

Math 104B, Number Theory, Winter 2003.

Lecture 23. Brahmagupta-Bhaskara equation.

Last time, we mentioned a Theorem:

Theorem. The best approximations of x are precisely the convergents of the continued fraction expansion of x .

We proved the corollary:

Corollary. If

$$\left| x - \frac{p}{q} \right| < \frac{1}{2q^2},$$

then p/q is a best approximation to x and so p/q is a convergent of the continued fraction expansion of x .

Hence if (x, y) is a solution to the Brahmagupta-Bhaskara equation $x^2 - dy^2 = 1$, then x/y is a convergent of the continued fraction expansion of \sqrt{d} .

Example. Find the solutions to $x^2 - 8y^2 = 1$.

Solution. The continued fraction expansion of $\sqrt{7}$ is $[2, \overline{1, 1, 1, 4}]$. The convergents are

$$\frac{p}{q} : \quad \frac{2}{1}, \frac{3}{1}, \frac{5}{2}, \frac{8}{3}, \frac{37}{14}, \frac{45}{17}, \frac{82}{31}, \frac{127}{48}, \frac{590}{223}, \frac{717}{271}, \frac{1307}{494}, \dots$$

and the values of $p^2 - 7q^2$ are

$$-3, 2, -3, 1, -3, 2, -3, 1, -3, 2, -3, \dots$$

We notice that the values of $p^2 - 7q^2$ are periodic with period 4, just like the continued fraction expansion of $\sqrt{7}$. Example 4.5.7 computes the values of $p^2 - 13q^2$ for the convergents p/q of $\sqrt{13}$. Slightly different behavior occurs in this case, but the next Theorem shows that every case is similar to one of these two.

Theorem. Suppose d is a positive integer which is not a perfect square and $\sqrt{d} = [a_0, \overline{a_1, \dots, a_m}]$, where m is the smallest period. If p_k/q_k is the k th convergent of the continued fraction expansion of \sqrt{d} , then the list of numbers $p_k^2 - dq_k^2$ is periodic with period m . If m is even, then the solutions of $x^2 - dy^2 = 1$ are the numbers $(x, y) = (p_{jm-1}, q_{jm-1})$ for $j \geq 1$. If m is odd, then the solutions are the numbers $(x, y) = (p_{jm-1}, q_{jm-1})$ for j even.

Proof. We showed by induction that the complete quotients x_k of the continued fraction expansion of \sqrt{d} have the form

$$x_k = \frac{A_k + \sqrt{d}}{B_k}$$

1

where A_k and B_k are integers. We claim that the smallest period m of the continued fraction expansion is the first positive value of m with $B_m = 1$. Indeed, if the continued fraction expansion of \sqrt{d} has period m then $x_{m+1} = x_1$, so $\{x_m\} = \{x_0\}$ and $x_m = \sqrt{d} + \text{integer}$, so $B_m = 1$. Conversely, if $B_m = 1$, then $x_m = A_m + \sqrt{d}$, so

$$x_{m+1} = \frac{1}{\{x_m\}} = \frac{1}{\{\sqrt{d}\}} = x_1.$$

Hence the period is m . We see that the $B_k = 1$ precisely when $k = jm$ for some integer j . We showed previously that for $k \geq 1$, A_k and B_k are both positive. We need the following result:

Theorem 12.1.2.

$$p_k^2 - dq_k^2 = (-1)^{k+1} B_{k+1}.$$

From this we see that $p_k^2 - dq_k^2 = 1$ precisely when $B_{k+1} = 1$ and $k + 1$ is even. Thus we need $k = jm - 1$ for some integer j , and jm even. But if m is even then jm is always even, while if m is odd, then jm is even precisely when m is even.

Proof. We gave the proof in the book.

Finally, we note that once we have found the **fundamental solution** to $x^2 - dy^2 = 1$ given by $(x, y) = (a, b) = (p_{m-1}, q_{m-1})$ if m is even and $(x, y) = (a, b) = (p_{2m-1}, q_{2m-1})$ if m is odd, then all other solutions (x, y) can be obtained from computing

$$x + y\sqrt{d} = (a + \sqrt{db})^k$$

for integers k . This is quicker than computing more terms in the continued fraction expansion, especially if the period m is large.

Example. The fundamental solution of $x^2 - 7y^2 = 1$ is $(a, b) = (8, 3)$. Then computing

$$(8 + 3\sqrt{7})^2 = 127 + 48\sqrt{7}$$

gives the next solution $(127, 48)$. The next solution will be obtained from $(8 + 3\sqrt{7})^3$, that is $(127 \cdot 8 + 3 \cdot 7 \cdot 48, 127 \cdot 3 + 8 \cdot 48) = (2024, 765)$