# Math 445 Number Theory

November 10, 2004

What can $h_s^2 - nk_s^2$ equal?

Wherever we choose to stop the continued fraction expansion of $\sqrt{n} = [\lfloor\sqrt{n}\rfloor, \overline{a_1, \ldots, a_{m-1}, 2\lfloor\sqrt{n}\rfloor}]$, $\sqrt{n} = [a_0, \ldots, a_s, \zeta_{s+1}] = [a_0, \ldots, a_s, \dfrac{\sqrt{n}+m_s}{q_{s+1}}]$, we find that

$$\sqrt{n} = \frac{\frac{\sqrt{n}+m_s}{q_{s+1}}h_s + h_{s-1}}{\frac{\sqrt{n}+m_s}{q_{s+1}}k_s + k_{s-1}} = \frac{(\sqrt{n}+m_s)h_s + q_{s+1}h_{s-1}}{(\sqrt{n}+m_s)k_s + q_{s+1}k_{s-1}}\ .$$ Then

$\sqrt{n}(m_s k_s + q_{s+1}k_{s-1} - h_s) = (m_s k_s + q_{s+1}h_{s-1} - nk_s)$ so both sides of this equation are 0 (otherwise $\sqrt{n}$ is rational!), so $h_s = m_s k_s + q_{s+1}k_{s-1}$ and $nk_s = m_s k_s + q_{s+1}h_{s-1}$ Then

$h_s^2 - nk_s^2 = h_s(m_s k_s + q_{s+1}k_{s-1}) - k_s(m_s k_s + q_{s+1}h_{s-1}) = q_{s+1}(h_s k_{s-1}) - h_{s-1}k_s) = (-1)^{s-1}q_{s+1}$ .

So the only $N$ with $|N| \le \sqrt{n}$ for which $x^2 - ny^2 = N$ can be solved are (squares and) those for which $N = (-1)^{s-1}q_{s+1}$ where $\zeta_{s+1} = \dfrac{\sqrt{n}+m_s}{q_{s+1}}$ .

Focusing on $N = 1$, note that since $\zeta_0 = \dfrac{\sqrt{n}+\lfloor\sqrt{n}\rfloor}{1}$, $m_0 = \lfloor\sqrt{n}\rfloor$ and $q_1 = 1$ . Then since $\zeta_0 = \zeta_m = \zeta_{2m} = \cdots$ , we have $q_{mt+1} = 1$ for all $t \ge 0$. So $h_{m-1}^2 - nk_{m-1}^2 = (-1)^m$ .

If $m$ is even, then we have found a solution to $x^2 - ny^2 = 1$ . If $m$ is odd, then apply the same reasoning, except with <u>two</u> periods of the continued fraction: $\sqrt{n} = [a_0, \ldots, a_{m-1}, a_m, \ldots, a_{2m-1}, \sqrt{n} + a_0]$, and the same argument shows that $h_{2m-1}^2 - nk_{2m-1}^2 = (-1)^{2m} = 1$ . In general, taking $t$ periods, we get $h_{tm-1}^2 - nk_{tm-1}^2 = (-1)^{tm}$ . So we have shown that $x^2 - ny^2 = 1$ always has a solution; $x = h_{2m-1}, y = k_{2m-1}$ where $m =$ the period of the continued fraction of $\sqrt{n}$ , will always work.

This is best illustrated with an example! Taking $n = 19$, we have

$a_0 = 4$ , $x_0 = \sqrt{19} - 4, \zeta_1 = \dfrac{\sqrt{19}+4}{3}$ ,

$a_1 = 2$ , $x_1 = \dfrac{\sqrt{19}-2}{3}, \zeta_2 = \dfrac{\sqrt{19}+2}{5}$ ,

$a_2 = 1$ , $x_2 = \dfrac{\sqrt{19}-3}{5}, \zeta_3 = \dfrac{\sqrt{19}+3}{2}$ ,

$a_3 = 3$ , $x_3 = \dfrac{\sqrt{19}-3}{2}, \zeta_4 = \dfrac{\sqrt{19}+3}{5}$ ,

$a_4 = 1$ , $x_4 = \dfrac{\sqrt{19}-2}{5}, \zeta_5 = \dfrac{\sqrt{19}+2}{3}$ ,

$a_5 = 2$ , $x_5 = \dfrac{\sqrt{19}-4}{3}, \zeta_6 = \dfrac{\sqrt{19}+4}{1}$ ,

$a_6 = 8$ , $x_6 = \sqrt{19} - 4 = x_0$ , and we can compute

$h_0 = 4, h_1 = 9, h_2 = 13, h_3 = 48, h_4 = 61, h_5 = 170, h_6 = 1421, \ldots$

$k_0 = 1, k_1 = 2, k_2 = 3, k_3 = 11, k_4 = 14, k_5 = 39, k_6 = 325, \ldots$

From our analysis above, $(h_5)^2 - 19(k_5)^2 = (-1)^6 = 1$ , so $(170, 39)$ is a solution to $x^2 - 19y^2 = 1$ . Also, the values of $(-1)^{s-1}q_{s+1}$ are $-3, 5, -2, 5, -3, 1, -3, 5, -2, 5, \ldots$, so among $-4, -3, \ldots, 3, 4$ , the only $N$ for which $x^2 - 19y^2 = N$ has a solution are $N = -3, -2$, and 1 (and 4, because it is a perfect square). By continuing to compute convergents, we can find infnitely many solutions for each such equation.