On the calculation of regulators and class numbers of quadratic fields

Lenstra, H.W.

Reprinted from J.V.Armitage (ed.), Journées Arithmétiques 1980. Printed in Great Britain at the University Press, Cambridge.

ON THE CALCULATION OF REGULATORS AND CLASS NUMBERS OF QUADRATIC FIELDS

H.W. Lenstra, Jr.

Introduction

In this lecture we present a mathematical model that can be used to analyze Shanks's algorithm to determine the regulator of a real quadratic field, see [24]. Let me briefly describe the situation.

In an earlier paper [23], Shanks indicated a method to calculate the class group of an imaginary quadratic field. For this method, it is convenient to view the class group as a group of equivalence classes of quadratic forms, the group multiplication being *composition* of forms. A basic fact underlying the algorithm is that every equivalence class contains exactly one *reduced* form. In the real quadratic case, this is not true any more; here every equivalence class contains a whole *cycle* of reduced forms. Shanks observed [24], that the principal cycle, corresponding to the neutral element of the class group, displays a certain group-like behaviour with respect to composition. In this lecture, we introduce a group F whose properties can be used to give precise formulations and proofs of Shanks's observations. The group is defined as the set of orbits of quadratic forms under $\begin{pmatrix} 1 & \mathbb{Z} \\ 0 & 1 \end{pmatrix}$ rather than $SL_2(\mathbb{Z})$. It has a close relationship to a certain group of idele classes. For a different approach to the analysis of Shanks's methods we refer to Lagarias [7; 8; 9].

In the first few sections below we present the standard dictionary between ideal classes and classes of quadratic forms in the way we need it, cf. [1]. Each of the languages has its merits: the ideals can be used for smooth and conceptual definitions and proofs, and the forms are a convenient vehicle for computations. In section 7 we describe Shanks's algorithm for imaginary quadratic fields, the main ideas of which also play a role in the more

complicated real quadratic case. Sections 8 to 12 are devoted to the group F mentioned above, and section 13 gives an informal description of how its properties can be used to calculate regulators and class numbers of real quadratic fields. The final section touches upon some applications of the material in this lecture.

The correctness and efficiency of most of the algorithms that we describe depend on the generalized Riemann hypothesis. It would be of interest to obtain explicit versions of all inequalities used, assuming the Riemann hypotheses. It would also be of interest to see what remains if no unproved hypotheses are assumed.

The quadratic field K that we consider is supposed to be given by its discriminant. Checking that a given integer is the discriminant of a quadratic field involves testing squarefree-ness. For this I know no essentially faster method than factoring the number, and there is a good reason not to do this: namely, one of the most efficient factoring algorithms is based on the connection between the factorizations of the discriminant and the elements of order two in the class group, and makes use of the ideas set forth in this lecture; see sec. 15 for references. The only way out is that we develop the entire theory for arbitrary orders in quadratic fields rather than just the maximal order.

Throughout this paper the terms "class group" and "regulator" are used in the *strict* (narrow) sense: see the definitions in sections 2 and 6, respectively, and the end of section 13.

We denote by $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ the ring of integers, the field of rational numbers, the field of real numbers, and the field of complex numbers, respectively. For a ring B with 1, we denote by B^* the group of units of B. The reader should note the distinction between N, R, P, F, G and N, R, P, F, G.

1. Orders in quadratic fields

Let K be a quadratic field extension of $\mathbb{Q}$. Denote by σ the non-trivial field automorphism of K, and define the *norm* $N: K \to \mathbb{Q}$ by

$$N(\alpha) = \alpha \cdot \sigma(\alpha), \qquad \text{for } \alpha \in K.$$

Let A_0 be the ring of algebraic integers in K. An *order* in K is a subring A of A_0 with $1 \in A$ and with field of fractions K. Every order A in K satisfies $\mathbb{Z} \subset A \subset A_0$, and since $A_0/\mathbb{Z}$ is cyclic as an additive group, every order is determined by its index in A_0. This index is finite and called the *conductor* of A. Every positive integer f occurs as the conductor of an order A in K, namely $A = \mathbb{Z} + fA_0$. If $A = \mathbb{Z}e_1 + \mathbb{Z}e_2$, then the *discriminant* Δ of A is defined by $\Delta = (e_1\sigma(e_2) - e_2\sigma(e_1))^2$; this is an integer which does not depend on the choice of the basis e_1, e_2. We have $\Delta = f^2 \cdot \Delta_0$, where f is the conductor of A and Δ_0 is the discriminant of A_0; we call Δ_0 also the discriminant of K. The integer Δ is not a square, and $\Delta \equiv 0$ or $1 \bmod 4$. Conversely, any non-square integer Δ that is 0 or $1 \bmod 4$ is the discriminant of a uniquely determined order in a quadratic field, namely $A = \mathbb{Z}[(\Delta + \sqrt{\Delta})/2] \subset K = \mathbb{Q}(\sqrt{\Delta})$. It will be convenient, in the sequel, to assume that K is embedded in $\mathbb{C}$; square-roots of real numbers will be assumed to lie on the non-negative part of the real or imaginary axis.

2. Invertible ideals

Let K be a quadratic field, and $A \subset K$ an order of discriminant Δ. The *product* $M \cdot M'$ of two subsets $M, M' \subset K$ is the additive subgroup of K generated by $\{x \cdot y : x \in M, y \in M'\}$. An *invertible* A-*ideal* is a subset $M \subset K$ with $A \cdot M = M$ for which there exists M' such that $M \cdot M' = A$. Its *inverse* $A \cdot M'$ is then also an invertible A-ideal, and the set of invertible A-ideals is a commutative group with respect to multiplication. We denote this group by I.

Let M be an invertible A-ideal, and $M \cdot M' = A$. We claim that

$$A = \{\alpha \in K : \alpha M \subset M\}. \tag{2.1}$$

The inclusion $\subset$ is obvious. Conversely, if $\alpha M \subset M$ then $\alpha = \alpha \cdot 1 \in \alpha A = \alpha M \cdot M' \subset M \cdot M' = A$, as required.

From $M \cdot M' = A$ we see that there exist $x_i \in M$, $y_i \in M'$ $(1 \le i \le t)$ such that $\sum_{i=1}^{t} x_i y_i = 1$. Then $Ax_1 + Ax_2 + \ldots + Ax_t$ coincides with M, since it has the same inverse. Hence M is finitely generated over A. It follows that M is a finitely

generated subgroup of K, and that we can write $M = \mathbb{Z}\alpha + \mathbb{Z}\beta$, where $\alpha, \beta \in K$ are linearly independent over $\mathbb{Q}$.

Let conversely $M = \mathbb{Z}\alpha + \mathbb{Z}\beta$, with $\alpha, \beta \in K$ linearly independent over $\mathbb{Q}$. Put $\gamma = \beta/\alpha$ $(\notin \mathbb{Q})$, and choose $a, b, c \in \mathbb{Z}$ such that $a\gamma^2 - b\gamma + c = 0$, $\gcd(a, b, c) = 1$. From $M = (\mathbb{Z} + \mathbb{Z}\gamma)\cdot\alpha$ and $a\gamma\cdot\gamma = b\gamma - c \subset \mathbb{Z} + \mathbb{Z}\gamma$ we see that $\mathbb{Z}[a\gamma]\cdot M = M$. Using that

$$\sigma(\gamma) = -\gamma + (b/a), \qquad \gamma\cdot\sigma(\gamma) = c/a,$$
$$\gcd(a, b, c) = 1$$

one calculates easily

$$M\cdot\sigma[M] = \mathbb{Z}[a\gamma]\cdot N(\alpha)/a, \tag{2.2}$$

so M is an invertible $\mathbb{Z}[a\gamma]$-ideal, with inverse $\sigma[M]\cdot a/N(\alpha)$. But by (2.1), the group M is an invertible ideal for at most one ring. We conclude that M is an invertible A-ideal if and only if $A = \mathbb{Z}[a\gamma]$, and, upon comparing the discriminants, if and only if $\Delta = b^2 - 4ac$.

In the sequel we shall always assume that $N(\alpha)/a > 0$. This can be achieved by changing the signs of a, b, c, if necessary. Further, we assume that in $\gamma = (b \pm \sqrt{\Delta})/(2a)$ the $+$-sign holds. This can be achieved by multiplying b and β by ± 1. We see that the invertible A-ideals are precisely the subgroups of K of the form

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

where $\alpha \in K^*$, $a, b \in \mathbb{Z}$ are such that

$$\left.\begin{aligned} &c = (b^2 - \Delta)/(4a) \in \mathbb{Z}, \qquad \gcd(a, b, c) = 1, \\ &N(\alpha)/a > 0. \end{aligned}\right\} \tag{2.3}$$

Given M, the numbers α, a, b are not unique. For α we can take any element of M that is part of a $\mathbb{Z}$-basis of M or, equivalently, that is *primitive*, i.e. does not belong to nM for any $n \in \mathbb{Z}$, $n > 1$. Given M and α, it is easy to check that a is uniquely determined, and that b is only uniquely determined modulo $2a$. Notice that $b \equiv \Delta \bmod 2$.

The *norm* $N(M)$ of $M \subset I$ is defined by $N(M) = |\det(\phi)|$, where ϕ is any $\mathbb{Q}$-linear endomorphism of K for which $\phi[A] = M$. We have $N(A\alpha) = |N(\alpha)|$ for $\alpha \in K^*$, and if M is specified by α, a, b as above, then $N(M) = N(\alpha)/a$. From (2.2) we see that

$$M\cdot\sigma[M] = A\cdot N(M).$$

It follows that $N\colon I \to \mathbb{Q}^*_{>0}$ is a group homomorphism.

Let $M_1, M_2 \in I$, and let M_i be given by α_i, a_i, b_i as above, for $i = 1, 2$. We show how to calculate $M_3 = M_1\cdot M_2$. We choose

$$\alpha_3 = \alpha_1\alpha_2/d, \tag{2.4}$$

where d is the unique positive integer for which $\alpha_1\alpha_2/d$ is a primitive element of M_3. Since $M_3 \in I$, we have

$$M_3 = (\mathbb{Z} + \mathbb{Z}\frac{b_3 + \sqrt{\Delta}}{2a_3})\cdot\alpha_3$$

for certain $a_3, b_3 \in \mathbb{Z}$ satisfying the analogue of (2.3). From $N(M_1)N(M_2) = N(M_3)$ and $N(M_i) = N(\alpha_i)/a_i$ we see that

$$a_3 = a_1a_2/d^2. \tag{2.5}$$

The equality $M_1M_2 = M_3$ now becomes

$$\begin{aligned}\mathbb{Z} + \mathbb{Z}\frac{b_1 + \sqrt{\Delta}}{2a_1} + \mathbb{Z}\frac{b_2 + \sqrt{\Delta}}{2a_2} + \mathbb{Z}\frac{\frac{1}{2}(b_1b_2 + \Delta) + \frac{1}{2}(b_1 + b_2)\sqrt{\Delta}}{2a_1a_2}\\ = \mathbb{Z}\frac{1}{d} + \mathbb{Z}\frac{b_3 + \sqrt{\Delta}}{2a_1a_2}d.\end{aligned} \tag{2.6}$$

Comparing the $\sqrt{\Delta}/2$-coordinate we see that $\mathbb{Z}a_1^{-1} + \mathbb{Z}a_2^{-1} + \frac{1}{2}(b_1 + b_2)\mathbb{Z}(a_1a_2)^{-1} = \mathbb{Z}(a_1a_2)^{-1}\cdot d$, i.e.

$$d = \gcd(a_2, a_1, \tfrac{1}{2}(b_1 + b_2)). \tag{2.7}$$

The integer b_3 is determined, modulo $2a_3$, by the property that $(b_3 + \sqrt{\Delta})d/(2a_1a_2)$ belongs to (2.6). Hence, if λ, μ, ν are integers such that

$$\lambda a_2 + \mu a_1 + \nu\tfrac{1}{2}(b_1 + b_2) = d \tag{2.8}$$

then

$$b_3 \equiv \frac{1}{d}(\lambda a_2b_1 + \mu a_1b_2 + \nu\tfrac{1}{2}(b_1b_2 + \Delta)) \bmod 2a_3. \tag{2.9}$$

From (2.7), (2.5), (2.8), (2.9) we see that a_3, b_3 can be calculated if a_1, b_1, a_2, b_2 are given. The gcd in (2.7) and integers λ, μ, ν such that (2.8) holds can be determined using the Euclidean algorithm. If in addition α_1, α_2 are given, α_3 can be calculated using (2.4). For computational purposes it is useful to note Shanks's formula [23]

$$b_3 \equiv b_2 + 2\frac{a_2}{d}(\lambda\frac{b_1 - b_2}{2} - \nu c_2) \bmod 2a_3$$

where $c_2 = (b_2^2 - \Delta)/(4a_2)$, and where $\lambda\frac{b_1 - b_2}{2} - \nu c_2$ may be taken modulo a_1/d. It is proved by eliminating μa_1 from (2.8) and (2.9).

If M is given by α, a, b, then it follows easily from (2.2) that M^{-1} is given by a/α (or $|a|/\alpha$), a, $-b$.

A *principal* A-ideal (in the strict sense) is an additive subgroup of K of the form $A\alpha$, with $\alpha \in K^*$, $N(\alpha) > 0$. The principal ideals are exactly the invertible ideals that have $a = 1$ for a suitable choice of α. They form a subgroup P of I. The *class group* C (in the strict sense) of A is defined by $C = I/P$. It is well known that this is a finite group, cf. sec. 4. Its order is called the *class number* (in the strict sense) of A, and denoted by h.

3. Quadratic forms

Let Δ be an integer. A *primitive integral binary quadratic form of discriminant* Δ is a polynomial $aX^2 + bXY + cY^2 \in \mathbb{Z}[X, Y]$ for which $\gcd(a, b, c) = 1$ and $b^2 - 4ac = \Delta$. For brevity, we shall simply speak of *forms*, or *forms of discriminant* Δ, and we impose the extra condition that $a > 0$ if $\Delta < 0$. Forms of discriminant Δ exist if and only if $\Delta \equiv 0$ or $1 \bmod 4$. From now on, we fix such an integer, and we assume for simplicity that Δ is not a square; see [4; 7] for the case that Δ is a square. We let $K = \mathbb{Q}(\sqrt{\Delta})$ and $A = \mathbb{Z}[(\Delta + \sqrt{\Delta})/2]$ be as in the preceding sections. We shall denote the form $aX^2 + bXY + cY^2$ by (a, b, c), or simply by (a, b), since c is determined by a, b and Δ.

The group $SL_2(\mathbb{Z}) = \{2\times2\text{-matrices over } \mathbb{Z} \text{ with determinant } 1\}$ acts on the right on $\mathbb{Z}[X, Y]$ as a group of ring automorphisms by $XT = tX + uY$, $YT = vX + wY$, for $T = \begin{pmatrix} t & u \\ v & w \end{pmatrix} \in SL_2(\mathbb{Z})$. This action transforms the set of forms of discriminant Δ into itself. Two forms are called *equivalent* if they are in the same orbit under $SL_2(\mathbb{Z})$. It is well known that there is a natural bijection

$$C = I/P \to \{\text{forms of discriminant } \Delta\}/SL_2(\mathbb{Z}).$$

This bijection maps the class of $M \in I$ to the $SL_2(\mathbb{Z})$-orbit of the form $N(X\alpha + Y\beta)/N(M)$, where α, β satisfy

$$M = \mathbb{Z}\alpha + \mathbb{Z}\beta, \qquad (\beta\cdot\sigma(\alpha) - \alpha\cdot\sigma(\beta))/\sqrt{\Delta} > 0. \tag{3.1}$$

If $M = (\mathbb{Z} + \mathbb{Z}(b + \sqrt{\Delta})/(2a))\alpha$ as in sec. 2, then a short calculation shows that the above form equals $aX^2 + bXY + cY^2$, where $c = (\Delta - b^2)/(4a)$. For further details, see [1].

The above bijection can be used to transport the group structure of C to the set of $SL_2(\mathbb{Z})$-orbits of forms of discriminant Δ. The product of the orbits of (a_1, b_1) and (a_2, b_2) is the orbit of (a_3, b_3), where a_3, b_3 are given by (2.7), (2.5), (2.9). The inverse of the orbit of (a, b) is the orbit of $(a, -b)$. For a different algorithm to multiply classes of quadratic forms, depending on "united" or "concordant" forms, we refer to [14, fifth supplement; 3; 7]. It will not suit our needs in sec. 8, cf. [6].

4. Reduction

A form (a, b, c) is called *reduced* if

$$\left.\begin{array}{ll} |\sqrt{\Delta} - 2|a|| < b < \sqrt{\Delta} & \text{if } \Delta > 0, \\ |b| \le a \le c & \\ b \ge 0 \text{ if } |b| = a \text{ or } a = c & \end{array}\right\} \text{ if } \Delta < 0.$$

We denote the set of reduced forms by R. For $(a, b) \in R$, we have

$$|a| < \sqrt{\Delta} \quad \text{if } \Delta > 0,$$
$$0 < a < \sqrt{|\Delta|/3} \quad \text{if } \Delta < 0.$$

It follows that the set R is *finite*.

We describe an efficient *reduction algorithm*, which for any form (a, b) of discriminant Δ produces a reduced form equivalent to it. The algorithm consists of successive applications of the following two types of elements of $SL_2(\mathbb{Z})$:

(i) $T = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}$, with $m \in \mathbb{Z}$. We have
$(a, b)T = (a, b + 2am)$.

(ii) $T = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. We have
$(a, b, c)T = (c, -b, a)$.

#Using (i), we can bring b in any interval J_a of length $2|a|$. For this interval we choose

$J_a = \{x \in \mathbf{R}: -|a| < x \le |a|\}$
if either $\Delta < 0$, or $\Delta > 0$ and $|a| \ge \sqrt{\Delta}$,

$J_a = \{x \in \mathbf{R}: \sqrt{\Delta} - 2|a| < x < \sqrt{\Delta}\}$
if $\Delta > 0$ and $|a| < \sqrt{\Delta}$.

Taking the second choice for all a, when $\Delta > 0$, as Gauss does [4; 14], leads to a worse algorithm, as was noted by Lagarias [7].

If, after this application of (i), the form (a, b) is reduced, stop. Otherwise, replace (a, b, c) by $(c, -b, a)$, using (ii), and go to #.

It can be shown that no more than $O(\max\{1, \log(|a|/\sqrt{|\Delta|})\})$ applications of (i), (ii) are needed to reduce a form (a, b) by this algorithm, cf. [7].

It follows that any form is equivalent to a reduced form. Since $\mathcal{R}$ is finite, this implies that the class number h is finite.

5. Reduced forms and the class group

Let $\Delta < 0$. In this case every form is equivalent to *exactly one* reduced form, see [14]. Hence the set $\mathcal{R}$ may be identified with the class group C. An efficient algorithm for the group multiplication $\mathcal{R} \times \mathcal{R} \to \mathcal{R}$ is obtained by combining the formulae of sec. 2 with the reduction algorithm of sec. 4. The inverse of $(a, b, c) \in \mathcal{R}$ is $(a, -b, c)$, except if $b = a$ or $a = c$, in which cases $(a, b, c)^{-1} = (a, b, c)$. This provides us with an explicit model for the class group.

Next let $\Delta > 0$. In this case it is not true that every form is equivalent to exactly one reduced form. Let $\rho: \mathcal{R} \to \mathcal{R}$ describe the effect of performing a reduction step on a form that is already reduced. More precisely, put $\rho((a, b, c)) = (c, b')$, where $b' \in J_c$, $b' \equiv -b \bmod 2c$; this form is equivalent to (a, b, c), and it belongs to $\mathcal{R}$. It can be proved that ρ is a *permutation* of $\mathcal{R}$, see [14, sec. 77]. The inverse of ρ is given by $\rho^{-1} = \tau\rho\tau$, where $\tau((a, b, c)) = (c, b, a)$. By a *cycle* of $\mathcal{R}$ we mean an orbit of $\mathcal{R}$ under the action of the powers of ρ. Since the leading coefficients alternate in sign, every cycle contains an *even* number of reduced forms.

It is a fundamental theorem that two reduced forms are equivalent if and only if they belong to the same cycle [14, sec. 82]. Hence C may be identified with the set of cycles of $\mathcal{R}$. The cycle corresponding to the neutral element of C is called the

principal cycle, notation: P; this is the cycle containing the form $(1, b_0)$, with $b_0 \in J_1$, $b_0 \equiv \Delta \bmod 2$.

The number of reduced forms in a cycle is $O(\Delta^{\frac{1}{2}+\varepsilon})$ for every $\varepsilon > 0$, by (6.2) and (11.4), and the exponent $\frac{1}{2}$ is best possible [8]. If Δ is large, it may be very difficult to decide whether two reduced forms are equivalent (see sec. 13 for an $O(\Delta^{\frac{1}{4}+\varepsilon})$-algorithm). Thus, while we can still do calculations in C using R, we have no efficient equality test. The way out of this difficulty is that, for the purposes of computation, we abandon the group C in favour of a group F, which resembles R more closely. The group F is defined in sec. 8; here we describe the phenomena that it is meant to explain.

We can define a multiplication $*: R \times R \to R$ as follows. Let (a_1, b_1), $(a_2, b_2) \in R$, and let (a_3, b_3) be defined by the formulae of sec. 2. Let $(a_4, b_4) \in R$ be the form obtained by reducing (a_3, b_3) using the algorithm of sec. 4. Then we put $(a_1, b_1) * (a_2, b_2) = (a_4, b_4)$. This multiplication satisfies the commutative law, the form $(1, b_0)$ defined above is a neutral element, and every $(a, b) \in R$ has an inverse (a, b'), with $b' \equiv -b \bmod 2a$, $b' \in J_a$. If the associative law were satisfied, then R would be a finite abelian group with subgroup $P \subset R$, and there would be an exact sequence

$$0 \to P \to R \to C \to 0.$$

It would follow that the cycles are the cosets of P, and that they all have the same cardinality. It is easy to find examples where this is not true, e.g. $\Delta = 40$. It can in fact be shown that $*$ makes R into a group if and only if all $(a, b) \in R$ are *ambiguous*, i.e. satisfy $b \equiv 0 \bmod a$. This occurs for only finitely many Δ, like $5, 8, \ldots, 5180$, which can be effectively determined if the generalized Riemann hypothesis for the L-functions $L(s, (\frac{\Delta}{\cdot}))$ is assumed.

Even if R is no group, it exhibits a certain group-like behaviour. We have, for example, an approximate associative law:

$$F * (G * H) = \rho^n((F * G) * H), \qquad \text{with } n \in \mathbb{Z}, \quad |n| \text{ "small"}, \tag{5.1}$$

for $F, G, H \in R$. Also, the cycles behave as the cosets of a cyclic

subgroup:

$$(\rho^k F) * (\rho^\ell G) = \rho^{m(k,\ell)}(F * G) \qquad \text{for } k, \ell \in \mathbb{Z}, \tag{5.2}$$

where $m(k,\ell)$ is a function of k and ℓ that exhibits certain monotonicity properties in both variables, like $k+\ell$ does. These observations are basically due to Shanks [24].

The group F to be defined in sec. 8 can be used to analyze the above situation, and in particular to prove precise versions of (5.1) and (5.2); e.g., "small" in (5.2) can be replaced by $O(\log \Delta)$, as we shall see in sec. 12.

6. The analytic class number formula

Denote by χ the Kronecker symbol $\left(\frac{\Delta}{\cdot}\right)$, and let $L(s, \chi) = \sum_{n=1}^{\infty} \chi(n) n^{-s}$ for $s \in \mathbb{C}$, $\mathrm{Re}(s) > 0$. First let $\Delta < 0$. Then we have

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

(see [14]) where w is the number of roots of unity in A; so $w = 2$ for $\Delta < -4$. The number $L(1, \chi)$ may be expressed by the slowly converging product

$$L(1, \chi) = \prod_{p \text{ prime}} \left(1 - \frac{\chi(p)}{p}\right)^{-1},$$

see [13, sec. 109]. The class number formula can be rewritten as a finite sum

$$h = \frac{w}{2} \cdot \frac{1}{2 - \chi(2)} \cdot \sum_{n=1}^{[\frac{1}{2}|\Delta|]} \chi(n)$$

if $\Delta = \Delta_0$. However, the number of terms is so large that for practical purposes the sum may be said to converge even slower than the non-absolutely converging product for $L(1, \chi)$.

Next let $\Delta > 0$. Let η be the smallest unit of A for which $\eta > 1$ and $N(\eta) = 1$. The *regulator* R (in the strict sense) of A is defined by $R = \log \eta$. The class number formula now reads

$$hR = \sqrt{\Delta} \cdot L(1, \chi)$$

(see [14]) where $L(1, \chi)$ is given by the same infinite product as above. The finite sum

$$hR = -2 \cdot \sum_{n=1}^{[\frac{1}{2}\Delta]} \chi(n) \log|1 - e^{2\pi i n/\Delta}|$$

(for $\Delta = \Delta_0$) is again useless for our purpose.

Satisfactory estimates for the rate of convergence of the

infinite product can be given if the Riemann-hypothesis for the zeta function of K is assumed. Then we have, both for $\Delta > 0$ and $\Delta < 0$:

$$\prod_{p \geq x} \left(1 - \frac{\chi(p)}{p}\right) = 1 + O(x^{-\frac{1}{2}} \cdot (\log|\Delta| + \log x)) \tag{6.1}$$

for $x \geq 2$, the constant implied by the O-symbol being absolute and effectively computable. This can be deduced from [11, theorem 1.1]; cf. [18, théorème 3].

Schur [22] proved that

$$|L(1, \chi)| < \tfrac{1}{2}\log|\Delta| + \log\log|\Delta| + 1. \tag{6.2}$$

If $\Delta > 0$, the term $\log\log|\Delta|$ can be omitted [5].

7. Shanks's algorithm for negative discriminants

Shanks described in [23] an algorithm to calculate h in the case that $\Delta < 0$. We indicate the main points of this algorithm.

Let X be some "large" integer, specified below. Calculate an integer $\tilde{h}$ that differs by at most 1 from

$$\frac{w\sqrt{|\Delta|}}{2\pi} \cdot \prod_{p \text{ prime},\ p < X} \left(1 - \frac{\chi(p)}{p}\right)^{-1}.$$

Then we expect that

$$h \text{ is "close" to } \tilde{h}. \tag{7.1}$$

Select a form $F \in \mathcal{R}$. By Lagrange's theorem in group theory, we have

$$F^h = 1, \tag{7.2}$$

where 1 denotes the unit element of $\mathcal{R}$. We try to determine h by combining (7.1) and (7.2). More specifically, we calculate $F^{\tilde{h}}$ and search for an integer n with

$$F^{\tilde{h}} = F^n, \qquad |n| \text{ "small"}. \tag{7.3}$$

Then $\tilde{h} - n$ is a likely value for h. Searching among the divisors of $\tilde{h} - n$, we can determine the order e of F in the group $\mathcal{R}$. If e is large, which it usually is, then $\tilde{h} - n$ is the only multiple of e that is sufficiently close to $\tilde{h}$, and we must have $h = \tilde{h} - n$. In that case we are done. If, on the other hand, e is small, then we select a second form $G \in \mathcal{R}$ and determine the order of the subgroup of $\mathcal{R}$ generated by F and G in a like manner. We proceed until a subgroup $S \subset \mathcal{R}$ has been found for which only one multiple of $\#S$ is sufficiently close to $\tilde{h}$ to be equal to h.

The exact meaning of "large", "close", "small" in the above

algorithm depends on how well one is able to estimate the convergence of the infinite product in sec. 6. Let us assume that (6.1) holds. Then we take for X an integer of order of magnitude $|\Delta|^{1/5}$. Let $\varepsilon > 0$ be an arbitrary real number. The calculation of $\tilde{h}$ can then be done in $O(|\Delta|^{(1/5)+\varepsilon})$ steps. From (6.1) and (6.2) we get

$$|h - \tilde{h}| \leq Y \qquad \text{with} \quad Y = O(|\Delta|^{(2/5)+\varepsilon}),$$

and this inequality can be made completely explicit. The calculation of $F^{\tilde{h}}$, for $F \in R$, can be done in $O(|\Delta|^{\varepsilon})$ steps, by repeated squarings and multiplications using the binary representation of $\tilde{h}$. Searching for n as in (7.3), with "small" now meaning "$\leq Y$", requires $O(|\Delta|^{(2/5)+\varepsilon})$ steps if one proceeds in the naive way. A significant improvement is made possible by using Shanks's "baby step - giant step" technique: if we write $n = iy + j$, where y has order of magnitude $\sqrt{2Y}$ and $|i|, |j| \leq \frac{1}{2}y = O(|\Delta|^{(1/5)+\varepsilon})$, then (7.3) can be rewritten as

$$F^{\tilde{h}} \cdot F^{-iy} = F^{j}.$$

So we just have to multiply $F^{\tilde{h}}$ by small powers of $F^{\pm y}$, and wait until a small power of F appears; here the small powers of F are assumed to be calculated beforehand. In this way, determining n as in (7.3) can be done in $O(|\Delta|^{(1/5)+\varepsilon})$ steps. Factoring $\tilde{h} - n$ can be done in $O(|\Delta|^{(1/8)+\varepsilon})$ steps, see [19]. If $e = \text{order}(F)$ is larger than $|n| + Y$ then we must have $h = \tilde{h} - n$, and we are done. So let e be smaller; then $e = O(|\Delta|^{(2/5)+\varepsilon})$, and we have to proceed with a second form G. We have to determine the earliest power of G that is in the subgroup generated by F. By a strategy similar to the baby step - giant step technique this can be done in $O(|\Delta|^{(1/5)+\varepsilon})$ steps. In the same way we proceed with further forms, if necessary.

Assuming some extra Riemann hypotheses, besides those needed for (6.1), one can show that the selection of the forms F, G, ... can be done in such a way that no more than $O((\log|\Delta|)^2)$ forms need be considered, see [10, Cor. 1.3].

We conclude that, modulo the Riemann hypotheses, the above method determines h in $O(|\Delta|^{(1/5)+\varepsilon})$ steps, for every $\varepsilon > 0$. If one does not stop before F, G, ... generate the entire class

group, one obtains an algorithm that determines the structure of the class group which runs in $O(|\Delta|^{(1/4)+\varepsilon})$ steps. In the present case of negative discriminants there is an additional technique, employing the decomposition of the class group in its p-primary subgroups, that reduces the exponent 1/4 to 1/5 in many cases; cf. [23, sec. 3]. This technique is, however, far less useful in the case of positive discriminants.

8. The group F

Let Γ denote the subgroup $\{\begin{pmatrix}1 & m\\ 0 & 1\end{pmatrix}: m \in \mathbb{Z}\}$ of $SL_2(\mathbb{Z})$. It is easy to see that two forms (a, b) and (a', b') are in the same orbit under Γ if and only if

$$a = a', \qquad b \equiv b' \bmod 2a.$$

We denote the orbit space $\{\text{forms of discriminant } \Delta\}/\Gamma$ by F. Each orbit contains exactly one form (a, b) with b belonging to the interval J_a defined in sec. 4. It will be convenient to identify F with the set of such forms.

From $\Gamma \subset SL_2(\mathbb{Z})$ we see that there is a natural surjective map $F \to \{\text{forms}\}/SL_2(\mathbb{Z}) \cong C$. We claim that there is a natural group law on F that makes this map into a group homomorphism. The easiest way to see this is, again, to use the connection with invertible ideals.

Consider the group $I \oplus (K^*/\mathbb{Q}^*_{>0})$ with I as in sec. 2. Elements of this group are pairs $(M, \alpha\mathbb{Q}^*_{>0})$ with $M \in I$ and $\alpha \in K^*$, and α can, in its coset mod $\mathbb{Q}^*_{>0}$, be uniquely chosen such that it is a primitive element of M. Choose $\beta \in M$ such that (3.1) holds; it is unique up to translation by $\mathbb{Z}\alpha$. Mapping the pair $(M, \alpha\mathbb{Q}^*_{>0})$ to the Γ-orbit of the form $N(X\alpha + Y\beta)/N(M)$, as in sec. 3, now defines a surjective map

$$I \oplus (K^*/\mathbb{Q}^*_{>0}) \to F.$$

Using that the form $N(X\alpha + Y\beta)/N(M)$ equals (a, b), where $\beta/\alpha = (b + \sqrt{\Delta})/(2a)$, one checks that two pairs $(M, \alpha\mathbb{Q}^*_{>0})$ and $(M', \alpha'\mathbb{Q}^*_{>0})$ have the same image in F if and only if there exists $\gamma \in K^*$ such that

$$\gamma M = M', \qquad \gamma\alpha\mathbb{Q}^*_{>0} = \alpha'\mathbb{Q}^*_{>0}, \qquad N(\gamma) > 0.$$

So if we embed $K^*_{N>0} = \{\gamma \in K^*: N(\gamma) > 0\}$ in $I \oplus (K^*/\mathbb{Q}^*_{>0})$ by

mapping γ to $(A\gamma, \gamma\mathbb{Q}^*_{>0})$, then we get a bijection

$$(I \oplus (K^*/\mathbb{Q}^*_{>0}))/K^*_{N>0} \to F.$$

The left hand side is a group, hence so is the right hand side, by transport of structure. Multiplication and inversion in F can be done by the formulae of sec. 2. We shall denote the unit element of F by 1; it is (the Γ-orbit of) the form $(1, b_0)$ with $b_0 \in J_1$, $b_0 \equiv \Delta \bmod 2$. It is obvious that the natural map $F \to C$ is a group homomorphism.

9. The algebraic structure of F

Some easy diagram chasing gives rise to an exact sequence

$$0 \to I/\mathbb{Q}^*_{>0} \to F \xrightarrow{\psi} K^*/K^*_{N>0} \to 0.$$

Here $\mathbb{Q}^*_{>0}$ is embedded in I by mapping x to Ax. To describe ψ, we first note that

$$K^*/K^*_{N>0} \cong \begin{cases} 0 & \text{if } \Delta < 0, \\ \{\pm 1\} & \text{if } \Delta > 0. \end{cases} \tag{9.1}$$

So ψ is trivial if $\Delta < 0$. If $\Delta > 0$, then ψ corresponds to the map sending (a, b) to $\operatorname{sign}(a)$.

We claim that the above exact sequence splits. This is clear if $\Delta < 0$, and if $\Delta > 0$ we can map the non-trivial element of $K^*/K^*_{N>0}$ to the element E of F corresponding to $(A, \sqrt{\Delta}\mathbb{Q}^*_{>0}) \in I \oplus (K^*/\mathbb{Q}^*_{>0})$; explicitly, E is the Γ-orbit of

$$(-\Delta, \Delta, (1-\Delta)/4) \qquad \text{if } \Delta \text{ is odd,}$$

$$(-\Delta/4, 0, 1) \qquad \text{if } \Delta \text{ is even.}$$

(We could also have used the form $(-1, b_0)$ to split the sequence, but E is more convenient in the sequel.) We have proved

$$F \cong (K^*/K^*_{N>0}) \oplus (I/\mathbb{Q}^*_{>0}). \tag{9.2}$$

The group $I/\mathbb{Q}^*_{>0}$ can be analyzed by standard techniques from commutative algebra. Let A_p denote the semilocal ring $\{r/s: r \in A, s \in \mathbb{Z}, s \not\equiv 0 \bmod p\}$. Then we have $I \cong \oplus_{p \text{ prime}} (K^*/A^*_p)$, and

$$I/\mathbb{Q}^*_{>0} \cong \oplus_{p \text{ prime}} (K^*/\langle p\rangle A^*_p) \tag{9.3}$$

where $\langle p\rangle$ denotes the subgroup of K^* generated by p. The groups $K^*/\langle p\rangle A^*_p$ can be calculated explicitly. The result, which will not be used in the sequel, is as follows.

Write $\Delta = f^2 \cdot \Delta_0$ as in sec. 1, and let k be the number of

factors p in f. The character χ is as in sec. 6, and χ_0 is the corresponding character for Δ_0. If $k = 0$ we have

$$K^*/\langle p\rangle A_p^* \cong \mathbb{Z} \quad \text{if } \chi(p) = 1,$$
$$\cong 0 \quad \text{if } \chi(p) = -1,$$
$$\cong \mathbb{Z}/2\mathbb{Z} \quad \text{if } \chi(p) = 0.$$

Next let $k > 0$. In most cases we have

$$K^*/\langle p\rangle A_p^* \cong \mathbb{Z} \oplus (\mathbb{Z}/(p-1)p^{k-1}\mathbb{Z}) \quad \text{if } \chi_0(p) = 1,$$
$$\cong \mathbb{Z}/(p+1)p^{k-1}\mathbb{Z} \quad \text{if } \chi_0(p) = -1,$$
$$\cong (\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/p^k\mathbb{Z}) \quad \text{if } \chi_0(p) = 0.$$

The precise list of exceptions is as follows. The group $K^*/\langle p\rangle A_p^*$ is isomorphic to

$\mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/2^{k-2}\mathbb{Z})$ if $p = 2$, $k > 2$ and $\chi_0(2) = 1$;

$(\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/3\cdot 2^{k-2}\mathbb{Z})$ if $p = 2$, $k > 2$ and $\chi_0(2) = -1$;

$\mathbb{Z}/4\mathbb{Z}$ if $p = 2$, $k = 1$ and $\Delta_0 \equiv -4 \bmod 16$;

$(\mathbb{Z}/4\mathbb{Z}) \oplus (\mathbb{Z}/2^{k-1}\mathbb{Z})$ if $p = 2$, $k > 2$ and $\Delta_0 \equiv -4 \bmod 32$;

$(\mathbb{Z}/3\mathbb{Z}) \oplus (\mathbb{Z}/2\cdot 3^{k-1}\mathbb{Z})$ if $p = 3$, $k > 1$ and $\Delta_0 \equiv -3 \bmod 9$.

Combining this description of $K^*/\langle p\rangle A_p^*$ with (9.2), (9.1) and (9.3) we obtain an algebraic description of F. In particular, we see that F is the direct sum of a finite group and a free abelian group of countably infinite rank. The natural action of σ (see sec. 1) on F is given by $\sigma(F) = F^{-1}$, for $F \in F$.

10. The topological structure of F

From this point onward we assume that Δ is positive. The case of negative Δ is similar, but will not be needed in the sequel.

The group homomorphism $F \to C$ defined in sec. 8 maps the coset $(M, \alpha\mathbb{Q}_{>0}^*)K_{N>0}^*$ to the ideal class of M. We denote by G the kernel of this homomorphism. The coset of $(M, \alpha\mathbb{Q}_{>0}^*)$ belongs to G if and only if $M = A\beta$ for some $\beta \in K_{N>0}^*$, so, dividing by β:

$$G = \{(A, \gamma\mathbb{Q}_{>0}^*)K_{N>0}^* : \gamma \in K^*\}.$$

For $\gamma_1, \gamma_2 \in K^*$ we have $(A, \gamma_1\mathbb{Q}_{>0}^*)K_{N>0}^* = (A, \gamma_2\mathbb{Q}_{>0}^*)K_{N>0}^*$ if and only if $\gamma_1\mathbb{Q}_{>0}^* = \zeta\gamma_2\mathbb{Q}_{>0}^*$ for some $\zeta \in A^*$ with $N(\zeta) = +1$. From this it follows that the map

$$d: G \to \mathbb{R}/R\mathbb{Z}$$
$$d((A, \gamma\mathbb{Q}_{>0}^*)K_{N>0}^*) = (\tfrac{1}{2}\log|\gamma/\sigma(\gamma)| \bmod R)$$

is a well defined group homomorphism; here R is the regulator of A, defined in sec. 6. The map d is a small modification of the "distance" defined by Shanks [24]. We have $\ker(d) = \{1, E\}$, with E as defined in sec. 9. It follows that the map

$$G \to (\mathbb{R}/R\mathbb{Z}) \oplus \{\pm 1\}$$

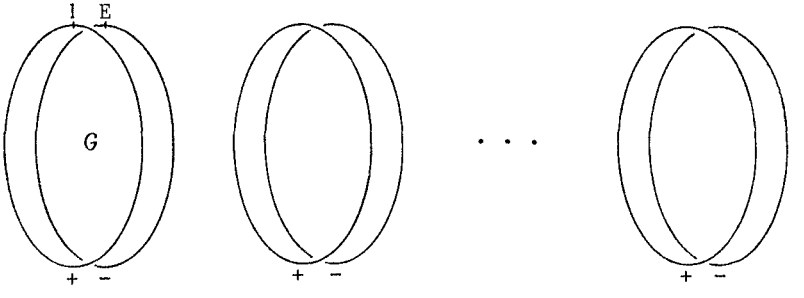
obtained by combining d with the map ψ from sec. 9 is an *injective* group homomorphism. For cardinality reasons it is not surjective. However, its image is *dense* in $(\mathbb{R}/R\mathbb{Z}) \oplus \{\pm 1\}$; this follows from the fact that G is infinite (sec. 9), and it can also be seen directly.

We conclude that G may be considered as a dense subgroup of the product of a circle group of 'circumference' R and a group of order two. The h cosets of G in F may be considered as the cosets of such a subgroup. A coset of G in F will be called a *cycle* of F, and G itself is the *principal cycle*. The agreement with the terminology introduced in sec. 5 is intentional, and will be justified in sec. 11. Every cycle consists of two *circles*, a *positive* and a *negative* circle, containing forms with positive and negative leading coefficients, respectively; cf. figure 1.

If $F_1, F_2 \in F$ belong to the same cycle, the *distance* from F_1 to F_2 is defined to be $d(F_2 F_1^{-1})$, which is a real number modulo R. The distance is zero if and only if $F_1 = F_2$ or $F_1 = F_2 \cdot E$. If $F_1, F_2 \in F$ do not belong to the same cycle, the distance from F_1 to F_2 is not defined.

Replacing G by the full group $(\mathbb{R}/R\mathbb{Z}) \oplus \{\pm 1\}$, and similarly with the cosets, we obtain an embedding of F as a dense

Figure 1. F.



subset in a compact topological space $\bar{F}$. It is not difficult to see that the group multiplication of F can be extended to $\bar{F}$, making it into a topological group. This can be done using fibred sums, or by defining $\bar{F} = (I \oplus ((K \otimes_{\mathbb{Q}} \mathbb{R})^* / \mathbb{R}^*_{>0}))/K^*_{N>0}$. It is of interest to notice that the group $\bar{F}$ can also be described as a certain group of idele classes of K, as follows. For background, see [2].

Let $\hat{A} = \varprojlim A/nA$ be the profinite completion of A, with n ranging over the positive integers. We may consider $\hat{A}$ as a subring of the restricted product $\Pi'_v K_v$, with v ranging over the finite places of K and K_v denoting the completion of K at v. Hence $\hat{A}^*$ may be considered as a subgroup of $\Pi'_v K^*_v$; for example, if $A = A_0$ (see sec. 1) then $\hat{A}^* = \Pi_v U_v$, where U_v consists of the local units at v. Adding 1's at the infinite places, we may consider $\hat{A}^*$ as a subgroup of the group J^1_K of ideles of K satisfying the product formula. Now we have

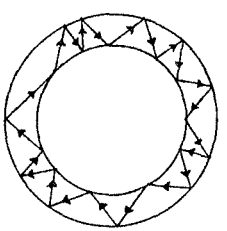
$$\bar{F} \cong J^1_K/(K^*_{N>0} \cdot \hat{A}^*). \tag{10.1}$$

This group is very similar to the group $J^1_K/(K^* \cdot \Pi_v U_v)$, the compactness of which is equivalent to the conjunction of the Dirichlet unit theorem and the finiteness of the class number. The isomorphism (10.1), which will not be used in the sequel, indicates what is the right generalization of F for algebraic number fields of higher degrees.

11. Reduced forms in F

Since no two forms in R are in the same orbit under Γ, we may consider R as a subset of F. By the fundamental theorem quoted in sec. 5, the cycles of R are precisely the intersections of the cycles of F with R; in particular, we have $P = G \cap R$. In fact, the cyclical structure of each cycle of R is reflected by the way it is sitting in the corresponding cycle of F, as suggested by fig. 2. More precisely, if $F \in R$, then $\rho(F)$ is the first element of R that is

Figure 2.



encountered if the two circles are simultaneously traversed in the positive direction, starting from F; this fixes $\rho(F)$ uniquely in the sense that for no $G \in \mathcal{R}$ one also has $G \cdot E \in \mathcal{R}$; and, finally, it is automatic that F and $\rho(F)$ are on different circles. The last statement reflects the fact that the sign of the leading coefficient is changed if ρ is applied.

The proof of these statements can most conveniently be given by interpreting $\mathcal{R}$ and ρ in terms of lattice points on the boundary of the convex hull of the totally positive part of a lattice in $\mathbb{R}^2$. We do not go into the details. The fundamental theorem quoted in sec. 5 is a consequence of the above results.

We calculate the distance from $F = (a, b) \in \mathcal{R}$ to $\rho(F)$. Let F correspond to the coset $(M, \alpha\mathbb{Q}^*_{>0})K^*_{N>0}$. Choosing α primitive in M we then have

$$M = \mathbb{Z}\alpha + \mathbb{Z}\beta, \qquad (\beta\sigma(\alpha) - \alpha\sigma(\beta))/\sqrt{\Delta} > 0,$$
$$aX^2 + bXY + cY^2 = N(X\alpha + Y\beta)/N(M).$$

Applying ρ means first applying the element $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ of $SL_2(\mathbb{Z})$ and next an element of Γ. The latter element does not change the Γ-orbit, so we only have to investigate the effect of $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. This changes the form into $N(X\beta - Y\alpha)/N(M)$, corresponding to the coset $(M, \beta\mathbb{Q}^*_{>0})K^*_{N>0}$. Since $(M, \beta\mathbb{Q}^*_{>0})(M, \alpha\mathbb{Q}^*_{>0})^{-1} = (A, (\beta/\alpha)\mathbb{Q}^*_{>0})$ and $\beta/\alpha = (b + \sqrt{\Delta})/(2a)$, we find that the distance from F to $\rho(F)$ is given by

$$d(\rho(F)F^{-1}) = \tfrac{1}{2}\log\left|\frac{\beta/\alpha}{\sigma(\beta/\alpha)}\right| = \tfrac{1}{2}\log\left|\frac{b + \sqrt{\Delta}}{b - \sqrt{\Delta}}\right|,$$

taken modulo R.

It is of interest to determine upper and lower bounds for this quantity. Since $0 < b < \sqrt{\Delta}$ for a reduced form (a, b), we have

$$\tfrac{1}{2}\log\left|\frac{b + \sqrt{\Delta}}{b - \sqrt{\Delta}}\right| = \tfrac{1}{2}\log\left|\frac{(b + \sqrt{\Delta})^2}{4ac}\right| < \tfrac{1}{2}\log\Delta. \qquad (11.1)$$

Using that $b \geq 1$ one can prove the lower bound $\Delta^{-\frac{1}{2}}$, but this is useless. A more satisfactory lower bound is obtained by considering the distance traversed if ρ is applied *twice*, i.e. from F to $\rho^2(F)$. Let, with the notation as before, ρ map the coset of $(M, \alpha\mathbb{Q}^*_{>0})$ to the coset of $(M, \beta\mathbb{Q}^*_{>0})$, and similarly $(M, \beta\mathbb{Q}^*_{>0})$ to $(M, \gamma\mathbb{Q}^*_{>0})$. Using the geometrical interpretation with convex hulls that we suppressed it is quite easy to see that $|\gamma| > 2|\alpha|$ and

$|\sigma(\gamma)| < \frac{1}{2}|\sigma(\alpha)|$, so $\frac{1}{2}\log\left|\frac{\gamma/\alpha}{\sigma(\gamma/\alpha)}\right| > \log 2$. This gives the following lower bound for the distance traversed if ρ is applied twice:

$$\frac{1}{2}\log\left|\frac{b+\sqrt{\Delta}}{b-\sqrt{\Delta}}\right| + \frac{1}{2}\log\left|\frac{b'+\sqrt{\Delta}}{b'-\sqrt{\Delta}}\right| > \log 2, \tag{11.2}$$

where $\rho((a, b)) = (c, b')$. A heuristic argument suggests that the average of $\frac{1}{2}\log|(b+\sqrt{\Delta})/(b-\sqrt{\Delta})|$ over all reduced forms should be somewhere near Lévy's constant $\pi^2/(12\cdot\log 2) = 1.18656911\ldots$.

Since the circumference of the whole cycle is R, we have

$$R = \Sigma\ \frac{1}{2}\log\left|\frac{b+\sqrt{\Delta}}{b-\sqrt{\Delta}}\right|, \tag{11.3}$$

the sum ranging over the reduced forms (a, b) belonging to a fixed cycle. If there are ℓ reduced forms in the cycle, the above inequalities yield

$$\tfrac{1}{2}\ell\cdot\log 2 < R < \tfrac{1}{2}\ell\cdot\log\Delta. \tag{11.4}$$

Therefore, if two cycles of $\mathcal{R}$ contain ℓ_1 and ℓ_2 forms, respectively, we have

$$\ell_1/\ell_2 < \frac{\log\Delta}{\log 2}.$$

This is an explicit version of a theorem of Skubenko, asserting that $\ell_1/\ell_2 = O(\log\Delta)$, see [27; 15, pp. 558, 586]. I am indebted to A. Schinzel for mentioning this theorem to me.

12. Reduction in $\mathcal{F}$

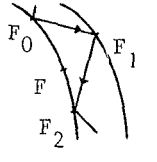
The reduction algorithm of sec. 4 can be formulated as follows. Extend the map $\rho: \mathcal{R} \to \mathcal{R}$ to a map $\rho: \mathcal{F} \to \mathcal{F}$ by

$$\rho((a, b, c)) = (c, b'), \qquad b' \equiv -b \bmod 2c, \qquad b' \in J_c,$$

where we assumed that $b \in J_a$. As in the previous section, one shows that applying ρ comes down to moving along the cycle over a distance of $\frac{1}{2}\log|(b+\sqrt{\Delta})/(b-\sqrt{\Delta})| = \log|(b+\sqrt{\Delta})/\sqrt{|4ac|}|$; also, if $|b| < \sqrt{\Delta}$, one changes to the companion circle. The reduction map $\rho_0: \mathcal{F} \to \mathcal{R}$ is defined by $\rho_0(F) = \rho^k(F)$, where k is the least non-negative integer for which $\rho^k(F)$ is reduced. Clearly, ρ_0 is the identity on $\mathcal{R}$.

The map ρ_0 assigns to every form in $\mathcal{F}$ a form in $\mathcal{R}$ that is "not too far away" from it. More precisely, let F_0, F_1, F_2 be three consecutive forms on a cycle of $\mathcal{R}$ (possibly $F_0 = F_2$), and let $F \in \mathcal{F}$ be in the interval

Figure 3.



between F_0 and F_2 that is opposite to F_1. Then it can be shown that $\rho_0(F)$ is one of F_0, F_1, F_2. By (11.1) it follows from this, that the distance from F to $\rho_0(F)$ is at most $\log \Delta$ in absolute value. A more detailed analysis shows, in fact, that

$$|d(\rho_0(F)F^{-1})| < \tfrac{1}{2}\log(1 + \theta\sqrt{\Delta}) \quad \text{for all } F \in \mathcal{F}, \tag{12.1}$$

where $\theta = (1 + \sqrt{5})/2$ and $|x| = \min\{|y|: y \in x\}$ for $x \in \mathbb{R}/R\mathbb{Z}$. This is usually very small with respect to R, the circumference of the cycle, which may have order of magnitude $\Delta^{\frac{1}{2}}$.

The multiplication $*$ on $\mathcal{R}$ defined in sec. 5 is just multiplication in $\mathcal{F}$ followed by the reduction map ρ_0. This remark, and the inequalities (11.2) and (12.1), easily imply the approximate associative law (5.1), with $|n| < 1 + 4\log(1 + \theta\sqrt{\Delta})/\log 2$. We leave the pleasure of investigating the properties of $m(k,\ell)$ in (5.2) to the reader.

13. The algorithm for positive discriminants

We shall mainly be concerned with the calculation of the regulator R, which is the circumference of each circle. It can be determined by applying the powers of ρ to a fixed form $F \in \mathcal{R}$, until we find $\rho^{\ell}(F) = F$, and then using (11.3). This is essentially the classical algorithm, which is often phrased in terms of continued fractions. It has running time $O(\Delta^{\frac{1}{2}+\varepsilon})$ for every $\varepsilon > 0$.

We describe two more efficient methods, which make use of the function d defined in sec. 10. The calculations are all done in the principal cycle G, and mostly in $P = G \cap \mathcal{R}$. A form $F \subset G$ is not only specified by its coefficients a, b, but also by a real parameter δ which is such that $d(F) = (\delta \bmod R)$. It is not easy to read δ directly from the coefficients, but one can keep track of δ under all operations built up from ρ and multiplication and inversion in $\mathcal{F}$, by the following rules:

$1 = (1, b_0)$ has $\delta = 0$;

when applying ρ to (a, b), add $\tfrac{1}{2}\log\left|\dfrac{b + \sqrt{\Delta}}{b - \sqrt{\Delta}}\right|$ to δ;

when multiplying in $\mathcal{F}$, add up both δ's;

when inverting in $\mathcal{F}$, change the sign of δ.

In particular, we can keep track of δ under the composition

$*: \mathcal{P} \times \mathcal{P} \to \mathcal{P}$ from sec. 5.

The inequality $R < \sqrt{\Delta} \cdot \log \Delta$ (see (6.2)) and the baby step - giant step technique now lead to an $O(\Delta^{(1/4)+\varepsilon})$-determination of R, as follows. Starting from the unit form $(1, b_0)$ we build up a stock of forms by successive applications of ρ ("baby steps"), until one of two things happens. It may happen, that (i) a form (a, b) $(\neq (1, b_0))$ is encountered that is its own inverse, i.e. for which a divides b; in that case, R is twice the current δ, and we stop. But for most large Δ it happens sooner, that (ii) one finds a form with $\delta \geq \delta_0 = (\sqrt{\Delta} \cdot \log \Delta)^{\frac{1}{2}}$. By (11.2), this happens after at most $1 + (2\delta_0/\log 2) = O(\Delta^{(1/4)+\varepsilon})$ applications of ρ. At this moment, we have a stock of forms that, together with their inverses, cover an interval of length $\geq 2\delta_0$ along the principal cycle. Now we start taking "giant steps", with step length a little bit less than $2\delta_0$. More precisely, by $*$-squaring the current form, and applying a small power of ρ^{-1}, one determines a form $F \in \mathcal{P}$ whose δ satisfies

$$2\delta_0 - \tfrac{1}{2}\log(1 + \theta\sqrt{\Delta}) - \tfrac{1}{2}\log \Delta < \delta \leq 2\delta_0 - \tfrac{1}{2}\log(1 + \theta\sqrt{\Delta}).$$

The giant steps are taken by calculating $F^{*1} = F$, $F^{*2} = F * F$, ..., $F^{*(i+1)} = F * (F^{*i})$, ... Our inequalities guarantee that the "step length", i.e. the distance from F^{*i} to $F^{*(i+1)}$, is for all i between δ_0 and $2\delta_0$. Hence after $O(R/\delta_0) = O(\Delta^{\frac{1}{4}+\varepsilon})$ giant steps we have traversed the entire cycle, and we will discover F^{*i} among our "baby" forms and their inverses. Then we have two values of δ for the same form, and the difference of these values is the regulator.

The above algorithm calculates the regulator to any prescribed precision in $O(\Delta^{(1/4)+\varepsilon})$ steps. The fundamental unit $\eta = e^R = (u + v\sqrt{\Delta})/2$ cannot be calculated in $O(\Delta^{(1/4)+\varepsilon})$ steps; in fact, since R ($\approx$ number of decimal digits of u and v) is often of order of magnitude $\Delta^{\frac{1}{2}}$, one cannot even write down η in time less than that, let alone calculate it. It is, however, possible to calculate u and v modulo any fixed positive integer m in time $O(\Delta^{(1/4)+\varepsilon})$, the implied constant depending on m, by a procedure similar to the above one, cf. [9]. The same remarks apply to the algorithm described below.

If the generalized Riemann hypothesis is assumed, we can give an $O(\Delta^{(1/5)+\varepsilon})$-algorithm for the calculation of R. The procedure is analogous to the determination of the order of F in the case $\Delta < 0$, see sec. 7, so we only sketch the main points. Using the class number formula, we find a number

$$\tilde{R} = \sqrt{\Delta} \cdot \prod_{p \text{ prime},\ p < X} \left(1 - \frac{\chi(p)}{p}\right)^{-1}, \qquad X \approx \Delta^{1/5}, \tag{13.1}$$

that is close to an integer multiple hR of R, the difference being $O(\Delta^{(2/5)+\varepsilon})$. The baby forms are now made as above, but with $\delta_0 \approx \Delta^{(1/5)+\varepsilon}$. Next, by repeated squarings and multiplications in P, we jump to a form F whose δ is close to $\tilde{R}$. Taking giant steps from this F, in both directions, we encounter a form that is already in the "baby" stock. That gives two δ's for the same form, and the difference $R^{\#}$ is an unknown integer multiple $\tilde{h}R$ of the regulator; here $\tilde{h}$ is supposedly not far from h. If $\tilde{h}$ is large ($\gtrsim \Delta^{1/10}$), this is discovered by finding another match after taking some more giant steps. The remaining cases $\tilde{h} \lesssim \Delta^{1/10}$ are checked by looking if the unit form $(1, b_0)$ is found at distance $\frac{1}{m}R^{\#}$ from itself, for $1 < m \lesssim \Delta^{1/10}$. We notice that the latter technique can also be applied in the case $\Delta < 0$, to avoid factoring.

This finishes our sketchy description of the algorithm to determine R. We notice that the Riemann hypothesis is only needed to guarantee the efficiency of the algorithm; once the answer is found, its correctness does not depend on any unproved assumptions.

The determination of the class number h now runs exactly as in the case $\Delta < 0$, with P and R playing the role of the subgroup generated by F, in sec. 7, and its order. If R is sufficiently large, h is determined by the class number formula. Otherwise, select a form $G \in R$, and determine its order in F/G. In this fashion one proceeds until a large enough subgroup of F/G has been determined to fix h uniquely.

In this procedure one needs an algorithm that tests if a given reduced form belongs to the principal cycle. By the baby step - giant step technique this can be done in $O(R^{\frac{1}{2}}\Delta^{\varepsilon})$ steps. In particular, equivalence of two reduced forms can be tested in $O(\Delta^{(1/4)+\varepsilon})$ steps.

The conclusion is exactly as in the case $\Delta < 0$. Modulo the Riemann hypotheses, h can be determined in $O(\Delta^{(1/5)+\varepsilon})$ steps, but the structure of the class group may take $O(\Delta^{(1/4)+\varepsilon})$ steps.

We have only considered the regulator, class number and class group in the *strict* sense. To obtain the regulator R', class number h' and class group C' in the *ordinary* sense, one has to look halfway the principal cycle, i.e. at distance $\frac{1}{2}R$ from the unit form $(1, b_0)$. If at this point the form $(-1, b_0)$ is found, then

$$R' = \tfrac{1}{2}R, \qquad h' = h, \qquad C' = C.$$

Otherwise, one finds halfway $\mathcal{P}$ a form $F = (a, b)$ with $|a| > 1$ and $b \equiv 0 \bmod a$. Then $|a|$ is a non-trivial factor of Δ, and one has

$$R' = R, \qquad h' = \tfrac{1}{2}h, \qquad C' = C/C_0$$

where $C_0 \subset C$ is the subgroup of order two generated by the class of the form $(-1, b_0)$.

The distance of two reduced froms (a, b) and (a', b') is an integer multiple of R' if and only if $|a| = |a'|$ and $b = b'$. This implies that the role of R in the above algorithm can also be played by R'. In particular, we can replace $\tilde{R}$ by $\frac{1}{2}\tilde{R}$, which is close to the integer multiple h'R' of R'. I am indebted to R. Tijdeman for this observation.

14. A numerical example

The algorithms described in sections 7 and 13 have been programmed in Amsterdam by R.J. Schoof on the CDC Cyber 750 computer system, for discriminants of up to 28 digits [21]. Using only a hand held calculator like the HP67 one can deal with discriminants of up to 10 digits. For much smaller discriminants - up to 6 digits, roughly - it is often faster to apply the classical algorithm (see sec. 13).

We give an example which was calculated using an HP67. Let $\Delta = 40919537$. In table 1 one finds forms lying on the principal cycle $\mathcal{P}$ belonging to this discriminant. The first column gives an identification number to each form. In the text below, form #n is indicated by F_n. The second column shows how the form is obtained

from previous forms in the table. Here ρ and the multiplication $*$ are as in sec. 5, and $\div$ is multiplication with the inverse. The next two columns contain the coefficients a, b of the form. The final column gives δ, the distance from F_1 to the form, rounded to five decimals from the value given by the calculator.

Table 1. $\Delta = 40919537$.

# def.	a	b	δ
1 = unit	1	6395	0
2 = ρ(1)	-5878	5361	4.42393
3 = ρ(2)	518	6035	5.63858
4 = ρ(3)	-2171	2649	7.40699
5 = ρ(4)	3904	5159	7.84756
6 = ρ(5)	-916	5833	8.96447
7 = ρ(6)	1882	5459	10.50290
8 = ρ(7)	-1477	6357	11.77140
9 = ρ(8)	86	6371	14.65578
10 = ρ(9)	-959	5137	17.75720
11 = ρ(10)	3788	2439	18.86435
12 = ρ(11)	-2308	2177	19.26591
13 = ρ(12)	3919	5661	19.62037
14 = ρ(13)	-566	5659	21.01860
15 = ρ(14)	3929	2199	22.41539
16 = ρ(15)	-2296	2393	22.77375
17 = ρ(16)	3832	5271	23.16692
18 = ρ(17)	-857	5013	24.33607
19 = ρ(18)	4606	4199	25.39088
20 = ρ(19)	-1264	5913	26.17737
21 = ρ(20)	1178	5867	27.79557
22 = 19*19	7	6385	51.50454
23 = 22*22	49	6385	103.00908
24 = 23*23	2401	2465	206.01816
25 = 23*24	-157	6151	308.07526
26 = 25*25	-172	6113	617.15922
27 = 26*26	2654	2391	1234.67199
28 = 27*27	-364	6159	2469.19812
29 = 28*28	-137	6371	4936.94461
30 = 29*29	-512	5671	9873.63784
31 = 30÷22	-3584	4647	9822.13330
32 = 31÷22	1586	3695	9770.79649
33 = 32÷22	-614	6129	9719.95084
34 = 33÷22	2294	3371	9668.63890
35 = 34÷22	2857	3553	9616.67814
36 = 35÷22	562	5345	9566.02209
37 = 36÷22	3934	1973	9514.51755
38 = 30*22	-3584	5671	9925.14238
39 = 38*22	-3581	1479	9976.97826
40 = 39*22	86	6371	10027.06848
41 = 29*22	-959	6371	4988.44915
42 = 28*21	-842	5735	2496.66310
43 = 42*3	794	5003	2502.05241
44 = ρ(43)	-5003	5003	2503.10318
45 = 36÷27	-1477	5459	8331.90585
46 = 37÷22	-56	6343	9461.41380
47 = 46÷22	-8	6391	9409.90926

Taking $X = 100$ in (13.1) we find $\tilde{R} = 9839.22$. Baby steps are taken from F_1 to F_{21}. Then we jump to F_{30}, which has $\delta \approx \tilde{R}$. Taking giant steps backward (F_{30} to F_{37}) we find no baby form, but going forward (F_{38} to F_{40}) we find one after three steps: $F_{40} = F_9$. Therefore R divides $R^\# = \delta(40) - \delta(9) = 10012.41270 = \tilde{h}R$, say. Since no other baby form, or inverse baby form, is found in the interval from F_{37} to F_{40}, we must have $R > 10012.41270 - \delta(37) + \delta(21) > 525$, so $\tilde{h} < 20$.

Looking halfway $R^\#$ we find another match: $F_{41} = F_{10}^{-1}$, since $6371 \equiv -5137 \bmod 2 \cdot 959$. Notice that $\delta(41) + \delta(10) = \frac{1}{2}R^\#$. Hence $\tilde{h}$ is *even*. Looking again halfway we find F_{42} with δ close to $\frac{1}{4}R^\#$ and $a = -842$. Since ± 842 is not in the baby list, this means that 4 does not divide $\tilde{h}$, and that exactly at $\frac{1}{4}R^\#$ a non-trivial factorization of Δ will be found. Looking there, out of curiosity, we find the ambiguous form F_{44}, yielding $\Delta = 5003 \cdot 8179$.

To test if 3 divides $\tilde{h}$, we look near $(5/6)R^\#$ and find the match $F_{45} = F_8^{-1}$. Therefore 6 divides $\tilde{h}$, and $\tilde{h} = 6$ or 18. We exclude the latter possibility by taking one more giant step (F_{46}) to improve the above upper bound to $R > 578$, $\tilde{h} < 18$. We have now proved that $R = (1/6)R^\# = 1668.73545$.

The most likely value for the strict class number h is $h = \tilde{h} = 6$. We show that in any case 6 *divides* h. By sec. 13, end, h is even. To see that 3 divides h we search for a form that is obviously a cube: e.g., $F_{47} = F_{46} * F_{22}$ has $a = -8$, and it is, in F, the cube of $F = (-2, 6395)$ (we could also have used $F_{26} : F_9$). We have $\delta(47) = 9409.90926 \equiv -602.50344 \bmod R$, so if F were on the principal cycle it would have $\delta \equiv (-602.50344)/3 \bmod R/3$, so $\delta \equiv -200.83448$, 355.41067 or $911.65582 \bmod R$. Multiplying F by F_{24} or by F_{34}, or raising it to the 11-th power, we derive in each of the three cases a contradiction. We conclude that F has order 3 in the class group, and that 6 divides h.

If one checks that 5003 and 8179 are primes, it is not difficult to prove that $h \equiv 2 \bmod 4$. So if $h \neq 6$ then $h \geq 18$, and

$$\prod_{p \text{ prime},\ p > 100} \left(1 - \frac{\chi(p)}{p}\right)^{-1} > 3.05,$$

which is very unlikely.

We leave to the reader the pleasure to find out how multiplicative relations between the a's can be exploited to shorten the above calculations.

15. Concluding remarks

(i) The algorithms described in this lecture can be used for an experimental approach to Gauss's class number problems [4, secs 302-307]. Thus, they have been employed in the search for fields with irregular class groups, see [20] for references. It would also be interesting to investigate the decreasing density of fields with class number one among the real quadratic fields with prime discriminants, cf. [25, sec. 5; 12; 16, sec. 1].

(ii) The connection between the factorizations of the discriminant and the elements of order two in the class group gives rise to interesting factorization algorithms. Using negative discriminants, as Shanks does in [23], one obtains an algorithm factoring any positive integer n in $O(n^{(1/5)+\varepsilon})$ steps, if we assume the Riemann hypotheses. Positive discriminants can be used in several ways. We can look halfway the principal cycle (cf. the end of sec. 13), for discriminants that are small multiples of n. Modulo the Riemann hypotheses it can be shown that this also leads to an $O(n^{(1/5)+\varepsilon})$-algorithm. A second factoring method employing positive discriminants will be described by Shanks [26], cf. [28; 17]. This method has expected running time $O(n^{(1/4)+\varepsilon})$, for composite n. It is so simple that it can be programmed for a pocket calculator like the HP67 for numbers of up to twenty digits.

(iii) As Shanks suggested in [25, sec. 1; 29, sec. 4.4], it should be possible to adapt his techniques for number fields of higher degrees, like complex cubic fields. From sec. 10 we know that the "right" group to consider is a group whose "size" is essentially the product of the class number and the regulator. The main complication is that the circles are replaced by higher dimensional tori.

References

1. Z.I. Borevič, I.R. Šafarevič, Teorija čisel, Moscow 1964. Translated into German, English and French.
2. J.W.S. Cassels, Global fields, pp. 42-84 in: J.W.S. Cassels, A. Fröhlich (eds), Algebraic number theory, Academic Press, London 1967.
3. J.W.S. Cassels, Rational quadratic forms, Academic Press, London 1978.
4. C.F. Gauss, Disquisitiones arithmeticae, Fleischer, Leipzig 1801.
5. L.-K. Hua, On the least solution of Pell's equation, Bull. Amer. Math. Soc. 48 (1942),731-735.
6. I. Kaplansky, Composition of binary quadratic forms, Studia Math. 31 (1968), 523-530.
7. J.C. Lagarias, Worst-case complexity bounds for algorithms in the theory of integral quadratic forms, J. Algorithms 1 (1980) 142-186.
8. J.C. Lagarias, On the computational complexity of determining the solvability or unsolvability of the equation $X^2 - DY^2 = -1$, Trans. Amer. Math. Soc. 260 (1980), 485-508.
9. J.C. Lagarias, Succinct certificates for the solvability of binary quadratic diophantine equations, Proc. 20th IEEE Symp. foundations comp. sci., 1979, 47-56.
10. J.C. Lagarias, H.L. Montgomery, A.M. Odlyzko, A bound for the least prime ideal in the Chebotarev density theorem, Inventiones math. 54 (1979), 271-296.
11. J.C. Lagarias, A.M. Odlyzko, Effective versions of the Chebotarev density theorem, pp. 409-464 in: A. Fröhlich (ed.), Algebraic number fields, Academic Press, London 1977.
12. R.B. Lakein, Computation of the ideal class group of certain complex quartic fields, II, Math. Comp. 29 (1975), 137-144.
13. E. Landau, Handbuch der Lehre von der Verteilung der Primzahlen, 2 Bände, Teubner, Leipzig 1909; 2nd ed., Chelsea, New York 1953.
14. P.G. Lejeune Dirichlet, R. Dedekind, Vorlesungen über Zahlentheorie, Braunschweig 1893^4; reprint, New York 1968.
15. A.V. Malyshev, Yu.V. Linnik's ergodic method in number theory, Acta Arith. 27 (1975), 555-598.
16. J.M. Masley, Where are number fields with small class number?, pp. 221-242 in: M.B. Nathanson (ed.), Number Theory Carbondale 1979, Lecture Notes in Mathematics 751, Springer, Berlin 1979.
17. L. Monier, Algorithmes de factorisation d'entiers, Thèse de 3^e cycle, Orsay 1980.
18. J. Oesterlé, Versions effectives du théorème de Chebotarev sous l'hypothèse de Riemann généraiisée, pp. 165-167 in: Astérisque 61 (Journées arithmétiques de Luminy), Soc. Math. de France 1979.
19. J.M. Pollard, Theorems on factorization and primality testing, Proc. Cambridge Philos. Soc. 76 (1974), 521-528.
20. R.J. Schoof, Quadratic fields and factorization, in: Number theory and computers, Mathematisch Centrum, Amsterdam, to appear.
21. R.J. Schoof, Two algorithms for determining class groups of quadratic fields, Mathematisch Instituut, Universiteit van Amsterdam, to appear.
22. I. Schur, Einige Bemerkungen zu der vorstehenden Arbeit des Herrn G. Pólya: Über die Verteilung der quadratischen Reste und Nichtreste, Nachr. Kön. Ges. Wiss. Göttingen, Math.-phys. Kl.

(1918), 30-36; pp. 239-245 in: Gesammelte Abhandlungen, vol. II, Springer, Berlin 1973.
23. D. Shanks, Class number, a theory of factorization, and genera, pp. 415-440 in: Proc. Symp. Pure Math. 20 (1969 Institute on number theory), Amer. Math. Soc., Providence 1971.
24. D. Shanks, The infrastructure of a real quadratic field and its applications, Proc. 1972 number theory conference, Boulder, 1972.
25. D. Shanks, A survey of quadratic, cubic and quartic algebraic number fields (from a computational point of view), pp. 15-40 in: Congressus Numerantium 17 (Proc. 7th S-E Conf. combinatorics, graph theory, and computing, Baton Rouge 1976), Utilitas Mathematica, Winnipeg 1976.
26. D. Shanks, Square-form factorization, a simple $O(N^{1/4})$ algorithm, unpublished manuscript.
27. B.F. Skubenko, The asymptotic distribution of integers on a hyperboloid of one sheet and ergodic theorems (Russian), Izv. Akad. Nauk SSSR Ser. Mat. 26 (1962), 721-752.
28. S.S. Wagstaff, Jr., M.C. Wunderlich, A comparison of two factorization methods, to appear.
29. H.C. Williams, D. Shanks, A note on class number one in pure cubic fields, Math. Comp. 33 (1979), 1317-1320.

H.W. Lenstra, Jr.

Mathematisch Instituut

Universiteit van Amsterdam

Roetersstraat 15

1018 WB Amsterdam

Netherlands.