THE PUBLISHING HOUSE
OF THE ROMANIAN ACADEMY

PROCEEDINGS OF THE ROMANIAN ACADEMY, Series A,
Volume 16, Number 1/2015, pp. 28–31

A NOTE ON BINARY QUADRATIC FORMS WITH POSITIVE DISCRIMINANT $D \neq \square$

Erwin BELTZ, Robbert FOKKINK, Cor KRAAIKAMP

Technische Universiteit Delft, Institute of Applied Mathematics, Mekelweg 4, 2628CD Delft, The Netherlands
E-mail: c.kraaikamp@tudelft.nl

In Theorem 1 [1, p. 122], in his monograph on zeta-functions and quadratic fields, Don Zagier states among other things that any two equivalent *reduced* binary quadratic forms belong to the same cycle. All the statements of the theorem are proved, except the statement just mentioned. In this note we show that Zagier's statement is also correct, thus completing Zagier's proof.

Key words: binary quadratic form, continued fraction, reduced form.

1. INTRODUCTION

In [1], Don Zagier studied – among other things – the so-called *binary quadratic forms*; these are forms f given by

$$f(x,y) = ax^2 + bxy + cy^2,$$

with $a,b,c \in \mathbf{Z}$ fixed, x, y variables, and where the discriminant D, given by

$$D = b^2 - 4ac,$$

is not a square (since otherwise we can factor f). We write $f = [a,b,c]$.

Two (binary quadratic) forms f and f' are *equivalent* if there exists a matrix $A \in SL_2(\mathbf{Z})$, say

$$A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}, \tag{1}$$

(with $\alpha,\beta,\gamma,\delta \in \mathbf{Z}$ and $\det(A) = 1$), such that $f'(x,y) = f(x',y')$, where

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = A \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \alpha x + \beta y \\ \gamma x + \delta y \end{pmatrix}.$$

Setting $f = [a,b,c]$ and $f' = [a',b',c']$, one easily finds that

$$\begin{aligned} a' &= a\alpha^2 + b\alpha\gamma + c\gamma^2 = f(\alpha,\gamma) \\ b' &= 2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta, \\ c' &= a\beta^2 + b\beta\delta + c\delta^2 = f(\beta,\delta) \end{aligned} \tag{2}$$

cf. [1, p 58]. We write $f' = Af$.

Since $SL_2(\mathbf{Z})$ is a group, the above relation is an equivalence relation. A simple counting argument then shows that there are only finitely many equivalence classes of a given discriminant $D \neq \square$; see [1], Satz 1, p. 59.

Among the matrices of $SL_2(\mathbf{Z})$ with positive discriminants $D \neq \square$ there is one subclass of particular interest. These are the matrices $S_n, n \in \mathbf{Z}$, given by

$$S_n = \begin{pmatrix} n & 1 \\ -1 & 0 \end{pmatrix}.$$

Let $\mathfrak{I}_D = \{f = [a,b,c]:\ a,b,c \in \mathbf{Z},\ b^2 - 4ac = D\}$, then we define the map $T : \mathfrak{I}_D \to \mathfrak{I}_D$ by

$$f' = Tf := S_n f,$$

where $n \in \mathbf{Z}$ is such, that

$$n - 1 < \frac{b + \sqrt{D}}{2a} < n.$$

The reason why we are interested in this particular map is, that if we view S_n as a Möbius transformation, i.e.,

$$S_n \cdot x = \begin{pmatrix} n & 1 \\ -1 & 0 \end{pmatrix} \cdot x = \frac{nx+1}{-x+0} = \frac{-1}{x} - n,$$

we find the Gauss map of the *backward* (or: *minus*) *continued fraction expansion*. If we go from f to the next form $f' = S_n f$ we in fact apply the Gauss map T of the backward continued fraction to the root $\frac{b+\sqrt{D}}{2a}$ of the quadratic equation $f(x,-1) = 0$.

Let $f = [a,b,c]$ be a (quadratic binary) form of positive discriminant $D \neq \square$, then f is called *reduced* if

$$a > 0,\ c > 0,\ b > a + c.$$

In [1, p.122], Zagier obtains with elementary means the following beautiful result.

THEOREM 1. *Let $D > 0, D \neq \square$. Then there exists only a finite number of reduced forms of discriminant D. After a finite number of applications of T, every form with discriminant D will eventually end up in a reduced form. Also, if we apply T to a reduced form, we again obtain a reduced form; this means reduced forms can be divided into disjunct cycles. In particular, two reduced forms are equivalent if and only if they belong to the same cycle.*

In fact, Zagier gives a full proof of all the statements, except the last one. He shows that there are only finitely many reduced forms of positive discriminant $D \neq \square$, that under T every form $\tilde{f}$ of discriminant D is mapped after finitely many steps to a reduced form f, and that under T every reduced form f is mapped to another reduced form. Since there are only finitely many reduced forms (of discriminant D), repeated application of T must therefore lead to periodicity. Finally, Zagier shows that if f and f' are two equivalent reduced forms, say $f' = Af$, with $A \in SL_2(\mathbf{Z})$ as in equation (1), then either $f' = f$ when $\gamma = 0$, or there exist positive integers k and $n_1, n_2, ..., n_k$ such that either

$$A = S_{n_1} S_{n_2} \cdots S_{n_k} \quad (\text{when } \gamma < 0),$$

or

$$A = (S_{n_1} S_{n_2} \cdots S_{n_k})^{-1} \quad \text{(when } \gamma > 0\text{)}.$$

In case $\gamma < 0$, the positive integers n_i are such, that if we set $f_1 = f$, and $f_{i+1} = Tf_i$, we have that $Tf_i = S_{n_i} f_i$ for $i = 1,2,...,k$. In case $\gamma > 0$, the roles of f and f' are reversed.

What is not immediately clear from Zagier's proof of Theorem 1, is that if we start at a reduced form f, under repeated application of T we get to a loop which 'closes' at f, i.e., that there exists a positive integer m such that $f = T^m f$. Going from one reduced form to another reduced form, it is obvious that we have to return to a form we have been before, since there are only finitely many reduced forms … but this does not necessarily imply that this is f. In the next section we show that actually it must be f, thus completing Zagier's proof.

2. REDUCED FORMS HAVE A UNIQUE REDUCED ANCESTOR

Let $f = [a,b,c]$ be a reduced form of discriminant $D \neq \square$. Then a form $\widetilde{f} = [\widetilde{a},\widetilde{b},\widetilde{c}]$ is an *ancestor* of f if $f = T\widetilde{f}$. So the collection $\aleph_f$ of all ancestors f is given by

$$\aleph_f = \{S_n^{-1}(f) : n \in \mathbf{Z}\}.$$

We have the following result.

THEOREM 2. *Let $f = [a,b,c]$ be a reduced form of positive discriminant $D \neq \square$. Then f has a unique reduced ancestor $\widetilde{f}$.*

Proof. Let $n \in \mathbf{Z}$ and $\widetilde{f} = [\widetilde{a},\widetilde{b},\widetilde{c}] = S_n^{-1}(f)$. It follows from (2) that

$$\widetilde{a} = c,\ \widetilde{b} = -b + 2n,\ \widetilde{c} = cn^2 - bn + a,$$

i.e. $\widetilde{f} = [c, -b + 2n, cn^2 - bn + a]$.

Now $\widetilde{f}$ is reduced if and only if $\widetilde{c} > 0$ and $\widetilde{b} > \widetilde{a} + \widetilde{c}$ (note that $\widetilde{a} = c > 0$ since f is reduced). So we must show there is only one $n \in \mathbf{Z}$ such that

$$cn^2 - bn + a > 0, \quad \text{and} \quad -b + 2cn > cn^2 - bn + a + c.$$

Note that the equation $cx^2 - bx + a = 0$ has roots $\dfrac{b \pm \sqrt{D}}{2c}$. Furthermore, $-b + 2cn > cn^2 - bn + a + c$ is the same as $cn^2 - (b + 2c)n + a + b + c < 0$. Since the roots $x_{1,2}$ of $cx^2 - (b + 2c)x + a + b + c = 0$ satisfy

$$x_{1,2} = \frac{b + 2c \pm \sqrt{(b + 2c)^2 - 4(a + b + c)c}}{2c} = \frac{b \pm \sqrt{D}}{2c} + 1,$$

we find that $n \in \mathbf{Z}$ must lie outside the interval $I_\ell = \left[\dfrac{b - \sqrt{D}}{2c}, \dfrac{b + \sqrt{D}}{2c}\right]$ and inside the interval $I_r = \left(\dfrac{b - \sqrt{D}}{2c} + 1, \dfrac{b + \sqrt{D}}{2c} + 1\right)$. So if these two intervals I_ℓ and I_r overlap, we see that $n \in \mathbf{Z}$ must lie in the interval

$$U_f = I_\ell^c \cap I_r = \left(\frac{b+\sqrt{D}}{2c}, \frac{b+\sqrt{D}}{2c} + 1 \right).$$

Obviously, there is only one $n \in \mathbf{Z}$ for which $n \in U_f$ in this situation. However, some caution is required since it may be possible that $I_\ell \cap I_r$ is empty, if the right end point of I_ℓ is smaller than the left end point of I_r. For example, if $k \geq 5,\ b = 2k+1,\ a = c = k$, then

$$D = b^2 - 4ac = (2k+1)^2 - 4k^2 = 4k+1 < k^2 = c^2,$$

which implies that

$$\frac{\sqrt{D}}{c} < 1,$$

which is equivalent with

$$\frac{b+\sqrt{D}}{2c} < \frac{b-\sqrt{D}}{2c} + 1.$$

If $I_\ell \cap I_r$ is empty, then it is not immediately clear that there necessarily exists an $n \in \mathbf{Z}$ in the interval $U_f = I_\ell^c \cap I_r = I_r$ (note that this interval has length smaller than 1). So one might be tempted to state that for any reduced form $f = [a,b,c]$ there is *at most* one reduced ancestor (and that there might be reduced forms with *no* reduced ancestor). The fact that there are only finitely many reduced forms (of discriminant *D*), and the fact that *T* maps reduced forms to reduced forms forces that there exists an $n \in \mathbf{Z}$ such that $n \in I_r$; suppose that the reduced form f does not have a reduced ancestor, then $T^i f \neq f$ for all $i \geq 1$. Since there are only finitely many reduced forms there must be indices $j > i \geq 1$, such that $T^j f = T^i f$ and we see that the reduced form $T^i f$ has two reduced ancestors, which is impossible since we just saw that reduced forms have at most one reduced ancestor.

REFERENCES

1. ZAGIER, D.B., Zetafunktionen und quadratische Körper, Eine Einführung in die höhere Zahlentheorie, Hochschultext, Springer-Verlag, Berlin, New York, 1981.

Received September 5, 2014