Zetafunktionen und quadratische Körper: eine Einfiihrung in die höhere Zahlentheorie –
Zeta Functions and Quadratic Fields: An Introduction to Higher Number Theory (Translation)
Don Zagier
Translation by Matt Litman (with the aid of Felix Biefel)

Chapter 13: Reduction Theory

In §8-9 we determined the number of equivalence classes of forms with a given discriminant as well as the number of inequivalent representations of a natural number by the totality of these forms (but not by the individual forms). In addition to these numbers, however, one wants to have effective algorithms in order to

(a) specify a finite set of forms with a given discriminant containing at least one member of each equivalence class.

(b) to decide whether two given forms are equivalent,

(c) to give a finite length of representations of a given number by a given form containing at least one representative of each equivalence class of representations, and

(d) to decide whether two given representations of a number are equivalent by a form.

Question (a) was answered in §8, Theorem 1, by showing that one can derive from an arbitrary form, by applying transformations of the form

$$S_n = \begin{pmatrix} n & 1 \\ -1 & 0 \end{pmatrix} : ax^2 + bxy + cy^2 \mapsto (an^2 - bn + c)x^2 + (2an - b)xy + ay^2 \tag{1}$$

finitely many times, a form $ax^2 + bxy + cy^2$ with

$$-|a| < b \leq |a| \leq |c| \tag{2}$$

and that there are only finitely many such forms with a given discriminant.

In the case where $D < 0$ we can leave out the absolute value signs in (2) (since we only consider positive definite forms) and also assume that in the case of $a = c$, that $b \geq 0$ (since $ax^2 + bxy + ay^2$ and $ax^2 - bxy + ay^2$ are equivalent). We call a positive definite form $ax^2 + bxy + cy^2$ *reduced* if

$$-a < b \leq a < c \quad \text{or} \quad 0 \leq b \leq a = c; \tag{3}$$

thus every positive definite form is equivalent to a reduced one. Conversely, we assert that the reduced positive definite forms are pairwise inequivalent; this not only gives a practical way of calculating the class numbers of negative discriminants, but also an answer to question (b) for definite forms; namely that two definite forms are equivalent if and only if they lead to the same reduced form. To prove the claim we first notice that for a reduced form f and $x, y \in \mathbf{Z}$, $(x, y) \neq (0, 0)$,

$$f(x, y) = ax^2 + bxy + cy^2 \geq a(x^2 - |xy| + y^2) \geq a \tag{4}$$

holds, so the first coefficient a of f is the smallest number represented by f. A matrix $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z})$ transfers the form f to f' with first coefficient $a' = f(\alpha, \gamma)$; if f' is also reduced, then a' must be equal

to a and therefore (considering the cases with equality in (4))

$$\begin{aligned} &(\text{if } c > a) && \alpha = \pm 1,\ \gamma = 0, \\ &(\text{if } c = a > b) && \alpha = \pm 1, \gamma = 0 \text{ or } a = 0, \gamma = \pm 1 \\ &(\text{if } c = a = b) && \alpha = \pm 1, \gamma = 0 \text{ or } \alpha\gamma = -1. \end{aligned}$$

In the first case, $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \pm \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix}$, so the second coefficient b' of f' is equal to $b + 2\beta a$, and from $-a < b, b' \leq a$ it follows that $\beta = 0$ and $f' = f$; in the other two cases it is also easy to see that in these cases the matrix $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ does not necessarily have to be equal to $\pm \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix}$, because the reduced forms $ax^2 + ay^2$ and $ax^2 + axy + ay^2$ have additional automorphisms.

For definite forms the questions (c) and (d) are very easy to answer. Due to the identities

$$f(x, y) = a(x + \frac{b}{2a}y)^2 + \frac{|D|}{4a}y^2 = \frac{|D|}{4c}x^2 + c(\frac{b}{2c}x + y)^2,$$

we have the a priori bounds $|x| \leq \sqrt{4nc/|D|}$ and $|y| \leq \sqrt{4na/|D|}$ for the solutions of $f(x, y) = n$, which implies the answer to (c) and (d) is completely trivial, because f (except in the special cases mentioned) has no automorphisms at all except $\pm I$.

In the case of indefinite forms, the problems (a)−(d) are much more difficult because one has no a priori bounds for the coefficients of the transition matrices between two given forms or for the arguments in the representation of a given number by a given form. Though the forms whose coefficients satisfy (2) delivered an answer to (a) again, this is now unsatisfactory because one can not easily describe the equivalences between these forms. In order to obtain a satisfactory answer to (a) and (b), one should choose inequalities other than (2) or (3) to define reduced forms. Then one still does not get, as in the definite case, exactly one reduced representative for each equivalence class (this can not be achieved by inequalities for the coefficients), but rather a complete description of the equivalences between reduced forms. To formulate the result, we define a transformation T on the set of all indefinite forms by

$$Tf = S_n f\ ,\ n \in \mathbf{Z}\ ,\ n > \frac{b + \sqrt{D}}{2a} > n - 1, \tag{5}$$

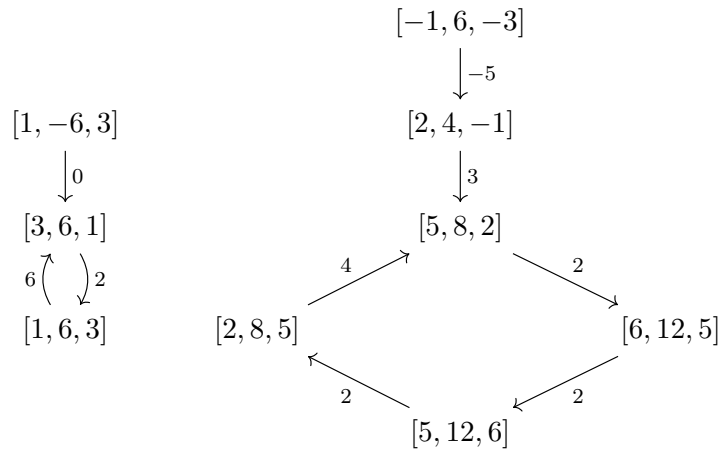
with S_n as in (1), where a, b, c denotes the coefficients of f and $\sqrt{D}$ the positive root of $D = b^2 - 4ac$. We call an indefinite form $ax^2 + bxy + cy^2$ *reduced* if

$$a > 0, \qquad c > 0, \qquad b > a + c. \tag{6}$$

Then:

Theorem 1. *Let $D > 0$, D not a square. Then there are only finitely many reduced form of the discriminant D. Every form of discriminant D is transformed by finitely many applications of the transformation T into a reduced form. The transformation T transforms reduced forms into reduced forms; thus, the set of reduced forms is split into disjoint cycles. Each equivalence between reduced forms is obtained by iteration of T; in particular, two reduced forms are equivalent if and only if they belong to the same cycle.*

Example: To determine if the form $x^2 - 6xy + 3y^2$ of discriminant 24 is equivalent to its negative, we apply the transformation T repeatedly to both and get



where we have the form $ax^2 + bxy + cy^2$ designated by $[a, b, c]$ and $f \overset{n}{\to} f^*$ means that $f^* = Tf = S_n f$. Since we land in different cycles, the forms are inequivalent. In addition, one can verify that all reduced forms of discriminant 24 are in one of the two cycles, that is $h(24) = 2$.

Proof. Let $[a, b, c]$ be a reduced form and let $k = b - 2a$. Then

$$D - k^2 = b^2 - 4ac - (b - 2a)^2 = 4a(b - a - c) > 0.$$

The reduced forms are therefore of the form

$$[a, k + 2a, k + a - \frac{D - k^2}{4a}] \text{ with } |k| < \sqrt{D}\ ,\ k^2 \equiv D \pmod 4\ ,\ a \left| \frac{D - k^2}{4}\ ,\ a > \frac{\sqrt{D} - k}{2}, \right. \tag{7}$$

and this is apparently a finite amount. This proves the first claim.

Now let $f = [a, b, c]$ be any form of discriminant D and $Tf = f^* = [a^*, b^*, c^*]$ its image under T, that is,

$$a^* = an^2 - bn + c\ ,\ b^* = 2an - b\ ,\ c^* = a \tag{8}$$

with

$$\frac{b + \sqrt{D}}{2a} = n - \theta\ ,\ 0 < \theta < 1. \tag{9}$$

Substituting (9) into (8) yields

$$a^* = a\theta^2 + \theta\sqrt{D}\ ,\ b^* = 2a\theta + \sqrt{D}\ ,\ c^* = a. \tag{10}$$

From the first of these equations it follows

$$a \geq 0 \Rightarrow a^* > 0\ ,\ a < 0 \Rightarrow a^* > a,$$

i.e. under repeated use of T, a grows until it's positive, and then it stays positive. Because $c^* = a$, c is also positive after no more than one more application of T. Since there are only finitely many natural numbers under a given number, after finitely many more applications of T we arrive at a form $f = [a, b, c]$, for whose successors $a^* \geq a$ applies. For this form, it follows from (10) that

$$0 \le a^* - a = \theta\sqrt{D} - a(1-\theta^2)$$
$$< (1+\theta)(\sqrt{D} - a(1-\theta)) = \frac{1+\theta}{1-\theta}(b^* - a^* - c^*) \ ,$$

therefore, the successor f^* of f is reduced and the second claim of the theorem is proved.

The third assertion is proved analogously: for a reduced form $f = [a, b, c]$, we already have seen that $|b - 2a| < \sqrt{D}$, so

$$\frac{b+\sqrt{D}}{2a} > 1 \ , \ \frac{b-\sqrt{D}}{2a} < 1. \tag{11}$$

Consequently the number n in (9) is at least 2 and

$$\frac{\sqrt{D}}{a} = n - \theta - \frac{b-\sqrt{D}}{2a} > 1 - \theta,$$

yielding

$$b^* - a^* - c^* = (1-\theta)(\sqrt{D} - a(1-\theta)) > 0;$$

and since we already know that a^* and c^* are positive, the form $Tf = [a^*, b^*, c^*]$ is again reduced. Since the set of reduced forms is finite, it follows that under the operation of T, this quantity decays into cycles. It only remains to be shown that there is exactly one cycle to each equivalence class of forms and that all equivalences between reduced forms arise from the same cycle by iteration of T.

So let $f = [a, b, c]$ and $f' = [a', b', c']$ be two reduced forms of the discriminant D and $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z})$ a matrix that converts f to f'. From the formula (8.6) for the coefficients of f' one obtains

$$a' = f(\alpha, \gamma) \ , \ c' = f(\beta, \delta) \ , \ a' + c' - b' = f(\alpha - \beta, \gamma - \delta).$$

Since f' is reduced, the first two numbers are positive and the one last negative. In particular, $\gamma \neq \delta$ (otherwise $f(\alpha - \beta, \gamma - \delta)$ would be positive); and by possibly replacing A by $-A$, we can assume that

$$\delta > \gamma. \tag{12}$$

We now distinguish three cases, depending on the sign of γ.

Case I: ($\gamma = 0$) We immediately have f' is equal to f and $A = I$. Namely, $1 = \alpha\delta - \beta\gamma = a\delta$ and combining this with (12) implies $\alpha = \delta = 1$, so

$$f(\beta, 1) = f(\beta, \delta) > 0 > f(\alpha - \beta, \gamma - \delta) = f(\beta - 1, 1).$$

But these inequalities imply $\beta = 0$, since for a quadratic polynomial $\phi(x)$ there can be at most one integer n with $\phi(n-1) < 0 < \phi(n)$.

Case II: ($\gamma < 0$) In this case, we assert that f' arises from f by repeated application of T, and that A is the product of the corresponding matrices S_n. Let $f^* = S_n f$ (n as in (5)) be the image of f under T and

$$A^* = \begin{pmatrix} \alpha^* & \beta^* \\ \gamma^* & \delta^* \end{pmatrix} = S_n^{-1} A = \begin{pmatrix} -\gamma & -\delta \\ \alpha + n\gamma & \beta + n\delta \end{pmatrix}$$

the matrix that converts f^* to f'. The matrix A^* again satisfies (12) (namely $\alpha^* - \beta^* = \delta - \gamma > 0$, and because of $f(\alpha^* - \beta^*, \gamma^* - \delta^*) < 0$, $\alpha^* - \beta^*$ and $\gamma^* - \delta^*$ have opposite signs). If we can show that $\gamma < \gamma^* \leq 0$, then our assertion follows with complete induction: in the sequence $\gamma < \gamma^* < \gamma^{**} < \ldots \leq 0$, at some point $\gamma * \cdots *$ must be zero, and then, according to case I, $f^{*\cdots*} = f$ and the corresponding transition matrix $A^{*\cdots*}$ is the identity. We have to prove the inequality $\gamma < \alpha + n\gamma \leq 0$ or

$$n - 1 < \frac{\alpha}{-\gamma} \leq n \tag{13}$$

Since $f(\alpha, \gamma) > 0 > f(\alpha - \beta, \gamma - \delta)$, the polynomial $f(x, -1) = ax^2 - bx + c$ has a positive value at $\frac{\alpha}{-\gamma}$ and a negative value at $\frac{\alpha-\beta}{-\gamma+\delta}$; additionally $\frac{\alpha}{-\gamma}$ is larger $\frac{\alpha-\beta}{-\gamma+\delta}$. It follows that the larger root of $f(x, -1) = 0$ lies between these numbers, that is,

$$\frac{\alpha - \beta}{-\gamma + \delta} < \frac{b + \sqrt{D}}{2a} < \frac{\alpha}{-\gamma}.$$

Because $n - 1 < \frac{b+\sqrt{D}}{2a}$, the first of the inequalities in (13) follows immediately. For the second we note that from $\frac{\alpha}{-\gamma} > n$ and $n > \frac{b+\sqrt{D}}{2a}$, the inequalities $\frac{\alpha-\beta}{-\gamma+\delta} < n < \frac{\alpha}{-\gamma}$ would follow, i.e. $-\alpha\gamma + \beta\gamma < n\gamma(\gamma - \delta) < -\alpha\gamma + \alpha\delta$, contradicting the condition $\alpha\delta - \beta\gamma = 1$.

Case III: ($\gamma > 0$) In this case we assert that we can obtain f from f' by repeated application of T (i.e. we have to go through the cycle in the other sense) and that A is the product of the corresponding matrices S_n^{-1}. Since $A^{-1} = \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix}$ the third coefficient is negative, and out of this it follows immediately from case II if we prove that A^{-1} again fulfills (12), that means $\alpha > -\gamma$. But this is easy: because $\frac{\alpha}{-\gamma} < \frac{\alpha-\beta}{-\gamma+\delta}$ and $f(\frac{\alpha}{-\gamma}, -1) > 0 > f(\frac{\alpha-\beta}{-\gamma+\delta}, -1)$, $\frac{\alpha}{-\gamma}$ is smaller than the smaller root of $f(-x, 1) = 0$, so with (11)

$$\frac{\alpha}{-\gamma} < \frac{b - \sqrt{D}}{2a} < 1, \quad \alpha > -\gamma.$$

With that the last claim of the theorem is proven. ■

Theorem 1 and its proof are closely connected to the theory of the backwards continued fraction. We describe now this connection.

Let $n_0, n_1, n_2, ...$ be integers with $n_1, n_2, ... \geq 2$. We use the notation $[[n_0, .n_1, ..., n_s]]$ to describe the finite continued fraction

$$[[n_0, n_1, ..., n_s]] = n_0 - \cfrac{1}{n_1 - \cfrac{1}{n_2 - \ddots - \frac{1}{n_s}}}$$

and with $[[n_0, n_1, ...]]$ to denote the limit $\lim_{s\to\infty}[[n_0, ..., n_s]]$, whose existence can easily be proven. This limit is a real number; or vice-versa every real number w has a clear backwards continued fraction

expansion $w = [[n_0, n_1, ...]]$ with $n_i \in \mathbf{Z}$ and $n_1, n_2, ... \geq 2$ given by $n_0 = \lfloor w \rfloor + 1, w_1 = \frac{1}{n_0 - w}$ and inductively setting $n_i = \lfloor w_i \rfloor + 1$, $w_{i+1} = \frac{1}{n_i - w_i}$. Consequently, there is a clear correspondence between the set of real numbers w and the set of sequences $n_0, n_1, ...$ with $n_0 \in \mathbf{Z}$, $n_1, n_2, ... \in \{2, 3, ...\}$. Under this correspondence, it follows that

(i) $w \in \mathbf{Q}$ iff from a certain point on, all $n_i = 2$;

(ii) w satisfies a quadratic equation with integer coefficients iff from a certain point on the n_i's repeat periodically (i.e. there exists $r \geq 1$ and $i_0 \geq 0$ such that $n_{i+r} = n_i$ for all $i \geq i_0$;

(iii) w is the highest root of the quadratic equation $ax^2 - bx + c = 0$, where $[a, b, c]$ is a reduced quadratic form of positive discriminant iff the backwards continued fraction expansion of w is purely periodic (i.e. $n_{i+r} = n_i$ for all $i \geq 0$).

The first claim can easily be proved (in the "$\Leftarrow$, even trivial since $[[2, 2, ...]] = 1$). The $\Rightarrow$ direction of (ii) and (iii) is proven in Theorem 1. Let $f = [a, b, c]$ be a quadratic form of discriminant $D > 0$ and

$$w = \frac{b + \sqrt{D}}{2a}, \quad w' = \frac{b - \sqrt{D}}{2a} \tag{14}$$

be the roots of $f(x, -1) = 0$. If $f^* = S_n f$ is the image of f under the transformation T and w^* is defined analogously to w, then $n = \lfloor w \rfloor + 1$ and $w = n - \frac{1}{w^*}$, so that the beginning of the BCF expansion of w is the digit n: if $f_i = [a_i, b_i, c_i]$ $(i \geq 0)$, the image of f under T^i, so $f_0 = f$, $f_1 = f^*$, $f_{i+1} = T f_i = S_{n_i} f_i$ with $n_i = \lfloor \frac{b_i + \sqrt{D}}{2a_i} \rfloor + 1 = \lfloor w_i \rfloor + 1$, then $w_i = n_i - \frac{1}{w_{i+1}}$ and it follows that $w = w_0 = [[n_0, n_1, ...]]$. Theorem 1 says there exists i_0 with f_{i_0} reduced and that f_i for $i \geq i_0$ are all reduced and are repeating periodically, in particular $n_{i+r} = n_i$ for a suitable r and all $i \geq i_0$. Before we prove the other direction of (ii) and (iii), we notice that the last part of Theorem 1, over the equivalence between reduced forms, can easily be transferred in the language of backwards continued fractions: for example if $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ with $\delta > \gamma$ and $\gamma < 0$, and $A \in \mathrm{SL}_2(\mathbf{Z})$ transforms a form f into a reduced form f', it implies for a suitable s (compare to case II of the proof above)

$$f' = T^{s+1} f, \quad A = S_{n_0} S_{n_1} ... S_{n_s}, \quad \frac{\alpha}{-\gamma} = [[n_0, n_1, ..., n_s]].$$

For a general, not necessarily reduced form f, which is related to the root w with BCF expansion

$$w = [[n_0, ..., n_{i_0 - 1}, \overline{n_{i_0}, n_{i_0+1}, ..., n_{i_0+r-1}}]] \tag{15}$$

(where the line over $n_{i_0}, ..., n_{i_0+r-1}$ means it repeats periodically and r is the least period), following Theorem 1 the automorphism group of f is given by

$$U_f = \{\pm S_{n_0} S_{n_1} ... S_{n_{i_0 - 1}} \left(S_{n_{i_0}} \dots S_{n_{i_0+r-1}} \right)^N S_{i_0-1}^{-1} ... S_{n_0}^{-1} : N \in \mathbf{Z}\}. \tag{16}$$

We are now proving $\Leftarrow$ of claims (ii) and (iii). The first is easy. If the real number w has BCF expansion (15) and $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ is any matrix in U_f with $N \neq 0$ (and $A \neq \pm I_2$), it implies that $w = \frac{\alpha w - \beta}{-\gamma w + \delta}$, i.e. w is a root of the quadratic equation $\gamma w^2 + (\alpha - \delta) w - \beta = 0$. The second is a formal consequence of the first and Theorem 1. Because if w is a number with a purely periodic BCF expansion of length r, then w is the root of a quadratic form f; for large enough N Theorem 1 tells us the form $T^{Nr} f$ is reduced, but has a root with the same expansion as w. But we give another BCF proof which is based

on the fact of independent interest: if w is a number with a purely periodic BCF expansion and w' the conjugate number (we already know that w is quadratic), it implies

$$w = [[\overline{n_0, ..., n_{r-1}}]], \quad \frac{1}{w'} = [[\overline{n_{r-1}, ..., n_0}]]. \tag{17}$$

Because $n_i \geq 2$, out of (17) for a number with w with a purely periodic BCF expansion, the inequalities follow

$$w > 1, \quad 0 < w' < 1, \tag{18}$$

which are therefore equivalent to the quadratic form with roots w and w' being reduced (compare (11)). To see (17), we define a number periodically by setting $n_{i+r} = n_i$ ($\forall i \in \mathbf{Z}$) and

$$x_i = \frac{1}{[[\overline{n_{i-1}, n_{i-2}, ..., n_{i-r}}]]}.$$

This implies $\frac{1}{x_{i+1}} = n_i - x_i$, or $x_i = n_i - \frac{1}{x_{i+1}}$, so that x_0 satisfies the quadratic equation

$$x_0 = n_0 - \cfrac{1}{n_1 - \cfrac{1}{\ddots - \cfrac{1}{n_{r-1} - \frac{1}{x_0}}}}.$$

But this is the same equation w satisfies, and since x_0 satisfies $x_0 < 1 < w$, it is not w, so $x_0 = w'$ which is what had to be proven.

We began this section with 4 questions about quadratic forms and the presentation of numbers through forms, that were all easily solved in the definite case. For the indefinite case, the 2 questions were answered through a method for determination of the equivalence classes of forms through Theorem 1. The answer to both questions (following the description of the equivalence classes of the presentation of a natural number through an indefinite form) will be giving through the following Theorem, which in contrast to Theorem 1 seems not to be found in classic literature.

Theorem 2. *Let $\{f_1, ..., f_r\}$ be the Theorem 1 constructed cycle of the reduced forms in the equivalence class of an indefinite quadratic form f and let n be a natural number. Then every presentation of n through f is equivalent to exactly one presentation $n = f_i(x, y)$ with $1 \leq i \leq r$, $x > 0$, $y \geq 0$. (Thereby equivalence means that if the presentation $n = f(x, y) = f'(x', y')$ is given through different forms f and f', there exists a matrix which transfers f to f' and (x, y) into (x', y'); to get a complete set of presentations of n through f by itself, we have to apply a matrix on every presentation in the set, which transfers f_i into f.)*

We see that the coefficients of $f_i = [a_i, b_i, c_i]$ are positive and therefore for a presentation $n = f_i(x, y)$ with x and y non-negative we have a priori $x \leq \sqrt{n/a_i}$, $y \leq \sqrt{n/c_i}$; so there are only finitely many of those representations and these can be effectively (and even easily) determined.

Proof. We enumerate the f_i so that $f_{i+1} = Tf_i = S_{n_i} f_i$, and also $f_i(x, y) = a_i(x + yw_i)(x + yw_i')$ with

$$w_i = \frac{b_i + \sqrt{D}}{2a_i} = [[\overline{n_i, n_{i+1}, ..., n_{i+r-1}}]] = n_i - \frac{1}{w_{i+1}}$$

(here we take i modulo r, so $f_{i+r} = f_i, n_{i+r} = n_i, w_{i+r} = w_i$ for all $i \in \mathbf{Z}$). WLOG we can assume that $f = f_0 = f_r$. From a given presentation

$$n = f(x_0, y_0)$$

we receive infinitely many equivalent presentations

$$n = f_i(x_i, y_i) \quad (i \in \mathbf{Z}) \tag{19}$$

with $\begin{pmatrix} x_i \\ y_i \end{pmatrix} = S_{n_i} \begin{pmatrix} x_{i+1} \\ y_{i+1} \end{pmatrix}$. Let $\xi_i = x_i + y_i w_i$; then (19) is equivalent to $n = a_i \xi_i \xi_i'$ (ξ_i' is the conjugate of ξ_i). In particular, ξ_i and ξ_i' have the same sign since

$$\xi_i = x_i + y_i(n_i - \frac{1}{w_{i+1}}) = \frac{1}{w_{i+1}} \xi_{i+1}, \tag{20}$$

which is independent of i. Because $(x, y) \mapsto (-x, -y)$ is an automorphism of f and we are only interested in the equivalence class of presentations, we can assume that the this sign is positive, yielding $\xi_i, \xi_i' > 0$. From (2) and $w_i > 1 > w_i' > 0$, it follows that

$$\frac{\xi_i}{\xi_i'} < \frac{\xi_{i+1}}{\xi_{i+1}'}, \quad \lim_{i \to \infty} \frac{\xi}{\xi_i'} = \infty, \quad \lim_{i \to -\infty} \frac{\xi_i}{\xi_i'} = 0,$$

so there exists exactly one $i \in \mathbf{Z}$ with

$$\frac{\xi_i}{\xi_i'} \geq 1 > \frac{\xi_{i-1}}{\xi_{i-1}'}. \tag{21}$$

But $\xi_i - \xi_i'$ is equal to $y_i(w_i - w_i')$ and $w_i - w_i'$ is positive, so $\xi_i / \xi_i' \geq 1$ is equivalent to $y \geq 0$ and therefore $\xi_{i-1}/\xi_{i-1}' < 1$ equivalent to $x_i = -y_{i-1} > 0$. Consequently $n = f_i(x_i, y_i)$ for i defined through (21) is equivalent to the presentation $n = f(x_0, y_0)$ whose existence is claimed in the theorem. The uniqueness follows out of the uniqueness of i in (21), and the fact the whole automorphism group of f is generated by $-I$ and $\prod_{i=1}^{r} S_{n_i}$. This proves Theorem 2. ■

The statement of Theorem 2 gives the formula

$$R(n, f) = \sum_{i \pmod r} \sum_{\substack{x,y \in \mathbf{Z} \\ x>0, y \geq 0 \\ f_i(x,y) = n}} 1 \qquad (n \in \mathbf{N})$$

for the presentation $R(n, f)$ of numbers given in section 8. It follows from section 10 that $\sum_{n=1}^{\infty} R(n, f) n^{-s} = \zeta(A, s)$, where A is the ideal class which corresponds to the form f. Theorem 2 is equivalent to the identity

$$\zeta(A, s) = \sum_{i \pmod r} \sum_{\substack{x,y \in \mathbf{Z} \\ x>0, y \geq 0}} \frac{1}{f_i(x, y)^s} \qquad (\Re(s) > 1).$$

It will be easier to replace the condition on x and y through the symmetric conditions

$$x \geq 0, y \geq 0, (x, y) \neq (0, 0);$$

because the presentation $n = f_i(x, 0)$ and $n = f_{i+1}(0, x)$ are equivalent, therefore the presentations with $x = 0$ or $y = 0$ are counted twice. Theorem 2 is equivalent to this theorem about Dirichlet series:

Theorem 3. *Let A be an ideal class in a real quadratic field. Then*

$$\zeta(A, s) = \sum_{f} Z_f(s) \qquad (s \in \mathbf{C},\ \Re(s) > 1),$$

where the summation is over the cycle of reduced forms f which correspond to the class A, and $Z_f(s)$ is given by

$$Z_f(s) = \sum_{x,y>0} \frac{1}{f(x, y)^s} + \frac{1}{2} \sum_{x>0} \frac{1}{f(x, 0)^s} + \frac{1}{2} \sum_{y>0} \frac{1}{f(0, y)^s} \qquad (\Re(s) > 1). \tag{22}$$

This theorem will be used in the next section to calculate $\zeta(A, 0)$.

Exercises:

(1) Prove the analogy of theorem 1 for the equivalence classes in a broad sense of indefinite forms, where "reduced" is now defined by the inequalities

$$w > 1, 0 > w' > -1 \quad \left(w = \frac{b + \sqrt{D}}{2a}\right) \tag{23}$$

(instead of (17)) and T is replaced by the transformation

$$T^+ f = S_m^+ f, \quad S_m^+ = \begin{pmatrix} m & -1 \\ -1 & 0 \end{pmatrix}, \qquad m < \frac{b + \sqrt{D}}{2a} < m + 1. \tag{24}$$

One should carry out this reduction method for the example according to Theorem 1 (also the equivalence of $[1, -6, 3]$ and $[-1, 6, -3]$ now in a broader sense).

(2) Show the equivalence of the reduction method of exercise 1 with the expansion of w in the continued fraction form

$$w = [[m_0, m_1, ...]]^+ := m_0 + \cfrac{1}{m_1 + \cfrac{1}{m_2 + \ddots}}$$

with $m_i \in Z$, $m_i \geq 1$ for $i \geq 1$: the sequence $\{m_i\}$ is eventually periodic for every quadratic irrationality w, and is exactly purely periodic if w satisfies (23).

(3) Show that the transition between both kinds of continued fractions is given by

$$[[m_0, m_1, m_2, ...]]^+ = [[m_0 + 1, \underbrace{2, ..., 2}_{m_1 - 1}, m_2 + 2, \underbrace{2, ..., 2}_{m_3 - 1}, m_4 + 2, ...]] \qquad (n_i \in \mathbf{Z}, m_1, m_2, ... \geq 1).$$

(4) Show with the help of exercise 3 that the ideal class in a broader sense equals the ideal class in a narrow sense or that it breaks into two pieces, depending on if the length s of the continued fraction period of $[[\overline{m_0, ..., m_s}]]^+$ is odd or even.

(5) Determine the cycles of reduced forms (in a narrow as well as broad sense) for all positive discriminants < 30.