Journal de Théorie des Nombres
de Bordeaux **8** *(1996), 283–313*

On the computation of quadratic 2-class groups

par Wieb BOSMA et Peter STEVENHAGEN

Résumé. Nous décrivons un algorithme dû à Gauss, Shanks et Lagarias qui étant donné un entier $D \equiv 0, 1 \mod 4$ non carré et la factorisation de D, détermine la structure du 2-sous-groupe de Sylow du groupe des classes de l'ordre quadratique de déterminant D ; la complexité de cet algorithme est en temps polynomial probabiliste en $\log |D|$.

Abstract. We describe an algorithm due to Gauss, Shanks and Lagarias that, given a non-square integer $D \equiv 0, 1 \mod 4$ and the factorization of D, computes the structure of the 2-Sylow subgroup of the class group of the quadratic order of discriminant D in random polynomial time in $\log |D|$.

1. Introduction.

Let $D \equiv 0, 1 \bmod 4$ be a non-square integer, and denote by $\mathrm{Cl}(D)$ the strict class group of the quadratic order $\mathcal{O} = \mathbf{Z}[(D + \sqrt{D})/2]$ of discriminant D. The group $\mathrm{Cl}(D)$ may be identified with the class group of primitive integral binary quadratic forms of discriminant D, and this yields a description that is very useful for explicit computations. There do exist algorithms that compute $\mathrm{Cl}(D)$ in a time that is subexponential in the length $\log D$ of the input; see [4] and [6, 8] for the respective cases $D > 0$ and $D < 0$. However, these algorithms are far from polynomial-time, and it is unlikely that they will be used in the near future for discriminants D having more than, say, 50 decimal digits.

The algorithm in this paper only computes the 2-Sylow subgroup $\mathcal{C}(D) = \mathrm{Cl}(D)_2$ of the class group. It runs in random polynomial time [9, 10] if the factorization of D is given as part of the input, and it handles most 50-digit discriminants in a matter of seconds. In contrast to the situation for algorithms that compute the full class group $\mathrm{Cl}(D)$, it turns out that not only the size of D, but also the number of prime factors of D and the

Class. Math. : Primary 11Y40, 11R11; Secondary 11E16, 11E20.
Mots-clés : Quadratic 2-class groups, binary and ternary quadratic forms.
Manuscrit reçu le 29 janvier 1996

'depth' of the resulting class group greatly influence the running time. For instance, consider the 501-digit discriminant

$$D = (10^{100}+949)(10^{100}+1293)(10^{100}+2809)(10^{100}+6637)(10^{100}+22261),$$

which is the product of five primes exceeding 10^{100} that are 1 mod 4 and squares modulo each other. It is chosen in such a way that $\mathcal{C}(D) \cong C_4^3 \times C_{128}$ has high 4-rank. It takes less than a second to find the elementary abelian 2-groups $\mathcal{C}(173 \cdot D) \cong C_2^5 \cong \mathcal{C}(-43 \cdot D)$. Now consider the sample of 2-class groups

$$\begin{aligned}
\mathcal{C}(-8 \cdot D) \cong \mathcal{C}(61 \cdot D) &\cong C_2 \times C_2 \times C_2 \times C_2 \times C_4 \quad \text{(30 and 81 sec)}\\
\mathcal{C}(-311 \cdot D) \cong \mathcal{C}(137 \cdot D) &\cong C_2 \times C_4 \times C_4 \times C_4 \times C_4 \quad \text{(127 and 183 sec)}\\
\mathcal{C}(-359 \cdot D) \cong \mathcal{C}(1129 \cdot D) &\cong C_4 \times C_4 \times C_4 \times C_4 \times C_8 \quad \text{(220 and 385 sec)}\\
\mathcal{C}(-2711 \cdot D) \cong \mathcal{C}(433 \cdot D) &\cong C_2 \times C_4 \times C_4 \times C_4 \times C_{64} \quad \text{(309 and 596 sec)}\\
C_{256}\mathcal{C}(-1663 \cdot D) &\cong C_2 \times C_4 \times C_4 \times C_4 \times C_{4096} \quad \text{(576 sec)}
\end{aligned}$$

with approximate timings on a Sun MP670 workstation indicated in brackets. We see that the algorithm takes more time if the resulting 2-class group is 'further' from elementary 2-abelian, and that the real quadratic case $D > 0$ appears to be somewhat harder than the imaginary quadratic case. We will give a complete quantitative explanation for both observations. Note that computation of the full class group for any of these discriminants is currently completely unfeasible.

The basis of our algorithm is a method to solve the duplication equation $2x = c$ in quadratic class groups that is due to Gauss [7, section 286]. It has been implemented and used to compute various imaginary quadratic 2-class groups $\mathcal{C}(D)$ by Shanks [11]. All of Shanks's examples were cyclic or almost cyclic, and he did not give an algorithm to handle general D. Doing so is essentially a matter of linear algebra, as was shown by Lagarias [10], who analyzed the algorithm from the point of view of its computational complexity but referred to [11] for a practical implementation. There does not seem to be a complete description of the mathematical content of the algorithm in the existing literature, and this paper intends to fill this gap. It turns out that a careful description of the mathematics leads to something which is not too far from an actual implementation in a high level programming language like that of MAGMA[1]. Moreover, it naturally yields an algorithm that includes the improvements of Shanks regarding the Gaussian solution of the duplication equation and avoids the unnecessary coprimality assumptions on the first coefficients of the quadratic forms in [10].

The algorithm has been successfully exploited [2] in the verification of the heuristics of the second author [12, 13] regarding the solvability in integers of the negative Pell equation $x^2 - dy^2 = -1$. This verification involved the computation of $\mathcal{C}(D)$ for several millions of large, highly non-cyclic real quadratic 2-class groups.

The description of the actual algorithm is contained in section 3 of this paper. It is preceded by a summary of the basic results on binary quadratic forms and followed by a worked example illustrating some technical points of the algorithm. The algorithm itself is essentially a matter of linear algebra once one knows how to generate the 2-torsion subgroup of $\mathrm{Cl}(D)$ and how to solve the equation $2x = c$ for elements c in the principal genus $2\mathrm{Cl}(D)$. The 'division-by-2-algorithm' used in solving $2x = c$ is based on the reduction theory of ternary quadratic forms. As this reduction theory is considerably less well known than the corresponding theory for binary quadratic forms, a concise description of it has been included as section 5. It is used in section 6, which deals with the solution of the duplication equation that forms the backbone of the algorithm. A final section 7 comments on the performance of the algorithm.

We thank Andreas Meyer for detecting a number of typos in an earlier version of this paper.

2. Quadratic class groups.

Let $D \equiv 0, 1 \bmod 4$ be an integer that is not a square. The class group $\mathrm{Cl}(D)$ of discriminant D is defined to be the quotient of the group of invertible ideals of the quadratic order $\mathcal{O}_D = \mathbf{Z}[(D+\sqrt{D})/2]$ by the subgroup of principal ideals having a *totally positive* generator. Note that the positivity requirement is automatically fulfilled for negative D, and that $\mathrm{Cl}(D)$ is the (strict) class group of the quadratic field $\mathbf{Q}(\sqrt{D})$ if D is fundamental, i.e., if D is the discriminant of the field $\mathbf{Q}(\sqrt{D})$.

The relative ease with which one can perform computations in $\mathrm{Cl}(D)$ comes from an alternative description in terms of binary quadratic forms which is due to Gauss. Consider the set $\mathcal{F}_D$ of primitive integral binary quadratic forms of discriminant D, i.e., forms $Q = (a, b, c) = ax^2+bxy+cy^2$ in two variables x, y with coefficients $a, b, c \in \mathbf{Z}$ that satisfy $\gcd(a, b, c) = 1$ and $b^2 - 4ac = D$. For $D < 0$, we require in addition that a is positive. The group $\mathrm{SL}_2(\mathbf{Z})$ of integral 2×2-matrices of determinant 1 has a natural right action on $\mathcal{F}_D$ defined by $Q^S(x, y) = Q(sx + ty, ux + vy)$ for $S = \binom{s\ t}{u\ v} \in \mathrm{SL}_2(\mathbf{Z})$, and the orbit space $\mathcal{F}_D/\mathrm{SL}_2(\mathbf{Z})$ maps bijectively to the group $\mathrm{Cl}(D)$ under the map

$$[ax^2 + bxy + cy^2] \longmapsto [(\mathbf{Z} \cdot 2a + \mathbf{Z} \cdot (b + \sqrt{D})) \cdot \sqrt{D}^{(1-\mathrm{sign}(a))/2}].$$

The power of $\sqrt{D}$ in the map above is only there to 'preserve orientation' and vanishes for negative D. By transport of structure, $\mathcal{F}_D/\mathrm{SL}_2(\mathbf{Z})$ becomes a group that we identify with $\mathrm{Cl}(D)$. Accordingly, we speak of the *class* rather than of the orbit of a form in $\mathrm{Cl}(D)$. In the case that D is a square, which we have excluded so far, the orbit space $\mathcal{F}_D/\mathrm{SL}_2(\mathbf{Z})$ can be made into a group by Gauss's original method that we will discuss later in this section. Following Gauss [7, end of section 249], we will write the group operation in $\mathrm{Cl}(D)$ *additively*. This appears to be the most convenient notation for computational purposes, as most computations in class groups use techniques coming from linear algebra, and it is in line with the common usage to treat divisor class groups as additive objects.

As the forms (a, b, c) and $(a, b + 2ka, c + kb + k^2a)$ are in the same class for all $k \in \mathbf{Z}$, every class contains a form (a, b, c) with $|b| \leq |a|$. It is not hard to show [3, propositions 5.3.4 and 5.6.3] that every class contains a quadratic form (a, b, c) with

$$|a| \leq \sqrt{|D|/3}, \tag{2.1}$$

so it follows that $\mathrm{Cl}(D)$ is finite for all D, square or not. Given a form in $\mathcal{F}_D$, one can efficiently compute [9] a unimodular transformation that reduces this form to one of the finitely many forms (a, b, c) satisfying $|b| \leq |a| \leq \sqrt{|D|/3}$. However, it is not in general possible to decide efficiently whether two quadratic forms are in the same class in $\mathrm{Cl}(D)$. This is a serious difficulty that prevents us from working directly in the class group itself. Instead, one has a finite set of *reduced forms* Φ_D that maps surjectively to the class group $\mathrm{Cl}(D)$, and one works with these reduced forms as representatives of the classes of $\mathrm{Cl}(D)$. For $D < 0$, an appropriate definition of reduced forms ensures that the map $\Phi_D \to \mathrm{Cl}(D)$ is a bijection and the situation is perfectly satisfactory. For $D > 0$ however, there are usually many reduced forms mapping to the same class in $\mathrm{Cl}(D)$, and in this case an arbitrary form in $\mathcal{F}_D$ can be efficiently reduced to a form in Φ_D, but not to an element of $\mathrm{Cl}(D)$. As an example, one can think of the form $(-1, 0, d)$ for $d > 0$ that represents the unit element in $\mathrm{Cl}(4d)$ if and only if the negative Pell equation $x^2 - dy^2 = -1$ is solvable in integers. This example is of fundamental importance in [2].

In the case of non-square discriminants D, our map shows that the *principal form* $(1, 0, -D/4)$ (for even D) or $(1, 1, (1 - D)/4)$ (for odd D) maps to the unit element in $\mathrm{Cl}(D)$. The *opposite form* $(a, -b, c)$ of (a, b, c) is the inverse of the class of (a, b, c) as it maps to the conjugate ideal class in $\mathrm{Cl}(D)$. If we work out how the multiplication of ideals translates into a composition formula for quadratic forms, we find [3, 5.4.6] that the sum of the classes of the primitive quadratic forms (a_1, b_1, c_1) and (a_2, b_2, c_2) in $\mathrm{Cl}(D)$ contains a form (a_3, b_3, c_3) satisfying

$$(2.2) \qquad a_3 = \frac{a_1 a_2}{d^2} \qquad \text{and} \qquad b_3 \equiv b_2 + 2\frac{a_2}{d}(\lambda \frac{b_1 - b_2}{2} - \nu c_2) \bmod 2a_3,$$

where

$$d = \gcd(a_1, a_2, \frac{b_1 + b_2}{2}) = \lambda a_1 + \mu a_2 + \nu \frac{b_1 + b_2}{2}.$$

It was shown by Dirichlet that the forms can be chosen in such a way inside their equivalence class that one only needs to perform compositions for which $d = 1$, known as compositions of 'concordant forms'. In fact, it suffices [5, lemma 3.2] to have a composition of concordant forms (a_1, b, c_1) and (a_2, b, c_2) having the *same* middle coefficient b that satisfies $b^2 \equiv D \bmod 4a_1 a_2$. In this situation, one has $c_1 = a_2 c$ and $c_2 = a_1 c$ for some integer c, and (2.2) yields an identity

$$(2.3) \qquad [(a_1, b, c_1)] + [(a_2, b, c_2)] = [(a_1 a_2, b, c)] \in \mathrm{Cl}(D)$$

that is known as *Dirichlet composition* of forms.

Together with the reduction of arbitrary forms to forms in a finite set Φ_D, the composition formulae provide us with a *computational model* for the class group. More precisely, there is for each D a finite set Φ_D of reduced forms of discriminant D that is usually too large to be enumerated. Given a form $F \in \mathcal{F}_D$, one can efficiently find some form $F^{\mathrm{red}} \in \Phi_D$ that is in the same class. Given $F_1, F_2 \in \Phi_D$, the composition formula (2.2) makes it possible to compute efficiently a reduced form $F_3 = F_1 \circ F_2 \in \Phi_D$ whose class in $\mathrm{Cl}(D)$ is the sum of the classes of F_1 and F_2. The opposite of a reduced form is trivially computed, so we can perform the 'group operations' of $\mathrm{Cl}(D)$ on the level of Φ_D. However, since equivalence cannot be tested efficiently when D is large and positive, passing from Φ_D to $\mathrm{Cl}(D)$ is an entirely non-trivial matter. It is exactly this complication which led Shanks [11, p. 849] to believe that one cannot always decide efficiently whether certain 2-torsion classes in $\mathrm{Cl}(D)$ are actually trivial. We will come back to this problem, which will turn out ot be non-existent, in section 3. The ambiguity between forms and their classes will however necessitate a careful formulation of our algorithm in section 3, where we compute the 2-primary part of $\mathrm{Cl}(D)$ while working with representing forms.

As we will be interested in duplication in the class group in later sections, we mention the following important example of concordant composition.

2.4. DUPLICATION LEMMA. *Let (a,b,c) be a form of discriminant D with $\gcd(a,b)=1$. If $\lambda,\nu\in\mathbf{Z}$ satisfy $\lambda a+\nu b=1$, then we have $2[(a,b,c)]=[(a^2,b-2\nu ac,c')]\in \mathrm{Cl}(D)$ for some integer c'. In particular, we have $2[(a,b,c)]=[(a^2,b,c/a)]$ if a divides c.* □

This lemma can be used in the opposite direction to solve the equation $2[P]=[Q]$ for a form Q that represents a square k^2 coprime to $2D$. Indeed, suppose we have $Q(u,v)=k^2$ for certain $u,v\in\mathbf{Z}$, and assume without loss of generality that u and v are coprime. Transforming Q by a unimodular matrix $S=\binom{u\ s}{v\ t}$, we obtain an equivalent form Q^S satisfying $Q^S(1,0)=k^2$, so we have $Q^S=(k^2,l,m)$ for certain $l,m\in\mathbf{Z}$. The form (k,l,km) of discriminant $l^2-4k^2m=D$ is primitive since $\gcd(k,l)=\gcd(k,2D)=1$, and the duplication lemma shows that we have $2[(k,l,km)]=[(k^2,l,m)]=[Q]$. however that (k,l,km) is primitive if k is odd and

In section 6, we will employ the original description of Gauss of the group structure on $\mathrm{Cl}(D)$, which is quite different from the one we have given above and also works for square discriminants. In this description, a form $Q=(a_3,b_3,c_3)$ of discriminant D is the composition of two primitive quadratic forms (a_1,b_1,c_1) and (a_2,b_2,c_2) of discriminant D if there exist bilinear relations

$$\begin{aligned} x_3 &= s_1x_1x_2+s_2x_1y_2+s_3x_2y_1+s_4x_2y_2\\ y_3 &= t_1x_1x_2+t_2x_1y_2+t_3x_2y_1+t_4x_2y_2 \end{aligned}$$

over $\mathbf{Z}$ that yield the identity

(2.5)
$$\begin{aligned}(a_1x_1^2+b_1x_1y_1+c_1y_1^2)\cdot(a_2x_2^2+b_2x_2y_2+c_2y_2^2) &=\\ = Q(x_3,y_3) &= a_3x_3^2+b_3x_3y_3+c_3y_3^2\end{aligned}$$

and satisfy an 'orientability condition' that distinguishes the forms (a_1,b_1,c_1) and (a_2,b_2,c_2) in (2.5) from their opposite forms $(a_1,-b_1,c_1)$ and $(a_2,-b_2,c_2)$. Write

$$\delta_{ij}=\begin{vmatrix} s_i & s_j\\ t_i & t_j\end{vmatrix}$$

for the subdeterminants of our bilinear relations. An elementary computation [5, exercise 3.1] shows that if (2.5) holds for a form Q of discriminant D, then we necessarily have $\delta_{12}=\pm a_1$ and $\delta_{13}=\pm a_2$. The orientability condition is that the $+$-sign holds in both cases. Note that the preceding definition for the composition of forms is indeed defined on $\mathrm{SL}_2(\mathbf{Z})$-equivalence classes.

If Q is a composition as specified above, the determinants δ_{ij} satisfy

$$(2.6)\qquad \begin{aligned} a_1 &= \delta_{12} & b_1 &= \delta_{14} - \delta_{23} & c_1 &= \delta_{34} \\ a_2 &= \delta_{13} & b_2 &= \delta_{14} + \delta_{23} & c_2 &= \delta_{24} \end{aligned}$$

and the coefficients of Q are

$$(2.7)\qquad \begin{aligned} a_3 &= t_2 t_3 - t_1 t_4 \\ b_3 &= s_1 t_4 + s_4 t_1 - s_2 t_3 - s_3 t_2 \\ c_3 &= s_2 s_3 - s_1 s_4. \end{aligned}$$

Conversely, given primitive forms $Q_1 = (a_1, b_1, c_1)$ and $Q_2 = (a_2, b_2, c_2)$ and integers s_i, t_i for which (2.6) and (2.7) hold, we have $b_1^2 - 4a_1c_1 = b_2^2 - 4a_2c_2 = D$ for some discriminant D and $[(a_3, b_3, c_3)] = [Q_1] + [Q_2] \in \mathrm{Cl}(D)$. For non-square D, Gauss's definition yields the same group structure on $\mathrm{Cl}(D)$ as the Dirichlet composition (2.3). This is immediate from the observation that the identities (2.6) and (2.7) are satisfied for the forms in (2.3) if one takes the bilinear relations equal to

$$\begin{pmatrix} s_1 & s_2 & s_3 & s_4 \\ t_1 & t_2 & t_3 & t_4 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & -c \\ 0 & a_1 & a_2 & b \end{pmatrix}.$$

In the particular case where we want to duplicate a form in $\mathrm{Cl}(D)$, the identities (2.6) suggest that we should take $s_2 = s_3$ and $t_2 = t_3$. The result will be used in section 6 to prove the correctness of the algorithm to solve the duplication equation $2x = c \in 2\mathrm{Cl}(D)$.

2.8. Lemma. *Let $F = (a, b, c)$ be a primitive quadratic form of discriminant D, and suppose we are given integers s_i, t_i for $i = 1, 2, 3$ satisfying the identities*

$$a = s_1 t_2 - t_1 s_2 \qquad b = s_1 t_3 - t_1 s_3 \qquad c = s_2 t_3 - t_2 s_3.$$

Then the class $2[F] \in \mathrm{Cl}(D)$ contains the form

$$(t_2^2 - t_1 t_3\ ,\quad s_1 t_3 + s_3 t_1 - 2 s_2 t_2\ ,\quad s_2^2 - s_1 s_3). \qquad \square$$

If a and b are coprime in this lemma, we can find λ and ν satisfying $\lambda a + \nu b = 1$ and take

$$\begin{pmatrix} s_1 & s_2 & s_3 \\ t_1 & t_2 & t_3 \end{pmatrix} = \begin{pmatrix} 1 & \nu c & -\lambda c \\ 0 & a & b \end{pmatrix}$$

to find the identity $2[(a, b, c)] = [(a^2, b - 2\nu ac, \nu^2 c^2 + \lambda c)]$ from lemma 2.4.

3. Computing quadratic 2-class groups.

Let $D \equiv 0, 1 \bmod 4$ be a non-square integer for which we have a complete factorization. We want to compute the strict 2-class group $\mathcal{C} \subset \mathrm{Cl}$ of the quadratic order of discriminant D. The computation is essentially a matter of linear algebra over the field of 2 elements $\mathbf{F}_2$. For this reason, we take the values of all quadratic characters in this section to lie in $\mathbf{F}_2$ rather than in the multiplicative group $\langle -1 \rangle$.

The factorization of D provides us with the two basic ingredients of our algorithm. The first is an $\mathbf{F}_2$-basis of the character group $\mathfrak{X}_D$ of $\mathcal{C}/2\mathcal{C} = \mathrm{Cl}/2\mathrm{Cl}$, commonly known as the group of genus characters of Cl. The second is a generating set of ambiguous forms, i.e., a set of forms whose classes generate the 2-torsion subgroup $\mathcal{C}[2] = \mathrm{Cl}[2]$ of $\mathcal{C} \subset \mathrm{Cl}$. The classes in Cl of the elements of our set will not in general form an $\mathbf{F}_2$-basis for $\mathcal{C}[2]$.

Let d be the discriminant of the field $\mathbf{Q}(\sqrt{D})$. We have $D = f^2 d$ for some integer $f \geq 1$ that equals the index of the quadratic order of discriminant D inside the maximal order in $\mathbf{Q}(\sqrt{D})$.

For an odd prime divisor p of D, we write $\chi_p : (\mathbf{Z}/D\mathbf{Z})^* \to \mathbf{F}_2$ for the quadratic character of conductor p and $\chi_d = \left(\frac{d}{\cdot}\right) : (\mathbf{Z}/D\mathbf{Z})^* \to \mathbf{F}_2$ for the quadratic character corresponding to the field $\mathbf{Q}(\sqrt{D})$.

The group of *field characters* $\mathfrak{X}_d$ corresponding to D is the group

$$\mathfrak{X}_d = \langle \{\chi_p\}_{p|d \text{ odd}}, \chi_d \rangle$$

of Dirichlet characters on $(\mathbf{Z}/D\mathbf{Z})^*$. Here p ranges over the odd prime divisors of d. If d is odd, the characters χ_p form a basis of $\mathfrak{X}_d$ and their product equals χ_d. If d is even, the product of χ_d and all characters χ_p is a quadratic character of 2-power conductor associated to the quadratic field of discriminant -4 or ± 8. This character, which we denote correspondingly by χ_{-4}, χ_8 or χ_{-8}, and the characters χ_p now form a basis for $\mathfrak{X}_d$. In all cases, the order of $\mathfrak{X}_d$ equals 2^t, with t the number of distinct prime divisors of d. The abelian field corresponding to $\mathfrak{X}_d$ is the genus field of the quadratic field $\mathbf{Q}(\sqrt{D})$. It is the maximal abelian extension of $\mathbf{Q}(\sqrt{D})$ that is unramified at all finite primes and abelian over $\mathbf{Q}$.

The full group $\mathfrak{X}_D$ of *genus characters* associated to the discriminant D has a similar definition, but special care is needed to obtain the correct characters of 2-power conductor. Writing $\mathfrak{X}'_D$ for the group of characters generated by $\mathfrak{X}_d$ and the quadratic characters χ_p for odd prime divisors p

of f, we have

(3.1)

$$\mathfrak{X}_D = \begin{cases} \langle \mathfrak{X}'_D \rangle & \text{if } 8|d \text{ and } f \text{ is odd, or if } 8 \nmid d \text{ and } 4 \nmid f; \\ \langle \mathfrak{X}'_D, \chi_{-4} \rangle & \text{if } 8|d \text{ and } f \text{ is even, or if } d \text{ is odd and } 4|f; \\ \langle \mathfrak{X}'_D, \chi_8 \rangle & \text{if } d \equiv 4 \bmod 8 \text{ and } 4|f; \\ \langle \mathfrak{X}'_D, \chi_{-4}, \chi_8 \rangle & \text{if } d \text{ is odd and } 8|f. \end{cases}$$

A basis of $\mathfrak{X}_D$ is obtained by adding to a basis for $\mathfrak{X}_d$ the characters χ_p for the odd prime divisors of f that do not divide d and the characters χ_{-4} and χ_8 as specified in the definition above. One finds that if D has u distinct prime divisors, then $\mathfrak{X}_D$ has dimension $u+1$ if D is divisible by 32 (and $\mathfrak{X}_D$ contains all quadratic characters of 2-power conductor), $u-1$ for $D \equiv 4 \bmod 16$ (when d is odd and $f \equiv 2 \bmod 4$) and u otherwise. The abelian field G_D corresponding to $\mathfrak{X}_D$ is the *genus field* of the quadratic order of discriminant D. It the maximal abelian extension of $\mathbf{Q}$ that is contained in the ring class field of conductor f of $\mathbf{Q}(\sqrt{D})$. By class field theory, the Galois group $\mathrm{Gal}(G_D/\mathbf{Q}(\sqrt{D}))$ is canonically isomorphic to $\mathrm{Cl}/2\mathrm{Cl} = \mathcal{C}/2\mathcal{C}$, and it follows that there is a perfect pairing of $\mathbf{F}_2$-vector spaces

$$\mathcal{C}/2\mathcal{C} \times \mathfrak{X}_D/\langle \chi_d \rangle \longrightarrow \mathbf{F}_2. \tag{3.2}$$

More explicitly, the value of a character $\chi \in \mathfrak{X}_D$ on a class $[Q] \in \mathrm{Cl}$ is the common χ-value of the integers coprime to D that are represented by Q. One deduces that the value of a character $\chi \in \mathfrak{X}_D$ of conductor k on the class of (a, b, c) in Cl equals

$$\chi([(a,b,c)]) = \begin{cases} \chi(a) & \text{if } \gcd(a,k) = 1 \\ \chi(c) & \text{if } \gcd(c,k) = 1. \end{cases} \tag{3.3}$$

If the conductor k of χ is a prime power dividing D, as in the case of the 'basis characters' of $\mathfrak{X}_D$ mentioned above, the primitivity of the form implies that at least one of these conditions is satisfied. Our algorithm will only use such basis characters. For general $\chi \in \mathfrak{X}_D$, one uses its representation on the basis. Alternatively, one can replace a form of discriminant D by an equivalent form (a, b, c) satisfying $\gcd(a, D) = 1$, cf. [5, ex. 2.18]. An element $[Q] \in \mathrm{Cl}$ is in the principal genus 2Cl if and only if all characters of $\mathfrak{X}_D$ vanish on it, so the genus characters enable us to decide efficiently whether an element of Cl is in 2Cl. In section 6, we will prove the following.

3.4. Division-by-2-algorithm. *Given a form $Q \in \mathcal{F}_D$ whose class lies in* 2Cl, *we can efficiently find a form $P \in \mathcal{F}_D$ satisfying $2[P] = [Q] \in \mathrm{Cl}$.*

The class of the form P in 3.4 is only determined up to composition with classes from Cl[2], and all we know is that the form P found by the algorithm lies in one of these classes. Even when Q is in the trivial class, there is no guarantee that P will be in the trivial class.

Apart from an explicit description of the character group of $\mathcal{C}/2\mathcal{C}$, the factorization of D also yields generators for the subgroup $\mathcal{C}[2]$ of ambiguous ideal classes in Cl. This is due to the well known fact that $\mathcal{C}[2]$ consists of classes of invertible $\mathcal{O}_D$-ideals $I \subset \mathcal{O}_D$ of index dividing D. We can take classes of ideals of prime power index as generators. If p is an odd prime dividing D, say $p^k || D$, there is an invertible $\mathcal{O}_D$-ideal $I_p = \mathbf{Z} \cdot p^k + \mathbf{Z} \cdot (D + \sqrt{D})/2$ of index p^k in the order $\mathcal{O}_D$. As this ideal is equal to its conjugate in $\mathcal{O}_D$, its class in $\mathrm{Cl}(D)$ is a 2-torsion element. It is the class of the quadratic form

$$Q_p = \begin{cases} (p^k, p^k, (p^k - D/p^k)/4) & \text{if } D \equiv 1 \bmod 4 \\ (p^k, 0, -D/4p^k) & \text{if } D \equiv 0 \bmod 4. \end{cases}$$

For $D \equiv 0 \bmod 4$, say $2^t || D$ with $t \geq 2$, we have an ambiguous form

$$Q_2 = \begin{cases} (2, 2, (4 - D)/8) & \text{if } D \equiv -4 \bmod 16 \\ (2^{t-2}, 0, -D/2^t) & \text{otherwise} \end{cases}$$

that is the principal form for $D \equiv 4 \bmod 16$. If D is divisible by 32, there is another ambiguous form

$$Q_2' = (4, 4, 1 - \tfrac{D}{16})$$

that is needed to complete our generating set of ambiguous forms. Thus, if we start with the set of forms $\{Q_p\}_{p|D \text{ prime}}$, we obtain a generating set S_0 by leaving out Q_2 for $D \equiv 4 \bmod 16$ and including Q_2' for $D \equiv 0 \bmod 32$. If D has u distinct prime divisors, then S_0 has $u + 1$ elements if D is divisible by 32, it has $u - 1$ elements for $D \equiv 4 \bmod 16$, and u elements otherwise. This is exactly the $\mathbf{F}_2$-dimension of the character group $\mathfrak{X}_D$, and as the cardinality of $\mathcal{C}[2]$ equals $\#(\mathcal{C}/2\mathcal{C}) = \#\mathfrak{X}_D/\langle \chi_d \rangle$, we conclude that there is exactly one non-trivial relation in Cl between the elements of S_0. For negative D, the triviality of the ideal class $[(\sqrt{D})] = [(\sqrt{d})] \in \mathrm{Cl}$ yields the desired relation in all cases but one (the easy case $d = -4$). We can then form an $\mathbf{F}_2$-basis for $\mathcal{C}[2]$ from S_0 by leaving out an appropriate element. For $D > 0$ however, the relation between the ambiguous ideal classes is much more subtle. If the fundamental unit $\varepsilon_D \in \mathcal{O}_D$ is of norm -1, the relation is again $[(\varepsilon_D\sqrt{D})] = [(\sqrt{d})] = 0$. If ε_D is of norm $+1$, the ambiguous ideal class $[(1+\varepsilon_D)] = 0$ yields the desired relation. The problem is of course that ε_D is usually too large to be computable in practice. For this reason, we have to start our algorithm for $D > 0$ with a generating set S_0 for $\mathcal{C}[2]$, not an $\mathbf{F}_2$-basis. This difference between the real and the imaginary case accounts for the slightly larger running times of the algorithm for positive D. The relation between the generators of $\mathcal{C}[2]$ for $D > 0$ can be obtained as a by-product of the computation of $\mathcal{C}$. From the relation we can determine the sign of the norm of ε_D without explicitly computing ε_D. This feature of the algorithm is exploited in [2].

The computation of $\mathcal{C}$ proceeds by the construction of an $\mathbf{F}_2$-basis for the left argument of the character pairing

$$\mathcal{C}/2\mathcal{C} \times \mathfrak{X}_D/\langle\chi_d\rangle \longrightarrow \mathbf{F}_2. \tag{3.2}$$

For the right argument $\mathfrak{X}_D/\langle\chi_d\rangle$ we have our basis X of characters of prime power conductor indicated above. The basis $B \subset \mathcal{F}_D$ of forms whose classes yield a basis for $\mathcal{C}/2\mathcal{C}$ will be constructed as a disjoint union of sets A_j $(j = 1, 2, \dots)$ in such a way that the classes of the forms in $B_i = \bigcup_{j=1}^{i} A_j$ form a basis for the canonical image of $\mathcal{C}[2^i]$ in $\mathcal{C}/2\mathcal{C}$. The basis A_1 for the image of the 2-torsion subgroup $\mathcal{C}[2]$ will be formed from the set S_0 of ambiguous forms. More generally, we will carry a set S_i of 2^{i+1}-torsion forms along at stage i. Roughly speaking, the character pairing is used to 'split' the set S_i into a set A_{i+1} of basis forms and a set of forms that map to $2\mathcal{C}$. We divide the latter forms by 2 using our algorithm 3.4 to obtain the set S_{i+1} of 2^{i+2}-torsion forms needed at the next level. We continue until the union $\bigcup_j A_j$ yields a basis for $\mathcal{C}/2\mathcal{C}$. We are then done by the following elementary lemma on abelian 2-groups.

3.5. LEMMA. *Let G be a finite abelian 2-group, X a basis for its group of quadratic characters, and suppose we have a disjoint union $B = \bigcup_{j=1}^{N} A_j$ of finite sets $A_j \subset G$ such that the following holds:*

a. *the 2-torsion subgroup $G[2]$ is generated by the elements $2^{j-1}a_j$ with $a_j \in A_j$ and $j \in \{1, 2, \dots, N\}$.*
b. *the matrix $(\chi(a))_{\chi\in X, a\in B}$ is a non-singular square matrix.*

Then B maps to an $\mathbf{F}_2$-basis for $G/2G$, the elements in A_j have exact order 2^j in G and the natural map

$$\prod_{j=1}^{N} (\mathbf{Z}/2^j\mathbf{Z})^{A_j} \xrightarrow{\sim} G$$

is an isomorphism of groups.

Proof. The non-singularity of the character matrix in (b) implies that the elements in B map to a basis for $G/2G$, so these elements generate the group G. As $G[2]$ and $G/2G$ have the same $\mathbf{F}_2$-dimension, the elements of the form $2^{j-1}a_j$ with $a_j \in A_j$ that occur in (a) necessarily form a basis for $G[2]$. In particular, the elements of A_j have exact order 2^j. In order to obtain the required isomorphism for G, we have to show that for any relation $\sum_{b\in B} k_b b = 0 \in G$ with coefficients $k_b \in \mathbf{Z}$, we have $\mathrm{ord}_2(k_b) \geq j(b)$ for all $b \in B$. Here $j(b)$ denotes the index j for which b is in A_j. Suppose that, on the contrary, the integer $n = \max_{b\in B}\{j(b) - \mathrm{ord}_2(k_b)\}$ is positive. Then we can multiply our relation by 2^{n-1} and write it as

$$\textstyle\sum_{b\in B}(2^{n-j(b)}k_b)\cdot 2^{j(b)-1}b = 0.$$

By definition of n, the expressions in brackets are integral and not all even. This implies that we would have a non-trivial relation between the basis elements $2^{j(b)-1}b$ of $G[2]$. Contradiction. □

Note that the conclusion of the lemma implies that the subset $B_i = \bigcup_{j=1}^{i} A_j \subset G$ maps to a basis of the canonical image of $G[2^i]$ in $G/2G$.

We now describe an inductive algorithm that computes sets of forms $A_j \subset \mathcal{F}_D$ such that the hypotheses of lemma 3.5 apply to their classes in $G = \mathcal{C}$. We noted already that the problem with working with forms is that we cannot decide whether two different forms are different as elements of $\mathcal{C}$. However, the forms in the sets A_j that are computed by our algorithm are constructed in such a way that the quadratic character values of each two of these forms are distinct. This means that $B = \bigcup_{j=1}^{N} A_j$ can indeed by viewed as a subset of $G = \mathcal{C}$, as required by 3.5. Thus, we do not run into the problem encountered by Shanks [11, p. 849]. The sets of forms S_i that are constructed during the algorithm do not in general map injectively to $\mathcal{C}$.

Our algorithm computes more than just a set of forms A_j at stage j. The data it stores after i steps are the following:

1. *a disjoint union $B_i = \bigcup_{j=1}^{i} A_j$ of finite sets of forms A_j, together with a collection of forms S_i such that $\mathcal{C}[2]$ is generated by elements of the form $2^{j-1}[a_j]$ with $a_j \in A_j$ and $2^i[s]$ with $s \in S_i$.*
2. *a subset $X_i \subset X$ of characters such that the matrix $(\chi(a))_{\chi\in X_i, a\in B_i}$ is a non-singular square matrix.*

Initialization. At the initial stage $i = 0$, we have $B_0 = X_0 = \emptyset$ and our set S_0 of ambiguous forms that meets the non-empty requirement (1).

Induction step. Suppose we have $X_i \neq X$ at stage i. Then the set B_i is not a set of generators for $\mathcal{C}$, and we proceed to the next stage as follows. Consider the character matrix

$$M_i = (\chi(a))_{\chi \in X, a \in B_i \cup S_i}.$$

whose columns $X(a) \in \mathbf{F}_2^X$ give the 'complete quadratic character' of the forms $a \in B_i \cup S_i$. By (2), the elements $X(a)$ for $a \in B_i$ are independent in $\mathbf{F}_2^X$, and we can compose each of the elements of S_i with forms from B_i to obtain that all characters in X_i vanish on it. After doing so, we still have (1) for our modified set S_i, and the new columns $X(s)$ for $s \in S_i$ span a subspace $V \subset \mathbf{F}_2^X$ that is linearly disjoint from the space spanned by the columns $X(a)$ with $a \in B_i$. We choose $A_{i+1} \subset S_i$ such that the columns $X(a)$ with $a \in A_{i+1}$ form a basis of V, and we pick a set of characters $Y_i \subset X$ such that the matrix $(\chi(a))_{\chi \in Y_i, a \in A_{i+1}}$ is non-singular. We clearly have $Y_i \cap X_i = \emptyset$, and we set $X_{i+1} = X_i \cup Y_i$ to obtain (2) for stage $i+1$.

The remaining forms in $S_i \setminus A_{i+1}$ are now composed with forms from A_{i+1} in such a way that the characters in $X \setminus X_i$ also vanish on them. Then all characters in X vanish on these modified forms, so their classes are in $2\mathcal{C}$. We now apply our division-by-2-algorithm 3.4 to each of the modified forms in $S_i \setminus A_{i+1}$, and take the solutions obtained as the set S_{i+1}.

If s is in S_i, we can by construction write $[s] \in \mathcal{C}$ as a sum of classes $[a_{i+1}]$ with $a_{i+1} \in A_{i+1}$ and $2[s_{i+1}]$ with $s_{i+1} \in S_{i+1}$. We conclude that the sets $\{2^i[s] : s \in S_i\}$ and $\{2^i[a_{i+1}] : a_{i+1} \in A_{i+1}\} \cup \{2^{i+1}[s_{i+1}] : s_{i+1} \in S_{i+1}\}$ generate the same subgroup of $\mathcal{C}[2]$, so we have (1) for stage $i+1$ as well.
Termination. The algorithm terminates at stage i if we have $X_i = X$. This is bound to happen as we have $X_i = X$ if and only if $\mathcal{C}$ is annihilated by 2^i. To see this, suppose first that $\mathcal{C}$ is annihilated by 2^i. Condition (1) then implies that the elements$2^{j-1}a_j$ for $j \leq i$ generate $\mathcal{C}[2]$, so the number $\#B_i$ of such elements is at least equal to $\dim \mathcal{C}[2] = \#X$. It follows from (2) that we have $\#X_i = \#B_i \geq \#X$, so $X_i = X$. Conversely, if we find $X_i = X$ at stage i, then $\mathcal{C}$ is annihilated by 2^i as it can be generated by a set B_i of 2^i-torsion elements.

We conclude that after N steps, with 2^N the exponent of $\mathcal{C}$, we have found a basis $B = \bigcup_{j=1}^N A_j$ for $\mathcal{C}$ that satisfies the conditions of lemma 3.5. This finishes the description of the algorithm.

In the actual implementation of the algorithm, we used a refinement that ensures that the final character matrix $(\chi(a))_{\chi \in X, a \in B}$ becomes lower triangular. Instead of taking for A_{i+1} some subset of S_i whose X-image spans V, one alternately picks a character and constructs a form to produce Y_i and

A_{i+1}, as follows. Let S_i be our set of forms, modified such that all characters in X_i vanish on S_i, and look at the submatrix $M_i^! = (\chi(a))_{\chi \in X \setminus X_i, a \in S_i}$ of M_i. We set $Y_i = \emptyset = A_{i+1}$ and do the following until all entries of $M_i^!$ equal zero. Pick a form $a \in S_i$ and a character $\chi \in X - X_i$ such that $\chi(a) \neq 0$, add χ to the set Y_i and move the form a from S_i to A_{i+1}. Compose the remaining forms $s \in S_i$ that have $\chi(a) \neq 0$ with a—this yields a new set S_i—and continue with the new, smaller matrix $M_i^!$. This process, which is called echelonization, produces a non-singular lower-triangular matrix $(\chi(a))_{\chi \in Y_i, a \in A_{i+1}}$ for the ordering of forms and characters suggested above. Moreover, it replaces S_i by a set of forms with classes in $2\mathcal{C}$, and S_{i+1} is constructed from this set applying 3.4.

At the final stage $i = N$ of the algorithm, there is no need to apply the division-by-2-algorithm 3.4 to compute a set S_N of 2^{N+1}-torsion forms. In the imaginary case $D < 0$, this is clear since we can take S_0 to be a basis for $\mathcal{C}[2]$ and find $S_N = \emptyset$. In the real case $D > 0$, we have to work with an extra generator in S_0. At the final stage N, we compute from S_{N-1} a set A_N that completes our basis B and a single form $s_D \in 2\mathcal{C}$ to which we can apply 3.4 to find the single element of S_N. As $[s_D]$ is divisible by 2 in a group of exponent 2^N, we have $2^{N-1}[s_D] = 0$. We can, at the cost of a little extra administration, carry not only the set S_i along at stage i, but also for each $s \in S_i$ the representation of $2^i[s]$ in terms of our original 2-torsion generators in S_0. This is simply done by keeping track of how the forms in S_{i+1} are constructed at stage i from the previous set S_i. If we do so, the relation $2^{N-1}[s_D] = 0$ for $D > 0$ provides us with the dependency between the ambiguous forms in S_0. If, for some reason, we would have even more generators in S_0, we could in the same way find a complete set of relations between them.

Given an element $c \in \mathcal{C}$, the explicit knowledge of the character pairing with respect to the basis B for $\mathcal{C}$ enables us to write c on the basis B. From the pairing, one computes a sum $b_0 \in \mathcal{C}$ of elements in $B \subset \mathcal{C}$ that has the same quadratic character values as $c = c_0$. This yields $c_0 = b_0 + 2c_1$ for some class $c_1 \in \mathcal{C}$ that can be found by 3.4. One inductively computes sums $b_i \in \mathcal{C}$ of elements in B such that $c_i = b_i + 2c_{i+1}$ for $i = 0, 1, \ldots, N-1$. The desired representation for c is then $c = \sum_{i=0}^{N-1} 2^i b_i$.

The number k of divisions by 2 performed by the algorithm to compute $\mathcal{C}$ can easily be derived from the group structure of $\mathcal{C}$: for any factor $(\mathbf{Z}/2^j\mathbf{Z})$ in the representation of lemma 3.5 one has to perform $j-1$ divisions by 2. However, since for $D > 0$ there is at any stage in the algorithm one more generator than the rank of the group necessitates, the number of divisions performed for the maximal j, which equals N, has to be counted twice.

Writing $h = \#\mathcal{C}$ for the 2-class number of D and $r \in \{u-2, u-1, u\}$ for the 2-rank of $\mathcal{C}$, we find

$$k = \begin{cases} \log_2(h) - r & \text{for } D < 0 \\ \log_2(h) - r - 1 + N & \text{for } D > 0. \end{cases} \tag{3.6}$$

This explains the observation in the introduction that our algorithm usually needs more time for real class groups than for comparable imaginary class groups.

4. A worked example.

In order to illustrate the abstract description in the previous section, we compute by way of example the real quadratic 2-class group $\mathcal{C}$ of discriminant

$$D = 33923894057872 = 1148^2 \cdot 25740793 = (4 \cdot 7 \cdot 41)^2 \cdot 13 \cdot 97 \cdot 137 \cdot 149,$$

which has 7 distinct prime factors. We use the notation from the previous section.

In our example, the group of field characters $\mathfrak{X}_d$ corresponding to D has order 2^3 and is generated by the quadratic characters χ_{13}, χ_{97}, χ_{137} and χ_{149}. The product of these four characters corresponds to the field $\mathbf{Q}(\sqrt{D})$ and vanishes on $\mathcal{C}$, so we can form an $\mathbf{F}_2$-basis of $\mathfrak{X}_d$ by dropping χ_{149} from our set of generators. By (3.1), we can complete this to a basis X for the group of genus characters $\mathfrak{X}_D$ on $\mathcal{C}$ by adding the characters χ_{-4}, χ_7 and χ_{41}. Our initial set S_0 of ambiguous forms consists of a form Q_p for each odd prime divisor of D and the form $Q_2 = (4, 0, -D/16)$ at 2.

We initialize our algorithm by taking $B_0 = X_0 = \emptyset$ and compute the character matrix $M_0 = (\chi(a))_{\chi \in X, a \in S_0}$ using (3.3). This yields

$$\begin{array}{c|ccccccc} & Q_2 & Q_7 & Q_{13} & Q_{41} & Q_{97} & Q_{137} & Q_{149} \\ \hline \chi_{-4} & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ \chi_7 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ \chi_{13} & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ \chi_{41} & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ \chi_{97} & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ \chi_{137} & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{array}.$$

The space V spanned by the columns of M_0 is 3-dimensional, and the 3×3-submatrix corresponding to the forms Q_2, Q_7 and Q_{13} and the set $Y_0 = \{\chi_{-4}, \chi_7, \chi_{13}\}$ of characters is non-singular. In order to obtain a lower-triangular matrix, we choose the 3 basis elements in A_1 as the classes of the forms

$$\begin{aligned} a_{11} &= Q_2 = (4, 5824416, -4519801), \\ a_{12} &= Q_7 = (49, 5824336, -5123556), \\ a_{13} &= Q_{13} \circ Q_7 = (637, 5823454, -4426047). \end{aligned}$$

These elements span the image C_2^3 of $\mathcal{C}[2]$ in $\mathcal{C}/2\mathcal{C}$. We obtain $B_1 = A_1 \cup B_0 = A_1$ and $X_1 = X_0 \cup Y_0 = Y_0$.

The 4 remaining forms Q_{41}, Q_{97}, Q_{137} and Q_{149} from S_0 are now composed with forms from A_1 to make all characters vanish on them,

and we use our division-by-2-algorithm to compute the forms $s_{1j} \in S_1$ from the duplication equations

$$\begin{aligned} 2s_{11} &= Q_{41} \\ 2s_{12} &= Q_{97} \circ Q_{13} = Q_{97} \circ a_{12} \circ a_{13} \\ 2s_{13} &= Q_{137} \circ Q_7 \circ Q_{13} = Q_{137} \circ a_{13} \\ 2s_{14} &= Q_{149} \circ Q_7 \circ Q_{13} = Q_{149} \circ a_{13}. \end{aligned}$$

The matrix M_1 of character values in the next iteration step is readily evaluated as

$$\begin{array}{c} \\ \chi_{-4} \\ \chi_7 \\ \chi_{13} \\ \chi_{41} \\ \chi_{97} \\ \chi_{137} \end{array} \begin{array}{c} \begin{array}{ccccccc} a_{11} & a_{12} & a_{13} & s_{11} & s_{12} & s_{13} & s_{14} \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix} \end{array}.$$

Only the column of s_{14} lies outside the space spanned by the columns of the forms in A_1. Thus A_2 contains a single element, for which we take

$$a_{21} = s_{14} \circ a_{12} = (-410164, 5326064, 3387021).$$

As χ_{41} is the only character that does not vanish on a_{12}, we take $Y_1 = \{\chi_{41}\}$ and obtain a set $X_2 = Y_0 \cup Y_1$ of cardinality 4. The three remaining forms in S_1 are now composed with forms in $B_2 = A_1 \cap A_2$ to make them divisible by 2, and we find forms in S_2 from the duplication equations

$$\begin{aligned} 2s_{21} &= s_{11} \circ a_{11} \circ a_{12} \circ a_{13} \\ 2s_{22} &= s_{12} \circ a_{12} \circ a_{13} \\ 2s_{23} &= s_{13} \circ a_{12} \circ a_{13}. \end{aligned}$$

The next matrix of character values M_2 becomes

$$\begin{array}{c} \\ \chi_{-4} \\ \chi_7 \\ \chi_{13} \\ \chi_{41} \\ \chi_{97} \\ \chi_{137} \end{array} \begin{array}{c} \begin{array}{ccccccc} a_{11} & a_{12} & a_{13} & a_{21} & s_{21} & s_{22} & s_{23} \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 \end{pmatrix} \end{array}.$$

All 3 columns of the forms $s_{2j} \in S_2$ lie in the space spanned by the columns of the forms in $B_2 = A_1 \cup A_2$. This immediately yields $Y_2 = \emptyset = A_3$, so we have $X_3 = X_2$ and $B_3 = B_2$, and S_3 contains 3 forms that are computed from the equations

$$\begin{aligned} 2s_{31} &= s_{21} \\ 2s_{32} &= s_{22} \circ a_{13} \\ 2s_{33} &= s_{23} \circ a_{11} \circ a_{21}. \end{aligned}$$

The character matrix M_3 becomes

$$\begin{array}{c} \\ \chi_{-4} \\ \chi_7 \\ \chi_{13} \\ \chi_{41} \\ \chi_{97} \\ \chi_{137} \end{array} \begin{array}{c} \begin{array}{ccccccc} a_{11} & a_{12} & a_{13} & a_{21} & s_{31} & s_{32} & s_{33} \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \end{pmatrix} \end{array},$$

which has maximal rank 6. This means that we have found the structure of our group to be $C_2^3 \times C_4 \times C_{16}^2$. In order to obtain a lower triangular character matrix, we take our final two generators of order 16 as

$$\begin{aligned} a_{41} &= s_{31} \circ a_{13} = (-1060801, 5626768, 533412), \\ a_{42} &= s_{33} \circ a_{13} \circ a_{21} = (875729, 4584376, -3684756), \end{aligned}$$

and add $Y_3 = \{\chi_{137}, \chi_{97}\}$ in the suggested order to our character basis. The result is the final character matrix

$$\begin{array}{c} \\ \chi_{-4} \\ \chi_7 \\ \chi_{13} \\ \chi_{41} \\ \chi_{137} \\ \chi_{97} \end{array} \begin{array}{c} \begin{array}{cccccc} a_{11} & a_{12} & a_{13} & a_{21} & a_{41} & a_{42} \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \end{array},$$

and our algorithm terminates. The elements a_{ij} listed in the top row form an *ordered basis* of $\mathcal{C}$, i.e., the sets $A_i = \{a_{ij}\}_j$ satisfy the hypotheses of lemma 3.5 for $G = \mathcal{C}$.

In the final stage of the algorithm, it turns out that the character column of the form $s_{32} \in S_3$ lies in the space generated by the previous columns, so we have to compute s_{33} before we find that the character matrix has maximal rank. In the cases where we are lucky enough to obtain already a character matrix of full rank *before* the final column has been computed, our algorithm suppresses the computation of the form corresponding to this final column. This saves an application of the division-by-2-algorithm. For large positive discriminants, the resulting gain can be considerable.

As observed in the previous section, the 'superfluous generator' s_{32} in the final stage of our algorithm is not entirely useless: it carries information on the relation between the ambiguous forms in the initial set S_0. More explicitly, the character values of s_{32} tell us that the element

$$s_D = s_{32} \circ a_{11} \circ a_{12} \circ a_{21} \circ a_{41}$$

is in $2\mathcal{C}$. As $\mathcal{C}$ is of exponent 16, this implies that s_D is annihilated by 8. Using the definition of s_{ij} and the order relations $2^i a_{ij} = 0$, the resulting relation $8s_{32} + 8a_{41} = 0$ is easily traced back to yield

$$s_{12} + s_{11} = [Q_{13}] + [Q_{97}] + [Q_{41}] = 0.$$

This is the unique non-trivial relation between the initial generators Q_p. We noted already that such relations can in principle be found from the fundamental unit ε_D. In this fairly small example it is still possible to compute ε_D explicitly. It has norm 1, and we have

$$\varepsilon_D + 1 = t \cdot (u + v \cdot 4 \cdot 7 \cdot 41 \cdot (\frac{1+\sqrt{D}}{2}))$$

where each of t, u, v is an integer of approximately 230 decimal digits. We find that $(\varepsilon_D + 1)/t$ is an element of norm $13 \cdot 97 \cdot 41^2$, from which we can read off the relation indicated above.

5. Ternary quadratic forms.

This section describes the reduction theory of ternary quadratic forms that is the basis of the division-by-2-algorithm in section 6.

Let $n \geq 1$ be an integer, and $L = \mathbf{Z}^n$ an n-dimensional lattice with standard inner product $\langle \cdot, \cdot \rangle : L \times L \to \mathbf{Z}$. For every endomorphism $A \in$

$\mathrm{End}(L) = M_n(\mathbf{Z})$, we have an associated quadratic form $F = F_A$ on L defined by $F(X) = \langle AX, X\rangle$. Writing A as a matrix $(a_{ij})_{i,j=1}^n$ with respect to the standard basis of L, we have

$$F(X) = F(x_1, \dots, x_n) = \sum_{1\le i,j\le n} a_{ij}x_ix_j.$$

For $n = 2$ and $n = 3$, we use variables x, y and z. If A ranges over the integral symmetric $(n \times n)$-matrices, then F_A ranges over the quadratic forms $F = \sum_{1\le i\le j\le n} c_{ij}x_ix_j$ for which the 'mixed coefficients' c_{ij} with $i \neq j$ are *even*. quadratic forms of this type in the current paper.

We define the *determinant* $\det(F)$ of a form F corresponding to a symmetric matrix A by $\det(F) = \det(A)$. In particular, the determinant of a quadratic form $Q = ax^2 + 2bxy + cy^2$ is for us equal to

$$\det(Q) = ac - b^2 = -\tfrac{1}{4}\mathrm{disc}(Q).$$

There is a natural right action of $\mathrm{GL}_n(\mathbf{Z})$ on the set of quadratic forms in n variables by 'coordinate transformations'. If a form F corresponds to a symmetric matrix A and $S \in \mathrm{GL}_n(\mathbf{Z})$ is a coordinate change, then $F^S = \langle ASX, SX\rangle = \langle S^TASX, X\rangle$ clearly corresponds to the matrix S^TAS. Here S^T denotes the transpose of S.

Two quadratic forms F and G are said to be equivalent if there exists a *unimodular* transformation $S \in \mathrm{SL}_n(\mathbf{Z})$ such that $F^S = G$. Note that $-\mathrm{id}_L$ acts trivially and has determinant $(-1)^n$, so the $\mathrm{GL}_n(\mathbf{Z})$-orbits and the $\mathrm{SL}_n(\mathbf{Z})$-orbits of forms coincide in odd dimension.

The *adjoint* A^* of a matrix $A = (a_{ij})_{i,j=1}^n$ is the matrix $((-1)^{i+j}m_{ij})_{i,j=1}^n$, where the (i,j)-minor m_{ij} of A is the determinant of the matrix that is obtained from A by deleting the i-th row and the j-th column. If A is invertible, one has

$$A^* = (\det A)\cdot(A^T)^{-1}.$$

This immediately yields the general identities $\det A^* = (\det A)^{n-1}$ and $A^*B^* = (AB)^*$, and an easy check yields the useful identity

$$A^{**} = (\det A)^{n-2}A. \tag{5.1}$$

For a quadratic form F corresponding to a symmetric matrix A, the adjoint form F^* of F is the form corresponding to A^*. Passing to the adjoint is compatible with the action of $\mathrm{SL}_2(\mathbf{Z})$ in the sense that we have $(F^S)^* = (F^*)^{S^*}$.

For $n=2$, we have Gauss's binary quadratic forms $(a,2b,c)=ax^2+2bxy+cy^2$ with even middle coefficient corresponding to symmetric matrices $\left(\begin{smallmatrix} a & b\\ b & c\end{smallmatrix}\right)$. Identity (2.1) tells us that every form of determinant Δ is equivalent to a form with first coefficient $|a|\le\sqrt{4|\Delta|/3}$. Moreover, a unimodular transformation that yields such an equivalent form can be efficiently computed [9].

For $n=3$ we obtain ternary forms, and for forms of non-zero determinant the reduction theory proceeds by a combination of binary reduction of both the form itself and its adjoint. Suppose the ternary form F of determinant $\Delta_F\neq 0$ corresponds to a symmetric matrix $A=(a_{ij})_{i,j=1}^3$ with adjoint $A^*=(A_{ij})_{i,j=1}^3$. Then we can use suitable unimodular transformations of the form

$$S_0=\begin{pmatrix} s_{11} & s_{12} & 0\\ s_{21} & s_{22} & 0\\ 0 & 0 & 1\end{pmatrix},$$

as if we were to reduce the quadratic form $F(x,y,0)=a_{11}x^2+2a_{12}xy+a_{22}y^2$ of determinant $a_{11}a_{22}-a_{12}^2=A_{33}$, and produce a ternary form F with unchanged adjoint coefficient A_{33} but with a_{11} satisfying $|a_{11}|\le\sqrt{4|A_{33}|/3}$. Similarly, by applying the unimodular matrix

$$S_1=\begin{pmatrix} 1 & 0 & 0\\ 0 & s_{22} & s_{23}\\ 0 & s_{32} & s_{33}\end{pmatrix}$$

to F we leave a_{11} invariant and change F^* by an application of

$$S_1^*=\begin{pmatrix} 1 & 0 & 0\\ 0 & s_{33} & -s_{32}\\ 0 & -s_{23} & s_{22}\end{pmatrix}.$$

Choosing the coefficients of S_1 as if reducing the quadratic form $F^*(0,y,x)=A_{33}x^2+2A_{23}xy+A_{22}y^2$, which has determinant $A_{33}A_{22}-A_{23}^2=\Delta_F a_{11}$ by (5.1), we can satisfy the inequality $|A_{33}|\le\sqrt{4|a_{11}\Delta_F|/3}$. Alternating these two transformations, we get smaller values of $|a_{11}|$ and $|A_{33}|$ until both inequalities $|a_{11}|\le\sqrt{4|A_{33}|/3}$ and $|A_{33}|\le\sqrt{4|a_{11}\Delta_F|/3}$ hold at the same time. The form F is then said to be *semi-reduced*, and it satisfies

$$\begin{aligned} |a_{11}| &\le \tfrac{4}{3}|\Delta_F|^{1/3}\\ |A_{33}| &\le \tfrac{4}{3}|\Delta_F|^{2/3}. \end{aligned} \tag{5.2}$$

A semi-reduced form remains semi-reduced under unimodular transformations of the form

$$S_2 = \begin{pmatrix} 1 & s_{12} & s_{13} \\ 0 & 1 & s_{23} \\ 0 & 0 & 1 \end{pmatrix},$$

and we can use these to produce a reduced ternary form. There are two possibilities, depending on whether the coefficient a_{11} of our semi-reduced form is zero or not.

In case $a_{11} = 0$ we also have $A_{33} = a_{12} = 0$, and therefore $\Delta_F = -a_{13}^2 a_{22}$. Looking at the effect of S_2 on F, we see that an appropriate choice of S_2 yields a form with

$$(5.3) \qquad |a_{33}| \le |a_{13}| \qquad \text{and} \qquad |a_{23}| \le \tfrac{1}{2}\gcd(a_{22}, a_{13}).$$

A semi-reduced form with $a_{11} = 0$ satisfying (5.3) is said to be *reduced*. For given Δ_F, there are only finitely many possible values of a_{13} and a_{22}, so the number of reduced forms of given determinant with $a_{11} = 0$ is finite.

For a semi-reduced form with $a_{11} \ne 0$, we apply S_2 with suitable s_{12} to obtain

$$(5.4) \qquad |a_{12}| \le \tfrac{1}{2}|a_{11}|.$$

As A_{33} does not vanish, a simple inspection of the action of

$$S_2^* = \begin{pmatrix} 1 & 0 & 0 \\ -s_{12} & 1 & 0 \\ s_{12}s_{23} - s_{13} & -s_{23} & 1 \end{pmatrix}$$

on F^* shows that we can further achieve

$$(5.5) \qquad |A_{23}| \le \tfrac{1}{2}|A_{33}| \qquad \text{and} \qquad |A_{13}| \le \tfrac{1}{2}|A_{33}|.$$

A semi-reduced form with $a_{11} \ne 0$ satisfying (5.4) and (5.5) is called *reduced*. It is again true that there are only finitely many reduced forms of given determinant with $a_{11} \ne 0$. Indeed, we have bounded the coefficients a_{11}, a_{12} and A_{13}, A_{23}, A_{33} in terms of Δ_F, and the following elementary completion lemma shows that in our situation, these coefficients and Δ_F uniquely determine the form.

5.6. LEMMA. *Suppose we are given rational numbers $\Delta, a_{11}, a_{12}, A_{13}, A_{23}$ and A_{33} satisfying $\Delta a_{11} A_{33} \neq 0$. Then there exists a unique rational symmetric (3×3)-matrix $A = (a_{ij})_{i,j=1}^3$ with determinant Δ and adjoint $A^* = (A_{ij})_{i,j=1}^3$, i.e., there is a unique way to define the starred entries in*

$$A = \begin{pmatrix} a_{11} & a_{12} & * \\ a_{12} & * & * \\ * & * & * \end{pmatrix} \qquad \text{and} \quad A^* = \begin{pmatrix} * & * & A_{13} \\ * & * & A_{23} \\ A_{13} & A_{23} & A_{33} \end{pmatrix}.$$

such that A is rational and symmetric with determinant Δ and adjoint A^*.

Proof. As a_{11} is non-zero, we can define a_{22} by the relation

$$(*) \qquad a_{11}a_{22} - a_{12}^2 = A_{33}.$$

We now use $A_{33} \neq 0$ to define A_{11}, A_{12}, A_{22} as the unique solutions to the equations

$$(5.7) \qquad \begin{aligned} \Delta a_{11} &= A_{22}A_{33} - A_{23}^2 \\ -\Delta a_{12} &= A_{12}A_{33} - A_{23}A_{13} \\ \Delta a_{22} &= A_{11}A_{33} - A_{13}^2, \end{aligned}$$

and form the rational symmetric matrix $B = (A_{ij})_{i,j=1}^3$. It is clear that if matrices A and A^* of the required sort exist, then the relations (5.7) hold by (5.1) and A is uniquely determined by the equality $A^* = B$. Let us therefore, in accordance with (5.7), define the rational symmetric matrix $A = (a_{ij})_{i,j=1}^3$ by the identity $\Delta A = B^*$. Passing to the adjoint yields $\Delta^2 A^* = \det(B) \cdot B$, so we see from $(*)$ that we have $\Delta^2 = \det(B)$ and $A^* = B$. Thus A has the correct adjoint, and from $\Delta A = B^* = A^{**}$ we see that its determinant equals Δ. $\square$

As every ternary form is equivalent to a reduced form, we see that the number of equivalence classes of ternary forms of determinant Δ is finite for every Δ. As an example that we will need in the next section, let us take$\Delta = -1$ and determine the equivalence classes. The entries of the symmetric matrices corresponding to the ternary form F and its adjoint will again be denoted by a_{ij} and A_{ij}, respectively.

By (5.2), a semi-reduced ternary form F of determinant $\Delta = -1$ has either $a_{11} = A_{33} = 0$ or $|a_{11}| = |A_{33}| = 1$. In the case $a_{11} = A_{33} = 0$ we have $a_{22}a_{13}^2 = 1$, so $a_{22} = 1$ and $a_{13} = \pm 1$. If F is reduced, (5.3) yields $a_{23} = 0$ and $a_{33} \in \{-1, 0, 1\}$, so we find 6 forms. If we are in the second case and F is reduced, then $a_{12} = A_{23} = A_{13} = 0$ by (5.4) and (5.5). This yields $a_{13} = a_{23} = 0$ and shows that F is one of the 4 forms $\pm x^2 \pm y^2 \pm z^2$ with an odd number of coefficients -1. This shows that there are $6 + 4 = 10$ reduced forms of determinant -1. Apart from the negative definite form $-x^2 - y^2 - z^2$, all these forms are indefinite. It is easily checked that the nine reduced indefinite forms are all equivalent, so there are two $\mathrm{SL}_3(\mathbf{Z})$-equivalence classes. We have proved the following.

5.8. Lemma. *An indefinite ternary form of determinant -1 is $\mathrm{SL}_3(\mathbf{Z})$-equivalent to the form $y^2 - 2xz$.* □

Our proof of this lemma is constructive, as it shows how to find a matrix $S \in \mathrm{SL}_3(\mathbf{Z})$ that maps a ternary form F of determinant -1 to $y^2 - 2xz$. One simply reduces F by the procedure outlined in this section to obtain one of the 9 reduced indefinite forms listed above, keeping track of the transformation matrices encountered along the way, and performs an explicit transformation that we did not bother to write down to obtain $y^2 - 2xz$. It has been shown by Lagarias [9] that this gives rise to a polynomial-time algorithm.

6. Division by 2 in quadratic class groups.

In order to complete the description of our algorithm, we explain in this section how one can explicitly divide by 2 the class of a binary quadratic form Q that is known to be in the principal genus. We have seen in the discussion following lemma 2.4 that finding a form P satisfying $2[P] = [Q]$ is closely related to the representation of suitable squares by the form Q, i.e., to finding solutions to a ternary quadratic equation $Q(x, y) = z^2$. Gauss [7, art. 286] observed that this can be done efficiently by extending the given binary form to a ternary form for which the represented squares can be trivially found after reduction. It is convenient to assume that we work with even discriminants. This is not a restriction as for odd D, the natural map $\mathcal{C}(4D) \to \mathcal{C}(D)$ is an isomorphism. The basic observation is the following.

6.1. Lemma. *Let Q be a binary quadratic form of even discriminant D. Then the class of Q is in $2\mathrm{Cl}(D)$ if and only if there exists a ternary quadratic form Q_1 of determinant -1 satisfying $Q_1(x, y, 0) = Q(x, y)$.*

Proof. It suffices to show that all genus characters in X_D vanish on the class of $Q = (\alpha, 2\beta, \gamma)$ if and only if there exists an integral symmetric matrix A of determinant -1 of the form

$$A = \begin{pmatrix} \alpha & \beta & a_{13} \\ \beta & \gamma & a_{23} \\ a_{13} & a_{23} & a_{33} \end{pmatrix}.$$

Suppose A exists, and write $\delta = -D/4 = \alpha\gamma - \beta^2$ for the determinant of Q. Then the adjoint of A is an integral matrix of the form

$$A^* = \begin{pmatrix} A_{11} & A_{12} & n \\ A_{12} & A_{22} & m \\ n & m & \delta \end{pmatrix},$$

and the relations (5.7) with $\Delta = -1$ yield

$$\begin{aligned} \alpha &= m^2 - \delta A_{22} \\ -\beta &= mn - \delta A_{12} \\ \gamma &= n^2 - \delta A_{11}. \end{aligned} \tag{6.2}$$

If p is an odd prime divisor of D, then p divides $\delta = \alpha\gamma - \beta^2$ and either α or γ is coprime to p, so we see from (3.3) and (6.2) that the genus character χ_p vanishes on Q. The characters of odd prime conductor generate the subgroup $X'_D/\langle\chi_d\rangle \subset X_D/\langle\chi_d\rangle$, and we see from definition (3.1) that δ is divisible by 4 if χ_{-4} is needed to generate the full group, and divisible by 8 if χ_8 is needed. As either α or γ is odd, (6.2) shows that these characters vanish on Q as well. We conclude that the existence of A implies that Q is in the principal genus of $\mathrm{Cl}(D)$.

Conversely, if Q is in the principal genus, we claim that the congruences

$$m^2 \equiv \alpha \bmod \delta \qquad mn \equiv -\beta \bmod \delta \qquad n^2 \equiv \gamma \bmod \delta$$

admit solutions $m, n \in \mathbf{Z}$. By the Chinese remainder theorem, this amounts to solving the congruences modulo all prime powers p^k dividing δ. Either α or γ is a unit modulo such a prime power, say α, and the vanishing of the corresponding genus character (or, for $p = 2$, characters) implies that we can solve $m^2 \equiv \alpha \bmod p^k$. Taking $n \equiv -\beta m^{-1} \bmod p^k$, we see that all three congruences are satisfied modulo p^k.

Now pick m and n satisfying the congruences modulo δ. As α and δ are non-zero, we can apply the completion lemma 5.6 to find a rational symmetric matrix A of determinant -1 and its adjoint A^* that are of the form given above. The coefficients A_{11}, A_{12} and A_{22} of A^* satisfy (6.2) and are clearly integral. This makes A^* and $A^{**} = -A$ integral, so we have found the required matrix A. $\square$

The preceding proof shows that finding the matrix A corresponding to Q_1 amounts to extracting square roots of integers modulo the prime powers dividing D. The prime powers dividing D are supposed to be known, and extracting square roots modulo prime powers can be done efficiently if one knows a quadratic non-residue modulo the prime occurring in the modulus [3, section 1.5.1]. Finding such a residue is easy in practice and can be done in random polynomial time. A deterministic polynomial algorithm however only exists if one assumes the generalized Riemann hypothesis. See [3, p. 33–34, remarks (2) and (3)]. It is only this minor non-deterministic step that makes our algorithm a random polynomial time algorithm.

In the situation of lemma 6.1, the binary form Q is represented by the ternary form Q_1. More generally, we say that a binary quadratic form Q is represented by a ternary quadratic form F if there exist integers a_i and b_i for $i = 1, 2, 3$ such that

$$F(a_1x + b_1y,\ a_2x + b_2y,\ a_3x + b_3y) = Q(x, y). \tag{6.3}$$

Writing A_F for the symmetric matrix corresponding to F and $Q = (\alpha, 2\beta, \gamma)$, we see that (6.3) is equivalent to the identities

$$\text{(6.4)}\quad \alpha = F(a_1, a_2, a_3) \qquad \beta = \langle (a_i)_{i=1}^3, A_F(b_i)_{i=1}^3 \rangle \qquad \gamma = F(b_1, b_2, b_3).$$

The representation (6.3) is *proper* if the integers a_i and b_i come from a unimodular transformation

$$S = \begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{pmatrix} \in \mathrm{SL}_3(\mathbf{Z}). \tag{6.5}$$

If this is the case, we have $Q(x, y) = Q_1(x, y, 0)$ for the ternary form $Q_1 = F^S$. Moreover, we have $Q_1^*(0, 0, 1) = \det Q$, and Q is represented by *every* ternary form that is equivalent to Q_1. As we do not consider binary quadratic forms that are negative definite, the form Q_1 and therefore the representing ternary form F are indefinite. Combining lemmas 6.1 and 5.8, we now obtain the following result.

6.6. THEOREM. *Let Q be a binary quadratic form of even discriminant D. Then the class of Q is in the principal genus $2\mathrm{Cl}(D)$ if and only if Q can be properly represented by the ternary form $\Phi = y^2 - 2xz$.* $\square$

The representation in theorem 6.6 is found by constructing a ternary form Q_1 of determinant -1 as in lemma 6.1 and reducing the form Q_1 to Φ as outlined in the previous section. We find $Q_1^M = \Phi$ for some $M \in \mathrm{SL}_3(\mathbf{Z})$, and $S = M^{-1}$ yields the representation $Q(x,y) = \Phi^S(x,y,0)$. However, as Shanks observed, we do not need S but only the reduction matrix M to to solve the equation $2[P] = [Q]$.

Indeed, if we have $Q(x,y) = \Phi^S(x,y,0)$ with $S \in \mathrm{SL}_3(\mathbf{Z})$ as in (6.5), the form Q represents the squares

$$Q(b_1, -a_1) = (a_1 b_2 - a_2 b_1)^2 \qquad \text{and} \qquad Q(b_3, -a_3) = (a_3 b_2 - a_2 b_3)^2$$

of integers $r = a_1 b_2 - a_2 b_1$ and $p = a_2 b_3 - a_3 b_2$ that occur in the last row

$$M^T(0,0,1) = (p,q,r) = (a_2 b_3 - a_3 b_2,\ a_3 b_1 - a_1 b_3,\ a_1 b_2 - a_2 b_1)$$

of the reduction matrix $M = S^{-1}$. In view of the observation following lemma 2.4, it is therefore to be expected that p and r occur as first coefficients of binary forms whose duplication lies in $[Q]$.

6.7. Theorem. *Let Q be a primitive binary quadratic form of even discriminant D, and suppose we have $M \in \mathrm{SL}_3(\mathbf{Z})$ and a ternary form Q_1 satisfying $Q_1(x,y,0) = Q(x,y)$ and $Q_1^M = \Phi = y^2 - 2xz$. Let $(p,q,r) = M^T(0,0,1)$ be the last row of M, and define the quadratic form*

$$P = \begin{cases} px^2 + 2qxy + 2ry^2 & \text{if } p \text{ is odd} \\ rx^2 - 2qxy + 2py^2 & \text{if } p \text{ is even.} \end{cases}$$

Then P is a primitive form of discriminant D, and we have $2[P] = [Q] \in \mathrm{Cl}(D)$.

Proof. As $\gcd(p,q,r)$ divides $\det M = 1$, we have $\gcd(p,q,r) = 1$, so in order to show that P is primitive we have to check that p and r cannot both be even. Suppose they are. Then q is odd. The last row of the matrix product $MS = \mathrm{id}$ yields the relations $pa_1 + qa_2 + ra_3 = pb_1 + qb_2 + rb_3 = 0$, so a_2 and b_2 are both even. It follows from (6.4) that the coefficients

$$\alpha = \Phi(a_1, a_2, a_3) = a_2^2 - 2a_1 a_3$$
$$\gamma = \Phi(b_1, b_2, b_3) = b_2^2 - 2b_1 b_3$$

and 2β of $Q = (\alpha, 2\beta, \gamma)$ are all even, contradicting the primitivity assumptions on Q.

There are various ways to check the identity $2[P] = [Q]$. One can multiply M by transformations stabilizing Φ and reduce to the case that p is coprime to D, which can be handled by the method given after lemma 2.4. However, it is much more efficient to apply lemma 2.8 directly. Taking F in that lemma to be equal to $(p, -2q, 2r)$ or $(2p, -2q, r)$, i.e., in the class of $-[P]$, we can take the bilinear form in 2.8 respectively equal to

$$\begin{pmatrix} s_1 & s_2 & s_3 \\ t_1 & t_2 & t_3 \end{pmatrix} = \begin{pmatrix} b_3 & b_2 & 2b_1 \\ a_3 & a_2 & 2a_1 \end{pmatrix} \qquad \text{and} \qquad \begin{pmatrix} 2b_3 & b_2 & b_1 \\ 2a_3 & a_2 & a_1 \end{pmatrix}.$$

As we have $\beta = -a_1 b_3 + a_2 b_2 - a_3 b_1$ by (6.4), it follows from 2.8 that the class inverse to $2[P]$ contains the form $(\alpha, -2\beta, \gamma)$. This implies $2[P] = [Q]$, and consequently P has the required discriminant $4(q^2 - 2pr) = D$. We can check this directly by substituting (p, q, r) in the adjoint $\Phi^* = -y^2 + 2xz$ of $\Phi = Q_1^M = y^2 - 2xz$. As M^* is the inverse of M^T, we obtain the desired value

$$\Phi^*(p, q, r) = -q^2 + 2pr = (Q_1^*)^{M^*}(p, q, r) = Q_1^*(0, 0, 1) = \det Q = -D/4. \qquad \square$$

Theorem 6.7 shows that we can divide $[Q] \in \mathrm{Cl}(D)$ by 2 if we can complete Q to a ternary form Q_1 of determinant -1 and find the transformation matrix M that reduces Q_1 to $\Phi = y^2 - 2xz$. Both of these steps can be efficiently performed whenever Q is in the principal genus. This finishes the description of the division-by-2-algorithm 3.4.

7. Performance of the algorithm.

The algorithms described in the previous sections have been implemented in the high-level language of the computer algebra system Magma. Table 7.1 below shows the results of an experiment devised to give an indication of the dependence of the performance of the algorithm on various parameters, in particular the size and sign of the discriminant and the structure of $\mathcal{C}$.

For several n ranging from 25 to 400 (as indicated at the top of each column in the tables), we found 5 primes close to 10^n that are squares modulo each other. The first table lists the primes used; the i-th prime used for each value of n is $10^n + r_i$. The primes $10^{100} + r_i$ are the prime factors of the discriminant D occurring in the introduction.

r	$n = 25$	50	100	200	400
r_1	13	577	949	357	69
r_2	609	709	1293	3381	2877
r_3	657	1137	2809	5541	16249
r_4	1821	2781	6637	11269	29857
r_5	3309	4209	22261	23317	32797

Each row in table 7.1 gives results for the discriminant pD built up from the product D of the five primes of size 10^n and an additional factor p that is indicated in the first column. As additional factors we chose the odd primes up to 79, with a sign chosen such that we have $p \equiv 1 \bmod 4$, and the even factors $p = \pm 8$. We are looking here then at discriminants of 125 to just over 2000 decimal digits. It would be out of the question to factor arbitrary discriminants of that size, or to compute a single full class group $\mathrm{Cl}(pD)$.

Each entry in the table consists of three values. The first is the 2-class number of pD, written in a way that corresponds to the structure of the 2-class group $\mathcal{C}(pD)$. The two values on the second line are the number of seconds it took our implementation to find this group structure and the (rounded) quotient of this running time by the number of times a division by 2 had to be performed to obtain the group structure. Thus, the first entry says that for D the product of our five primes $10^{25} + r_i$, we have $\mathcal{C}(-79 \cdot D) \equiv C_2^3 \times C_4 \times C_{16}$. This computation took 11 seconds. As the computation of such a group takes 4 divisions by 2 by formula (3.6), this is approximately 3 seconds per division.

In a given column, the time needed per division is roughly constant. This means that the time needed to find the 2-group structure is proportional to the number of divisions by 2, that is, to the combination of the width and depth of the 2-group given in (3.6). There is a small but noticeable difference in running time between imaginary and real class groups. In the table, they are separated by a row that indicates, for each value of n, the average time it took the algorithm per division for the imaginary and for the real class groups. On average, the algorithm is about 15% slower for real quadratic class groups.

The average running times per division in the central row give an indication of the complexity function for the major operations as a function of the number of decimal digits. The dominant factor is the slightly worse than quadratic time growth of ordinary integer arithmetic with the size of the integers.

A closer look at where the time is spent reveals that there are three main c omponents: the ternary reduction step, the modular square root used in the division by 2 of a class in the principal genus, and the composition and reduction of quadratic forms. The ternary reduction step takes up between 1/3 and 1/2 of the total time for a divison by 2. The fraction of time needed for the modular square root (with modulus the discriminant, but performed prime by prime) increases slightly with the size of the primes

Table 7.1. *Class groups and running times.*

p	$n = 25$	50	100	200	400
-79	$2^3 \cdot 4 \cdot 16$	$2 \cdot 4^3 \cdot 256$	$2^3 \cdot 4^2$	$2^3 \cdot 4 \cdot 16$	$2^3 \cdot 4 \cdot 8$
	11 3	100 10	64 32	811 203	3831 1277
-71	$2^2 \cdot 4 \cdot 8^2$	$2 \cdot 4^3 \cdot 8$	$2^2 \cdot 4^2 \cdot 8$	$2 \cdot 4^3 \cdot 8$	$2 \cdot 4^3 \cdot 8$
	12 2	44 9	137 34	922 184	5749 1150
-67	$2^3 \cdot 4 \cdot 8$	$2^3 \cdot 8 \cdot 64$	$2^3 \cdot 4 \cdot 8$	$2^3 \cdot 4 \cdot 8$	$2^3 \cdot 4 \cdot 8$
	7 2	68 10	101 34	604 201	3617 1206
-59	$2 \cdot 4^4$	$2^2 \cdot 4^2 \cdot 8$	$2^3 \cdot 4 \cdot 8$	$2^3 \cdot 4 \cdot 64$	$2^4 \cdot 4$
	8 2	35 9	102 34	1290 215	1067 1067
-47	$2^4 \cdot 4$	$2^4 \cdot 8$	$2 \cdot 4^2 \cdot 8 \cdot 64$	$2^4 \cdot 4$	$2^2 \cdot 4^2 \cdot 8$
	2 2	18 9	328 36	178 178	4933 1233
-43	$2^3 \cdot 8 \cdot 16$	$2^2 \cdot 4^2 \cdot 8$	2^5	$2^4 \cdot 16$	$2 \cdot 4^3 \cdot 16$
	13 3	36 9	0 –	631 210	7201 1200
-31	$2 \cdot 4^2 \cdot 8 \cdot 64$	$2^3 \cdot 4 \cdot 16$	$2^3 \cdot 8^2$	$2^3 \cdot 4 \cdot 8$	$2^2 \cdot 4 \cdot 8^2$
	25 3	37 9	149 37	597 199	6330 1266
-23	$2^2 \cdot 4^2 \cdot 64$	$4^4 \cdot 16$	$2^2 \cdot 4^3$	$2^2 \cdot 4^2 \cdot 64$	$2^3 \cdot 4^2$
	19 3	62 9	91 30	1464 209	2212 1106
-19	$2^2 \cdot 4^3$	$2^2 \cdot 4^3$	$2^4 \cdot 8$	$4^4 \cdot 32$	$2^4 \cdot 4$
	7 2	25 8	74 37	1554 194	1084 1084
-11	$2^2 \cdot 4 \cdot 8 \cdot 128$	$2^4 \cdot 4$	$2 \cdot 4^2 \cdot 8 \cdot 256$	$2^2 \cdot 4^2 \cdot 8$	$2^2 \cdot 4^2 \cdot 8$
	24 3	8 8	415 38	802 200	4703 1176
-8	$2^3 \cdot 8 \cdot 64$	$2^2 \cdot 4^3$	$2^4 \cdot 4$	2^5	$2^3 \cdot 4^2$
	23 3	22 7	30 30	0 –	2145 1072
-7	$2 \cdot 4^3 \cdot 16$	$2^2 \cdot 4^2 \cdot 32$	$2^3 \cdot 4 \cdot 16$	$2 \cdot 4^4$	$2^4 \cdot 4$
	14 2	56 9	144 36	694 173	1070 1070
-3	$2 \cdot 4^3 \cdot 8$	$2^2 \cdot 4^2 \cdot 8$	$2^4 \cdot 4$	$2^2 \cdot 4^2 \cdot 8$	$2^3 \cdot 4^2$
	11 2	33 8	30 30	791 198	2256 1128
mean	2.6	8.9	35.6	198.5	1176.9
	3.1	10.3	40.9	212.0	1350.0
5	$2^2 \cdot 4^2 \cdot 8$	$2^2 \cdot 4^3$	$2^2 \cdot 4^2 \cdot 16$	$2^2 \cdot 4^3$	$2^3 \cdot 4^2$
	19 3	38 10	341 43	796 199	3676 1225
8	$2^3 \cdot 4 \cdot 16$	$2^2 \cdot 4^3$	$2^4 \cdot 4$	2^5	$2^3 \cdot 4^2$
	23 3	43 11	94 47	2 –	4434 1478
13	$2^2 \cdot 4^3$	$2^3 \cdot 4^2$	$2 \cdot 4^4$	$2^2 \cdot 4^3$	$2^3 \cdot 4 \cdot 8$
	12 3	28 9	187 37	861 215	6630 1326
17	$2 \cdot 4^3 \cdot 8$	$2^2 \cdot 4^2 \cdot 8$	$2^3 \cdot 4^2$	$2^2 \cdot 4^3$	$2^3 \cdot 4^2$
	23 3	58 10	110 37	817 204	4102 1367
29	$2^4 \cdot 4$	$2^3 \cdot 4^2$	$2^3 \cdot 4 \cdot 16$	$2^3 \cdot 4^2$	$2^2 \cdot 4^3$
	7 3	30 10	306 44	601 200	5366 1341
37	$2^2 \cdot 4^3$	$2^3 \cdot 4^2$	$2^2 \cdot 4^2 \cdot 8$	$2^2 \cdot 4^2 \cdot 16$	$2^2 \cdot 4^3$
	11 3	29 10	255 43	1929 241	5653 1413
41	$2^2 \cdot 4^2 \cdot 8$	$2^3 \cdot 4 \cdot 8$	$2^2 \cdot 4^3$	$2^3 \cdot 4^2$	$2^2 \cdot 4^3$
	18 3	54 11	154 38	669 223	4749 1187
53	$2^2 \cdot 4^3$	4^5	$2 \cdot 4^4$	$2^4 \cdot 4$	$2^4 \cdot 4$
	12 3	61 10	190 38	373 187	2516 1258
61	$2^2 \cdot 4^3$	$2^2 \cdot 4^3$	$2^4 \cdot 4$	$2 \cdot 4^2 \cdot 8^2$	$2^2 \cdot 4^2 \cdot 16$
	12 3	45 11	81 40	1804 226	11044 1381
73	$2^2 \cdot 4^3$	$2^2 \cdot 4^3$	$2^4 \cdot 4$	$2^3 \cdot 4^2$	$2^3 \cdot 4 \cdot 8$
	12 3	45 11	81 41	626 209	7178 1436

involved, and in the largest case (of 400 digit primes) takes about as long as the ternary reduction. The contribution from the composition of forms varies considerably but is usually much smaller. It depends primarily on the number of reduction steps necessary after a single composition in the very last stage of the division-by-2-algorithm. In our examples sometimes several hundreds of reduction steps were needed, taking up to 1/5 of the total time for the large discriminant case.

References

[1] W. Bosma, J. J. Cannon, C. Playoust, *The Magma algebra system I: the user language*, J. Symbolic Comput. (to appear).

[2] W. Bosma and P. Stevenhagen, *Density computations for real quadratic units*, Math. Comp. **65** (1996), no. 215, 1327–1337.

[3] H. Cohen, *A course in computational algebraic number theory*, Springer GTM 138, 1993.

[4] H. Cohen, F. Diaz y Diaz, M. Olivier, *Calculs de nombres de classes et de régulateurs de corps quadratiques en temps sous-exponentiel*, Séminaire de Théorie des Nombres Paris 1990–91, Birkhäuser, 1993, pp. 35–46.

[5] D.A. Cox, *Primes of the form* $x^2 + ny^2$, Wiley-Interscience, 1989.

[6] S. Düllmann, *Ein Algorithmus zur Bestimmung der Klassengruppe positiv definiter binärer quadratischer Formen*, Dissertation, Universität des Saarlandes, Saarbrücken, 1991.

[7] C. F. Gauss, *Disquisitiones Arithmeticae*, Gerhard Fleischer, Leipzig, 1801.

[8] J. Hafner, K. McCurley, *A rigorous subexponential algorithm for computation of class groups*, J. Amer. Math. Soc. **2** (1989), no. 4, 837–850.

[9] J. C. Lagarias, *Worst-case complexity bounds for algorithms in the theory of integral quadratic forms*, J. of Algorithms **1** (1980), 142–186.

[10] J. C. Lagarias, *On the computational complexity of determining the solvability or unsolvability of the equation* $X^2 - DY^2 = -1$, Trans. Amer. Math. Soc. **260** (1980), no. 2, 485–508.

[11] D. Shanks, *Gauss's ternary form reduction and the 2-Sylow subgroup*, Math. Comp. **25** (1971), no. 116, 837–853; Erratum: Math. Comp. **32** (1978), 1328–1329.

[12] P. Stevenhagen, *The number of real quadratic fields having units of negative norm*, Exp. Math. **2** (1993), no. 2, 121–136.

[13] P. Stevenhagen, *A density conjecture for the negative Pell equation*, Computational Algebra and Number Theory, Sydney 1992, Kluwer Academic Publishers, 1995, pp. 187–200.

Wieb Bosma et Peter Stevenhagen
Faculteit Wiskunde, Informatica, Natuurkunde en Sterrenkunde
Universiteit van Amsterdam
Plantage Muidergracht 24
1018 TV Amsterdam
The Netherlands
e-mail: wieb@wins.uva.nl, psh@wins.uva.nl