2009 REU: REDUCTION FOR $D > 0$

1. Continued Fractions

In this section we review some basic results on continued fractions. We shall take a somewhat non traditional approach, and view continued fractions as an algorithm. More precisely, let $\alpha > 0$ be a real number, then continued fractions *algorithm* is the following:

(1) Let $\beta = \alpha - [\alpha]$ where $[\alpha]$ is the greatest integer.
(2) If β is zero then stop, else define $\alpha_1 = 1/\beta$ and go to the first step.

Example:

$$\alpha = \frac{29}{13} = 2 + \frac{3}{13}$$
$$\alpha_1 = \frac{13}{3} = 4 + \frac{1}{3}$$
$$\alpha_2 = \frac{3}{1} = 3 + \frac{0}{3}.$$

We can now write 29/13 as a fraction in a familiar form (note how 2 4 and 3 appear in it):

$$\frac{29}{13} = 2 + \frac{1}{4 + \frac{1}{3}}.$$

Example:

$$\alpha = \sqrt{2} = 1 + (\sqrt{2} - 1)$$
$$\alpha_1 = \sqrt{2} + 1 = 2 + (\sqrt{2} - 1)$$
$$\alpha_2 = \sqrt{2} + = 2 + (\sqrt{2} - 1)$$

we see that the last step keeps repeating. In particular, this process will never stop. It follows that $\sqrt{2}$ is not rational, and we should have

$$\sqrt{2} = 1 + \frac{1}{2 + \frac{1}{2} +}.$$

What does this exactly mean? To explain this, let us abbreviate notation a bit, and write $1 + \frac{1}{2+}\frac{1}{2+}\ldots$ or $[1, 2, 2, \ldots]$ for the continued fraction of $\sqrt{2}$. The numbers 1, $1 + \frac{1}{2}$, $1 + \frac{1}{2+}\frac{1}{2}, \ldots$ are called convergents of $\sqrt{2}$. It turns out that this sequence of rational number converges to $\sqrt{2}$.

The convergents, in general, can be written as fractions A_n/B_n defined as follows. Let $\alpha = [a_0, a_1, a_2, \ldots]$ be a continued fraction of α. Define

$$\begin{cases} A_n = a_n A_{n-1} + A_{n-2} \\ B_n = a_n B_{n-1} + B_{n-2} \end{cases}$$

where $A_{-1} = 1$, $B_{-1} = 0$, $A_0 = a_0$ and $B_0 = 1$. One can find a combinatorial proof (in Davenport's book, for example) that the quotients A_n/B_n are indeed the convergents.

However, for our purposes that result is not necessary as we shall adopt a different approach to continued fractions, based on action of $GL_2(\mathbb{Z})$

$$\alpha \mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix} \circ \alpha = \frac{a\alpha + b}{c\alpha + d}.$$

In terms of this action, the two steps in the algorithm correspond to

$$\begin{pmatrix} 1 & -[\alpha] \\ 0 & 1 \end{pmatrix} \circ \alpha = \alpha - [\alpha] \text{ and } \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \circ \beta = \frac{1}{\beta}.$$

Proposition 1.1. *Let α be an irrational number, and α_{n+1} be the number obtained by applying the continued fraction algorithm to α $n+1$ times. Then*

$$\alpha = \frac{A_n \alpha_{n+1} + A_{n-1}}{B_n \alpha_{n+1} + B_{n-1}}$$

where A_n and B_n are defined inductively as above, with $[a_0, a_1, \ldots]$ the continued fraction of α.

Proof. By rewriting the continued fraction algorithm in terms of the action of $GL_2(\mathbb{Z})$, we arrive to

$$\alpha_{n+1} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & -a_n \\ 0 & 1 \end{pmatrix} \cdot \ldots \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & -a_0 \\ 0 & 1 \end{pmatrix} \circ \alpha.$$

By moving these matrices to the other side, we get

$$\alpha = \begin{pmatrix} 1 & a_0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \ldots \cdot \begin{pmatrix} 1 & a_n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \circ \alpha_{n+1}.$$

We shall abbreviate

$$\begin{pmatrix} 1 & a_i \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} a_i & 1 \\ 1 & 0 \end{pmatrix}.$$

Now notice that

$$\begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} A_0 & A_{-1} \\ B_0 & B_{-1} \end{pmatrix}.$$

Induction shows that

$$\begin{pmatrix} A_{n-1} & A_{n-2} \\ B_{n-1} & B_{n-2} \end{pmatrix} \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} A_n & A_{n-1} \\ B_n & B_{n-1} \end{pmatrix}.$$

The proposition is proved. □

Proposition 1.2.

$$\lim_{n\to\infty} \frac{A_n}{B_n} = \alpha.$$

Proof. Substituting the expression for α in terms of α_{n+1} given by Proposition ?

$$|\alpha - \frac{A_n}{B_n}| = |\frac{A_{n-1}B_n - A_{n-1}B_n}{B_n(\alpha_{n+1}B_n + B_{n-1})}|.$$

Now notice that the numerator is equal to $(-1)^{n+1}$ (determinant of a matrix in $GL_2(\mathbb{Z})$). On the other hand, since α_{n+1} is bigger then a_{n+1}, it follows that

$$|\alpha - \frac{A_n}{B_n}| \leq |\frac{1}{B_n B_{n+1}}|.$$

□

2. Reduced quadratic irrationals

In this section we shall characterize numbers with purely periodic continued fraction expansion. More precisely, a quadratic irrational is called *reduced* if $\alpha > 1$ and $-1 < \bar{\alpha} < 0$. We shall show that a number has a purely periodic continued fraction expansion if and only it is a reduced quadratic irrational. To that end, assume that $\alpha = [a_0, a_1, \ldots a_n, a_0, \ldots]$. Then $\alpha_{n+1} = \alpha$, and α satisfies

$$\alpha = \frac{A_n \alpha + A_{n-1}}{B_n \alpha + B_{n-1}}.$$

This clearly is a quadratic equation in α. Now let $\beta = [a_n, \ldots a_0, a_n \ldots]$ be the quadratic irrational with the period reversed. Then

$$\beta = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & -a_0 \\ 0 & 1 \end{pmatrix} \cdot \ldots \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & -a_n \\ 0 & 1 \end{pmatrix} \circ \beta.$$

After moving the first matrix on the right side to the left side, the equation can be easily rearranged to read

$$-\frac{1}{\beta} = \begin{pmatrix} 1 & a_0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \ldots \cdot \begin{pmatrix} 1 & a_n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \circ (-\frac{1}{\beta}).$$

It follows that the α and $-1/\beta$ satisfy the same quadratic equation. Therefore $\bar{\alpha} = -1/\beta$, which is clearly between -1 and 0. Thus we have shown that numbers with purely periodic continued fraction expansion are reduced. The following theorem gives the converse of this statement.

Theorem 2.1. *Let α be a reduced quadratic irrational. Then its continued fraction expansion is purely periodical.*

Proof. Although this statement appears deep, and perhaps it is, its proof is not difficult. it is based on the following lemma.

Lemma 2.2. *Let α be a reduced quadratic irrational. Then α_1 is also reduced. Conversely, there exists presicely one reduced β such that $\beta_1 = \alpha$.*

Proof. We have $\alpha > 1$ and $-1 < \bar{\alpha} < 0$. It follows that $0 < \alpha - [\alpha] < 1$ and $\bar{\alpha} - [\alpha] < -1$. After taking the inverse of $\alpha - [\alpha]$, we get $\alpha_1 > 1$ and $-1 < \bar{\alpha_1} < 0$. The first part of the lemma is proved. To prove the second part, let $\gamma = 1/\alpha$. Then $0 < \gamma < 1$ and $\bar{\gamma} < -1$. Now note that $[-\bar{\gamma}]$ is unique positive integer such that $\gamma + [-\bar{\gamma}] > 1$ and $-1 < \bar{\gamma} + [-\bar{\gamma}] < 0$. It follows that $\beta = \gamma + [-\bar{\gamma}]$ is unique reduced quadratic irrational such that $\beta_1 = \alpha$. The lemma is proved. □

Let γ be a reduced quadratic irrational. Let $ax^2 + bx + c$ be the minimal polynomial of γ such that a, b and c are relatively prime integers. This polynomial is unique up to a sign. In any case, the discriminant $D = b^2 - 4ac$ is well defined. To be specific, assume that a is positive. Then, since $\gamma > \bar{\gamma}$, we must have

$$\gamma = \frac{-b + \sqrt{D}}{2a}.$$

Next, the inequalities $\gamma > 1$ and $-1 < \bar{\gamma} < 0$ can be rewritten as

$$-b + \sqrt{D} > 2a \text{ and } -2a < -b - \sqrt{D} < 0.$$

It follows that

$$-b + \sqrt{D} > 2a > b + \sqrt{D} \text{ and } 0 < -b < \sqrt{D},$$

where $0 < -b$ is forced by the first set of inequalities. In particular, it follows that there are only finitely many reduced γ with the fixed discriminant D.

We are now ready to finish the proof of the theorem. Note that the continued fraction algorithm does not change the discriminant of quadratic irrationals. In view of Lemma ? , the algorithm will break up the finite set of reduced irrationals with the fixed discriminant into a disjoint union of finitely many cycles. The theorem is proved. □

Proposition 2.3. *Let $\alpha > 1$ be a quadratic irrational. Then for sufficiently large n, α_{n+1} is reduced.*

Proof. Let $\alpha = [a_0, a_1, \ldots]$ be the continued fraction expansion of α. Recall that

$$\alpha = \frac{A_n \alpha_{n+1} + A_{n_1}}{B_n \alpha_{n+1} + B_{n-1}}$$

by Proposition ?. Since

$$\begin{pmatrix} A_n & A_{n-1} \\ B_n & B_{n-1} \end{pmatrix}^{-1} = \pm \begin{pmatrix} B_{n-1} & -A_{n-1} \\ -B_n & A_n \end{pmatrix}$$

(depending on the parity of n) we have

$$\alpha_{n+1} = \frac{B_{n-1}\alpha_{n+1} - A_{n_1}}{-B_n \alpha_{n+1} + A_n}$$

After conjugating, this equation can be rewritten as

$$\bar{\alpha_{n+1}} = -\frac{B_{n-1}}{B_n} \frac{\bar{\alpha} - A_{n-1}/B_{n-1}}{\bar{\alpha} - A_n/B_n}.$$

The first factor, B_{n-1}/B_n is always strictly less then one. On the other hand, the limit of A_n/B_n is α, and in addition, A_n/B_n is alternatively less then and greater then α. Thus, the second factor is alternatively just smaller and just bigger then 1. Thus, if we chose n such that the second factor is less then one, then $\bar{\alpha_{n+1}} > 1$, as desired. □

Corollary 2.4. *Let $\alpha > 1$ be a quadratic irrational. Then for some element in $GL_2(\mathbb{Z})$,*

$$\alpha' = \frac{a\alpha + b}{c\alpha + d}$$

is reduced.

Theorem 2.5. *Let R be a quadratic order of discriminant $D > 0$. Then its class number $h(D)$ is equal to the number of cycles (under the continued fraction algorithm) of reduced irrationals of discriminant D.*

Proof. Every module is M is similar to a module $M = \{1, \alpha\}$ with $\alpha > 1$. Now take an element in $GL_2(\mathbb{Z})$ as in the previous corollary. Then

$$M = \{c\alpha + d, a\alpha + b\} \sim \{1, \alpha'\}.$$

This shows that the class number is less then the number of the cycles. As far as the converse is concerned, I give up. □