18.781 — 16 Apr 2003

Goal: Find all solutions of $x^2 - dy^2 = 1$, with x, y positive integers, $d > 0$, not a square.

trivial sol'ns: $(\pm 1, 0)$.

$\sqrt{d} = \langle a_0, a_1, \dots \rangle$

$\xi_i = \langle a_i, \dots \rangle$ $\quad a_i = \lfloor \xi_i \rfloor$ $\quad \xi_i = \dfrac{m_i + \sqrt{d}}{q_i}$ $\quad m_{i+1} = a_i q_i - m_i$ $\quad q_{i+1} = \dfrac{d - m_{i+1}^2}{q_i}$

$h_n\ k_n$

Thrm 1: Any positive solution (s, t) of $x^2 - dy^2 = 1$ is equal to (h_n, k_n) for some n.

Thrm: $\sqrt{d} = \langle a_0, \overline{a_1, a_2, \dots, a_{r-1}, 2a_0} \rangle$ where $a_0 = \lfloor \sqrt{d} \rfloor$. Also, $q_i = 1$ iff $r \mid i$ and q_i is never -1.

Proof:

$\xi = \sqrt{d} + \lfloor \sqrt{d} \rfloor > 1$. $\quad \xi' = \lfloor \sqrt{d} \rfloor - \sqrt{d} \in (-1, 0)$.

Thus, from last time, $\xi = \langle \overline{b_0, \dots, b_{r-1}} \rangle$

$b_0 = \lfloor \xi \rfloor = 2 \lfloor \sqrt{d} \rfloor$.

$\sqrt{d} = -\lfloor \sqrt{d} \rfloor + \xi = -\lfloor \sqrt{d} \rfloor + \langle 2\lfloor \sqrt{d} \rfloor, \overline{b_1, \dots, b_{r-1}, b_0} \rangle = -\lfloor \sqrt{d} \rfloor + 2\lfloor \sqrt{d} \rfloor + \dfrac{1}{\dots} = \langle \lfloor \sqrt{d} \rfloor, \overline{b_1, \dots, b_{r-1}, 2\lfloor \sqrt{d} \rfloor} \rangle$

which is form of theorem.

$\xi_i = \langle a_i, a_{i+1}, \dots \rangle$ $\quad \xi_0 = \xi_r = \xi_{2r} = \dots$

and $\xi_1, \xi_2, \dots, \xi_{r-1}$ all different by minimality.

$\xi_{jr} = \dfrac{m_{jr} + \sqrt{d}}{q_{jr}} = \xi = \lfloor \sqrt{d} \rfloor + \sqrt{d} \Rightarrow m_{jr} - q_{jr} \lfloor \sqrt{d} \rfloor = (q_{jr} - 1)\sqrt{d} \Rightarrow q_{jr} = 1$.

$q_i = 1$. $\xi_i = m_i + \sqrt{d}$. ξ_i purely periodic, so $\xi_i > 1$ and $-1 < \xi_i' < 0$

$-1 < m_i - \sqrt{d} < 0 \Rightarrow -1 + \sqrt{d} < m_i < \sqrt{d} \Rightarrow m_i = \lfloor \sqrt{d} \rfloor$

which implies $\xi_i = \xi_0$, which only happens when $r \mid i$

If $q_i = -1$, $\xi_i = -m_i - \sqrt{d}$ $\qquad -m_i - \sqrt{d} > 1$ $\qquad -1 < -m_i + \sqrt{d} < 0 \Rightarrow -1 - \sqrt{d} > m_i > \sqrt{d}$

can't happen ($-1-\sqrt{d}$ negative, $\sqrt{d}$ positive).

Cor: $h_n^2 - dk_n^2 = (-1)^{n-1} q_{n+1}$ for all $n \geq -1$

Proof:

$\sqrt{d} = \xi_0 = \dfrac{\xi_{n+1} h_n + h_{n-1}}{\xi_{n+1} k_n + k_{n-1}} = \dfrac{(m_{n+1} + \sqrt{d}) h_n + q_{n+1} h_{n-1}}{(m_{n+1} + \sqrt{d}) k_n + q_{n+1} k_{n-1}} = \sqrt{d} \rightsquigarrow$

$dk_n = h_n m_{n+1} + q_{n+1} h_{n-1}$ $\qquad h_n = m_{n+1} k_n + q_{n+1} k_{n-1}$

$dk_n^2 = h_n k_n m_{n+1} + q_{n+1} k_n h_{n-1}$

$-\ h_n^2 = h_n k_n m_{n+1} + q_{n+1} k_{n-1} h_n$

$dk_n^2 - h_n^2 = q_{n+1}(k_n h_{n-1} - k_{n-1} h_n) \Rightarrow h_n^2 - dk_n^2 = q_{n+1}(-1)^{n-1}$.

More precise version of Thrm 1:

Thrm: r order of expansion of root d.

Case 1: r even, then set of sol'n of $x^2 - dy^2 = 1$ are given by $\{(h_{nr-1}, k_{nr-1})\}_{n=1}^{\infty}$

Case 2: r odd, then set of sol'n of $x^2 - dy^2 = 1$ are given by $\{(h_{nr-1}, k_{nr-1})\}$ $n = 2, 4, 6, 8, \dots$

Proof:

In general: $h_{nr-1}^2 - d k_{nr-1}^2 = (-1)^{nr-2} q_{nr} = (-1)^{nr-2} = (-1)^{nr}$

This show all of the above are solutions.

Recall:

$\left|\frac{E}{M} - \sqrt{d}\right| < \frac{1}{2M^2} \Rightarrow \frac{E}{M} = \frac{h_n}{k_n}$, proved some time ago.

Thus, we must show all sol'n satisfy this inequality

- Say (E, M) is a sol'n of $x^2 - dy^2 = 1$. Then (E, M) rel. prime. Thus enough to show $\frac{E}{M} = \frac{h_n}{k_n}$

$\frac{E}{M} - \sqrt{d} = \frac{1}{M(E + M\sqrt{d})}$, since $E^2 - dM^2 = 1 \Rightarrow (E - \sqrt{d}M)(E + \sqrt{d}M) = 1$

$0 < \frac{E}{M} - \sqrt{d} < \frac{\sqrt{d}}{M(E + M\sqrt{d})} = \frac{1}{M^2\left(\frac{E}{M\sqrt{d}} + 1\right)}$

$\frac{E}{M} - \sqrt{d} > 0 \Rightarrow \frac{E}{M\sqrt{d}} > 1 \Rightarrow \frac{E}{M\sqrt{d}} + 1 > 2$

$\Rightarrow \left|\frac{E}{M} - \sqrt{d}\right| < \frac{1}{2M^2} \Rightarrow \frac{E}{M} = \frac{h_n}{k_n}$

Note that since h_n, k_n strictly increasing, natural order on (h_n, k_n).

Thrm: If (x_1, y_1) is smallest solution, then all other solutions given by

$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n$