Pell's Equation, Units in real quadratic fields, Continued fractions, Approximations.

October 10, 2012

1 Reading Assignment:

1. Read **[I-R]**Chapter 13, section 1.
2. Suggested reading: Davenport IV sections 1,2.

2 How the Euclidean algorithm, Pell's Equation, Units in real quadratic fields, and continued fractions are all related

3 Pell's Equation

Let D be a positive square-free non-square integer.

$$X^2 - DY^2 = \pm 1$$

Given any solution $(X, Y) = (a, b)$ with $a, b \in Z$ of the above equation, i.e., any *way of expressing* ± 1 *by the (indefinite) binary quadratic form* $X^2 - DY^2$ we can change, appropriately, the sign of a and b to make them both positive, which is sometimes useful, and view the element

$$\alpha := a + b\sqrt{D} \;\in\; Z[\sqrt{D}]^*,$$

in the group of units of the ring $Z[\sqrt{D}]$. Here the four elements obtained by changing the signs of a and/or b—i.e., $\pm a \pm b\sqrt{D}$—give us

$$\pm\alpha, \text{ and } \pm\alpha'$$

where α' is the conjugate of α (and is either the inverse of α or its negative). We also can view α as a real number greater than 1; hence $\alpha \in Z[\sqrt{D}]^*$ is of infinite order. In fact, just forming a product (with positive integers a, b, c, d)

$$(a + b\sqrt{D})(c + d\sqrt{D}) = (ac + Dbd) + (ad + bc)\sqrt{D}$$

shows us that as you pass from α to its higher powers,

$$\alpha, \alpha^2, \alpha^3, \ldots$$

putting $\alpha^n := a_n + \sqrt{D} b_n$ the a_n's and b_n's are monotonically increasing.

Theorem 1 ** Let D be as above. The group of units $Z[\sqrt{D}]^*$ is generated by -1 and a unit $\alpha = a + b\sqrt{D}$ that has the property that*

- *a, b are positive integers, and*
- *among all units $\beta = u + v\sqrt{D}$ with u, v positive integers, we have $a \le u$ and $b \le v$.*

Definition 1 *The α in the theorem above is called the* **fundamental unit** *of* **the ring** *(sic)* $\mathbf{Z}[\sqrt{D}]$.

But discuss the issue of types I and types II. Work with $\sqrt{5}$.

4 The basic "continued fraction move"

Let $\alpha \in \mathbf{R}$ be a real number (say, not an integer; otherwise an ∞ will appear below). Put $a_0 := \lfloor \alpha \rfloor$; put $\beta := \frac{1}{\alpha - a_0}$. We have:

$$\alpha = a_0 + \frac{1}{\beta},$$

noting that such an equation is completely pinned down by α plus the knowledge that a_0 is some integer and β is some number > 1.

To avoid the embarrassment of what happens when α is an integer, you can throw ∞ into the works and let

$$\mathbf{P}^1(\mathbf{R}) = \mathbf{R} \cup \{\infty\}$$

be the real projective line, making this "continued fraction move" $\alpha \mapsto \beta$ well-defined on all elements of $\mathbf{P}^1(\mathbf{R})$ and record the above transformations for α to β and back again, this way:

4.1 $GL_2(\mathbf{Z})$-orbits

For $A \in \mathrm{GL}_2(\mathbf{Z})$

$$A := \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

and z a real number, put $A(z) := \frac{az+b}{cz+d}$.

Now, if

$$T_{a_0} = T := \begin{pmatrix} 0 & 1 \\ 1 & -a_0 \end{pmatrix}$$

we have $T(\alpha) = \beta$. And if

$$S_{a_0} = S := \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix}$$

then $S(\beta) = \alpha$.

5 Iteration of the basic "continued fraction move"

Let $\alpha = a_0 + \frac{1}{\beta}$ with $\beta > 1$. If β is an integer, then stop where you are. If not, rename $\beta =: \alpha_1$ and put

$$\alpha_1 = a_1 + \frac{1}{\alpha_2}$$

where a_1 is an integer and $\alpha_2 > 1$. we have:

$$\alpha = a_0 + \frac{1}{a_1 + \frac{1}{\alpha_2}}.$$

If α_2 is an integer, then stop where you are. If not, continue...

$$\alpha = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3} + \dots}}.$$

5.1 Various notations:

$$\alpha = a_0 + \frac{1}{a_1+}\frac{1}{a_2+}\frac{1}{a_3+}\dots$$

or:

$$\alpha = \{a_0; a_1, a_2, \ldots, a_{n-1}, \alpha_n\} = \{a_0; a_1, a_2, a_3, a_4, \ldots\}$$

This stops finitely if and only if α is rational.

5.2 Some vocabulary

Definition 2 *The a_i's above are called the* **terms**, *or the* **partial quotients**.

Definition 3 *The n*-**th convergent**, *or n-th* **complete quotient** *of α is the rational number:*

$$\frac{P_n}{Q_n} = \{a_0; a_1, a_2, \ldots, a_{n-1}, a_n\}.$$

Note that we've replaced the α_n at the end of $\alpha = \{a_0; a_1, a_2, \ldots, a_{n-1}, \alpha_n\}$ by the integer $a_n := \lfloor \alpha_n \rfloor$. These truncated continued fractions,

$$\frac{P_0}{Q_0} = \{a_0\}, \ \frac{P_1}{Q_1} = \{a_0 a_1\}, \ \ldots \ \frac{P_n}{Q_n} = \{a_0 a_1, a_2, \ldots, a_{n-1}, \alpha_n\} \ldots, a_{n-1}, a_n\}$$

are the rational numbers that occur in the application of Euclid's Algorithm.

To have a name for everything here, let us define:

Definition 4 *If α is a real number and $\alpha = \{a_0; a_1, a_2, \ldots, a_{n-1}, \alpha_n\}$, let's call the "$\alpha_n$" that appears at the end of the n-fold fraction above, the n*-**th revision of** α.

5.3 Revisions

Theorem 2 *If β is a revision of α, then there are matrices A, B inverses of one another in* $\mathrm{GL}_2(\mathbf{Z})$, *such that $A(\alpha) = \beta$ and $B(\beta) = \alpha$.*

Exercise 1 *If β is the n-th revision of α,with $n \geq 2$, then defining A to be the appropriate iterates of the matrices T_{a_i} of Subsection 4.1 above, show that*

$$A := \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

with

$$(-1)^n a > 0, \ (-1)^n d > 0, \ (-1)^{n+1} b > 0, \ (-1)^{n+1} c > 0.$$

Theorem 3 "(auto-revision)" *If α is (not rational and) equal to the n-th revision of itself, then α is a quadratic irrationality.*

Proof: If $\alpha = \frac{u\alpha+v}{w\alpha+t}$ then $w\alpha^2 + (t-u)\alpha - v = 0$.

Theorem 4 *The n-th convergent of α is greater than α if n is odd, and less than α if n is even.*

5.4 Recall examples

$$\sqrt{2} = \{1; 2, 2, 2, 2, \ldots\}$$
$$\sqrt{3} = \{1; 1, 2, 1, 2 \ldots\}$$
$$\sqrt{5} = \{2; 4, 4, 4, 4 \ldots\}$$
$$\sqrt{6} = \{2; 2, 4, 2, 4 \ldots\}$$
$$\frac{1+\sqrt{5}}{2} = \{1; 1, 1, 1, 1, \ldots\}$$

6 The 'general' continued fraction

We now take the 'terms' a_i to be independent variables, and call them q_i.

We'll study the structure of the rational function of the q_i's:

$$q_0 + \frac{1}{q_1+}\frac{1}{q_2+}\frac{1}{q_3+}\cdots$$

So, writing

$$\frac{P_n}{Q_n} = q_0 + \frac{1}{q_1+}\frac{1}{q_2+}\cdots\frac{1}{q_n}$$

(with P_n and Q_n in $\mathbf{Z}[q_0, q_1, \ldots, q_n]$ and the fraction $\frac{P_n}{Q_n}$ in 'lowest terms,' we have:

$$P_0 = q_0;\ Q_0 = 1;\ P_1 = q_0q_1 + 1;\ Q_1 = q_1,$$

and going forward:

$$q_0 + \frac{1}{q_1+}\frac{1}{q_2} = q_0 + \frac{q_2}{q_1q_2+1} = \frac{q_0q_1q_2 + q_0 + q_2}{q_1q_2+1}.$$

SO,

$$P_2 = q_0q_1q_2 + q_0 + q_2; \quad Q_2 = q_1q_2 + 1.$$

Go once more:

$$P_3 = q_0q_1q_2q_3 + q_0q_1 + q_0q_3 + q_2q_3 + 1.$$

$$Q_3 = q_1q_2q_3 + q_1 + q_3.$$

6.1 New notation!

Definition 5

$$P_n = [q_0, q_1, q_2, \ldots, q_n] \quad \in \quad Z[q_0, q_1, q_2, \ldots, q_n].$$

6.2 Recurence relations

Proposition 1

$$Q_n = [q_1, q_2, q_3, \ldots, q_n] \quad \in \quad Z[q_0, q_2, q_3, \ldots, q_n].$$

Proposition 2

$$[q_0, q_1, q_2, \ldots, q_n] = q_0[q_1, q_2, q_3, \ldots, q_n] + [q_2, q_3, \ldots, q_n].$$