A MIDPOINT CRITERION FOR THE DIOPHANTINE EQUATION $ax^2 - by^2 = \pm 1$

KEITH MATTHEWS

Let $1 < a < b, \gcd(a, b) = 1, d = ab$, where d is not a perfect square. Then it is well-known (Satz 3.10,[2, p. 81]) that the continued fraction expansion of $\alpha = \sqrt{b/a} = \sqrt{d/a}$ is periodic, with period length l:

$$\sqrt{b/a} = [a_0, \overline{a_1, \dots, a_{l-1}, 2a_0}]$$

and that the sequence a_1, \ldots, a_{l-1} is palindromic, as are P_1, \ldots, P_l and Q_1, \ldots, Q_l , where $(P_i + \sqrt{d})/Q_i$ is the *i*-th complete quotient to α .

Now assume (x, y) is a positive solution of the diophantine equation (1) $ax^2 - by^2 = \pm 1.$

Then gcd(x, y) = 1 and

$$\begin{aligned} x/y - \sqrt{b/a} &| = \frac{1}{(x\sqrt{a} + y\sqrt{b})y\sqrt{a}} \\ &= \frac{1}{(\frac{x}{y}\sqrt{\frac{a}{b}} + 1)y^2\sqrt{ab}} \\ &< 1/2y^2. \end{aligned}$$

Hence by Lagrange's criterion, $x/y = A_{t-1}/B_{t-1}$, a convergent to α . Also $aA_{t-1}^2 - bB_{t-1}^2 = (-1)^t Q_t$, where $(P_t + \sqrt{d})/Q_t$ is the *t*-th complete quotient for α . Hence $Q_t = 1$. As $(P_t + \sqrt{d})/Q_t$ is reduced, it follows that $P_t = \lfloor \sqrt{d} \rfloor$ and hence $P_t = P_{t+1}$, as $(P_{t+1} + \sqrt{d})/Q_{t+1}$ is also the first complete quotient in the continued fraction expansion of \sqrt{d} . This means that the period length l of $(\sqrt{d})/a$ is even, l = 2h and that t = (2k+1)h, or t = 2kh. But t = 2kh implies $Q_t = Q_0 = 1$, and so $a = Q_0 = 1$. Hence t = (2k+1)h and $Q_t = Q_h = 1$.

Conversely assume l = 2h and $Q_h = 1$. Then

$$aA_{h-1}^2 - bB_{h-1}^2 = (-1)^h Q_h = (-1)^h.$$

Also $Q_i > 1$ if $1 \le i < h$. Hence (A_{h-1}, B_{h-1}) is the least positive solution of $ax^2 - by^2 = \pm 1$. Also the evenness of h implies $ax^2 - by^2 = 1$ is soluble, but $ax^2 - by^2 = -1$ is insoluble, while h odd implies

Date: 17th May 2012.

 $ax^2 - by^2 = -1$ is soluble, but $ax^2 - by^2 = 1$ is insoluble. Hence we have proved the following.

Theorem 1. Let 1 < a < b, gcd(a, b) = 1, d = ab, where d is not a perfect square. Then

- (i) if (1) is soluble in positive integers (x, y), the period-length l is even, say l = 2h and $Q_h = 1$.
- (ii) Conversely if l = 2h and $Q_h = 1$, then

 - (a) (A_{h-1}, B_{h-1}) is the least positive solution of $ax^2 by^2 = \pm 1$. (b) If h is odd, then $ax^2 by^2 = -1$ is soluble, but $ax^2 by^2 = 1$ is insoluble.
 - (c) If h is even, then $ax^2 by^2 = 1$ is soluble, but $ax^2 by^2 = -1$ is insoluble.

Remark 1. Hence if the period length l is odd, or if l is even, say l = 2h and $Q_h \neq 1$, then $ax^2 - by^2 = \pm 1$ is not soluble.

Example 1. a = 9, b = 200. Here $l = 8, h = 4, Q_4 = 1$ and $9x^2 - 1$ $200y^2 = 1$ has least solution $(x, y) = (A_3, B_3) = (33, 7).$

Example 2. a = 23, b = 52. Here $l = 6, h = 3, Q_3 = 1$ and $23x^2 - 2x^2 - 3x^2 - 3x^2$ $52y^2 = -1$ has least solution $(x, y) = (A_2, B_2) = (3, 2)$.

Remark 2. We saw that the period lengths of \sqrt{ab} and $(\sqrt{ab})/a$ are equal if (1) is soluble. Hence if the diophantine equation $x^2 - aby^2 = -1$ is soluble and $1 < a < b, \gcd(a, b) = 1$ where ab is not a perfect square, it follows that $ax^2 - by^2 = \pm 1$ is not soluble in integers. As pointed out in [1], this was proved under more restrictive conditions in [3].

Remark 3. In the case of solubility of $ax^2 - by^2 = \pm 1$, we have $a_h =$ $2P_h$.

Acknowledgment. Theorem 1 was pointed out to the author by Jim White. Theorem 3 of [1] states a corresponding result in terms of the continued fraction expansion of \sqrt{ab} .

References

- [1] R. A. Mollin, A continued fraction approach to the Diophantine equation $ax^2 by^2 = \pm 1$, JP. J. Algebra Number Theory, Appl. 4, (2004), 159–207.
- O. Perron, Die Lehre von den Kettenbrüchen, Teubner 1954.
- [3] D. T. Walker, On the Diophantine Equation $mX^2 nY^2 = \pm 1$, Amer. Math. Monthly, 74 (1967), 504-513.

 $\mathbf{2}$