b^2}(b^2 - 9a^2 + P)^2 - \Delta . \end{aligned}$$

Finally, its minimum is reached at  $Q_{min} = 2bP/3a > 0$ , the sign of the minimal value being opposite to the sign of  $\Delta$ , and thus negative.

Call respectively  $P_1(D)$  and  $P_2(D)$  the positive real solution of the equations:

$$-4P^3 + (3a - 2b)^2P^2 + 27a^2D = 0 ,$$

$$-4P^3 + (3a + 2b)^2P^2 + 27a^2D = 0$$

(these always exist) and  $P_3(D) \leq P_4(D)$  the two positive solutions of

$$P^2(b^2 - 9a^2 + P)^2 - 4b^2P^3 + 27a^2b^2D = 0 .$$

Both  $P_3$  and  $P_4$  only exist when  $4P^2 \geq 3D$ , otherwise the left-hand expression remains positive. Of course, these three equations correspond to  $F(P) = 0$ ,  $F(-P) = 0$  and  $F(U) = 0$  respectively. There are two cases:

- $0 \leq b \leq 3a/2$ . Then  $Q_{min} \leq P$ . There is a solution in  $[-P, Q_{min}]$  if and only if  $f(-P) \geq 0$ ,  $U \leq Q_{min}$ , and  $f(U) \geq 0$ . And a solution in  $[Q_{min}, P]$  if and only if  $f(P) \geq 0$ , and either  $f(U) \leq 0$  or  $U \leq Q_{min}$ .
- $b > 3a/2$ . Now  $Q_{min} > P$ , thus any solution will lie in  $[-P, Q_{min}]$ . The corresponding statement from the preceding case holds verbatim, save that  $U \leq Q_{min}$  can be replaced by  $U \leq P$ , which is a little more precise but is a consequence of the other two inequalities.

Because of the trivial equality  $c = (b^2 - P)/3a$ , we only need to bound  $P$ . This will involve the quantities  $P_i(D)$  defined above. Applying the implicit function theorem yields that  $P_1(D)$ ,  $P_2(D)$ , and  $P_3(D)$  are increasing with  $D$ , while  $P_4(D)$  decreases. Recalling that  $P^2 \leq D \leq X$ , we call  $P_i(X) = P_i$ , for all  $1 \leq i \leq 4$ . We have  $P_1(P^2) = P_3(P^2) = 9a^2 - 3ab + b^2$  and  $P_2(P^2) = P_4(P^2) = 9a^2 + 3ab + b^2$ .

Remark first that, in the case  $U \leq Q_{min}$ , i.e.  $P + b^2 - 9a^2 \geq 0$ , we have  $f(-P) \leq f(U)$  if and only if  $P \leq 9a^2 + 3ab + b^2$ , i.e.  $c \geq -3a - b$ . Now we enumerate.

Suppose first that  $b > 3a/2$ .

As  $U \leq Q_{min}$ , we have  $P + b^2 - 9a^2 \geq 0$ , that is  $c \leq 2b^2/3a - 3a$ . But  $U \leq P$  yields  $c \leq b - 3a$  which is better. We see that  $P^2(b^2 - 9a^2 + P)^2 \geq b^2P^2(3a + 2b)^2$  if and only if  $c \leq -3a - b$ , in which case only  $f(-P)$  is involved.

- If  $-3a - b < c \leq b - 3a$ , we have  $P \leq P_3$  or  $P \geq P_4$  and this implies  $P \leq P_2$ .
- If  $c \leq -3a - b$ , we have  $P \leq P_2$ .

Now, we consider  $0 \leq b < 3a/2$ .

- If  $c > -3a + 2b^2/3a$ , then  $U > Q_{min}$ . And we have  $f(U) \leq 0 \leq f(P)$ , that is  $P_3(P^2) \leq P \leq P_4(P^2)$ , i.e.  $-3a - b \leq c \leq b - 3a$ , and  $P \leq P_1$ , which implies that  $P \leq P_2$ .
- If  $-3a - b \leq c \leq -3a + 2b^2/3a$ , we need  $f(U) \geq 0$ , i.e.  $P \leq P_3$  or  $P \geq P_4$ .
- If  $c \leq -3a - b$ , we still have  $P \leq P_2$ .

All of these imply that  $P \leq P_2$ . □

*Remark 3.6.* As far as  $c$  is concerned, we proved a much more precise statement than (3). But we will have no use for it, as it would only affect a small range of  $c$ , of the order of  $b$ , that is at most  $X^{1/4}$ . And we would then have to solve several extra equations involving cube roots. It turns out this is not a fair trade.

We now recall some of the densities computed by Davenport and Heilbronn in [4] and [6] :

**Theorem 3.7.** *Let  $H_3^+(X)$ , resp.  $N_3^+(X)$  denote the number of classes of equivalent cubic forms, resp. of isomorphism classes of real cubic fields, with positive discriminant less than  $X$ . As  $X$  tends to  $+\infty$ , we have:*

$$(7) \quad H_3^+(X) = \frac{\pi^2 X}{72} + C^+ \cdot X^{5/6} + O(X^{2/3+\epsilon}) \approx 0.137 \cdot X \quad ,$$

$$(8) \quad N_3^+(X) = \frac{X}{12\zeta(3)} + o\left(\frac{X}{\log^2 X}\right) \approx 0.0693 \cdot X \quad .$$

*Remark 3.8.* The non-principal part in (7) is actually due to Shintani [15], improving on Davenport’s original result [4]. The error term in (8) was proved in [2].

Once  $a, b, c$  are set as in Lemma 3.5, the coefficient  $d$  satisfies:

$$(9) \quad (-27a^2)d^2 + 2(9abc - 2b^3)d + (b^2c^2 - 4ac^3 - X) \leq 0$$

as well as

$$(10) \quad |bc - 9ad| \leq b^2 - 3ac \leq c^2 - 3bd \quad ,$$

and the number of such  $(a, b, c, d)$  is then about  $H_3^+(X)$ . Now, due to

$$\frac{H_3^+(X)}{N_3^+(X)} \longrightarrow \frac{12\zeta(3)\pi^2}{72} \approx 1.97$$

as  $X$  tends to infinity, only about half of these quadruplets will be eliminated for congruence reasons. So there is very little waste among the polynomials we produce.

Our reduction theory being so explicit, it is very easy to characterize subclasses of cubic fields:

**Proposition 3.9.** *Let  $K$  be a real cubic field,  $F_K$  be the associated reduced form, with the normalization  $Q \geq 0$ , and  $H_K = (P, Q, R)$  its Hessian. Then*

1.  $K$  is cyclic (i.e.  $\text{disc}(K) = f^2$ ) if and only if  $H_K = f_H(1, 1, 1)$ .
2.  $\text{disc}(K) = 5f^2$  if and only if  $H_K = f_H(1, 1, 4)$  or  $H_K = f_H(2, 1, 2)$ .
3.  $\text{disc}(K) = 8f^2$  if and only if  $H_K = f_H(1, 0, 6)$  or  $H_K = f_H(2, 0, 3)$ .
4.  $\text{disc}(K) = 12f^2$  if and only if  $H_K = f_H(1, 0, 9)$  or  $H_K = f_H(2, 2, 5)$ , or  $H_K = f_H(1, 0, 1)$ .
5. Let  $\Delta > 0$  be a fundamental discriminant, then  $\text{disc}(K) = \Delta f^2$  if and only if  $H_K$  is a multiple of a primitive reduced form whose discriminant is  $-3\Delta$  ( $f = f_H$ ) or  $-\Delta/3$  ( $f_H = 3f$  and  $3 \mid f$ ).

*Proof.* Part 5 is a simple consequence of Lemma 1.6 and our definition of reduced forms. The other assertions follow easily from this one. □

Due to the trivial equality

$$(11) \quad H(b, -3a) = P^2 \quad ,$$

we can “easily” build back the fields from a given discriminant. The preceding proposition gives all the possible Hessians. For all of them equation (11) has finitely many solutions, and given  $a, b$  and the Hessian, the cubic form is completely determined. An explicit study of the Hessian’s automorphisms would even yield a complete one-to-one parametrization for the fields whose discriminant has the form  $\Delta f^2$ .

4. COMPLEX CUBIC FIELDS

In the complex case, our version of Hermite reduction does not work anymore: there can be many reduced forms in a given class of indefinite quadratic forms, and selecting one among these is awkward. We use instead an even simpler idea of Mathews and Berwick: if an irreducible cubic form  $F = (a, b, c, d)$  has negative discriminant, it has a unique real root  $\theta \notin \mathbb{Q}$ , and we can factor  $F$  (in  $\mathbb{R}[x, y]$  !):

$$F(x, y) = (x - \theta y)(Ax^2 + Bxy + Cy^2) .$$

One easily computes

$$\text{disc } F = (B^2 - 4AC)(A\theta^2 + B\theta + C)^2 .$$

As  $\text{disc } F < 0$ , the “quadratic factor”,  $Q_F = (A, B, C)$ , has negative discriminant and we can impose  $A \geq 0$  by changing the signs of  $x$  and  $y$ . We have:

$$a = A, \quad b = B - \theta A, \quad c = C - \theta B \quad \text{and} \quad d = -\theta C .$$

Apart from a proportionality factor,  $(A, B, C)$  is covariant under  $\text{GL}_2(\mathbb{R})$ . Indeed given

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} ,$$

we have

$$Q_{F \circ M} = |a - \theta c| \cdot Q_F \circ M .$$

We define:

**Definition 4.1.** An integral binary complex cubic form  $F$  is *reduced* if  $0 < |B| < A < C$ , and

- $a > 0$ .
- $b \geq 0$ , with  $d > 0$  if  $b = 0$ .

Note that if  $F$  is irreducible, then  $\theta$  is an irrational number, and this excludes our former special cases:  $B = 0, A = |B|$  or  $A = C$ . Another nice feature is that we do not have to factor  $F$  at all:

**Lemma 4.2.** *A complex cubic form  $F = (a, b, c, d)$  is reduced if and only if:*

(12)  $d^2 - a^2 + ac - db > 0 ,$

(13)  $-(a - b)^2 - ac < ad - bc < (a + b)^2 + ac ,$

(14)  $a > 0, \quad b \geq 0 \quad \text{and} \quad d > 0 \quad \text{whenever} \quad b = 0 .$

*Proof.* See [13]. □

**Lemma 4.3.**

1. *A reduced complex cubic form belonging to  $U$  is irreducible.*
2. *Any irreducible complex cubic form is equivalent to a unique reduced one.*

*Proof.*

1. Just as in the proof of Corollary 3.3, a complex reducible form belonging to  $U$  is equivalent to  $G = y(x^2 + \delta y^2)$  or  $G' = y(x^2 + xy + \delta y^2)$ , with  $\delta \geq 1$ . If a reduced form  $F = (x - \theta y)(Ax^2 + Bxy + Cy^2)$  is equivalent to  $G$  or  $G'$ , then  $(A, B, C)$  is equivalent to a multiple of either  $(1, 0, \delta)$  or  $(1, 1, \delta)$ . As both are reduced,  $(A, B, C)$  is equal to one of them or their inverse, thus  $B = 0$  or  $A = \pm B$ , all of which are forbidden.
2. We only need to show that two reduced irreducible equivalent forms are equal. Let  $F = G \circ M$ ,  $M \in \text{GL}_2(\mathbb{Z})$  be two equivalent reduced forms. Then there exists  $\lambda \in \mathbb{R}_+^*$  such that  $\lambda Q_F = Q_G \circ M$ . We deduce  $\lambda Q_F = Q_G$ , thus  $M$  is an automorphism of  $Q_F$ . The proof then goes as before save that, as the forms are irreducible, all special cases are excluded.  $\square$

The equivalent of Lemma 3.5 is much simpler :

**Lemma 4.4.** *Let  $F = (a, b, c, d)$  be a reduced form whose discriminant lies in  $[-X, 0[$ . We have:*

$$(15) \quad 1 \leq a \leq \left(\frac{16X}{27}\right)^{1/4},$$

$$(16) \quad 0 \leq b \leq \frac{3a}{2} + \sqrt{\left(\frac{X}{3}\right)^{1/2} \frac{3a^2}{4}},$$

$$(17) \quad 1 - b \leq c \leq U(a, b) + \left(\frac{X}{4a}\right)^{1/3},$$

where  $U(a, b) = b^2/3a$  if  $a \geq 2b/3$ , and  $b - 3a/4$  otherwise.

*Proof.* Write  $F = (x - \theta y)(Ax^2 + Bxy + C)$ , and recall that

$$a = A, \quad b = B - \theta A, \quad c = C - \theta B.$$

Setting  $3\Delta = 4AC - B^2$ , we have

$$|B| < A < C \quad \text{and} \quad A^2 < \Delta.$$

We set  $D = |\text{disc } F|$ . From the equality  $D = 3\Delta(A\theta^2 + B\theta + C)^2$ , we get

$$2a\theta = -B \pm \sqrt{4a \left(\frac{D}{3\Delta}\right)^{1/2} - 3\Delta}.$$

The expression under the square root must be positive, so we obtain

$$(18) \quad 16a^2D \geq 27\Delta^3 \geq 27a^6$$

and, recalling that  $D \leq X$ , we get (15). From  $b = B - A\theta$ , we derive

$$b = \frac{3B}{2} \mp \sqrt{a \left(\frac{D}{3\Delta}\right)^{1/2} - \frac{3\Delta}{4}}.$$

The square root is a decreasing function of  $\Delta$ . Hence, using  $|B| \leq a$  and  $\Delta \geq a^2$ , (16) follows.

We have  $c = R - \theta B > A - \theta C > A - |\theta|A$ . From  $|B| < A$ , we get  $|b + \theta a| < a$ , which implies  $|\theta a| < a + b$ . Thus  $c > -b$ , which is the left-hand side of (17). To get the right-hand side, we use the explicit formulas for  $b$  and  $c$ , which yield

$$4ac = -3B^2 + 4bB + 3\Delta =: Q(B) .$$

The quadratic form  $Q(B)$  reaches its maximum  $4b^2/3$  when  $B = B_0 = 2b/3$ . But, as we must have  $B < A = a$ , this has to be replaced by  $U(a)$  whenever  $B_0 > a$ , and we are done. □

As before, we get a linear number of loops, and the corresponding theoretical values, as given in [2, 5, 6, 15], are as follows:

**Theorem 4.5.** *Let  $H_3^-(X)$ , resp.  $N_3^-(X)$ , denote the number of classes of equivalent cubic forms, resp. of isomorphism classes of cubic fields, with negative discriminant greater than  $-X$ . As  $X$  tends to  $+\infty$ , we have:*

$$(19) \quad H_3^-(X) = \frac{\pi^2 X}{24} + C^- \cdot X^{5/6} + O(X^{2/3+\epsilon}) \approx 0.411 \cdot X ,$$

$$(20) \quad N_3^-(X) = \frac{X}{4\zeta(3)} + o\left(\frac{X}{\log^2 X}\right) \approx 0.208 \cdot X .$$

*Remark 4.6.* If we want an equivalent to Proposition 3.9, the complex situation is not as favorable as the real one. The possible quadratic covariants are difficult to list directly in a practical computational sense: their coefficients are not even rational. Thus we resort to Hermite reduction. Let  $K$  be a complex cubic field and suppose that  $\text{disc}(K) = \Delta f^2$  ( $\Delta$  negative). We choose a system  $S$  of representatives for the classes (modulo  $\text{GL}_2(\mathbb{Z})!$ ) of quadratic forms of discriminant  $-3\Delta$  and  $-\Delta/3$ . Then the canonical form  $F_K$  is equivalent to a cubic form whose Hessian  $H_K$  is a multiple of a primitive form  $H$  in  $S$ .

Now another problem arises: (11) has positive discriminant, and thus an infinite number of solutions. This can be circumvented as we only need to find the solutions  $(a, b)$  modulo the cubes in  $\text{Aut } H$ . Namely, a simple computation shows that when  $M$  belongs to  $\text{Aut } H$ , replacing  $F$  by  $F \circ M$  multiplies  $(b, -3a)$  by  $M^3$ . The cubic forms obtained can now easily be reduced in our former sense.

### 5. IMPLEMENTATION

Let  $P$  be some integer. Using an elementary sieve, we need to precompute the list of “non-squarefree” numbers  $n \leq X$ , such that there exists a prime  $p \geq P$ , with  $p^2|n$ . One can trivially bound their number by:

$$\sum_{p \geq P} \frac{X}{p^2} \leq X \int_P^{+\infty} \frac{d\pi(t)}{t^2} .$$

The following well-known inequalities, due to Rosser and Schoenfeld [14, Theorem 1], give us a simple uniform bound:

$$\frac{x}{\log x} \left(1 + \frac{1}{2 \log x}\right) \leq \pi(x) \leq \frac{x}{\log x} \left(1 + \frac{3}{2 \log x}\right) ,$$

where the left-hand side is valid for  $x \geq 59$ , and the right-hand side for  $x > 1$ . Thus, if  $P \geq 59$ :

$$\begin{aligned} \int_P^{+\infty} \frac{d\pi(t)}{t^2} &= -\frac{\pi(P)}{P^2} + \int_P^{+\infty} \frac{2\pi(t)dt}{t^3} \\ &\leq -\frac{1}{P \log P} \left(1 + \frac{1}{2 \log P}\right) + \int_P^{+\infty} \frac{2dt}{t^2 \log t} + \int_P^{+\infty} \frac{3dt}{t^2 \log^2 t} \\ &= \frac{1}{P \log P} \left(1 - \frac{1}{2 \log P}\right) + \int_P^{+\infty} \frac{dt}{t^2 \log^2 t} \\ &\leq \frac{1}{P \log P} \left(1 + \frac{1}{2 \log P}\right). \end{aligned}$$

Thus, depending on available memory and  $X$ , one can fix a  $P$  such that we can test if an integer bounded by  $X$  is squarefree in at most  $\pi(P)$  divisions and a quick binary search, which can itself be optimized with hashing techniques. For instance, we can sort the lists according to the high-order bits of the discriminant; as we now only need to store the low-order bits, a careful implementation will keep to 32-bit integers far beyond the practical range of the algorithm. Having decided to use at most 32Mo in RAM for the hashing lists, we took  $P = 97$  to compute a table up to  $X = 10^{10}$  and  $P = 661$  up to  $X = 10^{11}$ , trial division up to  $P$  still taking most of the computational time.

Call  $M$  the maximum memory one is willing to spend for the hashing lists, i.e. we will keep at most  $M$  32-bit integers in RAM. We use the following initialization routine:

**Sub-Algorithm 5.1** (init).

1. [Initialize primes] Input  $X$ , the discriminant bound. Compute a table of primes up to  $\sqrt{X}$ ,  $\mathbf{p}[\ ]$ , as well as their squares  $\mathbf{pp}[\ ]$ . Using a binary search, find the minimal prime  $p$  such that:

$$\frac{X}{p \log p} \cdot \left(1 + \frac{1}{2 \log p}\right) \leq 3M.$$

If  $p \leq 53$ , find the minimal prime  $p$  such that

$$p^{-2} + \dots + 53^{-2} \leq \frac{3M}{X} - \frac{1}{\log 59} \cdot \left(1 + \frac{1}{2 \log 59}\right).$$

If  $p < 5$ , set  $p = 5$ . Set  $\mathbf{index}$  such that  $\mathbf{p}[\mathbf{index}] = p$ .

2. [Initialize sieve] Put in  $\mathbf{list}[\ ]$  all the integers less than  $X$ , prime to 6, and admitting a divisor  $\mathbf{pp}[i]$ ,  $i \geq \mathbf{index}$ . Fill in boolean array  $\mathbf{sqfull}[\ ]$  up to  $n = \sqrt{3X}$ , such that  $\mathbf{sqfull}[n]$  is **true** if and only if  $p^2|n$  for some prime  $p \geq 5$ .

The primes 2 and 3 are special cases anyway and can be readily suppressed from the discriminant factorization: a single division modulo 72 is enough. Thus, one can restrict the lists to integers prime to 6, and there are then  $6/\varphi(6) = 3$  times less numbers to keep in memory. Hence the  $3 \cdot M$  instead of  $M$  in Step 1, as well as the test for  $p < 5$ . The bound  $\sqrt{3X}$  in the definition of  $\mathbf{sqfull}$  was chosen because we primarily want to test  $f_H$  with it.

The following common subroutine checks whether a reduced form belongs to  $U_p$ , for  $p > 2$ .

**Sub-Algorithm 5.2** (`test`( $f_H, a, b, c, d, \Delta$ )).

Input:  $(a, b, c, d)$  a reduced cubic form belonging to  $U_2$ ,  $f_H$  and  $\Delta$  respectively the content and discriminant of its Hessian (recall that  $\Delta = -3 \text{disc}(a, b, c, d)$ ).

Output:  $F$  if it belongs to  $U$ , nothing otherwise.

1. If  $(a, b, c, d)$  does not belong to  $U_3$ , as in Lemma 1.2, or `sqfull`[ $f_H$ ] is `true`, then return.
2. Set  $t = \Delta/f_H^2$ , and  $t = t/\text{gcd}(t, 72)$  so that now  $t$  is prime to 6. If  $\text{gcd}(t, f_H) > 1$ , return.
3. Return if  $t$  is not squarefree. The test should be done as follows: if  $n$  is small enough ( $n \leq \sqrt{3X}$ ) return if `sqfull`[ $n$ ] is `true`. Else search the sorted by construction `list` for  $n$ , then trial divide  $n$  by `pp`[ $i$ ],  $2 \leq i < \text{index}$ , returning as soon as  $n$  is found or one `pp`[ $i$ ] divides  $n$ .
4. Output  $(a, b, c, d)$ .

5.1. **Real cubic fields.** The actual algorithms are now simple to write:

**Sub-Algorithm 5.3** (`is_real_field`( $a, b, c, d, P, Q, R$ )).

Input: a real cubic form  $F = (a, b, c, d)$ , and its reduced Hessian  $(P, Q, R)$ .

Output:  $F$ , if it corresponds to a real cubic field.

1. [Check special cases]
  - if  $P = Q$ : if  $|b| \geq |3a - b|$ , return.
  - if  $P = R$ : if  $a > |d|$ , return. If  $a = |d|$  and  $|b| \geq |c|$ , return.
  - if  $|Q| = R$ : if  $4|P|$  return. Execute `test`( $P, a, b, c, d, 3P^2$ ), then return.
2. Set  $\Delta = 4PR - Q^2$ . If  $16|\Delta|$  or  $[\Delta \equiv 12 \pmod{16}]$  and either  $P$  or  $R$  is odd], return.
3. Set  $f_H = \text{gcd}(P, Q, R)$ , then execute `test`( $f_H, a, b, c, d, \Delta$ ).

**Algorithm 5.4** (`CRFCRF`<sup>1</sup>).

1. Execute `init`.
2. [Special case  $b = 0$ ] Execute three embedded loops on  $a, c, d$  in this nesting order. Set the bounds using the reduction inequalities  $a > 0, b \geq 0$  and (10), as well as (9) and Lemma 3.5. Compute the Hessian  $(P, Q, R)$ , then execute `is_real_field`( $a, 0, c, d, P, Q, R$ ).
3. [General case] We now have four loops on  $a, b, c, d$  in this order, with the additional inequality  $b > 0$ . Compute the Hessian  $(P, Q, R)$ , then execute `is_real_field`( $a, b, c, d, P, Q, R$ ).

*Remark 5.5.* Great care must be taken in setting the bounds for the various loops to avoid round-off errors. Also, many computations can be done at an early stage. For instance,  $P = b^2 - 3ac$  can be computed before  $d$  is known. This is tedious but straightforward, so we chose not to hide the simplicity of the algorithm behind scores of auxiliary variables and explicit complicated bounds.

5.2. **Complex cubic fields.** Though it is now easier to test whether a form corresponds to a field, the general algorithm is a little more complicated than the previous one. First, because our reduction inequalities now involve solving (12) which is quadratic in  $d$ . And second, they do not imply anymore that the form discriminant has the expected sign: a test run of the algorithm after removing the

<sup>1</sup>stands for Cubic Real Fields Counting Reduced Forms.

sign condition will produce scores of counterexamples. Thus, we will have to deal with *three* quadratic inequalities instead of one.

**Sub-Algorithm 5.6** (`is_complex_field(a, b, c, d, P, Q, R)`).

1. Set  $\Delta = Q^2 - 4PR$ . If  $16|\Delta$  or  $[\Delta \equiv 4 \pmod{16}]$  and either  $P$  or  $R$  is odd], **false**.
2. Set  $f_H = \gcd(|P|, |Q|, |R|)$ , then execute `test(fH, a, b, c, d, Δ)`.

The shape of the algorithm is the same:

**Algorithm 5.7** (`CCFCCF2`).

1. Execute `init`.
2. [Special case  $b = 0$ ] Execute three embedded loops on  $a, c, d$  in this nesting order. The bounds are set using the reduction inequalities  $a > 0, b \geq 0$  and Lemma 4.2, and the discriminant ones arising from  $-X \leq \text{disc } F < 0$  and Lemma 4.4. Compute the Hessian  $(P, Q, R)$ . Execute `is_complex_field(a, 0, c, d, P, Q, R)`.
3. [General case] We now have four loops on  $a, b, c, d$  in this order, with the additional inequality  $b > 0$ . Compute the Hessian  $(P, Q, R)$ , then execute `is_complex_field(a, b, c, d, P, Q, R)`.

**5.3. General remarks.** All these algorithms have been implemented in ANSI C on a DEC alpha (64-bit machine) with the help of the PARI library – see [1] for details on this useful number theory package.

- One can sensibly compute the number of (isomorphism class of) cubic fields up to  $X \approx 10^{11}$  in this way. As one can see from Table 6.1, the overhead computations in subroutine `init` take a negligible time, thus the algorithm can easily be distributed.

- The intermediate results all fit in single precision long integers on 64-bit machines for reasonable  $X$ : say, less than  $10^{12}$  in the real case, and  $5 \cdot 10^{10}$  in the complex case.

- It might happen that for given  $(a, b, c)$  satisfying our bounds, there does not exist  $d$  such that the form  $(a, b, c, d)$  is both reduced and has a discriminant in the expected range. One can prove the number of these “empty loops” is a  $O(X^{3/4})$ .

- If one compares with methods originating from Hunter’s theorem, the gain is gigantic: no irreducibility check, no discriminant factorization, no search for automorphisms and thus, no need to keep all the fields found so far in memory. We get an essentially *linear* algorithm. The main loop is executed less than  $C \cdot X + o(X)$  times, with  $C = \pi^2/72$  in the real case and  $C = \pi^2/24$  in the complex case. And all the rest is overhead computations, dominated by the main loop, save for the time spent searching the lists for non-squarefree numbers, or trial dividing to locate small square factors, which remains reasonable for the practical range of the method. As a matter of fact, sorting the fields by increasing discriminant takes much more time than actually computing them.

- It is feasible to compute fields whose discriminants lie in an interval  $[X, X + Y]$ , for very large  $X$ , say  $10^{15}$ , when  $Y$  is small enough, say  $10^6$ . We incorporate the

---

<sup>2</sup>stands for Cubic Complex Fields Counting Companion Forms.

relevant discriminant inequality in the loops and, instead of using lists of precomputed numbers, we factor the discriminant using a suitable probabilistic factorization method. The running time is then more or less the time needed to factor around  $Y$  numbers of size  $X$ . Of course, the empty loops become a problem if  $X$  is too large.

## 6. RESULTS

The following tables give an idea of computational time and memory usage. First, we consider the `init` routine, which does not depend on the signature. Most of the time in there is spent building sieves. We call  $P = \mathbf{p}[\mathbf{index}]$  the prime chosen to build the hashing lists. For instance,  $P = 5$  means that no trial division actually takes place in `sqfree`. The “Square-full ints” column corresponds to the number of 32-bit integers stored in the lists:

Next, we give the data corresponding to the computation of real and complex cubic fields. Here,  $a$  is the maximal value for the first coefficient of the cubic form. They happen to be the ones given by the bound in Lemma 3.5 in the real case. And one less than the ones in Lemma 4.4 in the complex case, with the exception  $X = 10^4$  where we get the exact bound. As was expected, we get a roughly linear behavior as long as  $P = 5$ , which quickly “diverges” as  $P$  increases. Up to the same discriminant bound, time spent for the complex computations compared to the real ones should be in the same ratio as the number of fields found: slowly decreasing in the given examples, equal to 3 at infinity due to Davenport-Heilbronn’s result (not exactly so, the initializing step being exactly the same). But, as pointed out at the beginning of §5.2, the complex situation is a little worse, due to the extra square roots.

Such tables had previously been given by Fung-Williams [7] in the complex case (discriminant greater than  $-10^6$ ) and Llorente-Quer [12] in the real case (discriminant lower than  $10^7$ ). Our results are in accordance with the former but disagree by one field with the latter. As these authors already pointed out, the density of cubic discriminants slowly increases up to the Davenport-Heilbronn limit. Recall that it is respectively  $1/12\zeta(3) \approx 0.0693$  and  $1/4\zeta(3) \approx 0.2080$  in the real and complex case. Thus in our computations, up to  $X = 10^{11}$ , the third decimal is already wrong.

TABLE 6.1. Overhead computations

X	P	Square-full ints	Sieving time	
$10^4$	5	290	0.001 s	
$10^5$	5	2935	0.01 s	
$10^6$	5	29370	0.1 s	
$10^7$	5	293674	1.0 s	
$10^8$	5	2936998	7.0 s	
$P > 5$	$10^9$	17	5474664	43 s
	$10^{10}$	97	6409864	356 s (5 min 56 s)
	$10^{11}$	661	6644929	3427 s (58 min 15 s)

TABLE 6.2. Real cubic fields

X	# of fields	Elapsed time	$a$
$10^1$	0	0.000 s	0
$10^2$	2	0.000 s	1
$10^3$	27	0.000 s	2
$10^4$	382	0.005 s	3
$10^5$	4,804	0.05 s	6
$10^6$	54,600	0.5 s	12
$10^7$	592,922	5.7 s	21
$10^8$	6,248,290	64 s (1 min 04 s)	38
$P > 5$ $10^9$	64,659,361	774 s (12 min 54 s)	68
$10^{10}$	661,448,081	18,641 s (5 h 11 min)	121
$10^{11}$	6,715,824,025	714,488 s (8 days 7 h)	216

TABLE 6.3. Complex cubic fields

X	# of fields	Elapsed time	$a$
$10^1$	0	0.000 s	0
$10^2$	7	0.000 s	1
$10^3$	127	0.004 s	3
$10^4$	1520	0.04 s	7
$10^5$	17,041	0.3 s	14
$10^6$	182,417	2.2 s	26
$10^7$	1,905,514	21.3 s	49
$10^8$	19,609,185	224 s (3 min 44 s)	86
$P > 5$ $10^9$	199,884,780	2,575 s (42 min 55 s)	155
$10^{10}$	2,024,660,098	58,247 s (16 h 11 min)	276
$10^{11}$	20,422,230,540	2,207,413 s (25 days 13 h)	492

But not so slowly if one considers the best proven error term in (8) or (20):  $O(X/\log^2 X)$ . In fact, if we write the experimental remainder as  $X/\log^\alpha X$ , and use the least square method to guess a “correct” value for  $\alpha$ , we obtain an unstable behaviour:  $\alpha$  increases steadily with the bound  $X$ , up to  $\alpha \approx 3.9$  when  $X = 10^{11}$ . Thus, for all we know, this error term might even decrease faster than all negative powers of  $\log X$ .

#### APPENDIX A. TABLE OF REAL CUBIC FIELDS

The following lists the first hundred real cubic fields sorted by increasing discriminant. We give the following data from left to right: the discriminant, the canonical defining cubic form (instead of the binary form  $F(x, y)$ , we give  $F(x, 1)$ ), its Hessian written as  $f_H(P_1, Q_1, R_1)$ , with  $(P_1, Q_1, R_1)$  primitive, and the factor  $f$  from the discriminant ( $\text{Disc} = f^2 \Delta_2$ , with  $\Delta_2$  a fundamental discriminant). Up to

a factor 3,  $f$  corresponds to the content  $f_H$  of the Hessian. Starred discriminants denote cyclic fields, i.e. the ones whose Hessian is of the form  $(P, \pm P, P)$ .

Disc	$F(X)$	Hessian	$f$
49*	$X^3 + X^2 - 2X - 1$	$7(1, 1, 1)$	7
81*	$X^3 - 3X - 1$	$9(1, 1, 1)$	9
148	$X^3 + X^2 - 3X - 1$	$2(5, 3, 6)$	2
169*	$X^3 + X^2 - 4X + 1$	$13(1, -1, 1)$	13
229	$X^3 - 4X - 1$	$(12, 9, 16)$	1
257	$X^3 + 2X^2 - 3X - 1$	$(13, 3, 15)$	1
316	$X^3 + 2X^2 - 3X - 2$	$(13, 12, 21)$	1
321	$X^3 + X^2 - 4X - 1$	$(13, 5, 19)$	1
361*	$X^3 + 2X^2 - 5X + 1$	$19(1, -1, 1)$	19
404	$X^3 + X^2 - 5X + 1$	$2(8, -7, 11)$	2
469	$X^3 + 2X^2 - 4X - 1$	$(16, 1, 22)$	1
473	$X^3 - 5X - 1$	$(15, 9, 25)$	1
564	$X^3 + 2X^2 - 4X - 2$	$2(8, 5, 14)$	2
568	$X^3 + 4X^2 - X - 2$	$(19, 14, 25)$	1
621	$X^3 + 3X^2 - 3X - 2$	$9(2, 1, 3)$	3
697	$X^3 + 3X^2 - 4X - 1$	$(21, -3, 25)$	1
733	$X^3 + 2X^2 - 6X + 1$	$(22, -21, 30)$	1
756	$X^3 - 6X - 2$	$18(1, 1, 2)$	6
761	$X^3 + X^2 - 6X + 1$	$(19, -15, 33)$	1
785	$X^3 + 2X^2 - 5X - 1$	$(19, -1, 31)$	1
788	$X^3 + 4X^2 - 2X - 2$	$2(11, 5, 14)$	2
837	$X^3 - 6X - 1$	$9(2, 1, 4)$	3
892	$X^3 + 5X^2 - 2$	$(25, 18, 30)$	1
940	$X^3 + 3X^2 - 4X - 2$	$(21, 6, 34)$	1
961*	$2X^3 + X^2 - 5X - 2$	$31(1, 1, 1)$	31
985	$X^3 + X^2 - 6X - 1$	$(19, 3, 39)$	1
993	$X^3 + 2X^2 - 5X - 3$	$(19, 17, 43)$	1
1016	$X^3 + X^2 - 6X - 2$	$(19, 12, 42)$	1
1076	$X^3 + 3X^2 - 5X - 1$	$2(12, -3, 17)$	2
1101	$X^3 + 5X^2 - X - 2$	$(28, 13, 31)$	1
1129	$X^3 + 3X^2 - 4X - 3$	$(21, 15, 43)$	1
1229	$X^3 + 2X^2 - 6X - 1$	$(22, -3, 42)$	1
1257	$X^3 + 2X^2 - 7X + 1$	$(25, -23, 43)$	1
1300	$X^3 + 3X^2 - 7X + 1$	$10(3, -3, 4)$	10
1304	$2X^3 + 3X^2 - 4X - 2$	$(33, 24, 34)$	1
1345	$X^3 - 7X - 1$	$(21, 9, 49)$	1
1369*	$X^3 + 4X^2 - 7X + 1$	$37(1, -1, 1)$	37
1373	$X^3 + 3X^2 - 5X - 2$	$(24, 3, 43)$	1
1384	$X^3 + 5X^2 - 2X - 2$	$(31, 8, 34)$	1
1396	$X^3 + 2X^2 - 6X - 2$	$2(11, 3, 24)$	2
1425	$X^3 + 4X^2 - 3X - 3$	$5(5, 3, 9)$	5
1436	$X^3 + 6X^2 + X - 2$	$(33, 24, 37)$	1
1489	$X^3 + 4X^2 - 5X - 1$	$(31, -11, 37)$	1
1492	$X^3 + 4X^2 - 4X - 2$	$2(14, 1, 20)$	2
1509	$X^3 + 2X^2 - 6X - 3$	$(22, 15, 54)$	1
1524	$X^3 + X^2 - 7X - 1$	$2(11, 1, 26)$	2
1556	$X^3 + 5X^2 - X - 3$	$2(14, 11, 23)$	2
1573	$X^3 + X^2 - 7X - 2$	$11(2, 1, 5)$	11
1593	$X^3 + 3X^2 - 6X - 1$	$9(3, -1, 5)$	3
1620	$X^3 + 6X^2 - 2$	$18(2, 1, 2)$	18
1708	$X^3 + 4X^2 - 3X - 4$	$(25, 24, 57)$	1
1765	$X^3 + 5X^2 - 3X - 2$	$(34, 3, 39)$	1
1772	$2X^3 + X^2 - 6X - 2$	$(37, 30, 42)$	1
1825	$X^3 + 2X^2 - 7X - 1$	$5(5, -1, 11)$	5

1849*	$2X^3 + X^2 - 7X + 2$	$43(1, -1, 1)$	43
1901	$X^3 + 4X^2 - 4X - 3$	$(28, 11, 52)$	1
1929	$X^3 + 5X^2 - 2X - 3$	$(31, 17, 49)$	1
1937	$X^3 + X^2 - 8X + 1$	$(25, -17, 61)$	1
1940	$X^3 - 8X - 2$	$2(12, 9, 32)$	2
1944	$X^3 + 3X^2 - 6X - 2$	$27(1, 0, 2)$	9
1957	$X^3 + 2X^2 - 8X + 1$	$(28, -25, 58)$	1
2021	$X^3 - 8X - 1$	$(24, 9, 64)$	1
2024	$X^3 + 4X^2 - 5X - 2$	$(31, -2, 49)$	1
2057	$X^3 + 3X^2 - 8X + 1$	$11(3, -3, 5)$	11
2089	$2X^3 + 3X^2 - 5X - 2$	$(39, 21, 43)$	1
2101	$X^3 + 4X^2 - 6X - 1$	$(34, -15, 48)$	1
2177	$X^3 + 2X^2 - 7X - 3$	$(25, 13, 67)$	1
2213	$X^3 + 7X^2 + 3X - 2$	$(40, 39, 51)$	1
2228	$2X^3 + 2X^2 - 6X - 1$	$2(20, 3, 21)$	2
2233	$X^3 + X^2 - 8X - 1$	$(25, 1, 67)$	1
2241	$X^3 + 3X^2 - 6X - 3$	$9(3, 1, 7)$	3
2292	$2X^3 + 4X^2 - 4X - 3$	$2(20, 19, 26)$	2
2296	$X^3 + 7X^2 + 2X - 2$	$(43, 32, 46)$	1
2300	$X^3 + X^2 - 8X - 2$	$5(5, 2, 14)$	5
2349	$X^3 + 6X^2 - 3$	$9(4, 3, 6)$	9
2429	$2X^3 + X^2 - 7X + 1$	$(43, -25, 46)$	1
2505	$X^3 + 4X^2 - 5X - 3$	$(31, 7, 61)$	1
2557	$X^3 + X^2 - 9X + 2$	$(28, -27, 75)$	1
2589	$2X^3 + 5X^2 - 3X - 3$	$(43, 39, 54)$	1
2597	$X^3 + 2X^2 - 8X - 1$	$7(4, -1, 10)$	7
2636	$2X^3 - 7X - 1$	$(42, 18, 49)$	1
2673	$X^3 - 9X - 3$	$27(1, 1, 3)$	9
2677	$X^3 + 3X^2 - 7X - 2$	$(30, -3, 67)$	1
2700	$X^3 + 6X^2 - 3X - 2$	$45(1, 0, 1)$	15
2708	$X^3 + 4X^2 - 6X - 2$	$2(17, -3, 30)$	2
2713	$X^3 + 6X^2 - X - 3$	$(39, 21, 55)$	1
2777	$X^3 + 5X^2 - 6X - 1$	$(43, -21, 51)$	1
2804	$X^3 + X^2 - 9X + 1$	$2(14, -9, 39)$	2
2808	$X^3 - 9X - 2$	$9(3, 2, 9)$	3
2836	$X^3 + 2X^2 - 8X - 2$	$2(14, 1, 38)$	2
2857	$X^3 + 2X^2 - 9X + 1$	$(31, -27, 75)$	1
2917	$X^3 + 5X^2 - 5X - 2$	$(40, -7, 55)$	1
2920	$2X^3 + 4X^2 - 5X - 2$	$(46, 16, 49)$	1
2941	$2X^3 + X^2 - 7X - 1$	$(43, 11, 52)$	1
2981	$X^3 + 5X^2 - 3X - 4$	$(34, 21, 69)$	1
2993	$X^3 + 5X^2 - 4X - 3$	$(37, 7, 61)$	1
3021	$X^3 + 2X^2 - 8X - 3$	$(28, 11, 82)$	1
3028	$X^3 + 3X^2 - 7X - 3$	$2(15, 3, 38)$	2
3124	$2X^3 + 6X^2 - 2X - 3$	$2(24, 21, 29)$	2
3132	$2X^3 + 3X^2 - 6X - 2$	$9(5, 2, 6)$	3

## APPENDIX B. TABLE OF COMPLEX CUBIC FIELDS

The following gives the corresponding data for complex cubic fields.

Disc	$F(X)$	Hessian	$f$
-23	$X^3 + X^2 + 2X + 1$	$(-5, -7, 1)$	1
-31	$X^3 + X + 1$	$(-3, -9, 1)$	1
-44	$X^3 + 2X^2 + 2X + 2$	$2(-1, -7, -4)$	2
-59	$X^3 + 2X + 1$	$(-6, -9, 4)$	1
-76	$X^3 + X^2 + 3X + 1$	$2(-4, -3, 3)$	2
-83	$X^3 + X^2 + X + 2$	$(-2, -17, -5)$	1
-87	$X^3 + 2X^2 + 3X + 3$	$(-5, -21, -9)$	1

-104	$2X^3 + 2X^2 + 3X + 1$	$(-14, -12, 3)$	1
-107	$X^3 + X^2 + 3X + 2$	$(-8, -15, 3)$	1
-108	$X^3 + 3X^2 + 3X + 3$	$18(0, -1, -1)$	6
-116	$X^3 + X^2 + 2$	$(1, -18, -6)$	1
-135	$X^3 + 3X + 1$	$9(-1, -1, 1)$	3
-139	$X^3 + 2X^2 + 2X + 3$	$(-2, -23, -14)$	1
-140	$X^3 + 2X + 2$	$2(-3, -9, 2)$	2
-152	$2X^3 + 3X^2 + 4X + 2$	$(-15, -24, -2)$	1
-172	$2X^3 + 2X + 1$	$2(-6, -9, 2)$	2
-175	$X^3 + X^2 + 2X + 3$	$5(-1, -5, -1)$	5
-199	$X^3 + X^2 + 4X + 1$	$(-11, -5, 13)$	1
-200	$X^3 + 2X^2 + 3X + 4$	$5(-1, -6, -3)$	5
-204	$X^3 + X^2 + X + 3$	$2(-1, -13, -4)$	2
-211	$2X^3 + X^2 + 3X + 1$	$(-17, -15, 6)$	1
-212	$X^3 + X^2 + 4X + 2$	$(-11, -14, 10)$	1
-216	$X^3 + 3X + 2$	$9(-1, -2, 1)$	3
-231	$X^3 + 2X^2 + X + 3$	$(1, -25, -17)$	1
-239	$X^3 + 3X^2 + 2X + 3$	$(3, -21, -23)$	1
-243	$X^3 + 3X^2 + 3X + 4$	$27(0, -1, -1)$	9
-244	$2X^3 + 2X^2 + 3X + 2$	$(-14, -30, -3)$	1
-247	$X^3 + 3X^2 + 4X + 5$	$(-3, -33, -29)$	1
-255	$X^3 + X^2 + 3$	$(1, -27, -9)$	1
-268	$2X^3 + 4X^2 + 4X + 3$	$2(-4, -19, -10)$	2
-283	$X^3 + 4X + 1$	$(-12, -9, 16)$	1
-300	$2X^3 + 2X^2 + 4X + 1$	$10(-2, -1, 1)$	10
-307	$X^3 + 2X^2 + 4X + 5$	$(-8, -37, -14)$	1
-324	$2X^3 + 3X + 1$	$9(-2, -2, 1)$	9
-327	$3X^3 + 3X^2 + 4X + 1$	$(-27, -15, 7)$	1
-331	$X^3 + X^2 + 3X + 4$	$(-8, -33, -3)$	1
-335	$X^3 + 2X^2 + 5X + 5$	$(-11, -35, -5)$	1
-339	$X^3 + 2X^2 + 3$	$(4, -27, -18)$	1
-351	$X^3 + 3X + 3$	$9(-1, -3, 1)$	3
-356	$2X^3 + X^2 + 2X + 2$	$(-11, -34, -2)$	1
-364	$X^3 + 4X + 2$	$2(-6, -9, 8)$	2
-367	$X^3 + 2X^2 + 3X + 5$	$(-5, -39, -21)$	1
-379	$X^3 + X^2 + X + 4$	$(-2, -35, -11)$	1
-411	$X^3 + X^2 + 5X + 2$	$(-14, -13, 19)$	1
-419	$2X^3 + X^2 + 3X - 1$	$(-17, 21, 12)$	1
-424	$3X^3 + 4X^2 + 5X + 2$	$(-29, -34, 1)$	1
-431	$2X^3 + X^2 + 3X + 2$	$(-17, -33, 3)$	1
-436	$X^3 + 3X^2 + 4X + 6$	$(-3, -42, -38)$	1
-439	$X^3 + 2X^2 - X + 3$	$(7, -29, -17)$	1
-440	$2X^3 + X + 2$	$(-6, -36, 1)$	1
-451	$2X^3 + 3X^2 + 5X + 3$	$(-21, -39, -2)$	1
-459	$2X^3 + 3X^2 + 3X + 3$	$9(-1, -5, -2)$	3
-460	$X^3 + X^2 + 5X + 3$	$2(-7, -11, 8)$	2
-472	$2X^3 + 4X^2 + 5X + 4$	$(-14, -52, -23)$	1
-484	$X^3 + 2X^2 + 5X + 6$	$11(-1, -4, -1)$	11
-491	$X^3 + 2X^2 + 2X + 5$	$(-2, -41, -26)$	1
-492	$X^3 + 2X^2 + 4X + 6$	$2(-4, -23, -10)$	2
-499	$X^3 + 4X + 3$	$(-12, -27, 16)$	1
-503	$2X^3 + 5X^2 + 5X + 4$	$(-5, -47, -35)$	1
-515	$X^3 + 4X^2 + 4X + 5$	$(4, -29, -44)$	1
-516	$3X^3 + 3X^2 + 4X + 2$	$(-27, -42, -2)$	1
-519	$3X^3 + 5X^2 + 6X + 3$	$(-29, -51, -9)$	1
-524	$X^3 + X^2 + 3X + 5$	$2(-4, -21, -3)$	2
-527	$X^3 + 5X + 1$	$(-15, -9, 25)$	1
-543	$X^3 + X^2 + 2X + 5$	$(-5, -43, -11)$	1

-547	$3X^3 + 2X^2 + 4X + 1$	$(-32, -19, 10)$	1
-563	$X^3 + X^2 + 5X + 4$	$(-14, -31, 13)$	1
-567	$3X^3 + 3X + 1$	$9(-3, -3, 1)$	9
-588	$X^3 + 2X^2 + 6X + 6$	$14(-1, -3, 0)$	14
-620	$2X^3 + 4X + 1$	$2(-12, -9, 8)$	2
-628	$2X^3 + 5X^2 + 6X + 5$	$(-11, -60, -39)$	1
-643	$X^3 + 3X^2 + X + 4$	$(6, -33, -35)$	1
-648	$2X^3 + 3X + 2$	$9(-2, -4, 1)$	9
-652	$2X^3 + 2X^2 + 4X + 3$	$2(-10, -23, -1)$	2
-655	$X^3 + 2X^2 + X + 5$	$(1, -43, -29)$	1
-671	$X^3 + 3X^2 + 2X + 5$	$(3, -39, -41)$	1
-675	$X^3 + 3X^2 + 3X + 6$	$45(0, -1, -1)$	15
-676	$2X^3 + 2X^2 + 5X + 2$	$13(-2, -2, 1)$	13
-679	$X^3 + 3X^2 + 4X + 7$	$(-3, -51, -47)$	1
-680	$2X^3 + 2X^2 + 5X + 1$	$(-26, -8, 19)$	1
-687	$X^3 + 2X^2 + 5X + 7$	$(-11, -53, -17)$	1
-695	$X^3 + 4X^2 + 5X + 7$	$(1, -43, -59)$	1
-696	$X^3 + 2X^2 - X + 4$	$(7, -38, -23)$	1
-707	$X^3 + 3X^2 + 5X + 8$	$(-6, -57, -47)$	1
-716	$3X^3 + X^2 + 3X - 1$	$2(-13, 15, 6)$	2
-728	$X^3 + X^2 + 6X + 2$	$(-17, -12, 30)$	1
-731	$X^3 + 2X^2 + 4X + 7$	$(-8, -55, -26)$	1
-743	$X^3 + 5X + 3$	$(-15, -27, 25)$	1
-744	$2X^3 + X^2 + 4X - 1$	$(-23, 22, 19)$	1
-748	$X^3 + 2X^2 + 2X + 6$	$2(-1, -25, -16)$	2
-751	$X^3 + X^2 + 6X + 1$	$(-17, -3, 33)$	1
-755	$X^3 + 2X^2 + 6X + 7$	$(-14, -51, -6)$	1
-756	$2X^3 + 3X^2 + 6X + 3$	$9(-3, -4, 1)$	3
-759	$X^3 + X^2 + 6X + 3$	$(-17, -21, 27)$	1
-771	$X^3 + X^2 + 3X + 6$	$(-8, -51, -9)$	1
-780	$X^3 + 4X^2 + 4X + 6$	$2(2, -19, -28)$	2
-804	$X^3 + X^2 + 4X + 6$	$(-11, -50, -2)$	1
-808	$X^3 + X^2 + 2X + 6$	$(-5, -52, -14)$	1
-812	$2X^3 + 4X^2 + 6X + 5$	$2(-10, -33, -12)$	2
-815	$3X^3 + 4X^2 + 5X + 3$	$(-29, -61, -11)$	1

## REFERENCES

1. C. Batut, D. Bernardi, H. Cohen, & M. Olivier, *User's guide to PARI-GP, version 1.39.03*, available from `ftp: megrez.math.u-bordeaux.fr`, 1995.
2. K. Belabas, Crible et 3-rang des corps quadratiques, *Ann. de l'Inst. Fourier* **46** (1996), pp. 909–949. CMP 97:03
3. H. Cohen, *A course in computational algebraic number theory*, Springer-Verlag, 1993. MR **94i**:11105
4. H. Davenport, On the class number of binary cubic forms (i), *J. Lond. Math. Soc.* **26** (1951), pp. 183–192, errata *ibid* **27** (1951), p. 512. MR **13**:323e
5. H. Davenport, On the class number of binary cubic forms (ii), *J. Lond. Math. Soc.* **26** (1951), pp. 192–198. MR **13**:323f
6. H. Davenport & H. Heilbronn, On the density of discriminants of cubic fields (ii), *Proc. Roy. Soc. Lond. A* **322** (1971), pp. 405–420. MR **58**:10816
7. G. W. Fung & H. G. Williams, On the computation of complex cubic fields, with discriminant  $D \geq -10^6$ , *Math. Comp.* **55** (1990), pp. 313–325, errata *ibid* **63** (1994), p. 433. MR **90m**:11155; MR **94i**:11106
8. H. Hasse, Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage, *Math. Zeitschrift.* **31** (1930), pp. 565–582.
9. H. Hasse, *Zahlentheorie*, Akademie-Verlag GmbH, 1949. MR **11**:580c
10. C. Hermite, Note sur la réduction des formes homogènes à coefficients entiers et à deux indéterminées, *J. reine. angew. Math.* **36** (1848), pp. 357–364.

11. C. Hermite, Sur la réduction des formes cubiques à deux indéterminées, *C.R. Acad. Sci. Paris* **48** (1859), pp. 351–357.
12. P. Llorente & J. Quer, On totally real cubic fields with discriminant  $d < 10^7$ , *Math. Comp.* **50** (1988), pp. 581–594. MR **89g**:11099
13. G.-B. Mathews, On the reduction and classification of binary cubics which have a negative discriminant, *Proc. London Math. Soc.* **10** (1912), pp. 128–138.
14. J.-B. Rosser & L. Schoenfeld, Approximate formulas for some functions of prime numbers, *Illinois J. Math.* **6** (1962), pp. 64–94. MR **25**:1139
15. T. Shintani, On zeta-functions associated with the vector space of quadratic forms, *J. Fac. Sci. Univ. Tokyo, Sec. Ia* **22** (1975), pp. 25–66. MR **52**:5590

DÉPARTEMENT DE MATHÉMATIQUES (A2X), UNIVERSITÉ BORDEAUX I, 351, COURS DE LA LIBÉRATION, 33405 TALENCE, FRANCE

*Current address:* Max-Planck-Institut für Mathematik, Gottfried-Claren-str. 26, 53.225 Bonn, Germany

*E-mail address:* belabas@math.u-bordeaux.fr