QUADRATIC FIELDS AND FACTORIZATION

by

R.J. SCHOOF

1. INTRODUCTION

Let K be an algebraic number field and $\mathcal{O} = \mathcal{O}(K)$ its ring of integers. We recall a few basic definitions and facts concerning algebraic number fields.

By $I(K)$ we denote the group of fractional $\mathcal{O}$-ideals and by $P(K)$ its subgroup of principal fractional $\mathcal{O}$-ideals, which is a subgroup of $I(K)$. The class group $Cl(K)$ of K is defined by

$$Cl(K) = I(K)/P(K).$$

The class group is a finite abelian group and its order is denoted by $h(K)$, the class number of K. By $\mathcal{O}^\times$ we denote the multiplicative group of units of $\mathcal{O}$. The structure of $\mathcal{O}^\times$ as an abelian group, is given by Dirichlet's Unit Theorem:

THEOREM 1.1. *Let K be an algebraic number field and $\mathcal{O}$ its ring of integers, then*

$$\mathcal{O}^\times \simeq \mu(\mathcal{O}) \oplus \mathbb{Z}^{r_1+r_2-1}.$$

Here $\mu(\mathcal{O})$ denotes the finite group of roots of unity in K,

r_1 = number of embeddings $K \hookrightarrow \mathbb{R}$,

r_2 = half the number of embeddings $K \hookrightarrow \mathbb{C}$ with $\mathrm{im}(K) \not\subset \mathbb{R}$.

It holds that $r_1 + 2r_2 = n = [K:\mathbb{Q}]$, the (absolute) degree of K. For these and more definitions and facts from algebraic number theory see for instance [17].

In general, it is hard to determine the class group of a number field, which, for instance, is given by a generator; for this general problem see ZANTEMA's talk [13]. Here we shall concentrate on fields with small degrees; in this case, the rings of integers do not contain too many units and the computation of the class group is relatively easy. It appears to be possible to determine the class group of fields with small degrees, which have very large discriminants.

First we consider *complex quadratic number fields*. A field K is called complex quadratic if $[K:\mathbb{Q}] = 2$ and if $r_1 = 0$, $r_2 = 1$; it follows from Dirichlet's Unit Theorem that $\mathcal{O}(K)$ contains only finitely many units.

The study of the class groups of these fields is a very old one; it was initiated by Gauss, in the beginning of the 19th century [12]. Gauss studied the problem in the language of "binary quadratic forms" and he made extensive lists of class groups of complex quadratic fields. In Section 2 we shall discuss the complex quadratic fields in more detail; it appears that for our purposes, it is useful to formulate matters in the old-fashioned terms of binary quadratic forms again. An algorithm, due to D. SHANKS [31], to compute class groups of complex quadratic fields will be treated in Section 3.

Next we consider *real quadratic number fields* i.e. fields of degree 2 with $r_1 = 2$ and $r_2 = 0$. For a real quadratic field K, Dirichlet's Unit Theorem boils down to

$$\mathcal{O}(K)^\times \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}.$$

The determination of the class group of a real quadratic field cannot go, it seems, without the determination of the group of units; the latter is equivalent to finding a unit ε in $\mathcal{O}^\times$ such that $\mathcal{O}^\times$ is generated by ε and -1, which in turn is easily seen to be equivalent to solving a so-called Pellian equation, a problem which dates back to Fermat. The study of class groups of real quadratic fields was also begun by Gauss, who studied the subject in terms of binary quadratic forms.

In Section 4 we will discuss the structure of the class groups and unit groups of real quadratic fields in more detail, here some new ideas of LENSTRA and SHANKS come in [18,31], which give rise to a new, fast algorithm to determine the class group and, in some sense, the size of the group of units of a real quadratic field. We will describe this algorithm in Section 5: it is closely related to Shanks', discussed in Section 3, but slightly more complicated.

Complex cubic fields are fields of degree 3 over $\mathbb{Q}$ with $r_1 = 1$ and $r_2 = 1$. Complex cubic fields are not Galois extensions of $\mathbb{Q}$; the structure of their groups of units is the same as for real quadratic fields: if K is a complex cubic fields we have that

$$O(K)^\times \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}.$$

We do not discuss this class of fields; an algorithm to compute the class groups and the groups of units of these fields is being developed by WILLIAMS and SCHMID [40], their algorithm is along the same lines as the algorithm for real quadratic fields discussed in Section 5.

In Section 6 we point out how the algorithms, discussed in Sections 3 and 5 may be used to factor the discriminant of the number fields under consideration. We will in fact, describe two deterministic factorization algorithms which, on assumption of certain generalized Riemann hypotheses, factor an integer N in time, bounded by $N^{1/5+\varepsilon}$ for all $\varepsilon > 0$. For a discussion of related algorithms see [13,23].

The algorithms discussed are suitable to compute the class groups and units of quadratic fields that have *very* large discriminants. In fact, determining the class group and units of quadratic fields with discriminants of fewer than, say, 6 decimal digits, may be done faster by simpler and more direct methods. Therefore, in application of these algorithms, one should think of discriminants of 10 to 30 decimal digits.

Using these algorithms, one can practice a kind of experimental mathematics; it seems to be generally believed, that every finite abelian group occurs as a subgroup of the class group of some, say, complex quadratic field but theoretical results on this question are very scarce indeed. By means of these algorithms, however, one is able to compute class groups of quadratic fields with very large discriminants, and, guided by heuristic, one can search for explicit examples of quadratic fields that have unusual subgroups of their class groups. Only recently, some progress in this direction has been made. Some old and new results will be discussed in Section 7.

Finally, in Section 8, we will give a few details on the actual implementation of the algorithms on the SARA CDC-Cyber 170-750 computer.

2. CLASS GROUPS OF COMPLEX QUADRATIC NUMBER FIELDS

It is well known that the discriminant of complex quadratic number fields are negative integers, congruent to 0 or 1 (mod 4). Furthermore, complex quadratic fields are characterized by their discriminants, but it is not true that every negative integer $\equiv 0$ or 1 (mod 4) is the discriminant of some complex quadratic number field.

However, every $\Delta \in \mathbb{Z}_{<0}$, $\Delta \equiv 0$ or 1 (mod 4), can in one and only one way be written as $\Delta = f^2 D$, where D is the discriminant of a complex quadratic number field K, and $f \in \mathbb{Z}_{\geq 1}$. Now, $\Delta = \Delta(\mathcal{O})$ is the discriminant of the unique subring $\mathcal{O}$ of index f in $\mathcal{O}(K)$: the unique *quadratic order* of discriminant Δ.

So for every $\Delta \in \mathbb{Z}_{<0}$, $\Delta \equiv 0$ or 1 (mod 4), there exists a unique *complex quadratic order* $\mathcal{O} = \mathcal{O}(\Delta)$, with discriminant Δ, contained in the ring of integers of some complex quadratic number field. Rings of integers themselves are also called *maximal orders*. It is also possible to define the notion of class group for non-maximal orders:

Let $\mathcal{O}$ be a complex quadratic order, contained in a complex quadratic field K. By definition, a fractional $\mathcal{O}$-ideal M is a non-zero finitely generated $\mathcal{O}$-submodule of K, and M is called *invertible* if there is a fractional $\mathcal{O}$-ideal $N \subset K$ such that $MN = \mathcal{O}$. By $I(\mathcal{O})$ we denote the *group* of invertible fractional $\mathcal{O}$-ideals and by $P(\mathcal{O})$ the group of principal fractional ideals, a subgroup of $I(\mathcal{O})$. The class group of $\mathcal{O}$ is denoted by $Cl(\mathcal{O})$ and defined by $Cl(\mathcal{O}) = I(\mathcal{O})/P(\mathcal{O})$. The group $Cl(\mathcal{O})$ is finite abelian and its order will be denoted by $h(\mathcal{O})$, the class number of $\mathcal{O}$.

REMARK. If $\mathcal{O}$ is a *maximal* complex quadratic order, i.e. the ring of integers of some complex quadratic field, then $\mathcal{O}$ is a Dedekind ring and *all* fractional $\mathcal{O}$-ideals are invertible.

EXERCISE. Let $\mathcal{O}$ be a complex quadratic order, and M a fractional $\mathcal{O}$-ideal; then M is invertible iff $\{\alpha \in K \mid \alpha M \subset M\} = \mathcal{O}$.

The ring $\{\alpha \in K \mid \alpha M \subset M\}$ is called "the ring of coefficients of M", cf. [1].

For definitions, notations, terminology and facts on complex quadratic orders see [1]. Next we will discuss the correspondence between ideal classes of $\mathcal{O}$ and primitive positive definite binary quadratic forms of discriminant $\Delta(\mathcal{O})$.

DEFINITION 2.1. A polynomial $f = aX^2 + bXY + cY^2 \in \mathbb{Z}[X,Y]$ with $b^2 - 4ac = \Delta$ is called a *binary quadratic form* of discriminant Δ. A binary quadratic form $f = aX^2 + bXY + cY^2$ is called *positive definite* if $\Delta < 0$ and $a > 0$, and is called *primitive* if $\gcd(a,b,c) = 1$.

We will often denote a form $aX^2 + bXY + cY^2$ by (a,b,c), or even (a,b) since c is determined by $b^2 - 4ac = \Delta$.

DEFINITION 2.2. Let $f = aX^2 + bXY + cY^2$ and $g = a'X^2 + b'XY + c'Y^2$ be positive definite binary quadratic forms. We shall call f and g *equivalent* if there is a $\sigma = \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} \in SL_2(\mathbb{Z})$ such that

$$a'U^2 + b'UV + c'V^2 = aX^2 + bXY + cY^2;$$

where $U = \alpha X + \gamma Y$ and $V = \beta X + \delta Y$.

Since $SL_2(\mathbb{Z})$ is a group, "equivalence" is indeed an equivalence relation.

THEOREM 2.3. *Let $\mathcal{O}$ be a complex quadratic order with discriminant Δ. There is a 1-1 correspondence between classes of invertible fractional $\mathcal{O}$-ideals and equivalence classes of primitive positive definite binary quadratic forms of discriminant Δ.*

PROOF. Let M be a primitive invertible fractional $\mathcal{O}$-ideal i.e. a non-zero $\mathcal{O}$-submodule of K with its ring of coefficients equal to $\mathcal{O}$, we shall attach a primitive positive definite form f to M.

The fractional ideal M is a free $\mathbb{Z}$-module of rank 2 in K, i.e. a two dimensional lattice in $K \hookrightarrow \mathbb{C}$. We can attach a quadratic form to M in the following way:

Let $\{\alpha,\beta\}$ be an oriented $\mathbb{Z}$-basis for M (i.e. $\mathrm{Im}(\beta/\alpha) > 0$) and take

$$f = \frac{N(\alpha X+\beta Y)}{N(M)} .$$

(Here N denotes the *norm*; for definitions and properties of the norm see [1].)

The choice of the basis $\{\alpha,\beta\}$ does not affect the $SL_2(\mathbb{Z})$ class of f; it can be proved that f is of discriminant Δ, and that f is primitive if M is invertible. However, for future purposes, we prefer to give another

construction of the form f.

Let M denote a fractional $\mathcal{O}$-ideal; the ideal class, represented by M contains the ideals βM, with $\beta \in K^{\times}$, so we can find an $\mathcal{O}$-submodule of K, equivalent to M and of the form $\mathbb{Z} + \mathbb{Z}\alpha$, $\alpha \in K$; This module will be denoted by M again.

We can always choose α in the upper half plane and under this condition α is unique up to $SL_2(\mathbb{Z})$-action.

Next, let's exploit the fact that M is an $\mathcal{O}$-module: assume Δ is even, then $\{1, \frac{1}{2}\sqrt{\Delta}\}$ is a $\mathbb{Z}$-basis for $\mathcal{O}$ and $\frac{1}{2}\sqrt{\Delta} \cdot M \subset M$:

$$\frac{1}{2}\sqrt{\Delta} \in M \to \frac{1}{2}\sqrt{\Delta} = -\frac{1}{2}b + \alpha \cdot a \qquad (-\tfrac{1}{2}b, a \in \mathbb{Z})$$

$$\to \alpha = \frac{b+\sqrt{\Delta}}{2a}$$

with $a > 0$ since α is in the upper half plane;

$$\frac{1}{2}\sqrt{\Delta}\cdot\alpha \in M \to \frac{1}{2}\sqrt{\Delta}\cdot\alpha = c + \alpha \cdot d \qquad (c,d \in \mathbb{Z})$$

which, combined with the fact, that

$$\alpha = \frac{b+\sqrt{\Delta}}{2a},$$

gives us that

$$\frac{\Delta - b^2}{4a} = c \in \mathbb{Z}.$$

We conclude that $M = \mathbb{Z} + \mathbb{Z}\,\frac{b+\sqrt{\Delta}}{2a}$ with $a > 0$ and $c \in \mathbb{Z}$ such that $b^2 - 4ac = \Delta$. If Δ is odd, $\{1, \frac{1}{2}(1+\sqrt{\Delta})\}$ is a $\mathbb{Z}$-basis for $\mathcal{O}$, and a completely analogous proof gives exactly the same result.

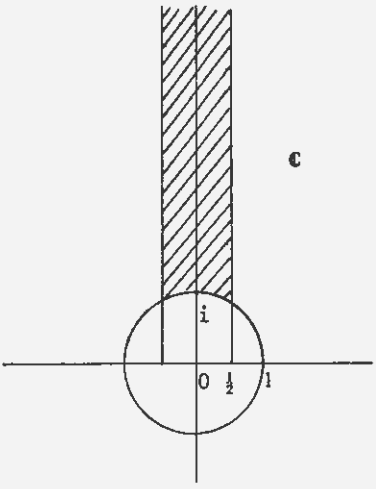
To the ideal class represented by M we associate the positive definite quadratic form $f = aX^2 + bXY + cY^2$. It remains to check that this association respects equivalence and that f is primitive if M is invertible; this is straightforward and left to the reader, see [1]. Next let $f = aX^2 + bXY + cY^2$ be a primitive binary quadratic form of discriminant Δ with $a > 0$. To f we associate the ideal class represented by $M = \mathbb{Z} + \frac{b+\sqrt{\Delta}}{2a}\mathbb{Z}$; since f is primitive, M is invertible and the association is correctly defined with respect to equivalence. This completes the proof of Theorem 2.3. □

Let $\mathcal{O}$ be a complex quadratic order with discriminant Δ, and let k be an $\mathcal{O}$-ideal class; then k consists of fractional ideals $(\mathbb{Z} + b+\sqrt{\Delta}/2a\ \mathbb{Z})\cdot\beta$, $\beta \in K^{\times}$, and to k is associated the quadratic form $aX^2 + bXY + cY^2$. The integers a and b are unique up to $SL_2(\mathbb{Z})$-action on $\mathbb{Z} + b+\sqrt{\Delta}/2a\ \mathbb{Z}$, so it is always possible to choose a and b such, that the number $b+\sqrt{\Delta}/2a$ is in the standard fundamental domain of $SL_2(\mathbb{Z})$, acting on the upper half plane. This choice gives the following conditions on a, b and c:

$$|\frac{b}{2a}| \leq \frac{1}{2} \quad \text{and} \quad |\frac{b+\sqrt{\Delta}}{2a}| \geq 1$$

i.e.

$$|b| \leq a \leq c.$$



DEFINITION. A binary quadratic form $f = aX^2 + bXY + cY^2$ is called *reduced* if $|b| \leq a \leq c$.

It is obvious that Theorem 2.3 can also be stated in the following form:

THEOREM 2.3'. *Let $\mathcal{O}$ be a complex quadratic order of discriminant Δ. The classes of invertible fractional $\mathcal{O}$-ideals are in 1-1 correspondence with the reduced primitive definite binary quadratic form of discriminant Δ.*

CONVENTION. We will always identify reduced forms (a,b,c) and (a,−b,c), whenever $|b| = a$ or $a = c$. These forms correspond to ideal classes represented by $\mathbb{Z} + \mathbb{Z}\cdot\alpha$, with α on the boundary of the fundamental domain.

It is easily seen, that the conditions $b^2 - 4ac = \Delta$ and $|b| \leq a \leq c$ imply that $a \leq \sqrt{|\Delta|/3}$ and this shows that the class group of $\mathcal{O}$ is finite. By means of the dictionary between ideal classes and quadratic forms, the problem of counting the ideal-classes of a given quadratic order is reduced to a finite problem.

Next, we transport the natural group structure of the group of ideal classes to the finite set of reduced binary quadratic forms.

If $f = aX^2 + bXY + cY^2 = (a,b,c)$ is a primitive positive definite form of discriminant Δ, then the ideal class associated to f consists of ideals $M = (\mathbb{Z} + b+\sqrt{\Delta}/2a\ \mathbb{Z})\cdot\alpha$, $\alpha \in K^{\times}$; the number α is a so-called primitive point of M, i.e. for all $n \geq 2$ in $\mathbb{Z}$ we have $\alpha/n \notin M$.

Let (a_1,b_1,c_1) and (a_2,b_2,c_2) be two primitive positive definite quadratic forms of discriminant Δ. Let M and N be two fractional ideals in the ideal classes associated to them:

$$M = (\mathbb{Z} + \frac{b_1+\sqrt{\Delta}}{2a_1}\mathbb{Z})\alpha \quad \text{and} \quad N = (\mathbb{Z} + \frac{b_2+\sqrt{\Delta}}{2a_2}\mathbb{Z})\beta\ .$$

Put

$$MN = (\mathbb{Z} + \frac{b_3+\sqrt{\Delta}}{2a_3}\mathbb{Z})\,\gamma$$

where we choose γ such that $\alpha\beta \in \gamma\mathbb{Z}$, say $\alpha\beta = d\gamma$;

$$(\mathbb{Z} + \frac{b_1+\sqrt{\Delta}}{2a_1}\mathbb{Z})\,(\mathbb{Z} + \frac{b_2+\sqrt{\Delta}}{2a_2}\mathbb{Z})\alpha\beta = (\mathbb{Z} + \frac{b_3+\sqrt{\Delta}}{2a_3}\mathbb{Z})\gamma$$

taking norms on both sides gives (cf. [1]):

$$\frac{N(\alpha\beta)}{a_1\cdot a_2} = \frac{N(\gamma)}{a_3} = \frac{N(\alpha\beta)}{d^2 a_3}\ .$$

So we find

$$(1) \qquad a_3 = \frac{a_1 a_2}{d^2}\ .$$

Multiplying out gives

$$(\mathbb{Z} + \frac{b_1+\sqrt{\Delta}}{2a_1}\mathbb{Z} + \frac{b_1+\sqrt{\Delta}}{2a_2}\mathbb{Z} + \frac{(b_1\cdot b_2+\Delta)+(b_1+b_2)\sqrt{\Delta}}{4a_1a_2})\alpha\beta = (\mathbb{Z} + \frac{b_3+\sqrt{\Delta}}{2a_3}\mathbb{Z})\gamma$$

whence, looking at "$\sqrt{\Delta}$ coefficients":

$$\left(\frac{1}{2a_1}\mathbb{Z} + \frac{1}{2a_2}\mathbb{Z} + \frac{b_1+b_2}{4a_1a_2}\mathbb{Z}\right)\alpha\beta = \frac{1}{2a_3}\mathbb{Z}\frac{\alpha\beta}{d} = \frac{d}{2a_1a_2}\mathbb{Z}\,\alpha\beta$$

$$a_2\mathbb{Z} + a_1\mathbb{Z} + \frac{b_1+b_2}{2}\mathbb{Z} = d\mathbb{Z}.$$

So

$$d = \gcd\left(a_1, a_2, \frac{b_1+b_2}{2}\right) \tag{2}$$

and we can easily compute $v_1, v_2, w \in \mathbb{Z}$ such that

$$v_1a_1 + v_2a_2 + w\,\frac{b_1+b_2}{2} = d.$$

Finally it is easily seen that b_3 can be taken to be

$$b_3 = v_2 \cdot b_1 \cdot \frac{a_2}{d} + v_1 \cdot b_2 \cdot \frac{a_1}{d} + w \cdot \frac{b_1b_2+\Delta}{2d}\,. \tag{3}$$

Formulas (1), (2) and (3) give a form (a_3,b_3,c_3) that corresponds to the ideal class that contains $\mathfrak{M}\mathfrak{N}$.

By Theorem 2.3', these formulas enable us to perform computations in the class group of a complex quadratic order, on condition, that we have a way to compute the *unique* reduced form equivalent to a given form. Fortunately there is a very simple and fast algorithm to do this:

REDUCTION ALGORITHM. Let $f = (a,b,c)$ be a primitive positive definite quadratic form of discriminant Δ.
(i) reduce b (mod $2a$) such that $|b| \le a_3$ and adjust c;
if f is not reduced then
(ii) $f \leftarrow (c,-b,a)$ and start all over.

It is left to the reader to verify that this algorithm terminates and is correct. Perhaps, it is worth noting that $(a,b,c) \leftarrow (c,-b,a)$ corresponds to action of $S = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$ and reducing b (mod $2a$) correspond to action of T^k where $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$ and k is some suitable integer. The group $SL_2(\mathbb{Z})$ is generated by S and T.

EXERCISE. In order to reduce a form (a,b,c) no more than $O(\max(1,\log(|a|/\sqrt{|\Delta|}))$ applications of (i) and (ii) are needed.

Now we can calculate in the class group by means of computations with *reduced* quadratic forms. For completeness we give: the inverse of a reduced form (a,b,c) equals (a,-b,c) and the unit element of the class group corresponds to the form $(1,1,\frac{1-\Delta}{4})$ or $(1,0,-\frac{\Delta}{4})$ depending on whether Δ is odd or even.

In the next section we will give Shanks' algorithm to compute class groups of quadratic orders. One of the basic ingredients of the algorithm is the ability to do calculations in the class group itself in an *efficient* way. The formulas given above are sufficiently efficient for these purposes.

Perhaps it is worth quoting the following formulas, which are essentially the formulas (1), (2) and (3), but somewhat more suitable for computation [31]:

Let $f = (a_1,b_1,c_1)$, $g = (a_2,b_2,c_2)$ be two primitive positive definite binary quadratic forms of discriminant Δ. Put $d = \gcd(a_1,a_2,(b_1+b_2)/2)$ and let $v_1,v_2,w \in \mathbb{Z}$ such that $v_1a_1 + v_2a_2 + w(b_1+b_2)/2 = d$. Let

$$a_3 = \frac{a_1a_2}{d^2},$$

$$b_3 = b_2 + 2\frac{a_2}{d}\overbrace{(\frac{b_1-b_2}{2}v_2 - c_2v)}^{(*)};$$

the form (a_3,b_3,c_3) now needs reduction. The term (*) does only matter mod a_1/d.

The algorithm for composition and reduction of binary quadratic forms can easily be programmed on a pocket calculator, like TI58, TI59, HP67, HP41C. In fact it is possible to compute class groups of complex quadratic orders, with the aid of a calculator like that, if the discriminant of the order is not too large, say, $\leq$ 10 decimal digits.

3. SHANKS' ALGORITHM

Let K be a finite abelian extension of $\mathbb{Q}$, then the following formula, the class number formula holds [17]:

$$(4) \qquad h = \frac{w\sqrt{|\Delta|}}{2^{r_1}(2\pi)^{r_2}R} \prod_{\chi\neq 1} L(1,\chi)$$

where

$w = w(K) = \#\mu(K)$ = the number of roots of unity in K,

$\Delta = \Delta(K)$ = the discriminant of K,

$r_1 = r_1(K)$ = the number of embeddings $K \hookrightarrow \mathbb{R}$,

$r_2 = r_2(K)$ = half the number of embeddings $K \hookrightarrow \mathbb{C}$ ($\mathrm{im}(K) \not\subset \mathbb{R}$),

$R = R(K)$ = the regulator of K,

χ runs over the non-trivial characters of $\mathrm{Gal}(K/\mathbb{Q})$,

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_{p \text{ prime}} (1 - \chi(p)p^{-s})^{-1}, \quad s \in \mathbb{C}, \ \mathrm{Re}\ s \geq 1.$$

Any complex quadratic field K is abelian over $\mathbb{Q}$ and the only non-trivial character of $\mathrm{Gal}(K/\mathbb{Q})$ is the Legendre-symbol $(\frac{\Delta}{\cdot})$, where Δ is the discriminant of K. The class number formula reduces to

$$h = \frac{w(\mathcal{O})}{2\pi} \sqrt{|\Delta|}\, L(1,\chi),$$

and this formula also holds for non-maximal orders [1]. Here $w(\mathcal{O})$ denotes the number of roots of unity contained in $\mathcal{O}$. If $\Delta = -3$ or $\Delta = -4$, the class number of the order of discriminant Δ equals 1, so there is no harm in assuming that $\Delta \neq -3,-4$. Then always $w = 2$ and the class number of formula reduces further to

$$(5) \qquad h = \frac{\sqrt{|\Delta|}}{\pi} L(1,\chi) = \frac{\sqrt{|\Delta|}}{\pi} \prod_{p \text{ prime}} (1 - (\tfrac{\Delta}{p})\tfrac{1}{p})^{-1}.$$

The infinite product (5) converges slowly to h. An analysis on assumption of the Generalized Riemann Hypothesis (GRH in the sequel) for this field, shows that only an expansion of this product that uses all primes $\leq c \cdot |\Delta|^{1+\varepsilon}$ for some universal c and ε, gives an approximation of h, accurate enough to determine h.

There are also explicit "finite" formulas for the class number of complex quadratic orders $\mathcal{O}$ with discriminant Δ; for maximal orders it holds that

$$h = \frac{1}{2-\chi(2)} \sum_{\substack{0<x<|\Delta/2| \\ (x,\Delta)=1}} \chi(x), \qquad (\Delta \neq -3,-4)$$

here χ denotes the Legendre symbol $(\frac{\Delta}{\cdot})$, see [1]. However, calculation of the class number of a quadratic order with a discriminant of say 10 decimal digits, using this formula, would be hardly possible.

Using the 1-1 correspondence between $\mathcal{O}$-ideal classes and reduced primitive forms of discriminant $\Delta = \Delta(\mathcal{O})$, one can also determine the class number of $\mathcal{O}$ by counting integral triples (a,b,c) with gcd(a,b,c) = 1, $a > 0$, $b^2 - 4ac = \Delta$ and $|b| \le a \le c$.

EXAMPLE. $\Delta = 691$.
(Recall that if (a,b,c) is reduced, $|b| \le a < \sqrt{\frac{|\Delta|}{3}}$ and realize that for any form $b \equiv \Delta \pmod 2$).

$\pm b$	$\frac{-\Delta+b^2}{4}$	forms
15	229	
13	5·43	
11	7·29	
9	193	
7	5·37	
5	179	
3	$5^2 \cdot 7$	(7,±3,25), (5,±3,35)
1	173	(1,1,173)

So the class number of $\mathbb{Q}(\sqrt{-691})$ is 5. But this method is only efficient for small discriminants.

Counting methods of this sort are very useful to compute tables of class numbers; one then computes forms (a,b,c) with $|b| \le a \le c$, $a > 0$ and counts them, sorting them on discriminant $\Delta = b^2 - 4ac$. This is a very fast method and D.A. BUELL [3] used it, to compile a table of class numbers of complex quadratic number fields with discriminants Δ with $0 < -\Delta < 4000000$.

In 1970, Shanks introduced his algorithm to determine the structure of class groups of complex quadratic orders [31]. His algorithm relies upon an estimate of the class number of the order and computations in the class group itself; it is particularly effective if the discriminant of the order is very large.

Let $\mathcal{O}$ be a complex quadratic order of discriminant Δ, and let h be the class number of $\mathcal{O}$. The starting point in Shanks' algorithm is an approximation of the class number; this is obtained by means of the class number formula

$$(5) \qquad h = \frac{\sqrt{|\Delta|}}{\pi} L(1,\chi) = \frac{\sqrt{|\Delta|}}{\pi} \prod_{p \text{ prime}} (1 - (\tfrac{\Delta}{p})\tfrac{1}{p})^{-1}.$$

We approximate h, by simply evaluating

$$\tilde{h} = \frac{\sqrt{|\Delta|}}{\pi} \prod_{\substack{p \text{ prime} \\ p \le X}} (1 - (\tfrac{\Delta}{p})\tfrac{1}{p})^{-1}$$

for some X (which we will take $O(|\Delta|^{\frac{1}{5}})$; we'll say more on choices of particular constants later). Due to convergence of the product (5), we have that

$$(6) \qquad (1-\varepsilon)\tilde{h} < h < (1+\varepsilon)\tilde{h},$$

where ε is a *small* positive number depending on X. This gives us a rough idea of the size of h. Next we choose a form $f = (a,b,c)$ of discriminant Δ (for instance by taking $a = p$, a prime with $(\frac{\Delta}{p}) = +1$, and $b^2 \equiv \Delta \pmod{4a}$). By group theory, we have that $f^h = 1$ and we use this fact together with the estimate $h \approx \tilde{h}$, to find h by searching in the (relatively short!) interval

$$(7) \qquad ((1-\varepsilon)\tilde{h}, (1+\varepsilon)\tilde{h})$$

for a number h' such that $f^{h'} = 1$. Perhaps $h' = h$, but this need not be the case. Next we compute the precise order of f, by factoring h', which has size $O(|\Delta|^{\frac{1}{2}+\varepsilon})$ and we put H = the cyclic group generated by f; we keep H by means of a list of (independent) generators of its p-Sylow subgroup. If $(1-\varepsilon)\tilde{h} \le \#H \le (1+\varepsilon)h$ we conclude that $H = C\ell(0)$; if not, we pick a new form f' and compute its order in the same way, now using that $\#H | \#C\ell(0)$ and compute the group generated by H and f', by computing a set of independent generators for its Sylow-subgroup; we call this group H again.
We repeat this procedure until $(1-\varepsilon)\tilde{h} < \#H < (1+\varepsilon)\tilde{h}$ and then we conclude that $H = C\ell(0)$.

A few remarks on this algorithm:
- The search for a number h' in the interval (7), such that $f^{h'} = 1$ can be performed effectively, by means of the so-called "baby-giant-step strategy":

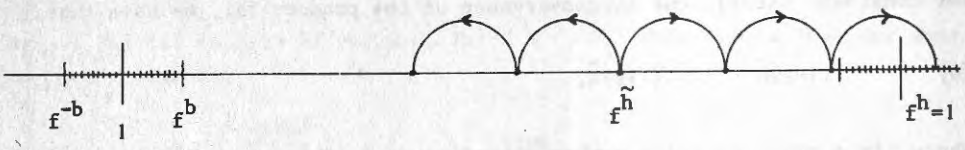
Let $\ell = 2\varepsilon\tilde{h}$ be the length of the interval (7), then compute $f^{\tilde{h}}$ and search successively for $f^{\tilde{h}}, f^{\tilde{h}}g^{\pm 1}, f^{\tilde{h}}g^{\pm 2}, \ldots$, etc. (the giant steps) in the list of baby-steps. If one finds

$$f^{\tilde{h}} g^{i} = f^{a}$$

with $|a| \leq b$, for some i,

$$f^{\tilde{h}+2ib-a} = 1$$

and $h' = \tilde{h} + 2ib - a$.



The number of calculations needed to perform this strategy is proportional to $\sqrt{\ell}$.

- Determining the precise order of f, knowing that $f^{h'} = 1$, is done by factoring h' ($\sim \sqrt{|\Delta|}$) and by computing suitable powers of f; it is a relatively fast procedure.
- It is possible that many forms are needed to generate the whole class group, but usually, the time consuming baby-giant-step strategy need only be performed once: usually one of the first forms picked generates a large part of the class group; its order n is often divisible by some large primes q such that $q \mid n \mid h$, since no multiple of qn is in the interval

$$((1-\varepsilon)\tilde{h},\ (1+\varepsilon)\tilde{h}).$$

This implies that the q-Sylow subgroups of the group generated by this form equal the q-Sylow subgroups of $Cl(\mathcal{O})$.

After encountering a form like that, we can raise new forms f to the power m, being the part of n consisting of these large primes q; then we know that f^m has a multiple of its order in the interval

$$((1-\varepsilon)\frac{\tilde{h}}{m},\ (1+\varepsilon)\frac{\tilde{h}}{m})$$

which is a very short interval. Usually we need not perform the baby-giant-step strategy and we can avoid computations in the q-Sylow subgroups for the large primes q.

- We will sketch a derivation, under GRH, of the order of the algorithm. For the details we refer to Section 6, where an analysis of the factorization algorithm that is based on Shanks' algorithm is given.

Put

$$\tilde{h} = \tilde{h}(X) = \frac{\sqrt{|\Delta|}}{\pi} \prod_{\substack{p \text{ prime} \\ p \le X}} (1 - (\tfrac{\Delta}{p})\tfrac{1}{p})^{-1}$$

then for some effectively computable, universal constant C and for all X large enough:

$$\left|\frac{\tilde{h}(X)}{h} - 1\right| \le C \frac{\log|\Delta X|}{\sqrt{X}}$$

(cf. Section 6).

If we take $X \approx |\Delta|^{\alpha}$ for some α, to be determined, we have that

$$\left|\frac{\tilde{h}(|\Delta|^{\alpha})}{h} - 1\right| = O(|\Delta|^{-\frac{1}{2}\alpha+\varepsilon}), \tag{8}$$

where the O constant depends on ε.

The length of the interval (7) equals

$$\ell \approx |\Delta|^{\frac{1}{2}+\varepsilon} \cdot |\Delta|^{-\frac{1}{2}\alpha+\varepsilon} = |\Delta|^{\frac{1}{2}-\frac{1}{2}\alpha+\varepsilon},$$

where we used that $h(\mathcal{O}(\Delta)) = O(|\Delta|^{1/2+\varepsilon})$. [37]. Since evaluating Legendre symbols is logarithmic in the arguments, we have, by the prime number theorem, that the time for evaluating a truncated product

$$\frac{\sqrt{|\Delta|}}{\pi} \prod_{\substack{p \text{ prime} \\ p \le X}} (1 - (\tfrac{\Delta}{p})\tfrac{1}{p})^{-1},$$

is $O(X^{1+\varepsilon})$, if we take $X \approx |\Delta|^{\alpha}$. So

$$\text{"time for approximating h"} \sim |\Delta|^{\alpha} \tag{9}$$

The time needed to perform the baby-giant strategy is proportional to $\sqrt{\ell}$, so

$$\text{"baby-giant costs"} \sim |\Delta|^{\frac{1}{4}-\frac{1}{4}\alpha+\varepsilon}.$$

We will have an optimum if

$$\frac{1}{4} - \frac{1}{4}\alpha = \alpha \qquad \text{i.e. } \alpha = \frac{1}{5}.$$

This indicates that Shanks' algorithm has order $|\Delta|^{1/5+\varepsilon}$; however, there are some details:

- Many primes may be needed to generate the whole class group. However, it easily follows from results of LAGARIAS, MONTGOMERY and ODLYZKO [15], obtained under assumption of GRH, that the class group is generated by the classes of the primes with norm $\ll \log^2|\Delta|$, cf. Section 6.
- The computations necessary to compute a presentation of the class group by independent generators, may become time consuming if the structure of the class group is complicated i.e. "highly non-cyclic". At present we cannot estimate the computing time for these calculations better than $|\Delta|^{1/4+\varepsilon}$, but since "almost all" class groups appear to have a large cyclic factor (cf. Section 7), $|\Delta|^{1/5+\varepsilon}$ seems to be a more practical estimate. For bounds on the exponent of class groups see [2,41]. However, computing *the class number* can always be done in time $O(|\Delta|^{1/5+\varepsilon})$. Also determining the isomorphy type of $Cl(\mathcal{O})$ as an abelian group can be done in time $O(|\Delta|^{1/5+\varepsilon})$, without, however, giving a set of independent generators.

4. CLASS GROUPS AND UNITS OF REAL QUADRATIC NUMBER FIELDS

If K is a real quadratic number field, let $\mathcal{O}(K)$ denote its ring of integers and $\Delta(K)$ its discriminant. Real quadratic fields are characterized by their discriminants, which are positive integers congruent to 0 or 1 (mod 4), but, like in the complex case, not every positive integer $\equiv 0$ or 1 (mod 4), is the discriminant of a real quadratic field.

However, every *non-square* positive integer $\Delta \equiv 0$ or 1 (mod 4) is the discriminant of a unique *real quadratic order* $\mathcal{O}$, a subring of a ring of integers of a real quadratic field: Δ can uniquely be written as $\Delta = f^2 D$ where $f \in \mathbb{Z}_{\geq 1}$ and D is the discriminant of a real quadratic field K; then Δ is the discriminant of the unique subring $\mathcal{O}$ of index f in $\mathcal{O}(K)$.

The class group of a real quadratic order $\mathcal{O}$ is defined as the group of invertible fractional $\mathcal{O}$-ideals modulo the principal fractional $\mathcal{O}$-ideals.

If $\Delta = f^2$ is a square, we can consider Δ to be the discriminant of the subring $\mathbb{Z}(1,1) \times \mathbb{Z}(0,f)$ of index f in $\mathbb{Z} \times \mathbb{Z}$; the class group of this ring is isomorphic to $(\mathbb{Z}/f\mathbb{Z})^\times/\{\pm 1\}$. We do not enter into these rather pathological cases. For the "imtermediate case" $\Delta = 0$ see GAUSS [12].

Let $\mathcal{O}$ be a real quadratic order, then

$$\mathcal{O}^\times \simeq \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z};$$

more precisely: there exists an $\varepsilon \in \mathcal{O}^\times$ such that every unit $u \in \mathcal{O}^\times$ can be written as $\pm\varepsilon^k$, $k \in \mathbb{Z}$. There are four numbers in $\mathcal{O}^\times$, that each, together with -1, generate $\mathcal{O}^\times$; fixing an embedding $K \hookrightarrow \mathbb{R}$, one of these numbers is greater than 1. We denote this number by ε_0 and call it *the fundamental unit of* $\mathcal{O}$.

DEFINITION If ε_0 is the fundamental unit of $\mathcal{O}$ then

$$R(\mathcal{O}) = \log \varepsilon_0$$

is called *the regulator of* $\mathcal{O}$.

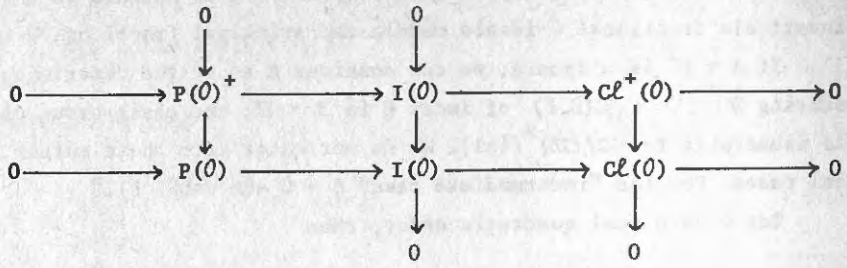
If no confusion is likely, we will omit the indices $\mathcal{O}$. Let K be a real quadratic field with discriminant Δ.

DEFINITION. $N: K^\times \to \mathbb{Q}^\times$ by $N\alpha = \alpha \cdot \sigma(\alpha)$ where $1 \neq \sigma \in \mathrm{Gal}(K/\mathbb{Q})$. We call N *the norm map*; it is a homomorphism and if we write $\alpha \in K^\times$, $\alpha = p+q\sqrt{\Delta}$ then

$$N\alpha = p^2 - \Delta q^2.$$

By means of the norm map we can refine the concept of the class group somewhat:

DEFINITION. Let $\mathcal{O}$ be a real quadratic order and let $P(\mathcal{O})^+ = \{$principal ideals generated by elements of positive norm$\}$. We have the following commutative diagram with exact rows and columns:



$Cl^+(O)$ is called *the narrow class group of* O; it maps surjectively to $Cl(O)$ and it is easy to see, that the kernel of this map has order 1 or 2. By h^+ we denote the order of $Cl^+(O)$: $h^+ = h$ or $h^+ = 2h$.

DEFINITION. $\varepsilon^+ := \varepsilon$ if $N\varepsilon = +1$ and $\varepsilon^+ := \varepsilon^2$ if $N\varepsilon = -1$; $R^+ := \log \varepsilon^+$.

Now the units with positive norm are precisely the numbers $\pm(\varepsilon^+)^k$, $k \in \mathbb{Z}$.

PROPOSITION 4.1.

(i) *if* $N\varepsilon = -1$ *then* $h^+ = h$ *and* $R^+ = 2R$,
if $N\varepsilon = +1$ *then* $h^+ = 2h$ *and* $R^+ = R$;

(ii) $2hR = h^+R^+$.

PROOF. □

Next we'll explain the setting, in which the calculation of the class group and the regulator, as discussed in the next section, are performed. The ideas involved are due to LENSTRA and SHANKS [18,33].

DEFINITION. Let O be a real quadratic order; put

$$F'(O) = \{(M,\alpha) \mid M \text{ an invertible } O\text{-submodule of } K;\ \alpha \in M \text{ primitive}\}$$

$$G'(O) = \{(\beta O,\alpha) \mid \beta \in K^\times,\ N\beta > 0;\ \alpha \in \beta O \text{ primitive}\}$$

$$K^\times_{N>0} = \{\alpha \in K \mid N\alpha > 0\}.$$

We turn $F'(O)$ into an abelian group, by defining

$$(M,\alpha)(N,\beta) = (MN,\gamma),$$

where $\alpha\beta = d\gamma$, with $d \in \mathbb{Z}_{\geq 1}$ and $\gamma \in MN$ primitive. We then have the series of subgroups

$$K^{\times}_{N>0} \subset G'(\mathcal{O}) \subset F'(\mathcal{O}).$$

Here $K^{\times}_{N>0} \hookrightarrow G'(\mathcal{O})$ by $\alpha \to (\alpha\mathcal{O}, \alpha)$.

DEFINITION.

$$F(\mathcal{O}) = F'(\mathcal{O})/K^{\times}_{N>0},$$

$$G(\mathcal{O}) = G'(\mathcal{O})/K^{\times}_{N>0}.$$

PROPOSITION 4.2. *There is an exact sequence*

$$0 \to G(\mathcal{O}) \to F(\mathcal{O}) \to Cl^{+}(\mathcal{O}) \to 0.$$

PROOF. Define $F'(\mathcal{O}) \to Cl^{+}(\mathcal{O})$ by $(M,\alpha) \to$ class of M; the kernel of this map is precisely $G'(\mathcal{O})$. □

In terms of binary quadratic forms we have that

$$F(\mathcal{O}) = \left\{\begin{matrix}\text{primitive binary quadratic forms} \\ \text{of discriminant } \Delta = \Delta(\mathcal{O})\end{matrix}\right\} \Big/ \begin{pmatrix} 1 & \mathbb{Z} \\ 0 & 1 \end{pmatrix},$$

$$G(\mathcal{O}) = \left\{\begin{matrix}\text{primitive binary quadratic forms of discriminant} \\ \Delta = \Delta(\mathcal{O}) \text{ that are } SL_2(\mathbb{Z})\text{-equivalent to} \\ X^2 + \Delta XY + (\Delta^2 - \Delta)/4\, Y^2\end{matrix}\right\} \Big/ \begin{pmatrix} 1 & \mathbb{Z} \\ 0 & 1 \end{pmatrix}.$$

(For definitions and facts on quadratic forms see [1], or Section 2.) A translation between the different descriptions of $F(\mathcal{O})$ and $G(\mathcal{O})$ can be given as follows:

Let Δ be the discriminant of $\mathcal{O}$ and suppose $(M,\alpha) \in F'(\mathcal{O})$; let

$$M = \left(\mathbb{Z} + \frac{b+\sqrt{\Delta}}{2a}\,\mathbb{Z}\right)\alpha$$

with $\operatorname{sgn} a = \operatorname{sgn} N\alpha$. The image of (M,α) in $F(\mathcal{O})$ corresponds to the $\begin{pmatrix} 1 & \mathbb{Z} \\ 0 & 1 \end{pmatrix}$-orbit of $aX^2 + bXY + cY^2$ with $b^2 - 4ac = \Delta$. So we can look at $F(\mathcal{O})$ as consisting

of binary quadratic forms (a,b,c) where we identify forms (a_1,b_1,c_1) and (a_2,b_2,c_2) whenever $a_1 = a_2$ and $b_1 \equiv b_2 \pmod{2a_1}$.

$G(\mathcal{O})$ consists of $\begin{pmatrix} 1 & \mathbb{Z} \\ 0 & 1 \end{pmatrix}$-orbits of quadratic forms that are $SL_2(\mathbb{Z})$-equivalent to those corresponding to the image of $(0,1)$ in $G(\mathcal{O})$; these are precisely the $\begin{pmatrix} 1 & \mathbb{Z} \\ 0 & 1 \end{pmatrix}$- orbits of form that are $SL_2(\mathbb{Z})$-equivalent to $X^2 + \Delta XY + (\Delta^2-\Delta/4)Y^2$.

DEFINITION. Let $\alpha \in K$ and let $i_1: K \to \mathbb{R}$ be a fixed embedding and $i_2: K \to \mathbb{R}$ the other one; then

$$|\alpha|_{\infty 1} := |i_1(\alpha)| \quad \text{and} \quad |\alpha|_{\infty 2} := |i_2(\alpha)|.$$

We define a map, the *distance map*,

$$D: G(\mathcal{O}) \to \mathbb{R}/R^+\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z},$$

by

$$D((\beta\mathcal{O},\alpha)K^{\times}_{N>0}) = (\tfrac{1}{2}\log(|\tfrac{\alpha}{\beta}|_{\infty 1}/|\tfrac{\alpha}{\beta}|_{\infty 2}), \operatorname{sgn} N\alpha).$$

Here we use the isomorphism of groups: $\{+1,-1\} \cong \mathbb{Z}/2\mathbb{Z}$.

PROPOSITION 4.3. *D is a well defined homomorphism and* D *is injective.*

PROOF. It is trivial to check, that the value of D on $(\beta\mathcal{O},\alpha)$ and on $\xi\cdot(\beta\mathcal{O},\alpha) = (\xi\beta\mathcal{O}, \frac{\xi\alpha}{d})$, $(d \in \mathbb{Z}_{\geq 1},\ N\xi > 0)$ is the same. If $(\beta\mathcal{O},\alpha) = (\beta'\mathcal{O},\alpha)$ in $G(\mathcal{O})$, we have that β and β' differ by a norm positive unit, say, that $\beta' = \pm(\epsilon^+)^k\cdot\beta$, for some $k \in \mathbb{Z}$. Then

$$d(\beta'\mathcal{O},\alpha) = \left(\tfrac{1}{2}\log\left(\left|\frac{\alpha}{(\epsilon^+)^k\beta}\right|_{\infty 1}\Big/\left|\frac{\alpha}{(\epsilon^+)^k\beta}\right|_{\infty 2}\right), \operatorname{sgn} N\alpha\right)$$

$$= (\tfrac{1}{2}\log(|\tfrac{\alpha}{\beta}|_{\infty 1}/|\tfrac{\alpha}{\beta}|_{\infty 2}) - kR^+, \operatorname{sgn} N\alpha)$$

$$= d(\beta\mathcal{O},\alpha),$$

and we see that D is well defined. To prove injectivity, let $(\beta\mathcal{O},\alpha) \in G(\mathcal{O})$, with

$$d(\beta\mathcal{O},\alpha) = (\tfrac{1}{2}\log(|\tfrac{\alpha}{\beta}|_{\infty 1}/|\tfrac{\alpha}{\beta}|_{\infty 2}),\ \operatorname{sgn} N\alpha) = (0,0).$$

This implies

$$|\tfrac{\alpha}{\beta}|_{\infty 1} = |\tfrac{\alpha}{\beta}|_{\infty 2} \quad \text{and} \quad N\alpha > 0.$$

So $\frac{\alpha}{\beta} \in \mathbb{Q}$ or $\frac{\alpha}{\beta} \in \mathbb{Q}\cdot\sqrt{\Delta}$, whence, since $N\alpha, N\beta > 0$, it follows that $\frac{\alpha}{\beta} \in \mathbb{Q}$ and so, since $\alpha \in \beta\mathcal{O}$ primitive, we have that $\alpha = \pm\beta$ and we find that

$$(\beta\mathcal{O},\alpha) = (\mathcal{O},1) \bmod K^{\times}_{N>0}. \qquad \square$$

NB. The image of D is dense in $\mathbb{R}/R^{+}\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$; however for cardinality reasons, D is not surjective.

DEFINITION 4.4. Let ϕ_1, ϕ_2 be two elements of $F(\mathcal{O})$, that are in the same $G(\mathcal{O})$-coset. We define the *distance from* ϕ_1 *to* ϕ_2 to be the first coordinate of $D(\phi_2\phi_1^{-1})$.

So distances between elements of F, that are in different $G(\mathcal{O})$-cosets, *are not defined*. However, it is possible to define a notion of *absolute* distance, as follows: It is possible to lift the map

$$(\beta\mathcal{O},\alpha) \to \operatorname{sgn} N\alpha,$$

to the whole of $F(\mathcal{O})$ in a *canonical* way:

$$(M,\alpha) \to \operatorname{sgn} N\alpha.$$

Since $\mathbb{R}/R^{+}\mathbb{Z}$ is a divisible group, one can lift

$$(\beta\mathcal{O},\alpha) \to \tfrac{1}{2}\log(|\tfrac{\beta}{\alpha}|_{\infty 1}/|\tfrac{\beta}{\alpha}|_{\infty 2}),$$

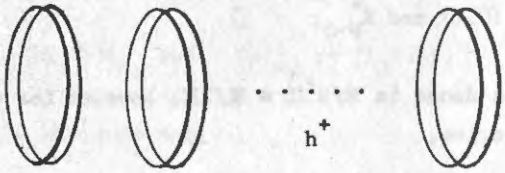
to the whole of F(O) as well (*uncanonically* this time). Combining these maps one finds a lift of D to the whole of F(O):

$$\begin{array}{ccccccccc} & & & & 0 & & & & \\ & & & & \downarrow & & & & \\ 0 & \longrightarrow & G(\mathcal{O}) & \longrightarrow & F(\mathcal{O}) & \longrightarrow & Cl^{+}(\mathcal{O}) & \longrightarrow & 0. \\ & & & & \downarrow D & \swarrow D & & & \\ & & & & \mathbb{R}/R^{+}\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z} & & & & \end{array}$$

We will denote this lift by D again, and if $(M,\alpha) \in F(O)$, we will call $D(M,\alpha)$ the *absolute distance* of (M,α). Note, that the absolute distance depends upon the lift of D: $G(O) \to \mathbb{R}/R^+\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ to $F(O)$.

The class group $Cl^+(O)$ can now be viewed as a set of h^+ double circles, each of "circumference" R^+, each point of the image of D on a double circle representing a $\left(\begin{smallmatrix}1 & \mathbb{Z}\\ 0 & 1\end{smallmatrix}\right)$-orbit, or $\mathbb{Z}$-orbit for short, of a quadratic form. We will call these $\left(\begin{smallmatrix}1 & \mathbb{Z}\\ 0 & 1\end{smallmatrix}\right)$-orbits forms again.

$Cl^+(O)$:



We will call the ideal classes, pictured as these double circles, also *cycles*.

The double circle, corresponding to the principal ideal class, will be called the *principal cycle*. On the principal cycle, there is always a form $(1,\Delta,\Delta^2-\Delta/4)$ (a $\mathbb{Z}$-orbit!), which we will call the principal form.

Two forms on a double circle that are at the same absolute distance, but on different circles, differ by the sign of a: One circle contains forms (a,b,c) with $a > 0$, the other one contains forms (a,b,c) with $a < 0$.

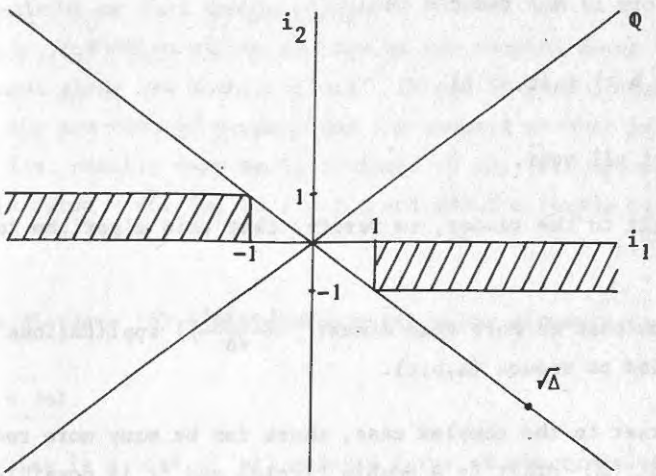
Like in the complex case, it is possible to translate the composition law in terms of quadratic forms (or rather $\mathbb{Z}$-orbits of forms); this yields the same formulas as the formulas (1), (2) and (3) given in Section 2.

The notion of a reduced form is slightly different however:

DEFINITION. Let $f = (a,b,c)$ be a primitive binary quadratic form of discriminant Δ; then f is called *reduced* if

$$|\sqrt{\Delta} - |2a|| < b < \sqrt{\Delta}$$

i.e. if we picture K as embedded in $\mathbb{R} \times \mathbb{R}$ via its embeddings $i_1, i_2 : K \to \mathbb{R}$ via $x \to (i_1(x), i_2(x))$, the point $b+\sqrt{\Delta}/a$ is in the shaded area.



The condition for a form (a,b,c) to be reduced implies that

$$0 < b < \sqrt{\Delta} \quad \text{and} \quad |a| < \sqrt{\Delta};$$

from this it follows easily, that only finitely many reduced forms of discriminant Δ exist; the $\mathbb{Z}$-orbits of these forms form a discrete subset of $F(\mathcal{O})$ and every ideal class (= double circle) contains at least one reduced form.

In view of the applications to the algorithm discussed in Section 5, we like to do our calculations in the *finite* set of reduced forms: We need a *reduction algorithm*, in order to determine a reduced form equivalent to a given form.

Reduction algorithm. Let (a,b,c) be a quadratic form of discriminant Δ:
(i) if $|a| < \sqrt{\Delta}$ reduce b (mod 2a) such that

$$\sqrt{\Delta} - |2a| < b < \sqrt{\Delta}$$

and adjust c;
if $|a| > \sqrt{\Delta}$ reduce b (mod 2a) such that

$$|b| \leq |a|$$

and adjust c;

(ii) if the form is *not* reduced then

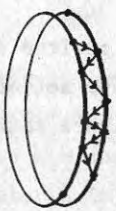
$$(a,b,c) \leftarrow (c,-b,a)$$

and start all over.

It is left to the reader, to verify, that this algorithm terminates and is correct.

EXERCISE: Show that no more than $O(\max(1, \frac{\log|a|}{\sqrt{\Delta}}))$ applications of (i) and (ii) are needed to reduce (a,b,c).

In contrast to the complex case, there can be many more reduced forms in the same $SL_2(\mathbb{Z})$-orbit (= a double circle) and it is possible to jump from one form to another by means of *reduction*: If f is a reduced form in a fixed coset of $G(0)$, say $f = (a,b,c)$, then let $g = (c,b',c')$ with $b' \equiv -b \pmod{2c}$ and $\sqrt{\Delta} - |2c| < b' < \sqrt{\Delta}$ and c' such that $b'^2 - 4cc' = \Delta$. Then g is also reduced and g is on the opposite circle since $ac < 0$ (this follows directly from the fact, that f is reduced). Furthermore, if f is a reduced form on some double-circle, then one finds *all other* reduced forms on this double circle by successive reduction [12].



The distance from the reduced form f, to its successor g equals

$$(11) \qquad \frac{1}{2} \log\left(\frac{\sqrt{\Delta}+b}{\sqrt{\Delta}-b}\right).$$

Now we can compute in the set of reduced forms: we can "jump" from one form to the "next" one on the same double-circle, and we can compute the product of two reduced forms: a not necessarily reduced form, which we can reduce

by means of the reduction algorithm. In doing this, we can keep track of the absolute distance of the product. The ultimate reduction gives a form which is one the same double circle as the non-reduced product, but in general at a different position on that double circle.

Fortunately, reduction of the product of two reduced forms "causes only small replacement along the double circle". It can be shown, that the distance between the non-reduced product and the reduced product is at most $\frac{1}{4}\log \Delta + O(1)$, i.e. usually very small compared to the circumference of the cycle, which is often $\sim \sqrt{\Delta}$. So, if f and g are reduced forms, the following "holds".

$$\text{abs.distance}(f) + \text{abs.distance}(g) \approx \text{abs.distance}(\text{reduced}(f \cdot g)).$$

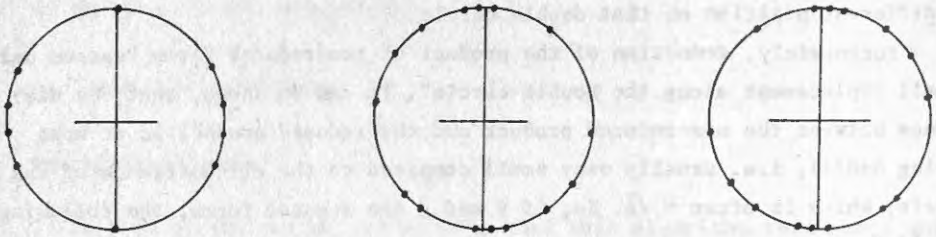
An example: $\Delta = 761$.

The following is a list of all reduced forms of discriminant Δ:

(1,27, -8): 0.0 .	(2,27, -4): 1.704.	(2,25,-17): 13.052.
(-8,21, 10): 2.267.	(-4,21, 20): 3.971.	(-17, 9, 10): 14.558.
(10,19,-10): 3.266.	(20,19, -5): 4.970.	(10,11,-16): 0.141.
(-10,21, 8): 4.112.	(-5,21, 16): 5.815.	(-16,21, 5): 0.563.
(8,27, -1): 5.111.	(16,11,-10): 6.814.	(5,19,-20): 1.562.
(-1,27, 8): 7.378.	(-10, 9, 17): 7.237.	(-20,21, 4): 2.408.
(8,21,-10): 9.645.	(17,25, -2): 7.757.	(4,27, -2): 3.407.
(-10,19, 10): 10.644.	(-2,27, 4): 9.081.	(-2,25, 17): 5.674.
(10,21, -8): 11.489.	(4,21,-20): 11.348.	(17, 9,-10): 7.180.
(-8,27, 1): 12.489.	(-20,19, 5): 12.347.	(-10,11, 16): 7.519.
(1,27, -8): 14.756.	(5,21,-16): 13.193.	(16,21, -5): 7.941.
	(-16,11, 10): 14.192.	(-5,19, 20): 8.940.
	(10, 9,-17): 14.614.	(20,21, -4): 9.786.
	(-17,25, 2): 0.197.	(-4,27, 2): 10.785.
	(2,27, -4): 1.704.	(2,25,-17): 13.052.

The first column lists all reduced forms in the principal cycle with their (approximate) absolute distance, the next two columns list the reduced forms in the cycles, that represent the two other ideal classes: the class number equals 3. The real numbers, given there, are the absolute distances of these forms (depending on the lift of D...).

We can picture the class group as a set of cycles:



Since $(-1,27,8)$ is in the principal cycle, the norm of the fundamental unit is -1. In fact

$$\varepsilon = 800 + 29\sqrt{761}$$

and

$$\varepsilon^{+} = 1280001 + 46400\sqrt{761}.$$

The reader is invited to check the values, given for the absolute distance, by means of composition and reduction.

The example shows, that it is possible to have a different number of forms in the circles; however, the "circumference" is the same for every circle.

Finally, some remarks:

- In the principal cycle there is a reduced form at distance exactly $\frac{1}{2}R^{+}$; if this is the $\mathbb{Z}$-orbit of $(-1,\Delta,\Delta^2-\Delta/4)$, we have that $(0,\varepsilon_0)$ and $(0,1)$ are equal mod $G(0)$ i.e. $N\varepsilon_0 = -1$; if not, we must have, that $N\varepsilon_0 = 1$. So, by computing in the principal cycle, we can find out, whether $N\varepsilon = +1$ or -1.
- In Section 2 we described a method, to compile tables of class numbers of *complex* quadratic orders by means of counting reduced forms. We cannot apply this method straightaway to real quadratic orders; but still an analogous method is possible. One computes positive binary quadratic forms (a,b,c) and counts them, sorting them on $\Delta = b^2 - 4ac$; however, one does not simply count the forms, but one sums their distances to their successors in their double circles i.e.

$$\frac{1}{2}\log\left(\frac{\sqrt{\Delta}+b}{\sqrt{\Delta}-b}\right).$$

Once this is done, one knows the complete "length" of the class group; after computing R^+ for each Δ, by means of successive reduction of $(1,\Delta,\Delta^2-\Delta/4)$, one divides the length of the class group by R^+; this gives h^+; the norm of the fundamental unit is found as a by-product of the computation of R^+.
- Due to the formulas for composition and reduction we can efficiently calculate in $Cl(\mathcal{O})$. However, some problems remain hard, it seems. For instance, suppose that one knows, that for a given order $\mathcal{O}$ the class number h^+ equals one, and suppose $(\Delta(\mathcal{O})/2) = +1$; then there must be a form (2,B,C) (some B, C) in the principal cycle. Where to find it? Apart from a rigorous search in the principal cycle, (for instance, by means of a baby-giant-step strategy), there seems to be no way, to find this form in this double circle, which has circumference $\approx \sqrt{\Delta}$ in this case. We'll come back to this problem in the next section.

5. DETERMINATION OF THE CLASS GROUP AND THE REGULATOR OF A REAL QUADRATIC NUMBER FIELD

Let K be a real quadratic number field with discriminant equal to Δ; the class number formula (4) applied to K becomes

$$h = \frac{\sqrt{\Delta}}{2R} L(1,\chi), \tag{12}$$

where $\chi_\Delta = (\frac{\Delta}{\cdot})$, the Kronecker symbol; and this formula also holds for non-maximal orders of discriminant Δ. So, in order to derive an estimate of h from (12), one should compute the regulator R. The classical way to do this is, to determine the continued fraction expansion of $\sqrt{\Delta}$. However, experience shows, that the length of the period of this expansion may well be $\sim \sqrt{\Delta}$, so, a straightforward computation of R by this method would take much more time than $c\cdot\Delta^{1/5}$.

By means of the theory, developed in Section 4, we can overcome this difficulty and finally give an algorithm to determine both the regulator and the class number of a real quadratic order, which is similar to Shanks'.

There is not much sense in determining the fundamental unit of a real quadratic order with a large discriminant; for instance suppose $\Delta(\mathcal{O})$ has 20 digits (a *very* reasonable number for our algorithm) and suppose $h^+(\mathcal{O}) = 1$, then $R^+(\mathcal{O}) \approx 10^{10}$ and $\varepsilon^+ = e^{R^+}$ is gigantic. In fact, even writing down this

number, by means of the fastest line printers now available, would take a few weeks!

Let us first mention some simple methods to determine the class number of a real quadratic order $\mathcal{O}$ of discriminant Δ, which are suitable if Δ is not too large, say $\Delta \approx 6$ decimal digits.

One can compute R^+ by successive reduction in the principal cycle: one starts with $(1,b,c)$, the principal form, and reduces it, until for two successive forms (a_1,b_1,c_1) and (a_2,b_2,c_2) one has that $b_1 = b_2$. En route, one sums

$$\log\left(\frac{b+\sqrt{\Delta}}{b-\sqrt{\Delta}}\right) ,$$

for all reduced forms (a,b,c); the sum equals R^+ ($= R$ if $a_2 \neq -1$; $= 2R$ if $a_2 = -1$).

There is the following formula for the class number of a maximal order $\mathcal{O}(\Delta)$:

$$h(\mathcal{O}) = -\frac{1}{R} \sum_{\substack{c<x<\Delta/2 \\ (x,\Delta)=1}} \chi(x) \log \sin \frac{\pi x}{\Delta} ;$$

a similar, but more complicated formula holds for non-maximal orders.

Using the dictionary between $\mathcal{O}$-ideal classes and primitive binary quadratic forms, one can also find the class number by counting all the forms of discriminant $\Delta(\mathcal{O})$ and sorting them by double-circles (by periods). Many investigators determined class numbers and regulators by means of these algorithms; they are completely unfeasible if the discriminants of the orders are very large, say $\Delta = 20$ decimal digits.

Let's explain the algorithm: Let h^+ denote the narrow class number of a real quadratic order $\mathcal{O}$; let $\Delta = \Delta(\mathcal{O})$ and $R^+ = R^+(\mathcal{O})$. By Proposition (4.1) we have that $h^+R^+ = 2hR$; so formula (12) becomes

$$(13) \qquad h^+R^+ = \sqrt{\Delta} \prod_{p \text{ prime}} \left(1 - \left(\frac{\Delta}{p}\right)\frac{1}{p}\right)^{-1} .$$

Like in the complex case, the starting point of the algorithm is an approximation of h^+R^+, obtained from (13): let

$$(14) \qquad \tilde{R} = \sqrt{\Delta} \prod_{\substack{p \text{ prime} \\ p \leq X}} \left(1 - \left(\frac{\Delta}{p}\right)\frac{1}{p}\right)^{-1} ,$$

for some X, which we will take $c \cdot \Delta^{1/5}$. We find, that

$$(15) \qquad (1-\varepsilon)\tilde{R} \le h^+R^+ \le (1+\varepsilon)\tilde{R},$$

for some small $\varepsilon \in \mathbb{R}_{>0}$.

Now the principal cycle has length R^+, a number, that we do not know yet. However $\tilde{R}$ is close to h^+R^+, a multiple of R^+, so we can jump to a form f, in the principal cycle at distance $\approx \tilde{R}$ of the principal form (mod R^+ of course; but we do not know R^+ yet) and search for the principal form in the interval

$$(16) \qquad (\tilde{R}(1-\varepsilon),\ \tilde{R}(1+\varepsilon)).$$

If we've found this form, we know a multiple of the narrow regulator R^+.

Then by looking half way the cycle, at $\frac{1}{3}$, at $\frac{1}{5}$ etc., we can determine R^+. This immediately gives us an approximation of h^+:

$$(17) \qquad h^+ \approx \tilde{h} = \frac{\sqrt{\Delta}}{R^+} \prod_{\substack{p \text{ prime} \\ p \le X}} \left(1 - \left(\frac{\Delta}{p}\right)\frac{1}{p}\right)^{-1},$$

and we can complete the calculations by computing the structure of the class group in a way similar to the complex quadratic case.

Some remarks:

- Finding a multiple of R^+ in the interval (15) can efficiently be done by means of a baby-giant strategy (see Section 3). Here, the baby-steps are, very cheaply, computed by successive reduction of the principal form and for computing the giant-steps, one uses composition of forms. If X in (14) is $O(\Delta^{1/5})$, then the baby-giant computations will also be done in $c \cdot \Delta^{1/5+\varepsilon}$ operations.
- Determining the precise regulator R^+, can also be done in $c \cdot \Delta^{1/5+\varepsilon}$ operations. We won't give the details; suffice it to say, that for small primes p ($<< \Delta^{1/10}$), one jumps at $\frac{1}{p}$ of the principal cycle and looks for the principal form, while for large p one solves the problem, by making more giant steps.
- Knowing R^+, we can copy Shanks' algorithm to compute the class group of $\mathcal{O}$. There are some complications however; first of all: testing for equality of two ideal classes, represented by quadratic forms, is now much harder than in the complex case, since *many* forms may represent the same class. However, if one knows for two forms f_1 and f_2 that for some integer n, the forms f_1^n

and f_2^n are in the principal cycle at absolute distance d_1 resp. d_2, then one can test for equality by computing $f_2 f_1^{-1}$, and checking whether this form is in the principal cycle at distance (d_2-d_1) *modulo* R^+/n. If one does not know any distance, we know nothing better to do than a rigorous search in the principal cycle (e.g. by means of a baby-giant-step strategy). This is a time consuming operation and turns the algorithm into a $\Delta^{1/4+\varepsilon}$-algorithm. Fortunately, there is some "trade-off": if h^+ is very small, R^+ is very large, and searching for a form in the principal cycle is very expensive. However if R^+ is very large, h^+ is very accurately determined by formula (17); perhaps h^+ is even known with certainty and one can stop the calculations after having determined R^+, if one is satisfied with the class number without knowing the structure of the class group and without knowing explicit generators of the class group. On the other hand, if h^+ is large and R^+ is small, more searching will be necessary, but this is not so expensive since R^+ is small i.e. the principal cycle is short. We can compute the class number in time bounded by $O(\Delta^{1/5+\varepsilon})$; computing the class group can be done in time bounded by $O(\Delta^{1/4+\varepsilon})$.

- Finally, notice that, in contrast to the computed value of the class number, the regulator R, once it is determined, is known with *certainty*, i.e. without any assumption of a generalized Riemann hypothesis. This hypothesis was only used to guarantee termination in $O(\Delta^{1/5+\varepsilon})$ computing time.

6. FACTORIZATION

In this section we will discuss two deterministic factorization algorithms based on computations in class groups of complex quadratic orders and on computations in the principal cycles associated to class groups of real quadratic orders respectively.

If $N \in \mathbb{Z}_{>1}$ denotes the number that will be factored, then, on assumption of certain generalized Riemann hypotheses (GRH), both algorithms run in time bounded by $N^{1/5+\varepsilon}$ for all $\varepsilon > 0$.

First we briefly indicate how the algorithms discussed in the previous sections are related to factorization algorithms.

Let Δ denote the discriminant of a complex quadratic order $\mathcal{O}$. By an *ambiguous* form f in the class group of $\mathcal{O}$ we mean a form f for which $f^2 = 1$ holds. The ambiguous forms make up a subgroup of the class group; they have the following shape:

$$f = (a,\pm a,c) \quad \text{or} \quad (a,b,c) \quad \text{or} \quad (a,0,c).$$

In other words, the ambiguous forms are precisely the forms that correspond to ideal classes

$$\{(\mathbb{Z} + \frac{b+\sqrt{\Delta}}{2a}\,\mathbb{Z})\,\alpha\colon\ \alpha \in K^{\times}\}$$

with $b+\sqrt{\Delta}/2a$ on the imaginary axis or on the edge of the funamental domain. Every ambiguous form gives rise to a factorization of Δ:

$$f = (a,\pm a,c) : \Delta = a(a-4c)$$
$$f = (a,b,a) : \Delta = (b+2a)(b-2a)$$
$$f = (a,0,c) : \Delta = -4ac.$$

Conversely it is possible to reveal, in an efficient way, the complete factorization of Δ into prime powers from the subgroup of ambiguous forms in $Cl(O(\Delta))$ cf. [18].

Briefly, the algorithm that is based on computations in the class groups of complex quadratic orders consists of computing an ambiguous form in $Cl(O(-N))$ of $N \equiv 3 \pmod 4$ resp. in $Cl(O(-3N))$ if $N \equiv 1 \pmod 4$. To find this ambiguous form takes about as much effort as it takes to compute $Cl(O)$ following the strategy discussed in Section 3.

Next, let Δ denote the discriminant of a real quadratic order. Ambiguous forms are defined to be forms of order ≤ 2, in F; ambiguous forms f have the following shape:

$$f = (a,b,c) \quad \text{where } a|b,$$

so like in the complex case, an ambiguous form provides us with a factor of Δ.

In the principal cycle there are two reduced ambiguous forms: the principal form $(1,\Delta,\Delta^2-\Delta/4)$ and one diametrically opposite to it at distance $\frac{1}{2}R^+$. The algorithm computes these ambiguous forms at distance $\frac{1}{2}R^+$ on the principal cycles $G(O(\Delta))$ for suitable multiples Δ of N.

Note that if (a,b,c) is any quadratic form on the principal cycle $G(O(\Delta))$, it holds that there are $X,Y \in \frac{1}{2}\mathbb{Z}$ such that $N(X+Y\sqrt{\Delta}) = a$, i.e. $X^2 - \Delta Y^2 = a$, whence for all $q|\Delta$ with $\gcd(q,2a) = 1$ we have that $(\frac{a}{q}) = 1$. For instance, if $(-1,\Delta,\Delta-\Delta^2/4)$ is the reduced ambiguous form at distance

$\frac{1}{2}R^+$, it holds that $(\frac{-1}{q}) = 1$ for every odd prime dividing Δ i.e., all odd prime dividing Δ are congruent to 1 (mod 4).

Before entering into a more detailed discussion of the algorithms, we quote some theorems from analytic number theory, which at present can only be proved on assumption of certain generalized Riemann hypotheses.

THEOREM 6.1. (GRH). *There exists an absolute, effectively computable constant* $C_1 > 0$ *such that for every finite extension* K *of* $\mathbb{Q}$ *and every Dirichlet character* χ *of* K, *there exists a prime ideal* p *of* K *of degree* 1 *with*

$$\chi(p) \neq 1 \text{ or } 0 \quad \text{and} \quad N_{K/\mathbb{Q}}(p) < C_1 \log^2 (|\Delta_{K/\mathbb{Q}} N_{K/\mathbb{Q}}(\text{cond } \chi)|)$$

PROOF. Cor. 1.3 of Theorem 1.2 of [15].

One needs the Riemann hypothesis for the zeta function of K and for $L(s,\chi)$: if ρ is any zero of $\zeta_K(s)$ or $L(s,\chi)$ with $0 < \text{Re}\,\rho < 1$, we assume that $\text{Re}\,\rho = \frac{1}{2}$. □

COROLLARY 6.2. (GRH). *Let* $\mathcal{O}$ *be a complex quadratic order of discriminant* Δ, *then* $Cl(\mathcal{O})$ *is generated by quadratic forms* (p,b,c) *of discriminant* Δ *and* p *prime with* $(\frac{\Delta}{p}) = 1$ *and* $p < C_1 \log^2 |\Delta|$.

PROOF. Let $\Delta = f^2 D$ with D the discriminant of a complex quadratic number field. Let G_f denote the ray class group mod f of K. We have a surjective map

$$G_f \twoheadrightarrow Cl(\mathcal{O}(\Delta))$$

via

$$[\underline{a}] \longrightarrow [\underline{a} \cap \mathcal{O}].$$

Here we used the correspondence between equivalence classes of primitive quadratic forms of discriminant Δ and classes of invertible $\mathcal{O}(\Delta)$-ideals. We apply Theorem 6.1 to K and all characters of G_f.

Let H denote the subgroup of G_f generated by the image of the classes of prime ideals p of degree 1 in K and for which

$$N(p) < C_1 \log^2 |D \cdot N_{K/\mathbb{Q}} f| = C_1 \log^2 |\Delta|,$$

holds. The group H then equals G_f because, if $H \not\subset G_f$ we can find a nontrivial character χ of G_f with $H \subset \ker \chi$, but this contradicts Theorem 6.1, since all characters of G_f have conductor dividing f. This proves Corollary 6.2. □

The following theorem gives us an estimate of the rate of convergence of the product expansion of L-series at 1. The proof is along the lines of the proofs in [15] but, since the result we need is not explicitly stated there we will give an outline of a proof below.

THEOREM 6.3. (GRH). *There exists absolute, effectively computable positive constants* C_2 *and* C_3 *such that for all* Δ, *discriminants of quadratic orders and for all* $x > C_2 \log^2 |\Delta|$ *it holds that*

$$\left|1 - \prod_{p>x} \left(1 - \left(\frac{\Delta}{p}\right)\frac{1}{p}\right)\right| < \frac{C_3 \log|\Delta x|}{\sqrt{x}} .$$

Theorem 6.3 is a specialization of a more general theorem. In the proof one assumes the Riemann hypothesis for $L(s,\chi)$, where $\chi(p) = \left(\frac{\Delta}{p}\right)$. All O-symbols that occur in the proof below are absolute and effectively computable.

PROOF OF THEOREM 6.3. Let χ denote the Dirichlet character $\left(\frac{\Delta}{\cdot}\right)$.

def. for $n \in \mathbb{Z}_{\geq 1}$, $\Lambda(n,\chi) = \chi(p^k) \log p$ if $1 \neq n = p^k$ a prime power
$= 0$ otherwise.

def. for $x \in \mathbb{R}_{\geq 1}$: $\psi_1(x,\chi) = \sum_{n \leq x} (x-n)\Lambda(n,\chi)$.

Initially we assume that Δ is a fundamental discriminant i.e. Δ is the discriminant of a number field.

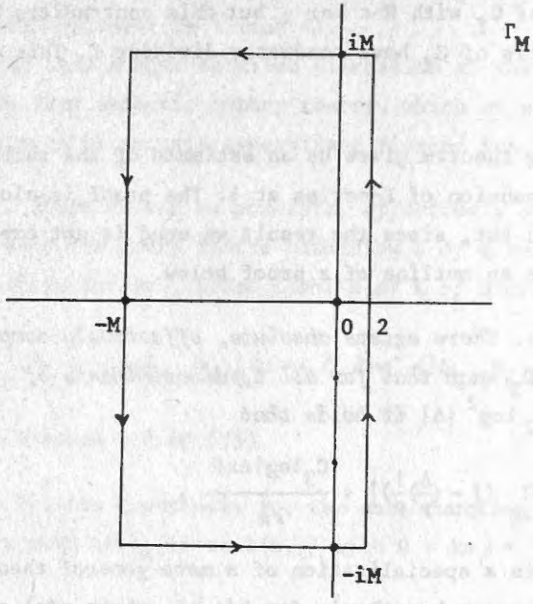
It holds that for $x \in \mathbb{R}_{\geq 1}$

$$\psi_1(x,\chi) = \frac{1}{2\pi i} \int_{2-i\infty}^{2+i\infty} -\frac{L'}{L}(s,\chi) \frac{x^{s+1}}{s(s+1)}\, ds$$

which follows by integrating term by term.

The right hand side of this equation can also be evaluated by computing

$$\frac{1}{2\pi i} \int_{\Gamma_M} -\frac{L'}{L}(s,\chi) \frac{x^{s+1}}{s(s+1)}\, ds$$



for suitable M by applying the residue theorem and by letting $M \to \infty$. One finds

$$\psi_1(x,\chi) = -\sum_{\rho} \frac{x^{\rho+1}}{\rho(\rho+1)} + b_0 - a_0 x + ax$$

$$- \frac{a}{2}\log\left((x-1)^{x-1}(x+1)^{x+1}\right) - \frac{b}{2}\log\left(\frac{(x-1)^{x-1}}{(x+1)^{x+1}}\right) .$$

Here

$$\frac{L'}{L}(s,\chi) = \frac{a}{s} + a_0 + \ldots \qquad \text{near } 0$$

$$\frac{L'}{L}(s,\chi) = \frac{b}{s+1} + b_0 + \ldots \qquad \text{near } -1;$$

it holds that $(a,b) = (1,0)$ if $\Delta > 0$ and $(a,b) = (0,1)$ if $\Delta < 0$. The sum is taken over all ρ, zeros of $L(s,\chi)$ with $0 < \mathrm{Re}\,\rho < 1$.

Subtracting $\psi_1(x,\chi)$ from $\psi_1(x+1,\chi)$ one finds

$$\sum_{n\le x} \Lambda(n,\chi) = (x-[x])\Lambda(n+[x],\chi) - \sum_{\rho \text{ zero}} \frac{(x+1)^{\rho+1}-x^{\rho+1}}{\rho(\rho+1)} - a_0$$

$$- \frac{a}{2}\left(\log \frac{(x+2)^{x+2}x^x}{(x+1)^{x+1}(x-1)^{x-1}} - 2\right) - \frac{b}{2}\left(\log \frac{(x+1)^{x+1}x^x}{(x+2)^{x+2}(x-1)^{x-1}}\right)$$

from which it follows that

$$\left|\sum_{n\le x} \Lambda(n,\chi) + a_0\right| \le \left|\sum_{\rho} \frac{(x+1)^{\rho+1}-x^{\rho+1}}{\rho(\rho+1)}\right| + 2\log(x+1).$$

Let $N(t)$ denote the number of zeros ρ of $L(s,\chi)$ with $0 < \mathrm{Re}\,\rho < 1$ and $t-1 \le \mathrm{Im}\,\rho \le t+1$. Hence, we have

$$N(t) = O(\log(\Delta(|t|+2)))$$

cf. Lemma 5.4 of [15]. Using this estimate and the inequality

$$\left|\sum_{\rho} \frac{(x+1)^{\rho+1}-x^{\rho+1}}{\rho(\rho+1)}\right| \le \sum_{|\mathrm{Im}\rho|\le x} \frac{\sqrt{x+1}}{|\rho|} + \sum_{|\mathrm{Im}\rho|>x} \frac{2(x+1)^{\frac{3}{2}}}{|\rho(\rho+1)|}$$

it is not difficult, assuming the Riemann hypothesis for $L(s,\chi)$, to arrive at

$$\left|\sum_{\rho} \frac{(x+1)^{\rho+1}-x^{\rho+1}}{\rho(\rho+1)}\right| = O(\sqrt{x}\,\log|\Delta x|\,\log x).$$

Finally we find that

$$\left|\sum_{n\le x} \Lambda(n,\chi)\right| = O(\sqrt{x}\log|\Delta x|\log x),$$

(disposing of a_0 by using our estimates for $x = \frac{3}{2}$). It is easy to prove that the estimate also holds for non-fundamental Δ (using the estimate for fundamental Δ to be sure; one may arrive at larger (absolute) constants); so from now on we let Δ be an arbitrary discriminant of a quadratic order.

By partial summation we find

$$\sum_{n>x} \frac{\Lambda(n,\chi)}{n\log n} = \sum_{n>x} \left(\sum_{k=2}^{n} \Lambda(k,\chi)\right)\left(\frac{1}{(n+1)\log(n+1)} - \frac{1}{n\log n}\right)$$

and

$$\Big|\sum_{n>x}\frac{\Lambda(n,\chi)}{n\log n}\Big| = O\Big(\frac{\log|\Delta x|}{\sqrt{x}}\Big).$$

We have that

$$\Big|\sum_{n>x}\frac{\Lambda(n,\chi)}{n\log n} - \sum_{p>x}\log\Big(1-\frac{\chi(p)}{p}\Big)\Big|.$$

$$= \Big|\sum_{k=2}^{\infty}\sum_{k\sqrt{x}<p\le x}\frac{\chi(p)^k}{kp^k}\Big|$$

$$\le \sum_{k>[^2\log x]}\sum_{p\le x}\frac{1}{kp^k} + \sum_{k=2}^{[^2\log x]}\sum_{p>\sqrt[k]{x}}\frac{1}{kp^k} = O\Big(\frac{1}{\sqrt{x}}\Big),$$

and it follows that

$$\Big|\sum_{p>x}\log\Big(1-\frac{\chi(p)}{p}\Big)\Big| = O\Big(\frac{\log|\Delta x|}{\sqrt{x}}\Big).$$

From this estimate one deduces that there exist absolute, effectively computable positive constants C_2 and C_3 such that if $x > C_2\log^2|\Delta|$ then

$$\Big|1-\prod_{p>x}\Big(1-\frac{\chi(p)}{p}\Big)\Big| < \frac{C_3\log|\Delta x|}{\sqrt{x}}.$$

which proves the theorem. □

Next we present the algorithms.

ALGORITHM 6.4. Factorization algorithm based on computations in class groups of complex quadratic orders.

Let $N \in \mathbb{Z}_{>1}$ denote the number to be factored.

Step 1. Test whether gcd(N,6) > 1 or whether N is a proper power of an integer; if this is the case, we can either factor N or decide it is prime; otherwise, if $N \equiv 3 \pmod 4$ put $\Delta = -N$ and if $N \equiv 1 \pmod 4$ put $\Delta = -3N$. In both cases Δ is the discriminant of a complex quadratic order.

Step 2. Compute

$$\tilde{h} = \frac{\sqrt{|\Delta|}}{\pi} \prod_{p \le X} \left(1 - \left(\frac{\Delta}{p}\right)\frac{1}{p}\right)^{-1}$$

with an accuracy of $\log|\Delta|$ significant decimal digits; the product is taken over all primes $p \le X = \max(|\Delta|^{1/5}, C_2 \log^2 |\Delta|)$.

Next for successive primes $p \ge 2$ with $\left(\frac{\Delta}{p}\right) = 1$ do the following step until either a factorization of N is found or $p \ge C_1 \log^2 |\Delta|$; if the latter occurs one concludes that N is prime.

Step 3. Compute a quadratic form $f = (p,b,c)$ and compute a multiple of its order using the estimate $\tilde{h} \approx h(\mathcal{O}(\Delta))$ obtained in Step 2 and the baby-giant-step strategy discussed in Section 3. If $N \equiv 3 \pmod 4$, compute the form of order two in the cyclic group generated by f; if a form of order two is actually existing one obtains a nontrivial factorization of N. If $N \equiv 1 \pmod 4$ denote by H a subgroup of the class group of $\mathcal{O}(\Delta)$ which initially, i.e. before entering Step 3, equals $\{(1,1,1-\Delta/4),(3,3,N+3/4)\}$. Compute a form g, a generator of the 2-primary part of the cyclic group generated by f; compute the group generated by H and g and call it H again. If for some p the group H "becomes" non-cyclic, there are three forms of order 2 in H and those different from (3,3,N+3/4) give rise to a nontrivial factorization of N.

This completes the description of the algorithm.

The algorithm is correct by genus theory and Corollary 6.3: If N passes the tests in Step 1 we can be sure that, if N is composite, there exists a form of order 2 in $Cl(\mathcal{O}(\Delta))$ which gives a nontrivial factorization of N; for details see [12]. By Cor. 6.2 the class group is generated by forms (p,b,c) with $\left(\frac{\Delta}{p}\right) = 1$ and $p < C_1 \log^2 |\Delta|$, so, if we did never find a form of order 2 in Step 3 of the algorithm we can be sure that no such form exists i.e. that N is a prime.

A brief running time analysis runs as follows: Step 1 is polynomial in $\log N$; Step 2 takes time $O(N^{1/5+\varepsilon})$ as explained in Section 3. Theorem 6.2 and the class number formula imply that $|h(\Delta) - \tilde{h}| = O(N^{2/5+\varepsilon})$, so the baby-giant-step strategy in Step 3 takes $O(N^{1/5+\varepsilon})$; The rest of the computations in Step 3 is polynomial in $\log N$: computing a form (p,b,c) can be done in time $O(p \log N) = O(\log^3 N)$ and computing a generator of the 2-primary part of the cyclic group generated by f and computing a form therein can be done by evaluating certain powers of f which takes time polynomial in $\log N$; all computations concerning the group H can be done in time polynomial in $\log N$.

Since Step 3 is repeated at most $C_1 \log^2|\Delta|$ times, we conclude that the algorithm takes time $O(N^{1/5+\varepsilon})$ for all $\varepsilon > 0$.

The algorithm uses memory proportional to $N^{1/5+\varepsilon}$ to store all the baby-steps.

ALGORITHM 6.5. Factorization algorithm based on computations in the principal cycles $G(\Delta)$ of the groups $F(\Delta)$.

Let $N \in \mathbb{Z}_{>1}$ denote the number to be factored.

Step 1. Test whether N is divisible by the primes $\leq (4C_1 \log^2(8N))^2$ and test whether N is a proper power of an integer. If this is the case we can factor N or decide it is prime, otherwise we know that

$$N > (4C_1 \log^2(8N))^2$$

We distinguish two cases:

Case $N \equiv 3 \pmod 4$: For successive primes $p \equiv 3 \pmod 4$ let $\Delta = pN$: the discriminant of a real quadratic order and do the following steps until either a factorization of N is found or $p > C_3 \log^2 N$; if the latter occurs one concludes that N is prime.

Step 2. Compute $\tilde{R} = \sqrt{\Delta} \prod_{p \leq X} (1 - (\frac{\Delta}{p})\frac{1}{p})^{-1}$ with an accuracy of $\log \Delta$ significant decimal digits; the product is taken over all primes $\geq \max(\Delta^{1/5}, C_2 \log^2 \Delta)$.

Step 3. Find a multiple of $R^+(O(\Delta))$ using the baby-giant-step strategy as discussed in Section 3. Compute the ambiguous form g at distance $\frac{1}{2} R^+$ on the principal cycle; if $g \neq (-1,b,c)$ or $(\pm p,b,c)$ then g gives rise to a nontrivial factorization of N.

Case $N \equiv 1 \pmod 4$:

Step 2. First put $\Delta = N$, the discriminant of a quadratic order; compute $\tilde{R}$ (step 2), find a multiple of $R^+(O(N))$ and compute the ambiguous form g at $\frac{1}{2} R^+$ on $G(N)$; if $g \neq (-1,N,N^2-N/4)$, one obtains a nontrivial factorization of N; otherwise do the following:

For successive pairs of primes $p_1, p_2 \equiv 3 \pmod 4$ and $p_1 < p_2 < 4c_1 \log^2(8N)$ (successive in the sense that the products $p_1 p_2$ form an increasing sequence) put $\Delta = p_1 p_2 N$, the discriminant of a real quadratic order. Do

the following steps until a factorization of N is found; if this does not happen for the finitely many pairs (p_1,p_2) one concludes that N is prime.

Step 3. Compute $\tilde{R} = \sqrt{\Delta} \prod_{p \le X} (1 - (\frac{\Delta}{p})\frac{1}{p})^{-1}$ as before.

Step 4. Find a multiple of $R^+(O(\Delta))$ and the ambiguous form $g = (a,b,c)$ at $\frac{1}{2} R^+$ on the principal cycle; if $a \neq -1, \pm p_1, \pm p_1 p_2$ the form g gives rise to a nontrivial factorization of N.

This completes the description of the algorithm.

To prove correctness we distinguish the two cases again:

Case $N \equiv 3 \pmod 4$: Assume that N is composite and that N passed the tests in Step 1. Let q denote a prime congruent to 3 (mod 4) that divides N.

LEMMA (GRH). *There exists a prime* $\equiv 3 \pmod 4$ *satisfying* $(\frac{p}{N/q}) = -1$ *and* $p < C_1 \log^2 (4N)$.

PROOF. Apply Theorem 6.1 to the (non-primitive) quadratic character χ of $K = \mathbb{Q}(\sqrt{-N/q})$ belonging to the extension $K(i)/K$ of conductor (2). By Theorem 6.1 there exists a prime p of K of degree 1 with $\chi(p) = -1$ and

$$N(p) < C_1 \log^2 (\Delta_K N_{K/\mathbb{Q}}(\text{cond } \chi)) \le C_1 \log^2 (4N).$$

Let $p = N(p)$ then p splits in $\mathbb{Q}(\sqrt{-N/q})$ (since $p \neq 2$) and we have $(\frac{-1}{p}) = (\frac{p}{N/q}) = -1$. □

Let $\Delta = pN$ with p a prime as in the lemma; then the reduced form $g = (a,b,c)$ at $\frac{1}{2} R^+$ in $G(\Delta)$ cannot have $a = \pm N$ since the fact that g is reduced implies that $N < \sqrt{\Delta}$ i.e. $p > N$ which contradicts $p < C_1 \log^2 (4N)$ and the fact that N passed the tests in Step 1. Nor can g have $a = -1$ or $\pm p$ since we have that $(\frac{-1}{p}) = -1$ and $(\frac{\pm p}{N/q}) = -1$. We conclude that for this p we will encounter a nontrivial factorization of N in Step 3 of the algorithm.

Case $N \equiv 1 \pmod 4$: Assume that N is composite and that N passed Steps 1 and 2 of the algorithms. This implies inter alia that all divisors of N are congruent to 1 (mod 4): let q_1 and q_2 be *distinct* primes dividing N.

LEMMA (GRH). *There exists two primes* $p_1,p_2 \equiv 3 \pmod 4$ *satisfying* $(p_1/q_1) = -1$; $(p_2/q_1) = 1$ *and* $(p_2/q_2) = -1$ *and* $p_1,p_2 \le 4C_1 \log^2 8N$.

PROOF. For p_1 consider the non-primitive character χ of $K = \mathbb{Q}(\sqrt{-q_1})$ of conductor (2) belonging to K(i)/K and for p_2 consider the non-primitive character χ of $L = \mathbb{Q}(\sqrt{q_1}, \sqrt{-q_2})$ of conductor (2) belonging to L(i)/L. We have $|\Delta_K| = 4q_1$ and $|\Delta_L| = (4q_1q_2)^2$. As in the proof of the lemma in the case $N \equiv 3 \pmod 4$ we can find p_1 and p_2 smaller than

$$C_1 \log^2((4q_1q_2)^2 \cdot 2^4) < 4C_1 \log^2(8N).$$

This proves the lemma.

Let $\Delta = p_1p_2N$ with p_1 and p_2 a pair of primes as in the lemma; the reduced form $g = (a,b,c)$ at $\frac{1}{2}R^+$ in $G(\Delta)$ cannot have $a = \pm N$, $\pm p_1N$, $\pm p_2N$ and $\pm p_1p_2N$ since this implies $p_1p_2 > N$ whence $(4C_1 \log^2(8N))^2 > N$ which contradicts the fact that N passed Step 1 of the algorithm. Nor can g have $a = -1$, $\pm p_1$, $\pm p_2$ or $\pm p_1p_2$ since $(-1/p_1) = -1$; $(\pm p_1/q_1) = -1$; $(\pm p_2/q_2) = -1$ and $(\pm p_1p_2/q_1) = -1$ respectively. We conclude that for this pair (p_1,p_2) the form g provides us with a nontrivial factorization of N. This finishes the proof of the correctness of the algorithm.

We leave a running rime analysis to the reader; it is analogous to the analysis of the running time of the algorithm based on computations of class groups of complex quadratic orders.

This finishes the description of the algorithms.

7. IRREGULAR CLASS GROUPS

In this section we will consider the structure of the class groups of quadratic orders.

First some terminology: for a finite abelian group A, and a prime p, the minimal number of generators of the p-Sylow subgroup of A is called *the p-rank of A, notation* d_pA.

By C(n) we denote the cyclic group of n elements. For instance, $d_p(C(n)) = 1$ for all primes p, that divide n.

DEFINITION. Let $\mathcal{O}$ be a quadratic order and let $Cl(\mathcal{O})$ be its class group. We call $Cl(\mathcal{O})$ *irregular* if $Cl^2(\mathcal{O})$ is non-cyclic, or, equivalently, if $d_pCl^2(\mathcal{O}) \geq 2$. We call $d_pCl^2(\mathcal{O})$ the *exponent* of p-irregularity.

REMARK. If p is an *odd* prime, then $Cl(\mathcal{O})$ is p-irregular iff $d_pCl(\mathcal{O}) \geq 2$.

Although inspection of a list of class groups of orders of small discriminantes might suggest differently, irregular class groups do exist! For instance the class group of the order of discriminant -3299 is isomorphic to $C(3) \times C(3)$. Gauss considered the phenomenon of irregularity to be of great importance [12]:

> *Hoc argumentum, quod ad arithmeticae sublimioris mysteria maxima recondita pertinere, disquisitionibusque difficillimis locum relinquere videtur, paucis tantum observationibus hic illustrare possumus,... .*

In his "Disquisitiones Arithmeticae", Gauss considers irregular class groups of both maximal and non-maximal orders. For non-maximal orders there is for obvious reasons more irregularity, and indeed Gauss found many examples of this kind. Here we will confine ourselves to class groups of maximal orders i.e. class groups of quadratic number fields.

Recently D.A. BUELL [3] made a list of class groups of complex quadratic fields with discriminant > -4000000; it is the largest list available up to now, and it appeared that 95.74% of the listed class groups had a cyclic subgroup of squares, i.e. 95.74% of the class groups were p-regular *for all primes* p. So it seems, that, for complex quadratic fields, irregular class groups are rare, and, as it turns out, even rarer for real quadratic fields.

Let us first consider complex quadratic fields. It is easy to construct 2-irregular class groups with a high exponent of irregularity, e.g. as follows: Let

$$\Delta_1 = -3 \cdot 13,$$

$$\Delta_{k+1} = \Delta_k \cdot p \text{ with } p \text{ the smallest prime } \equiv 1 \pmod 4 \text{ such that } \left(\frac{p}{q}\right) = 1 \ \forall q \mid \Delta_k.$$

It can be proved, that $d_2 Cl^2 \mathbb{Q}(\sqrt{\Delta_k}) = k$. For example

$$\Delta_3 = -3.13.61.601 = -1429779$$

and $\mathbb{Q}(\sqrt{\Delta_3})$ has a class group $\cong C(4) \times C(4) \times C(4) \times C(5)$. So the exponent of 2-irregularity equals 3.

It turns out to be very hard, to construct p-irregular class groups for odd p. The only example. I could find in Gauss' "Disquisitiones", was the

maximal order of discriminant -9748. (determinant = -2437 in his terminology); the class group is isomorphic to $C(3) \times C(3) \times C(2)$.

In the beginning of the 20th century some more examples of p-irregular class groups, with p odd, were known, but, it seems, always 3-irregular of exponent 2.

In 1936, G. PALL [26] seemed to have obtained the first new result on the matter since more than a century: he claimed, that the field $\mathbb{Q}(\sqrt{-12379})$ has a class group isomorphic to $C(5) \times C(5)$.

However, 25 years later, in 1961, LIPPMANN [19] proved that the class group of $\mathbb{Q}(\sqrt{-12379})$ is cyclic of order 25. Lippmann used a computer; he also gave some correct examples of 5-irregular and 7-irregular class groups, viz.

$$Cl(\mathbb{Q}(\sqrt{-12451})) \simeq C(5) \times C(5) \times C(2)$$

$$Cl(\mathbb{Q}(\sqrt{-63499})) \simeq C(7) \times C(7).$$

Lippmann also searched for 11-irregular class groups, but was not successful in this case.

In 1970, YAMAMOTO [42] proved, for all $n \in \mathbb{Z}_{\geq 1}$, the existence of infinitely many complex quadratic fields with $C(n) \times C(n)$ as a subgroup of their class groups. A trivial consequence is, that for all primes p, infinitely many p-irregular class groups exist.

Yamamoto gave his fields explicitly; he parametrized their discriminants by a polynomial of degree 2n. Consequently, the discriminants of his fields, having p-irregular class groups with p large, are huge.

In 1971, SHANKS [32] using the algorithm discussed in Section 3, found that

$$Cl(\mathbb{Q}(\sqrt{-564552759})) \simeq C(3) \times C(3) \times C(3) \times C(604),$$

$(564552759 = 3(3^6 + 4.19^6))$.

It is the first example of a p-irregular class group with p odd and index of p-irregularity > 2. From then on, things go a *bit* faster; some theoretical results are obtained by M. CRAIG [4,5], who proves the existence of infinitely many complex quadratic fields K with $d_3 Cl(K) \geq 4$, and many explicit examples are found by SHANKS and others [6,7,8,9,10,24,28, 34,35,36,38,39]. At present the, perhaps diappointing, state of affairs is:

p	d	-Δ	
3	2	3299	[3]
	3	3321607	[3,7]
	4	653329427	[6]
5	2	11199	[3]
	3	18397407	[11,28]
	4	258559351511807	[28]
7	2	63499	[3]
	3	480544612303251864826851O536	[39]
11	2	65591	[3]
13	2	228679	[3]
17	2	1997799	[3]
19	2	373391	[3]
23	2		
+	+		

where

d: an integer ≥ 2, for which a class group $Cl(O)$ is known to exist with $d_p Cl(O) = d$.

Δ: smallest known discriminant with $d_p Cl(O) = d$. For the p-rank = 2 cases and the 3-rank = 3 case, these discriminants have been *proved* to be minimal (in absolute value).

All examples, with p-rank = 2, have been taken from BUELL's list [3]. The 7-rank = 3 example has been found by J. Solderitsch; he used polynomials

$$D_p(s,t) = s^{2p} - 6(st)^p + t^{2p}$$

taking p = 7 and (s,t) = (87,85) gives the example. The 5-rank = 4 case was found by myself by means of ideas of J.F. MESTRE [21].

Perhaps it shouls be indicated that the first examples of class groups with high p-rank, for odd p, were usually very large; for instance, the example of the class group with 7-rank equal to 3, is, at present, the only example known; it is not unlikely, that (say) a 10-digit discriminant exists with the same property, but this one has to be found yet. On the other hand, the 3-rank = 3 example, given here, is much smaller than the first one found by Shanks. At present, many examples of class groups with 3-rank = 3,4 or 5-rank = 3 are known.

As far as the real quadratic fields are concerned, the situation is perhaps even more disappointing.

As in the complex case we'll confine ourselves to p-irregular class groups with p *odd* of *maximal* orders. In [12] GAUSS says, that he did not encounter any example of a real quadratic order which is p-irregular for odd p; he also expresses his firm belief in the existence of these orders, and he was right.

In 1936, PALL [26] gives the first (correct) example: the discriminant 62501 determines a maximal order with class group isomorphic to $C(3) \times C(9)$. In 1972 SHANKS [32] finds the prime $188184253 = 3^6 + 4.19^6$; the field $Q(\sqrt{188184253})$ has class group isomorphic to

$$C(3) \times C(3) \times C(3).$$

In fact, Shanks used this example and an old theorem of SCHOLZ [27], that connects the 3-ranks of the class groups of $Q(\sqrt{\Delta})$ and $Q(\sqrt{-3\Delta})$, to construct his example of the complex quadratic field with 3-rank of its class group equal to 3, that was mentioned above. Scholz's theorem implies, that every example of a real quadratic field having a class group with high exponent of 3-irregularity implies an example of a complex quadratic field, with the same property and vice versa. This explains why we know at least some examples of 3-irregular class groups of real quadratic fields. The state of affairs is:

p	d	Δ	
3	2	32009	[30]
3	3	39345017	[6]
3	4	1284062551036124923952823484951333 3657649481047277182572850406316022 7 1618734625153213764715019579977295 7	[10]
5	2	1129841	[16]
7	2	2068117	[16]
11			

In his thesis, Diaz y Diaz announces a proof of the existence of infinity many real quadratic fields, admitting $C(3) \times C(3) \times C(3) \times C(3)$ as a subgroup of their class groups, but his proof has not yet been published cf. [9].

Finally, we'll explain how the example of a complex quadratic field K with $d_5 Cl(K) = 4$, that is given above, was found. In order to do this, we'll

sketch, how certain polynomials $M_E(t) \in \mathbb{Z}[t]$, may be derived from a Weierstrass equation of an elliptic curve E, which is defined over $\mathbb{Q}$; these polynomials are used to parametrize discriminants of quadratic fields. The computations are based on work of J.F. MESTRE [21].

Let E be an elliptic curve defined over an algebraic number field K; assume that P is a K-rational point on E and that the order of P is n. Let F be the elliptic curve $E/\langle P\rangle$; then F is K-rational and there is a K-isogeny $E \overset{\phi}{\to} F$. If $Q \in F$ is K-rational and $R \in \phi^{-1}(Q)$ (not necessarily K-rational) then K(R)/K is an *unramified cyclic extension of degree* n, on the condition that

(i) Q is not singular modulo any prime of K; this condition guarantees that the extension K(R)/K is unramified.

(ii) A rather involved condition, which guarantees that K(R)/K is of degree n; we do not give the precise condition, since, numerically, it is not a very interesting one.

Recall, that by class field theory, the fact that K(R)/K is unramified cyclic of degree n implies that $C\ell(K) \twoheadrightarrow C(n)$. We shall apply the above to elliptic curves defined over $\mathbb{Q}$:

$$F:\ Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X^2 + a_4X + a_6.$$

Let $x \in \mathbb{Q}$ and find y such that $(x,y) \in F$; the number y will be in a quadratic number field K, and we'll apply the above to K. Conditions (i) and (ii) boil down to simple congruence conditions on x.

Mestre's idea is, to find two different points, Q_1 and Q_2 on F that satisfy the above conditions. By submitting Q_1 and Q_2 to certain conditions, he can prove that for n prime, the group $C(n) \times C(n)$ is a subgroup of $C\ell(K)$. We do not bother about all of these conditions, since computations suggest, that perhaps they are too stringent.

The computation of $M_F(t)$: F is given by

$$\eta^2 = \xi^3 - \frac{c_4}{48}\xi - \frac{c_6}{864}$$

cf. [22]. Assume $\xi_1 \neq \xi_2$ and

$$\eta^2 = \xi_1^3 - \frac{c_4}{48}\xi_1 - \frac{c_6}{864} = \xi_2^3 - \frac{c_4}{48}\xi_2 - \frac{c_6}{864}\ . \tag{19}$$

We take $Q_1 = (\xi_1,\eta)$ and $Q_2 = (\xi_2,\eta)$ the two (different) points on F and we want to compute $\mathbb{Q}(\eta)$. Equation (19) becomes

$$\xi_1^2 + \xi_1\xi_2 + \xi_2^2 = \frac{c_4}{48}. \tag{20}$$

Now, if c_4 is the norm of a number in $\mathbb{Q}(\zeta_3)$, the curve (20) is a non-empty rational conic and it can be parameterized e.g. if $\alpha^2 + \alpha\beta + \beta^2 = c_4$, by

$$\begin{aligned} \xi_1(t) &= \frac{1}{12}\,\frac{-\beta t^2+2\alpha t+(\alpha+\beta)}{t^2+t+1}, \quad t \in \mathbb{P}_1(\mathbb{Q}), \\ \xi_2(t) &= \frac{1}{12}\,\frac{(\alpha+\beta)t^2+2\beta t-\alpha}{t^2+t+1}, \quad t \in \mathbb{P}_1(\mathbb{Q}). \end{aligned} \tag{21}$$

Substituting (21) in (19), one easily finds that

$$\mathbb{Q}(\eta) = \mathbb{Q}(\sqrt{M_F(t)})$$

with $M_F(t) \in \mathbb{Z}[t]$ of degree 8.

EXAMPLE. If we take $E \xrightarrow{\phi} F$ to be $X_1(11) \to X_0(11)$, (or 11A $\xrightarrow{\phi}$ 11B in the notation of [22]) then this is a 5-isogeny $E \xrightarrow{\phi} F$, with a point of order 5 in $\ker \phi$. We find, that, up to a square,

$$M_{11B}(t) = -(t^2+t+1)(47t^6+21t^5+598t^4+1561t^3+1198t^2+261t+47).$$

Condition (i) now becomes:

$$t \not\equiv 2,-4,4 \pmod{11}.$$

Substituting special values for t we find:

t	Δ	$Cl(\mathbb{Q}(\sqrt{\Delta}))$
1	-11199	$C(5) \times C(5) \times C(4)$
1/4	-18397407	$C(5) \times C(5) \times C(5) \times C(2) \times C(8)$
14/25	-258559351511807	$C(5) \times C(5) \times C(5) \times C(5) \times C(2) \times C(4) \times C(2957)$

These are precisely the examples given above. By taking other elliptic curves, one can search for other types of class groups. In particular, it is possible, to get information on class groups of real quadratic fields as well.

On the other hand, the method is limited in the sense that, using elliptic curves that are defined over $\mathbb{Q}$, one cannot construct p-irregular class groups for $p > 7$; this is a consequence of B. Mazur's classification theorem on the torsion of Mordell-Weil groups of elliptic curves defined over $\mathbb{Q}$, see [20].

8. IMPLEMENTATION

Shanks' algorithm (see Section 3) has been programmed by some people e.g. Solderitsch, Shanks and his collaborators and myself.

The algorithm discussed in Section 5, has been programmed by me on the SARA CDC-Cyber 170-750 computer. At present, four programs are available: SHANKS, LONSH, PODISH and LOPOD.

SHANKS is a program, completely written in PASCAL that determines the class group of a complex quadratic order, given its discriminant Δ, with $|\Delta| < 2.5_{10}14$. It is hard to predict the time needed, to compute the class group of a given quadratic order; apart from the size of Δ, also factors like the accuracy of the approximation of $L(1,\chi)$ and the complexity of the structure of the class group have their influence on the computing time. Roughly speaking, a 10-digit discriminant takes not more than 0.1 seconds and a 15 digit discriminant takes 0.2 seconds. It is possible to give extra data, like an a priori known divisor of the class number, or forms whose order in the class group is known beforehand. In computing an approximation of $L(1,\chi)$, SHANKS uses a file of primes: PRIME, which contains, at present, all primes ≤ 240000.

Apart from the difficulties that arise, when the class group is very complicated, the most time consuming parts of Shanks' algorithm are the computation of the approximation of the class number and the baby-giant-step strategy (both $\sim |\Delta|^{1/5+\varepsilon}$). In order to have an optimum in costs, some care was taken to "balance" the program: the amount of primes used in the evaluation of the approximation of the class number depends upon the size of the current approximation of the class number; the constants involved are chosen in such a way, that the baby-giant-step strategy and the evaluation of the approximation of the class number take about the same amount of time. It

should be remarked, that for the discriminants of the size, that can be handled by SHANKS, only 10 to 15% of the computing time is spent in these "time-comsuming" parts of the algorithm. The reason for this is that discriminants of this size are, in fact, a bit too small for the algorithm (!); most of the time is spent doing "administration" i.e. computations in the class groups, determination of precise orders of forms etc. Considerably larger discriminants can be handled by LONSH and only then, a large part of the computation time is spent in computing an approximation of the class number and in doing the baby-giant-step strategy.

It was suggested by L. Monier to do the search procedures in the baby-giant-step computations by means of hash-coding [14]. SHANKS gives as output:
- the structure of the class group of $O(\Delta)$;
- the complete factorization of Δ;
- the "precise" value of $L(1,\chi)$;
- a lot of information on how the group was computed, how good the approximations were, computing times etc.

LONSH is a double length version of SHANKS; LONSH computes the class groups of orders with discriminant Δ, where $|\Delta| < 10^{29}$. The bulk of LONSH is written in PASCAL, but the composition and reduction algorithms are written in FORTRAN and COMPASS, The CDC assembler language. In fact, since the coefficients of the quadratic forms are $\sim \sqrt{|\Delta|}$, only these parts of LONSH differ essentially from the algorithms used in SHANKS.

LONSH uses the DOUBLE PRECISION facilities of FORTRAN. A 20 digit Δ will take ~ 2 seconds and a 25-digit Δ roughly 20. As indicated before, LONSH displays more clearly the order of the algorithm. Concerning transput facilities: LONSH has exactly the same possibilities as SHANKS.

PODISH computes the regulator and the class group of a real quadratic order, given its discriminant Δ, where $\Delta < 2.5_{10}14$. PODISH uses PRIME and it performs its searching routines, in determining the regulator, by means of hash-coding.

PODISH first computes the regulator and then, depending on an option: "R", PODISH computes the class group. Under the option "R", PODISH only computes the regulator, the norm of the fundamental unit ε, and if $N\varepsilon = 1$, the factorization induced by the non-trivial reduced ambiguous form in the principal cycle, at distance $\frac{1}{2}R^+$. Care has been taken to balance the program, although this is harder to do than in the complex case. Due to the computations that are performed in the principal cycle to determine the precise regulator, *after* a "match" has been found, the algorithm is not as sensitive

to the accuracy of the approximation of the class number, as in the complex case. PODISH gives as output.

- the value of R^+, $L(1,\chi)$ and the norm of the fundamental unit;
- the structure of the class group;
- information on how the regulator and the class group were obtained, like computing times, etc.

LOPOD is a double length version of PODISH.

For a detailed description of the programs mentioned here, see [29].

REFERENCES

[1] BOREVIČ, Z.I. & I.R. ŠAFAREVIČ, *Number Theory*, Academic Press, 1966.

[2] BOYD, D.W. & H. KISILEVSKY, *On the exponent of the ideal class groups of complex quadratic fields*, Proc. Amer. Math. Soc. (1972) 433-436.

[3] BUELL, D.A., *Class groups of quadratic fields*, Math. Comp. 30 (1976) 610-623.

[4] CRAIG, M., *A type of class groups for imaginary quadratic fields*, Acta Arithm. 22 (1973) 449-459.

[5] CRAIG, M., *A construction for irregular discriminants*, Osaka J. of Math. 14 (1977) 365-402.

[6] DIAZ Y DIAZ, F., *Sur le 3-rang des corps quadratiques*, Thèse, Orsay, (1978).

[7] DIAZ Y DIAZ, F., *On some families of imaginary quadratic fields*, Math. Comp. 32 (1978) 637-650.

[8] DIAZ Y DIAZ, F., *Quelques discriminants irreguliers*, Actas de las VII Jornadas Mathematicas Hispano-Lusas, Santander, Iunio, 1979.

[9] DIAZ Y DIAZ, F., *Sur le 3-rang des corps quadratiques*, preprint.

[10] DIAZ Y DIAZ, F., D. SHANKS & H.C. WILLIAMS, *Quadratic fields with 3-rank equal to 4*, Math. Comp. 33 (1979) 836-840.

[11] DIAZ Y DIAZ, F., *Private communication*.

[12] GAUSS, C.F., *Disquisitiones Arithmeticae*.

[13] GUY, R.K., *How to factor a number*, Proc. 5th Manitoba Conf. on Num. Math., October 1975.

[14] KNUTH, D., *The Art of Computer Programming, II*, Addison-Wesley, 1973.

[15] LAGARIAS, J.C., H.L. MONTGOMERY & A.M. ODLYZKO, *A bound for the least prime ideal in the Chebotarev Density Theorem*, Inv. Math. 54 (1979) 271-296.

[16] LAKEIN, R.B., *Computation of the ideal class group of certain complex quadratic fields, II*, Math. Comp. 29 (1975) 137-144.

[17] LANG, S., *Algebraic Number Theory*, Addison-Wesley, 1968.

[18] LENSTRA, H.W., *On the calculation of regulators and class numbers of quadratic fields*, To appear in Proceedings of the Journées Arithmétiques, Exeter 1980.

[19] LIPPMANN, R.A., *Note on irregular discriminants*, J. London Math. Soc. 38 (1963) 385-386.

[20] MAZUR, B., *Rational points on modular curves*, In: *Modular Functions of One Variable*, V. Bonn, J.P. Serre and D.B. Zagier (eds), Lecture Notes in Math. 601, Springer, 1976.

[21] MESTRE, J.F., *Courbes elliptiques et groupes de classes d'idéaux de certaines corps quadratiques*, Sém. de Théorie des nombres, Bordeaux, 1979/1980, Exp. 15.

[22] TATE, J., *Algorithm for determining the type of a singular fiber in an elliptic pencil*, In: *Modular Functions of One Varible, IV*, Anvers, Ed. Birch and Luyk, Lecture Notes in Math. 476, Springer, 1972.

[23] MONIER, L., *Algorithmes de factorisation d'entiers*, Thèse, 3^{me} Cycle, Orsay, 1980.

[24] NEILD, C. & D. SHANKS, *On the 3-rank of quadratic fields and the Euler product*, Math. Comp. 28 (1974) 279-291.

[25] ODLYZKO, A.M., Private Communication.

[26] PALL, G., *Note on irregular determinants*, J. London Math. Soc. 11 (1936) 34-35.

[27] SCHOLZ, A., *Über die Beziehung der Klassenzahlen quadratischer Zahlkörper zu einander*, J. Reine u. Angew. Math. 166 (1932) 201-203.

[28] SCHOOF, R.J., *Class groups of complex quadratic fields*, To appear in Math. Comp..

[29] SCHOOF, R.J., *Two algorithms for determining class groups of quadratic fields*, Report Dept. of Math. Univ. of Amsterdam, to appear.

[30] SHANKS, D., *On Gauss' class number problems*, Math. Comp. 23 (1969) 151-163.

[31] SHANKS, D., *Class number, a theory of factorization and genera*, Proc. Symp. Pure Math. 20 AMS (1971) 415-440.

[32] SHANKS, D. & P. WEINBERGER, *A quadratic field of prime discriminant, requiring three generators for its class group, and related theory*, Acta Arithm. 21 (1972) 71-87.

[33] SHANKS, D., *The infra-structure of a real quadratic field and its applications*, Proc. of the 1972 Number Theory Conf. Boulder, Colorado, 1973, 217-224.

[34] SHANKS, D. & R. SERAFIN, *Quadratic fields with four invariants divisible by 3*, Math. Comp. 27 (1973) 181-187.

[35] SHANKS, D., *New types of quadratic fields having three invariants divisible by 3*, J. Number Theory 4 (1972) 537-556.

[36] SHANKS, D., *Class groups of the quadratic fields, found by F. Diaz y Diaz* Math. Comp. 30 (1976) 173-178.

[37] SCHUR, *Einige Bemerkungen zu den Vorstehenden Arbeit des Herrn G. Polya: über die Verteilung der quadratischen Reste und Nichtreste*, Nachr. Kön. Ges. Wiss. Göttingen, Math.-Phys. Kl. (1918), 30-36.

[38] SOLDERITSCH, J.J., *Imaginary quadratic number fields with special class groups*, Thesis, Lehigh Univ., 1977.

[39] SOLDERITSCH, J.J., *Quadratic fields with special class groups*, To appear in Math. Comp.

[40] WILLIAMS, H.C. & B.K. SCHMID, *A rapid method of evaluating the regulator and class number of a pure cubic field*, to appear in Math. Comp.

[41] WEINBERGER, P., *Exponents of the class group of complex quadratic fields*, Acta. Arithm. 22 (1973) 117-124.

[42] YAMAMOTO, Y., *On unramified Galois extensions of quadratic number fields*, Osaka J. of Math. 7 (1970) 57-76.

[43] ZANTEMA, H., *Class numbers and units*, these proceedings.