ON QUADRATIC FIELDS WITH LARGE 3-RANK

KARIM BELABAS

Abstract. Davenport and Heilbronn defined a bijection between classes of binary cubic forms and classes of cubic fields, which has been used to tabulate the latter. We give a simpler proof of their theorem, then analyze and improve the table-building algorithm. It computes the multiplicities of the $O(X)$ general cubic discriminants (real or imaginary) up to X in time $O(X)$ and space $O(X^{3/4})$, or more generally in time $O(X + X^{7/4}/M)$ and space $O(M + X^{1/2})$ for a freely chosen positive M. A variant computes the 3-ranks of all quadratic fields of discriminant up to X with the same time complexity, but using only $M + O(1)$ units of storage. As an application, we obtain the first 1618 real quadratic fields with $r_3(\Delta) \geqslant 4$, and prove that $\mathbb{Q}(\sqrt{-5393946914743})$ is the smallest imaginary quadratic field with 3-rank equal to 5.

Contents

1. Introduction

Let $d \neq 1$ be a squarefree integer and $\mathrm{Cl}(d)$ be the class group of the quadratic field $\mathbb{Q}(\sqrt{d})$. The Cohen-Lenstra heuristics [7] give a clear conjectural picture of what $\mathrm{Cl}(d)$ should look like on average. In particular, let $r_p(d) =$

1991 *Mathematics Subject Classification.* 11R11, 11R16, 11Y40.
Key words and phrases. Cubic Fields, Quadratic Fields, 3-Rank.

$\dim_{\mathbb{F}_p} \mathrm{Cl}(d)/\mathrm{Cl}(d)^p$, which counts the number of cyclic factors in the p-Sylow subgroup of $\mathrm{Cl}(d)$. The case $p = 2$ is easy since genus theory gives a formula for $r_2(d)$, depending only on the primes dividing the discriminant Δ of $\mathbb{Q}(\sqrt{d})$, see e.g. [19]; in particular, $r_2(d) = \omega(d) + O(1)$ is unbounded as $d \to \infty$, where $\omega(d)$ counts the number of distinct prime divisors of d. For odd primes p, the heuristics predict that the set $\{\Delta : r_p(\Delta) = k\}$ should have positive natural density, for all $k \geqslant 0$. (The density is trivially 0 for $p = 2$ and any given k, since the condition $r_2(\Delta) = k$ bounds $\omega(\Delta)$.) When $p > 2$, this has not been proved for a single pair (p, k); nor is it known that the set is non-empty for a single $k > 6$.

On the other hand, for any fixed p, explicit constructions of Yamamoto [31], Mestre [24] , Craig [8] and Diaz y Diaz [15, 14] provide sparse but infinite families of Δ satisfying $r_p(\Delta) \geqslant r(p)$, where $r(3) = 4$, $r(5) = 3$ and $r(p) = 2$ otherwise. These families all have density 0: they are given by values of polynomials of large degree at well chosen integer points. Most constructions produce independent elements in what Cohen [6] calls the p-Selmer group of $K = \mathbb{Q}(\sqrt{d})$, which is defined as

$$\{\gamma \in K^* : (\gamma) = I^p, I \in I(K)\}/K^{*p} \sim \mathrm{Cl}(K)/\mathrm{Cl}(K)^p \oplus U(K)/U(K)^p,$$

where $I(K)$ and $U(K)$ are the ideal and unit group of K. So, usually, the constructions for imaginary quadratic fields guarantee a p-rank which is larger by 1 than the corresponding construction for real fields, where the fundamental unit interferes. This is consistent with the Cohen-Lenstra heuristics which predict lower p-ranks in the latter case. A number of miscellaneous individual Δ are also known, such that $r_p(\Delta)$ is a little larger; published records include $r_3 = 5$ and 6 (Llorente – Quer [22] and Quer [26]), $r_5 = 4$ (Schoof [28]), $r_7 = 3$ (Solderitsch [30]), $r_{11} = 3$ (Leprévost [21]).

For $p = 3$, Davenport and Heilbronn [12] have computed the average order of the quantity $3^{r_3(\Delta)}$, as Δ runs through the discriminants of quadratic fields, thus bounding from below the density of $\{\Delta : r_3(\Delta) = 0\}$, and from above that of $\{\Delta : r_3(\Delta) \geqslant 1\}$. Their proof doesn't provide any explicit Δ belonging to either set. It uses class field theory to link $3^{r_3(\Delta)}$ to cubic fields of discriminant Δ, and an explicit bijection between these and classes of binary cubic forms satisfying simple adelic conditions.

The present paper is a sequel to [1] which counted cubic fields using Davenport and Heilbronn theory, an approach pioneered by Ennola and Turunen [17]. In §2, we review this algorithm and the theory of cubic rings, with a significantly simpler proof than Davenport and Heilbronn's original one. In §3, we improve the algorithm and analyze its new complexity. In §4, we specialize to the 3-rank of quadratic fields and present a heuristic improvement to detect quadratic fields with large 3-rank, reducing memory use by a linear factor depending on the target rank. Finally we give some timings and find the smallest quadratic field of 3-rank equal to 5.

ACKNOWLEDGEMENTS: I would like to thank Henri Cohen for many stimulating discussions on these subjects, as well as Francisco Diaz y Diaz who provided the original motivation for this work. I am indebted to Manjul Bhargava for the communication of [3]. The computer searches were run at the *Unité Mixte de Service* Medicis (`medicis.polytechnique.fr`). Part of this paper was written as the author enjoyed the hospitality of the Max-Planck-Institut für Mathematik (Bonn).

2. The original algorithm

2.1. **Davenport-Heilbronn theory.** Let $(a,b,c,d) \in \mathbb{Z}^4$ denote the integral binary cubic form $F(x,y) = ax^3 + bx^2y + cxy^2 + dy^3$. Such a form is said to be primitive if $\gcd(a,b,c,d) = 1$. Let Φ be the set of classes of primitive irreducible integral binary cubic forms modulo the natural action of $\mathrm{GL}(2,\mathbb{Z})$: $\gamma.F(x,y) = F\big((x,y)\gamma\big)$. If F belongs to Φ and (a,b,c,d) to F, we write

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

The following theorem is due to Delone and Faddeev [13, §15]:

Theorem 2.1. *The index form induces a one-to-one correspondence preserving the discriminant, between binary classes of irreducible integral cubic forms modulo* $\mathrm{GL}(2,\mathbb{Z})$ *and isomorphism classes of orders of cubic number fields. The inverse map is given by* $\phi_{FO} : F \mapsto \mathbb{Z}[1, a\theta, a\theta^2 + b\theta]$, *where* $F = (a,b,c,d)$ *and* $(\theta : 1)$ *is a root of* F.

Let FD denote the set of fundamental discriminants by the standard local conditions: $\mathrm{FD} = \cap\, \mathrm{FD}_p$, where p runs over all prime numbers and

$$\mathrm{FD}_2 = \big\{\Delta \in \mathbb{Z} : \Delta \equiv 1 \pmod 4 \text{ or } \Delta \equiv 8, 12 \pmod{16}\big\} \ ,$$

$$\mathrm{FD}_{p\neq 2} = \big\{\Delta \in \mathbb{Z} : p^2 \nmid \Delta\big\} \ .$$

Davenport and Heilbronn [12], unaware of Delone-Faddeev's result, specialized it to *maximal* orders, themselves associated to their quotient field: let $U = \cap U_p$ and $V = \cap V_p$, where

$$V_p = \big\{F \in \Phi : \mathrm{disc}\, F \in \mathrm{FD}_p\big\} \ ,$$

$$U_p = \big\{F \in \Phi : F \text{ is not equivalent to a form } (a,b,pc,p^2d)\big\} \supset V_p$$

(This is different from, but equivalent to, the original formulation.)

Theorem 2.2 (Davenport-Heilbronn)**.** *The cubic extensions of* $\mathbb{Q}$ *(embedded in a fixed algebraic closure* $\overline{\mathbb{Q}}$*), up to isomorphism, are in one-to-one correspondence with the elements of* U. *This bijection preserves the discriminant.*

Proof. It follows from the proof of Theorem 2.1 that the image of a cubic order is an irreducible form F. Let $\mathcal{O} := \phi_{FO}(F)$. If F is not primitive, F/λ is integral for some $\lambda > 1$, and $\mathcal{O}$ would be a strict suborder of $\phi_{FO}(F/\lambda)$, hence not maximal.

Maximality is a local property: $F \in U_p$ if and only if $\mathcal{O}$ is maximal at p. Indeed, we can assume that p divides $\mathrm{disc}(F) = \mathrm{disc}(\mathcal{O})$, as there is no problem

otherwise. Since $p \nmid F$, one can pick a representative f such that f modulo p has no root at infinity, and has its multiple root at 0. The characterization of U_p follows immediately from Dedekind's criterion, see e.g. [5, §6.1.2]. □

The original proof was much more involved. Bhargava [3] independently worked out a direct proof of this result, valid for general cubic rings. In his thesis [4], he generalized these constructions to quartic rings, and proved many related density results.

Corollary 2.3. *If $\Delta \in \mathrm{FD}$, and $k = \mathbb{Q}(\sqrt{\Delta})$, the cyclic cubic unramified extensions of k correspond bijectively to the classes of V of discriminant Δ. In particular*

$$\#\{F \in V, \mathrm{disc}(F) = \Delta\} = \frac{3^{r_3(\Delta)} - 1}{2}.$$

Proof. See [12] and Hasse [18]. □

2.2. **Old algorithm and new analysis.** In [1], we gave an algorithm to enumerate isomorphism classes of cubic fields up to a given discriminant bound using the results of §2.1. An essential ingredient was the nice reduction theory for classes of binary cubic forms[1], yielding two computationally convenient fundamental domains for the $\mathrm{GL}(2,\mathbb{Z})$ action on binary cubic forms, one for each signature.

We make a slight change in the definition of Davenport and Heilbronn sets, which is convenient for algorithmic purposes: U_p, V_p are subsets of Φ, *i.e.* are classes of forms, assumed to be primitive and irreducible. We denote by $\widehat{\Phi}$ the set of *reduced* integral binary cubic forms (in the sense of [1]), *not necessarily primitive nor irreducible*, and define subsets $\widehat{U}_p$, $\widehat{V}_p$, of $\widehat{\Phi}$ by the same congruence conditions as in §2.1, adding the condition that forms in $\widehat{U}_p$ are not 0 modulo p. The global objects $\widehat{U} = \cap_p \widehat{U}_p$ and $\widehat{V} = \cap_p \widehat{V}_p$ are the same as before, $\widehat{U}$ (resp. $\widehat{V}$) is a set of canonical representatives for classes in U (resp. V):

Lemma 2.4. *$F \in \widehat{U}$ if and only if the class of F belongs to U. The same statement holds for V and $\widehat{V}$.*

Proof. It suffices to prove that elements of $\widehat{U}$ are primitive and irreducible (since $\widehat{V} \subset \widehat{U}$). The first statement is obvious, the second one is [1, Lemma 1.2(5)]. □

The algorithm iterates over reduced forms using four embedded loops on a, b, c, d in this order, enforcing intricate but essentially trivial inequalities. For each such point the local conditions $(a,b,c,d) \in \widehat{U}$ is checked. We first evaluate the number of needed iterations:

Lemma 2.5. *Let (a,b,c,d) be a reduced form such that $|\mathrm{disc}(a,b,c,d)| \leqslant X$. Then*

$$0 < a \ll X^{1/4}, \quad b \ll X^{1/4}, \quad ac^3 \ll X, \quad bc \ll X^{1/2},$$

[1]Cremona [9] later pointed out that an even nicer reduction, due to G. Julia, was available for the imaginary case, and worked out improved bounds.

where all constants are effective. The number of triples (a, b, c) satisfying the above inequalities is $O(X^{3/4})$.

Proof. The first assertions are due to Davenport ([10, Lemma 1], [11, Lemma 1]). The last follows by summation. □

Theorem 2.6. *Let $0 \leqslant X$. The number of reduced forms F, of given signature, such that $|\mathrm{disc}(F)| \leqslant X$ is*

$$C^{\pm}\zeta(2)X + \lambda^{\pm}X^{5/6} + O(X^{2/3+\varepsilon}), \tag{1}$$

where $C^{+} = 1/12$ and $C^{-} = 3C^{+}$ for real and imaginary forms respectively, $\lambda^{\pm} \neq 0$ and any $\varepsilon > 0$. Out of these,

$$\frac{C^{\pm}}{\zeta(3)}X + O(X\exp(-c\sqrt{\log X})) \tag{2}$$

satisfy $F \in \widehat{U}$, and

$$\frac{C^{\pm}}{\zeta(2)}X + O(X\exp(-c\sqrt{\log X})) \tag{3}$$

satisfy $F \in \widehat{V}$, for some $c > 0$.

Proof. The first estimate is due to Shintani [29], who counts the number of *proper* classes, hence twice the cardinality that is of interest to us. The other two are proved in [2], providing a remainder term for Davenport and Heilbronn's original results [12]. □

Remark 2.7. Following Shintani's argument, Roberts [27] gives convincing heuristics leading to a conjectural error term of the form $\Lambda^{\pm}X^{5/6}(1 + o(1))$ in (2), with $\Lambda^{\pm} = \lambda^{\pm}/(2\zeta(2)\zeta(5/3))$, that matches remarkably available numerical data. A conjectural expansion for (3) can be derived in the same way from Roberts refined heuristics [27, Section 5] by letting $\mathrm{Support}(\alpha)$ contain all places.

Corollary 2.8. *Let $1 \leqslant Y \leqslant X$. The number of reduced forms F of given signature such that $X - Y < |\mathrm{disc}(F)| \leqslant X$ is $O(Y + X^{2/3+\varepsilon})$. The number of iterations in the algorithm exhibiting them is $O(Y + X^{3/4})$. Needed bounds are obtained by operating on integers which are $O(X^{3/2})$.*

Proof. The assertion about reduced forms follows from (1). Given (a, b, c), $\mathrm{disc}(F)$ is quadratic in d and the set of suitable d's is easy to determine from the inequalities on $\mathrm{disc}(F)$: either it is empty (at most $O(X^{3/4})$ triples (a, b, c) because of Lemma 2.5), or it yields a list of reduced forms, whose total number, as (a, b, c) runs over all possible triples, is the number of reduced forms. The quadratic equation in d is

$$-27a^2d^2 + (18abc - 4b^3)d + b^2c^2 - 4ac^3 - Z =: Ad^2 + Bd + C$$

for $Z = X$ or $X - Y$. From Lemma 2.5, we obtain $A = O(X^{1/2})$, $B = O(X^{3/4})$, $C = O(X)$, hence the final assertion. □

Remark 2.9. The expected order of magnitude is $O(Y)$, and Theorem 2.6 says it holds when $X^{2/3+\varepsilon} \ll Y$. It cannot hold uniformly in X since discriminants of arbitrarily large multiplicity appear as $X \to \infty$. For instance, if f is a product of n distinct primes $\equiv 1 \pmod{\ell}$, class field theory shows that the number of cyclic fields of prime degree ℓ with discriminant $f^{\ell-1}$ is ℓ^{n-1}. We can apply this to $\ell = 3$, $Y = 1$ and $X_n = (p_1 \dots p_n)^2$, where p_i is the i-th prime congruent to 1 modulo 3.

The local conditions were checked as follows [1, Algorithm 1.3 and Lemma 1.6]:

Lemma 2.10. *Let $F = (a, b, c, d)$ be a reduced cubic form. Let*

$$H_F := (b^2 - 3ac, bc - 9ad, c^2 - 3bd)$$

its Hessian, f_H the content of H_F, and $\Delta_H := \operatorname{disc}(H)/f_H^2$. Then $F \in \widehat{U}$ if and only if

- *$F \in \widehat{U}_2 \cap \widehat{U}_3$.*
- *f_H is squarefree up to powers of 3.*
- *Δ_H and f_H are coprime up to powers of 3.*
- *Δ_H is squarefree up to powers of 2.*

Assuming $F \in \widehat{U}$, then it is in $\widehat{V}$ if and only if $f_H = 1$.

This involves the costly factorization of Δ_H in each iteration: the worst case is $F \in \widehat{V}$, which occurs with probability $1/\zeta(2)^2 \approx 37\%$ according to Theorem 2.6, and implies that $f_H = 1$ and Δ_H is of the order of X. The content $f_H = O(X^{1/2})$ is uniformly much smaller.

We proved in [1] that one can find a canonical equation for cubic fields whose discriminant was bounded by X in time and space linear in the output size. We checked that an integer is squarefree by dividing small primes away (less than some bound P) and using precomputed hashing lists of integers with large square factors. Unfortunately, performance deteriorates quickly if memory is not plentiful: assuming available space is $0 < M \leqslant X$, the algorithm requires that P is of the order of X/M, hence runs in time $O(X^2/M)$: $O(P)$ trial divisions and one hashtable lookup for each of the $O(X)$ iterations. The behavior is quadratic rather than linear as X gets larger and M remains fixed.

3. A better algorithm

3.1. **A modified test for squarefree-ness.** In this section we develop a more efficient approach to check whether a point satisfies the Davenport-Heilbronn conditions. To avoid irrelevant discussion of multiprecision operations in our estimates, we count elementary arithmetic operations on integers. Bit complexity estimates are then easily derived since all needed quantities are $O(X^{3/2})$ integers by Corollary 2.8. These fit in 2 or 3 computer words far beyond the practical range of the algorithms.

Let $F \in \mathbb{Z}[x,y]$ be an integral binary cubic form. For $D \in \mathbb{Z}$, we define an ad hoc function

$$f_U(D) = \begin{cases} 0 & \text{if } p^3 \mid D \text{ for some prime } p \geqslant 5 \\ \prod_{p \geqslant 5,\, p^2 \mid D} p & \text{otherwise} \end{cases}$$

such that computing $f_U(\operatorname{disc} F)$ is almost equivalent to the test $F \in \widehat{U}$:

Lemma 3.1. *$F \in \widehat{U}_p$ for all $p \geqslant 5$ if and only if $f_U(\operatorname{disc} F) \neq 0$ and divides the Hessian of F.*

Proof. This follows from [1, Lemma 2.1]. □

We now explain how to efficiently compute $f_U(a)$:

Lemma 3.2. *We allow precomputations needing time $O(X^{1/2} \log\log X)$ and space $O(X^{1/2})$. Then all $F \in \widehat{U}$ such that $X - Y < |\operatorname{disc}(F)| \leqslant X$ can be output in time $O(Y + X^{3/4})$ and space $O(Y + X^{1/2})$.*

Proof. A list of all primes $p \leqslant X^{1/2}$ is built once and for all, via Erathostenes's sieve, for the listed precomputation cost. Sieving by squares and cubes of the precomputed primes $p \in [5, X^{1/2}]$, we compute the value of $f_U(a)$ for all a in the range $I =]X - Y, X]$, and store the result in a table T_I of length Y. This is done in time

$$\sum_{p \leqslant X^{1/2}} (1 + Y/p^2) + \sum_{p \leqslant X^{1/3}} (1 + Y/p^3) = O(X^{1/2} + Y)$$

and space $O(Y)$.

In each iteration producing a point F, whose discriminant is known to have absolute value $D \in]X - Y, X]$, we check whether F belongs to $\widehat{U}_2$ and $\widehat{U}_3$. If so, we compute D and look up $f := f_U(D)$ in T_I. Then $F \in \widehat{U}$ iff f is non-zero and divides H_F by Lemma 3.1. There are $O(Y + X^{2/3+\varepsilon})$ points to check, all in time $O(1)$ once the lookup table is built, and $O(X^{3/4})$ "empty loops" by Corollary 2.8. □

Corollary 3.3. *The list of cubic fields of discriminant bounded in absolute value by X can be output in time $O(X)$ and space $O(X^{3/4})$, or more generally in time $O(X + X^{7/4}M^{-1})$ and space $O(M + X^{1/2})$ for any $M > 0$.*

Proof. For $k \leqslant X/M$, we apply the previous lemma on subintervals of the form $I_k =](k-1)M, kM]$. We discard T_{I_k} once I_k has been treated, hence we only need $O(X^{1/2} + M)$ space. The running time is dominated by

$$X^{1/2} \log\log X + \sum_{k \leqslant X/M} \left(M + (kM)^{3/4}\right) = O(X(1 + X^{3/4}/M))$$

□

Since the discriminants are produced in narrow intervals, a Distribution Counting sort (see [20, §5.2, Algorithm D]) orders them in time

$$O(M + \#\left\{F \in \widehat{U}, \operatorname{disc}(F) \in I_k\right\})$$

for each I_k; summing over k, ordering the list takes linear time $O(X)$, rather than $O(X \log X)$, invalidating one of the remarks in [1, §5.c]. If we are only interested in 3-ranks, the construction is easier:

Corollary 3.4. *Computing all unramified cyclic cubic extensions of all quadratic fields of discriminant bounded by X can be done in time $O(X + X^{7/4}M^{-1})$, using $M + O(1)$ units of storage, where $M > 0$ can be freely chosen.*

Proof. We compute all reduced forms belonging to $\widehat{V}$ in the requested discriminant range. The result follows from Corollary 2.3, the proof of Lemma 3.2 and Corollary 3.3, with a minor variation. Namely, for F in $\widehat{V}$, we always have $f_U(\operatorname{disc} F) = 1$. So, we define instead a boolean-valued function f_V which is `true` iff its argument is not divisible by p^2 for any $p \geqslant 3$.

We build a lookup table T_{I_k} of `true`/`false` values for squarefree numbers in I_k by sieving with squares of ordinary integers this time (in time $O(M + (kM)^{1/2})$). Then $F \in \widehat{V}$ iff it is in $\widehat{V}_2$ and $f_V(\operatorname{disc} F)$ is `true`. □

In this last Corollary, we compute a generating polynomial for the cubic extensions, a priori not monic, not a class-field theoretic description. Both Corollaries are easily adapted to compute multiplicities of cubic discriminants or 3-ranks of the quadratic fields: we use an auxiliary table of length M to store the multiplicities as the forms belonging to an elementary interval I_k are computed. These algorithms parallelize for a running time $O(M + X^{3/4})$ on X/M processors (linear speedup if $M \approx X^{3/4}$).

3.2. **Further improvements.** When Y is small, there is a discrepancy between the number of forms $O(X^{2/3+\varepsilon})$ and our bound for the number of iterations $O(X^{3/4})$ in Corollary 2.8. It is straightforward to improve on the estimates given in [1] to only generate triples (a, b, c) so that the set of $d \in \mathbb{R}$, such that (a, b, c, d) is both reduced and has a discriminant in the requested range, has positive measure. This still does not guarantee that a suitable $d \in \mathbb{Z}$ exists. We conjecture that this implementation results in only $O(X^{2/3})$ empty loops, but gave up checking all the special cases.

The ratio of the first two main terms in (2) and (3) is $\zeta(2)\zeta(3) \approx 1.98$ so there is little waste: half the reduced forms produce a field. This can be further improved using that if $f \in U_p$, then $p^2 \mid a$ implies $p \nmid b$, which is easily enforced in the *outer* loops. The number of reduced F satisfying this latter condition, and such that $|\operatorname{disc}(F)| \leqslant X$ is asymptotic to $C^{\pm}\zeta(2)X/\zeta(3)$. The waste ratio is now down to $\zeta(2) \approx 1.64$. (All such estimates are proven as in Lemma 4.2 below.)

As an extreme example, take $X = 58343207081 \in \mathrm{FD}$ and $Y = 1$. This is a good stress test for an implementation, since it should point out roundoff

errors and overflows. Generating all 40 reduced forms of discriminant X with the general purpose algorithm described above, we run through $t = 14257624$ triples (a, b, c) and obtain $\log(t)/\log X \approx 0.664$, supporting the $O(X^{2/3})$ empty loops conjecture. Taking advantage of the improvement above, we would get $t' = 11947227$ triples. (Note that $t'/t \approx 0.838$ while $1/\zeta(3) \approx 0.832$.)

If we restrict to fundamental cubic discriminants, it follows from the fact that the Hessian should be primitive that $\gcd(a, b, c) = \gcd(b, c, 3) = 1$. All this is easily enforced and selects only about

$$\frac{35}{38}\prod_p \left(1 - \frac{2p-1}{p^4}\right) \approx 68.6\%$$

of all triples (a, b, c), from local density considerations. Applying this to the above example reduces the number of triples to $t'' = 9844448 \quad (t''/t \approx 0.690)$.

To select a single discriminant as here, it is more efficient to follow Cremona [9, Algorithm 2] and exploit the syzygy between the seminvariants a and $P := b^2 - 3ac$ saying that $4P^3 - 27a^2X$ is a square. For a given (a, b), one can then use a quadratic sieve to dismiss most values of c. Cremona's procedure still runs in time $O(X^{3/4})$, though. Also, this improvement is not practical when Y gets larger. So, to scan a small range of huge discriminants, the direct approach of computing all class groups via subexponential "index calculus" using factor bases, as described for instance in Cohen [5], remains the only choice. Computing multiplicities of general cubic discriminants Δf^2, $\Delta \in \mathrm{FD}$, in this way is equally easy for a given discriminant using a criterion of Hasse [18, Satz 1.] to distinguish between the cubic extension of the quadratic base field which have Galois group $C(6)$ and S_3 over $\mathbb{Q}$, and ray class field machinery as described in Cohen [6] to compute the ring class field mod f of $\mathbb{Q}(\sqrt{\Delta})$.

4. The 3-rank of quadratic fields

4.1. **Quadratic forms.** Another natural way to tabulate 3-ranks would be to use Gauss reduction of *quadratic* forms. But even in the easier imaginary case, it is not a practical alternative:

Lemma 4.1. *Let $0 \leqslant Y \leqslant X$. Computing all reduced quadratic forms F such that $X - Y < -\operatorname{disc}(F) \leqslant X$ requires $O(YX^{1/2} + X)$ steps and $O(1)$ storage.*

Computing the 3-ranks of the corresponding quadratic fields (when $F \in \widehat{V}$) using M units of storage requires time $O(X^{3/2}\log X + X^2/M)$.

Proof. A reduced definite form (a, b, c) in the requested range satisfies $|b| \leqslant a \leqslant \sqrt{X/3}$, and $0 \leqslant (X + b^2)/4a - c \leqslant Y/4a$, which adds up to

$$\sum_{a \ll X^{1/2}} \sum_{|b| \leqslant a} \big(1 + (Y/4a)\big) \ll X + X^{1/2}Y$$

iterations. We check whether the discriminant is fundamental using the same sieve as in Corollary 3.4; summing up over the $](k-1)M, kM]$, we obtain the required

time complexity. Storing all forms in that range would result in space complexity of $O(M^{3/2})$, but it is enough to store the number of forms F of exponent 3 (checked by reducing F^3 to the principal form, using $O(\log X)$ reduction steps) for each discriminant in the range, since the number of such forms is 3^{r_3}, assuming the discriminant is fundamental. This results in $O(M + X^{1/2})$ storage. □

This is worse than Corollary 3.4 by a rough factor of $\sqrt{X}$. Computing the 3-ranks of real quadratic fields with this method would be even more problematic since reduced forms would have to be grouped into cycles; also the principal cycle may contain many reduced forms, and the check $F^3 = 1$ cannot be expected to run in time $O(\log X)$. Of course, this direct approach could afford much more information (the full class groups) than what the algorithm of §3.1 can provide.

4.2. **A heuristic variant: looking for high 3-ranks.** Even though the algorithm from §3.1 improves significantly on the original one, it still suffers from huge memory requirements, due to the necessity to maintain sieves in order to check for squarefree-ness on the one hand, and on the other hand to store multiplicities of discriminants. We will improve on the second aspect in the next subsection, with the specific aim of locating quadratic fields with high 3-rank but this requires switching to a heuristic variant of the algorithm, which we now describe.

4.2.1. *Relaxing the Davenport-Heilbronn conditions.* Corollary (2.3) implies that to find Δ such that $r_3(\Delta)$ is large, we need to find many cubic fields sharing the same fundamental discriminants. Moreover, their number is of the very special form $(3^r - 1)/2$, $r \in \mathbb{N}$. If we forget about the Davenport-Heilbronn conditions, we still expect to find about $O(Y)$ reduced forms in our fundamental domains, counting multiplicities; Theorem 2.6 gives a rigorous, if pessimistic, bound of the order of $Y + X^{2/3+\varepsilon}$. We also expect very few of the resulting multiplicities to be of the form $(3^r - 1)/2$ provided we aim for a large enough r, e.g 4 or 5. We can then check directly the resulting short list of discriminants to weed out the non-fundamental ones, using our favourite factorization algorithms. Any remaining discriminant Δ, being fundamental, is associated to elements of $\widehat{V}$.

In fact, it is better not to relax completely these conditions, since otherwise we will produce too many extraneous forms, which will hide out the interesting clusters from the next section. By Lemma 2.10, one eliminates all forms whose Hessian is not primitive. Instead of checking whether the discriminant is fundamental, we check it belongs to V_2 and trial divide by the square of a few small primes, up to 13^2 say, ensuring that $\Delta \in \cap_{p \leqslant 13} V_p$.

Let $N^{\pm}(X, P)$ denote the number of classes of binary cubic forms F whose Hessian is primitive, $F \in V_p$ for $p \leqslant P$, and such that $0 < \pm \operatorname{disc}(F) \leqslant X$. Theorem 2.6 (3) states that

$$N^{\pm}(X, \infty) \sim \frac{C^{\pm}}{\zeta(2)} X$$

asymptotically; the simplified check described above corresponds to truncating the Euler product:

Lemma 4.2. *Let $P \geqslant 3$ and $N^{\pm}(X,P)$ be as above. We have*

$$N^{\pm}(X,P) \sim C^{\pm} \prod_{p \leqslant P} (1-p^{-2})\, X$$

where $C^{\pm}$ is as in Theorem2.6.

Proof. We use [2, Theorem 2.3]. Let

$$s(p) = \frac{1}{p^8} \#\{F \pmod{p^2}, F \in V_p\}$$

and

$$s_2(p) = \frac{1}{p^2} \#\{F \pmod{p}, H_F \not\equiv 0 \pmod{p}\}$$

Davenport and Heilbronn [12] computed $s(p) = (1-p^{-2})^2$, and proved that the number of forms such that $|\mathrm{disc}(F)| \leqslant X$ and $p^2 \mid \mathrm{disc}(F)$ (this is in particular the case when $H_F \equiv 0 \pmod{p}$) is $O(X/p^2)$.

We have $H_F \equiv 0 \pmod{p}$ if and only if $b^2 \equiv 3ac$, $c^2 \equiv 3bd$, and $bd \equiv 9ad$ modulo p; a straightforward count yields $s_2(p) = (1-p^{-2})$ for $p \neq 3$. The hypotheses from [1, Theorem 2.3] are now satisfied, and we obtain

$$\frac{N^{\pm}(X,P)}{X} \;\; \to \;\; C^{\pm} \zeta(2) \prod_{p \leqslant P} \frac{s(p)}{s_2(p)} \prod_{p \geqslant 2} s_2(p)$$

□

Hence taking $P = 13$, we see that the percentage of correct fields among the forms we find tends to

$$\prod_{p>13} (1-p^{-2}) = \frac{715715}{442368\,\zeta(2)} \approx 98.4\%.$$

So the vast majority of surviving forms do correspond to a field. Taking $P > 13$ would only yield a marginal improvement, whereas we can use the fact that $q = \prod_{p \leqslant 13} p^2 < 2^{32}$ is smaller than the computer word size to efficiently weed out all small square factors in a single reduction modulo q, followed by a few small divisions.

It is hard to analyze precisely the behavior of this algorithm: we can count the number of cubic fields of given discriminant in terms of 3-ranks of ring class groups as in Mayer [23]. Unfortunately, it is difficult to use the resulting formulas to decide how likely non-fundamental discriminant are to have a multiplicity of the form $(3^r-1)/2$. In practice it works remarkably well, a typical run with $Y = 10^8$ aiming for rank larger than 3 produces at most one or two discriminants, which always happen to be fundamental. Note that, although the efficiency of the algorithm is based on a heuristic argument, namely that few Δ will survive before the expensive final factorizations, the correctness of its output is not.

4.2.2. *Clusters.* Using the fact that a fundamental discriminant is $\equiv 0, 1 \pmod 4$, one could divide the memory requirements by 2 by compacting the lookup tables. However, when looking for high 3-ranks it is preferable to use a "cluster" approach: count the multiplicity of a range of k consecutive integers, instead of individual discriminants; then investigate interesting small ranges (the ones with high multiplicity) via direct class group computations, or by letting the same algorithm run on this much smaller interval.

From (3), a typical cluster of k consecutive integers should have multiplicity around $C^{\pm}k/\zeta(2)$. Although the known or conjectured remainder terms ($O(e^{-c\sqrt{\log X}})$ and $O(X^{5/6})$ respectively) are far too weak to prove anything useful in this context, a good heuristic seems to take

$$k \approx \alpha B \frac{\zeta(2)}{C^{\pm}} \quad \text{for some } 0 < \alpha < 1 \tag{4}$$

where $B = (3^{r_3} - 1)/2$ is the multiplicity one is interested in for individual fields. If we only check clusters of multiplicity larger than B, we never miss an interesting field (contributing B to the total multiplicity) and few uninteresting clusters should survive (the average cluster has multiplicity αB). Experiments for $B = 40$ (looking for 3-rank equal to 4) indicate that $\alpha \approx 1/4$ or $1/3$ is a good practical choice.

Few class group computations are necessary to check a cluster: for each fundamental discriminant in it, compute the class group and the 3-rank r, and decrease the cluster multiplicity by $(3^r - 1)/2$; when the latter drops below B, we are done. It is also possible to store individual discriminants separately as soon as the cluster they fall into has multiplicity $B - 1$, to optimize the order in which those class group computations are done (picking the discriminants with largest apparent multiplicity first). But class group computations take a negligible amount of time compared to the time spent locating the clusters. It does not seem worthwile to decrease the robustness of the cluster algorithm for these optimizations: in fact even if a given implementation misses a few fields due to roundoff errors or hardware faults, it has a good chance of locating the cluster nevertheless since neighboring discriminants should more than make up for the forms it lost. This is no longer true if we take the computed cluster multiplicity at face value and use an early abort strategy.

4.2.3. *Mirror theorem.* Scholz's mirror theorem asserts that $\delta(d) := 1 + r_3(d) - r_3(-3d) \in \{0, 1\}$ if $d > 0$. Hence it is enough to consider real fields and to check directly the mirror complex field once a high enough real 3-rank is detected. Using only the heuristic (4) above, one does not gain anything for the cluster size, since k is 3 times larger for a real field of the same rank (since $C^- = 3C^+$), but the target rank is a priori one less.

On the other hand, under the Cohen-Lenstra model, Dutarte's heuristic [16] predicts that the probability to improve on a 3-rank by looking through the mirror (changing $d \to -3d$) is small:

Conjecture 4.3 (Dutarte)**.** *Let P be the Cohen-Lenstra "probability"; then*

$$P(\delta(\Delta) = 0 \mid r_3(\Delta) = r) = 3^{-r-1}$$

$$P(\delta(\Delta) = 1 \mid r_3(-3\Delta) = r) = 3^{-r}$$

as $\Delta > 0$ runs through the discriminant of real quadratic fields.

The apparent paradox that both these quantities should be small comes from the fact that, under Cohen-Lenstra's model, $P(r_3(\Delta > 0) = r)$ is roughly 3^r times smaller than $P(r_3(\Delta < 0) = r)$. From this new heuristic it looks a good idea to find imaginary quadratic fields of high 3-rank by targeting real quadratic fields of the *same* rank. Unfortunately, we now run the risk of missing a few fields.

5. Results and timings

5.1. **Looking for $r_3 = 4$.** We ran our implementations of the standard (rigorous checks, no cluster) and modified (relax local conditions, use clusters) algorithms on a Pentium III computer (1GHz CPU, 1GB RAM). We allocated 256MB to the standard program, and 128MB to the one using clusters.

We produced the list of $-10^{10} < \Delta < 0$, such that $r_3(\Delta) \geqslant 4$. There are 26 such imaginary fundamental discriminants, and they all satisfy $r_3(\Delta) = 4$ (the starred fields were discovered by Diaz y Diaz [14]):

$$-653329427^*,\ -1876623871,\ -2520963512^*,\ -2676277123,\ -3146813128^*,$$
$$-3972542271,\ -4724490703^*,\ -5252241199^*,\ -5288116947^*,\ -5866841451,$$
$$-6127792087,\ -6223830596,\ -6903777631,\ -6905985272^*,\ -7189850292,$$
$$-7309564084,\ -7311232679^*,\ -7592829611,\ -7993105123^*,\ -8308370723^*,$$
$$-8417780779,\ -8418280523^*,\ -8624990111,\ -9552870967,\ -9775810067^*,$$
$$-9906365947^*.$$

The computing time for the standard algorithm was 4 hours. This goes down to 44 minutes using clusters of size 2^6 ($\alpha \approx 1/4$): the program found 39 clusters of multiplicity larger than $(3^4 - 1)/2$ in 42 minutes and spent 2 more minutes for unconditionnal direct class group computations, yielding the 26 fields above.

The required class groups were computed by PARI/GP [25], using the routine `quadclassunit`, with third parameter equal to $[0.1, \sqrt{|\Delta|/3} / \log^2 |\Delta|]$, preventing it from assuming the GRH. With these parameters, PARI outputs forms which are guaranteed to generate the class group, from which we obtain a set of generators for the 3-Sylow. We then checked, using Gauss reduction, that the computed order for these generators was correct, and that they were independent[2].

According to Conjecture 4.3, given that the imaginary 3-rank is 4, we should have $r_3(-\Delta) = 4$ with probability $3^{-4} \approx 1.2\%$. As expected, $r_3(-3\Delta) = 3$ for all these fields.

We then experimented with real quadratic fields with $r_4(\Delta) \geqslant 4$, letting the program run until it had found the first 26 such fields:

[2]The more general built-in PARI routines `bnfinit`/ `bnfcertify` could have been used here, but would make checking the clusters more expensive than locating them.

58343207081, 117097095001, 165780397949, 185418133372, 193395920824, 198267101688, 241178598748, 274688570237, 297414764897, 314582172161, 352054233697, 360366596041, 369883565164, 380649804421, 459967693253, 461887196156, 468433123709, 479292608317, 501493520533, 509316379432, 555103596037, 594823573237, 604233145121, 610409578681, 647704535605, 653339592337.

The computing time was 10 days and 14 hours with the standard algorithm. We then looked for interesting clusters up to $\Delta = 653339592337$, for comparison. Using clusters of size 2^7 ($\alpha \approx 1/6$), the program finds 36 clusters in 16 hours. Raising cluster size to 2^8 ($\alpha \approx 1/3$), we get 419 clusters in 15 hours. Again, no pleasant surprise: these 26 fields all have 3-rank exactly equal to four and Scholz defect 1.

5.2. **Looking for $r_3 = 5$.** The quadratic field of discriminant

$$\Delta_0 = -5393946914743$$

was discovered by Quer, and has $r_3(\Delta_0) = 5$. Our objective was to look for the first real quadratic field of the same 3-rank (the smallest known, also found by Quer, has discriminant about 10^{18}, out of reach of our programs), and to prove that Δ_0 is the smallest discriminant in absolute value such that $r_3(\Delta_0) = 5$.

We ran a search for $r_3(\Delta) = 4$ for all $0 < \Delta \leqslant 3\,|\Delta_0| \approx 1.6\,10^{13}$, using clusters of size $2^8 = 256$ ($\alpha \approx 1/3$). The search ran for a total of 136 days divided between eight PIII at 500MHz. Each PC was in charge of an interval of length $M = 10^{12}$, using 128MB of memory, which enabled it to check an interval of length 2^{35} in one pass. They found 16686 clusters of multiplicity larger than 40, all of which happen to have multiplicity lower than both $2 \times (3^4 - 1)/2$ and $(3^5 - 1)/2$. This means that we expect at most one interesting field per cluster and it will have 3-rank less than 4 in any case.

The same program was ran again on each of these 16686 intervals of length 256 (for about 20 days), yielding 1618 real fields of 3-rank equal to 4, with the following distribution:

k	$\Delta \in [(k-1)M, kM]$	Time cluster generation	#clusters
1	59	2.1	709
2	79	2.8	885
3	80	3.3	898
4	95	3.8	996
5	104	4.5	939
6	105	5.2	1054
7	96	6.0	1094
8	120	6.7	1044
9	107	7.3	1113
10	89	8.0	992
11	119	8.6	1096
12	86	9.1	1155
13	121	9.7	1115

14	108	10.2	1137
15	126	10.7	1123
16	104	11.2	1131
17	20 (up to $3\,\lvert\Delta_0\rvert$)	1.5	410
Total	1618 fields	110 days	16686 clusters

The average size of a good cluster (yielding a field) was $\mu = 52.9$, with standard deviation $\sigma = 3.7$, the smallest of which had multiplicity 43. The average size of a bad cluster was 42.0 ($\sigma = 3.4$), the largest of which had multiplicity 68, due to a non-fundamental discriminant of multiplicity 39.

To double check these results, we ran PARI/GP to directly compute class groups for all fields in the clusters, letting it assume the truth of the GRH so as to use a subexponential algorithm (using `quadclassunit`; about 7 hours total time). There was no discrepancy.

The predicted value for $P(r_4(\Delta > 0) = 4)$ in the Cohen-Lenstra model is

$$\frac{243}{268029132800}\prod_{k\geqslant 1}(1-3^{-k}) \approx 5.078\ 10^{-10}$$

Using our 17 data points, and dividing by the well-known density for quadratic discriminants $3/\pi^2$, the experimental probability increases monotonously from $1.94\ 10^{-10}$ to $3.29\ 10^{-10}$. The order of magnitude looks right, but not much can be said about the actual value.

Using PARI/GP again, this time using the technique described in the previous subsection, we computed unconditionally the 3-ranks of the complex mirrors of the 1618 real fields we found (4 hours time). According to Dutarte's heuristic, roughly $1618/3^5 \approx 6.7$ of them should have a complex mirror of 3-rank equal to 5. In fact there are exactly 6 of them, yielding the pairs

3011319569053	−9033958707159
3612077876156	−10836233628468
5659632455069	−16978897365207
11339239749913	−34017719249739
16039985807017	−48119957421051
16181840744229	−5393946914743

and $\lvert\Delta_0\rvert$ is indeed the smallest. This computation also proves that there exists no $0 < \Delta \leqslant 3\,\lvert\Delta_0\rvert$ such that $r_3(\Delta) > 4$.

References

[1] K. Belabas, A fast algorithm to compute cubic fields, *Math. Comp.* **66** (1997), pp. 1213–1237.

[2] K. Belabas, On the mean 3-rank of quadratic fields, *Compositio Mathematica* **118** (1999), pp. 1–9.

[3] M. Bhargava, A simple proof of the Davenport-Heilbronn theorem, 1999, preprint.

[4] M. Bhargava, Higher composition laws, Ph.D. thesis, Princeton University, 2001.

[5] H. Cohen, *A course in computational algebraic number theory*, third ed., Springer-Verlag, 1996.

[6] H. Cohen, *Advanced topics in computational number theory*, Springer-Verlag, 2000.

[7] H. Cohen & H. W. Lenstra, Jr., Heuristics on class groups of number fields, in *Number theory, Noordwijkerhout 1983* (Berlin), Lecture Notes in Math., vol. 1068, Springer, Berlin, 1984, pp. 33–62.
[8] M. Craig, A construction for irregular discriminants, *Osaka J. Math* **14** (1977), pp. 365–402.
[9] J. E. Cremona, Reduction of binary cubic and quartic forms, *LMS J. Comput. Math.* **2** (1999), pp. 64–94 (electronic).
[10] 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.
[11] H. Davenport, On the class number of binary cubic forms (ii), *J. Lond. Math. Soc.* **26** (1951), pp. 192–198.
[12] H. Davenport & H. Heilbronn, On the density of discriminants of cubic fields (ii), *Proc. Roy. Soc. Lond. A* **322** (1971), pp. 405–420.
[13] B. N. Delone & D. K. Faddeev, *The theory of irrationalities of the third degree*, Translations of Mathematical Monographs, vol. 10, American Mathematical Society, 1964.
[14] F. Diaz y Diaz, On some families of imaginary quadratic fields, *Math. Comp.* **32** (1978), no. 142, pp. 637–650.
[15] F. Diaz y Diaz, Sur le 3-rang des corps quadratiques réels, *Prépublications de la faculté d'Orsay*, 1978.
[16] P. Dutarte, Compatibilité avec le Spiegelungssatz de probabilités conjecturales sur le p-rang du groupe des classes, in *Number theory, 1983–1984* (Besançon), Univ. Franche-Comté, Besançon, 1984, pp. Exp. No. 4, 11.
[17] V. Ennola & R. Turunen, On totally real cubic fields, *Math. Comp.* **44** (1985), no. 170, pp. 495–518.
[18] H. Hasse, Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage, *Math. Zeitschrift.* **31** (1930), pp. 565–582.
[19] C. S. Herz, *Seminar on Complex Multiplication. VII. Construction of class fields*, Lect. notes in Math., vol. 21, Springer-Verlag, Berlin, 1966.
[20] D. E. Knuth, *The art of computer programming. Vol. 2*, second ed., Addison-Wesley Publishing Co., Reading, Mass., 1981, Seminumerical algorithms, Addison-Wesley Series in Computer Science and Information Processing.
[21] F. Leprévost, Courbes modulaires et 11-rang de corps quadratiques, *Experiment. Math.* **2** (1993), no. 2, pp. 137–146.
[22] P. Llorente & J. Quer, On the 3-Sylow subgroup of the class group of quadratic fields, *Math. Comp.* **50** (1988), no. 181, pp. 321–333.
[23] D. C. Mayer, Multiplicities of dihedral discriminants, *Math. Comp.* **58** (1992), no. 198, pp. 831–847, S55–S58.
[24] J.-F. Mestre, Corps quadratiques dont le 5-rang du groupe des classes est $\geqslant 3$, *C. R. Acad. Sci. Paris Sér. I Math.* **315** (1992), no. 4, pp. 371–374.
[25] PARI/GP, version `2.1.5`, Bordeaux, 2003, `http://pari.math.u-bordeaux.fr/`.
[26] J. Quer, Corps quadratiques de 3-rang 6 et courbes elliptiques de rang 12, *C.R. Acad. Sci. Paris Série I Math.* **305** (1987), pp. 215–218.
[27] D. P. Roberts, Density of cubic field discriminants, *Math. Comp.* **70** (2001), no. 236, pp. 1699–1705.
[28] R. J. Schoof, Class groups of complex quadratic fields, *Math. Comp.* **41** (1983), no. 163, pp. 295–302.
[29] 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.
[30] J. J. Solderitsch, Quadratic fields with special class groups, Ph.D. thesis, Lehigh University, 1977.

[31] Y. Yamamoto, On unramified Galois extensions of quadratic number fields, *Osaka J. Math.* **7** (1970), pp. 57–76.

Karim Belabas
Université Paris–Sud
Département de Mathématiques (bât. 425)
F-91405 Orsay (France)
Karim.Belabas@math.u-psud.fr