Math 445 Number Theory

November 12, 2004

Our basic result: if $\sqrt{n} = [\lfloor\sqrt{n}\rfloor, \overline{a_1, \ldots, a_{m-1}, 2\lfloor\sqrt{n}\rfloor}]$, with period of length m, then if $\sqrt{n} = [a_0, \ldots, a_s, \dfrac{\sqrt{n}+m_s}{q_{s+1}}]$, then $h_s^2 - nk_s^2 = (-1)^{s-1}q_{s+1}$. In particular, since $1 = q_m = q_{2m} = \ldots$, we have $h_{mt-1}^2 - nk_{mt-1}^2 = (-1)^{mt-2} = (-1)^{mt}$. So if m is even, we find solutions for $x^2 - ny^2 = 1$ with every turn through the period; if m is odd, we find solutions with every two turns (and solutions to $x^2 - ny^2 = -1$ for the alternate turns).

For example: $x^2 - 11y^2 = N$.

$3 < \sqrt{11} < 4$, so $a_0 = 3$, $x_0 = \sqrt{11} - 3$; $\zeta_1 = \dfrac{\sqrt{11}+3}{2}$, $a_1 = 3$, $x_1 = \dfrac{\sqrt{11}-3}{2}$;
$\zeta_2 = \dfrac{\sqrt{11}+3}{1}$, $a_2 = 6$, $x_2 = \dfrac{\sqrt{11}-3}{1}$;
and so $\sqrt{11} = [3, \overline{3, 6}]$, and $q_0 = 1$, $q_1 = -2$, $q_2 = 1$, $q_3 = -2$, etc.
Since the length of the period of the continued fraction of $\sqrt{11}$, 2, is even, after the first trip through the repeating part, $h_1^2 - 11k_1^2 = 10^2 - 11 \cdot 3^2 = (-1)^0 q_2 = 1$. Also, since the only numbers occuring as $(-1)^{s-1}q_{s+1}$ are -2 and 1, the only N with $|N| \leq \sqrt{11}$ for which $x^2 - 11y^2 = N$ has solutions are $N = -2, 1$ and 4 (since 4 is a perfect square). So, e.g., $x^2 - 11y^2 = 3$ has no solutions with $x, y \in \mathbb{Z}$.
On the other hand, $x^2 \equiv 3 \pmod{11}$ <u>does</u> have solutions, since we can compute (as we have before) that $\left(\dfrac{3}{11}\right) = 1$. So $x^2 - 11y = 3$ does have solutions with $x, y \in \mathbb{Z}$.

Since we know that, if n is not a perfect square, $x^2 - ny_2 = 1$ has inifinitely many solutions with $x, y \in \mathbb{Z}$, the equation $(x^2 - ny^2)(a^2 - nb^2) = (xa \pm nyb)^2 - n(xb \pm ya)^2$ shows that if $a^2 - nb^2 = N$ has a solution, then it in fact has infinitely many solutions. By choosing a solution to $x^2 - ny_2 = 1$ with x and y large, we can build a solution to $a^2 - nb^2 = N$ with a and b as large as we like.

There is an alternative approach to generating solutions to $a^2 - nb^2 = N$: if we have that $a^2 - nb^2 = N$ and $x^2 - ny^2 = 1$, then, for any m,

$$(a^2 - nb^2)(x^2 - ny^2)^m = N = (a - \sqrt{n}b)(x - \sqrt{n}y)^m (a + \sqrt{n}b)(x + \sqrt{n}y)^m$$

But we can, by collecting terms, write $(a - \sqrt{n}b)(x - \sqrt{n}y)^m = A - \sqrt{n}B$ for some $A, B \in \mathbb{Z}$; then $(a + \sqrt{n}b)(x + \sqrt{n}y)^m = A + \sqrt{n}B$, because the product of the *rational conjugates* of two quadratic irrationals is the conjugate of their product (just like complex conjuagtion). So $(A - \sqrt{n}B)(A + \sqrt{n}B) = A^2 - nB^2 = N$ gives another solution to the same Pell equation.