Thursday, November 28

Lemma: Every quadratic irrational $r + s\sqrt{c}$, where $r, s \in \mathbb{Q}$ and $c \in \mathbb{N}$ that is not a square ($c \in \mathbb{N} \setminus \mathbb{N}^2$), can be written as $(m+\sqrt{d})/q$ where $m, q \in \mathbb{Z}$, $d \in \mathbb{N} \setminus \mathbb{N}^2$, and $q \mid (d-m^2)$.

Proof: If we write $r = \frac{a}{e}$ and $s = \frac{b}{e}$ with a common denominator, then

$$r+s\sqrt{c} = \frac{a+b\sqrt{c}}{e} = \frac{a+\sqrt{cb^2}}{e} = \frac{ae+\sqrt{cb^2e^2}}{e^2}$$

//

The Quadratic Irrational Process:

Let $\xi_0 = \frac{m_0+\sqrt{d}}{q_0}$, where $m_0, q_0 \in \mathbb{Z}$, $d \in \mathbb{N} \setminus \mathbb{N}^2$, and $q_0 \mid (d-m_0^2)$. For $j \geq 0$, define

$a_j = \lfloor \xi_j \rfloor$, $m_{j+1} = a_j q_j - m_j$, $q_{j+1} = \dfrac{d-m_{j+1}^2}{q_j}$,

and $\xi_{j+1} = \dfrac{m_{j+1}+\sqrt{d}}{q_{j+1}}$.

Then the a_j and ξ_j are the same as what we'd get from The Process, so that $\xi_0 = \langle a_0, a_1, \ldots, a_{j-1}, \xi_j \rangle$. Moreover, $q_j \in \mathbb{Z}$ and $q_j \mid (d-m_j^2)$ for all $j \geq 0$.

Sketch of proof:

- We need to check $\dfrac{1}{\xi_j - a_j} = \xi_{j+1} = \dfrac{m_{j+1}+\sqrt{d}}{q_{j+1}}$; use definitions to show both sides equal $\dfrac{q_j}{m_j - a_j q_j + \sqrt{d}}$.
- Showing $q_j \in \mathbb{Z}$ means showing $q_{j-1} \mid (d-m_j^2)$.

But modulo q_{j-1},

$$d-m_j^2 = d-(a_{j-1}q_{j-1}-m_{j-1})^2$$
$$\equiv d-(0-m_{j-1})^2 = d-m_{j-1}^2 \equiv 0 \pmod{q_{j-1}}$$

by definition.

... ...

//

Theorem: Given a quadratic irrational ξ_0, let (q_j) and (m_j) be from the Quadratic Irrational Process.

(1) The sequence (q_j) is eventually positive.

(2) The (q_j) and (m_j) are bounded.

(3) The continued fraction for ξ_0 is eventually periodic.

Sketch of proof:

(1) is somewhat nontrivial. See Theorem 7.19 in Niven/Zuckerman/Montgomery.

(1) $\Rightarrow$ (2): Note that $q_j q_{j+1} + m_{j+1}^2 = d$; once the q_j are positive, we deduce that

$|m_{j+1}| \le \sqrt{d}$ and $q_{j+1} \le d$.

(2) $\Rightarrow$ (3): Since (m_j) and (q_j) are bounded, there are only finitely many possibilities for $\xi_{j+1} = \dfrac{m_{j+1}+\sqrt{d}}{q_{j+1}}$; once (ξ_j) hits a duplicate, the whole sequence repeats. //

Theorem: Let $d \in \mathbb{N} \setminus \mathbb{N}^2$ and set $c = \lfloor \sqrt{d} \rfloor$. Then $c + \sqrt{d}$ has a purely periodic continued fraction $\langle \overline{a_0; a_1, \ldots, a_{r-1}} \rangle$. (Note $a_0 = 2c$.) It follows that

$\sqrt{d} = \langle c; \overline{a_1, \ldots, a_r} \rangle$ where $a_r = 2c$.

Example: $\sqrt{41} = \langle 6; \overline{2, 2, 12} \rangle$ $(r=3)$

$\sqrt{28} = \langle 5; \overline{3, 2, 3, 10} \rangle$. $(r=4)$

Proof omitted; uses the Quadratic Irrational Process on $\dfrac{0+\sqrt{d}}{1}$. (Chapter 7 of NZM).

Facts coming out of the proof:

- q_j never equals -1;
- q_j equals 1 if and only if $r \mid j$

(where r is the period).

Pell's equation: We want to solve

$X^2 - dY^2 = \pm 1$ in integers X, Y, for $d \in \mathbb{N} \setminus \mathbb{N}^2$.

"Pell" has $< \varepsilon$ to do with Pell's equation.

History:

- $d=2$ case goes back to 4th century BCE (India, Greece).
- General case: 7th century CE, India (Brahmagupta). ....
- Europe: 17th century, Brouncker.
- Euler mistakenly said it was due to Pell.

Theorem: Let $d \in \mathbb{N} \setminus \mathbb{N}^2$, and let $x, y \in \mathbb{Z}$. If $|x^2 - dy^2| \le \sqrt{d}$, then $\frac{x}{y}$ is a convergent to $\sqrt{d}$.

Sketch of proof: If $x^2 - dy^2 = s$ where s is "small", then (say $x, y > 0$)

$$s = (x - y\sqrt{d})(x + y\sqrt{d}) \approx (x - y\sqrt{d})\, 2y\sqrt{d};$$

so $x - y\sqrt{d} \approx \frac{s}{2y\sqrt{d}}$

$$\frac{x}{y} - \sqrt{d} \approx \frac{1}{y^2} \frac{s}{2\sqrt{d}}.$$

There's a theorem that if $\frac{x}{y} - \xi$ is small enough, then $\frac{x}{y}$ is a convergent. //

So we care about the values $h_j^2 - dk_j^2$, where h_j/k_j are the convergents to $\sqrt{d}$. But we saw a pattern from Group Work #10: with q_j from the Quadratic Irrational Process,

$$h_j^2 - dk_j^2 = (-1)^{j+1} q_{j+1}.$$

(Theorem 7.22 in NZM)

(proof uses: if $a + b\sqrt{d} = a' + b'\sqrt{d}$, then $a = a'$ and $b = b'$.)

Theorem (solving Pell's equation)

(Theorem 7.25 in NZM)

Let $d \in \mathbb{N} \setminus \mathbb{N}^2$, and let h_j/k_j be the convergents to $\sqrt{d}$, and let r be the period of the continued fraction to $\sqrt{d}$.

- All positive solutions to $x^2 - dy^2 = \pm 1$ are $x = h_{jr-1}$, $y = k_{jr-1}$ for all $j \geq 0$.

(Note $h_{-1} = 1$, $k_{-1} = 0$ is a solution)

- If r is even, then $h_{jr-1}^2 - dk_{jr-1}^2 = 1$ always, and $x^2 - dy^2 = -1$ has no solutions.
- If r is odd, then $h_{jr-1}^2 - dk_{jr-1}^2$ equals -1 when j is odd, and equals $+1$ when j is even.

Definition: Let the fundamental solution to $x^2 - dy^2 = \pm 1$ be $x_1 = h_{r-1}$, $y_1 = k_{r-1}$.

Theorem: (Theorem 7.26 in NZM)

All positive solutions to $x^2 - dy^2 = \pm 1$ are given by (x_j, y_j) where

$$x_j + y_j\sqrt{d} = (x_1 + y_1\sqrt{d})^j.$$

Examples: For $\sqrt{41}$, the fundamental solution is $x_1 = 32$, $y_1 = 5$.

$\sqrt{41} = \langle 6; \overline{2, 2, 12} \rangle$, so $r = 3$ is odd.

So $32^2 - 41 \cdot 5^2 = -1$.

The next solutions come from

$(32 + 5\sqrt{41})^2 = 2{,}049 + 320\sqrt{41}$,

$(32 + 5\sqrt{41})^3$, ...

- For $\sqrt{28} = \langle 5; \overline{3, 2, 3, 10} \rangle$, $r = 4$.

- No solutions to $x^2 - 28y^2 = -1$.
- fundamental solution is $x_1 = 127$, $y_1 = 24$.

$\therefore (127 + 24\sqrt{28})^j$.

Observation: Suppose $x^2 - dy^2 = -1$.

Then $x^2 \equiv -1 \pmod{d}$; this implies that ($4 \nmid d$ and) no prime of the form $4k+3$ divides d.

- If $3 \mid d$, then the period of the CF for $\sqrt{d}$ has even length.

But this is not sufficient: there are moduli d for which -1 is a quadratic residue, yet $x^2 - dy^2 = -1$ has no solutions.

Ex: $d = 34$, $d = 205$.

[Algebraic number theory:

- lying about a few details!

When $d \in \mathbb{N} \setminus \mathbb{N}^2$, the ring $\mathbb{Z}[\sqrt{d}]$ has infinitely many units (elements w/ multiplicative inverse), of the form $x + y\sqrt{d}$ where $x^2 - dy^2 = \pm 1$.

($(x+y\sqrt{d})(x-y\sqrt{d}) = x^2 - dy^2$)

$\varepsilon = x_1 + y_1\sqrt{d}$ is the fundamental unit of $\mathbb{Z}[\sqrt{d}]$; and every unit is of the form $\pm \varepsilon^j$ for some $j \in \mathbb{Z}$.

Fundamental unit big or small

"class group" or "class number" of $\mathbb{Q}(\sqrt{d})$]