

# A divisibility property of the continued fraction of a quadratic irrational

KEITH MATTHEWS

krm@maths.uq.edu.au

*Department of Mathematics, University of Queensland, Brisbane, Australia*

JOHN ROBERTSON

jpr2718@aol.com

*Platinum Underwriters Reinsurance, Inc., New York, NY, USA*

**Abstract.** The divisibility property  $\gcd(Q_0, B_n) | Q_{n+1}$  of the continued fraction of  $(P_0 + \sqrt{D})/Q_0$  is proved. This implies that the main algorithm presented in a recent paper of K.R. Matthews on the diophantine equation  $x^2 - Dy^2 = N$  finds only primitive solutions.

**Keywords:** gcd, continued fraction, convergents

2000 Mathematics Subject Classification: Primary-11A55

## 1. Introduction

In the introduction to a paper of W. Patz [5], O. Perron showed how to construct integer solutions of the equation  $x^2 - Dy^2 = N$ , where  $D > 1$  is not a perfect square. Let  $Q_0 = |N|$  and  $P_0$  be a solution of the congruence  $P_0^2 \equiv D \pmod{Q_0}$ . If  $\omega_n = (P_n + \sqrt{D})/Q_n$  is the  $n$ -th complete quotient of the simple continued fraction for  $\omega = (P_0 + \sqrt{D})/Q_0$  and  $A_n/B_n$  is the  $n$ -th convergent to  $\omega$ , then  $G_n = Q_0 A_n - P_0 B_n$  and (see [3, pages 246-248])

$$G_n^2 - DB_n^2 = (-1)^{n+1} Q_0 Q_{n+1}. \quad (1)$$

Hence if  $Q_{n+1} = (-1)^{n+1} N/|N|$ , it follows that equation (1) gives a solution  $(x, y) = (G_n, B_n)$  of  $x^2 - Dy^2 = N$ . As a consequence of this note, such a solution must satisfy  $\gcd(x, y) = 1$ .

As  $\gcd(A_n, B_n) = 1$ , we have  $\gcd(G_n, B_n) = \gcd(Q_0, B_n)$  and hence the implication

$$Q_{n+1} = \pm 1 \Rightarrow \gcd(G_n, B_n) = 1$$

will follow from the following result:

**THEOREM 1**  $\gcd(Q_0, B_n)$  divides  $Q_{n+1}$ .

**Remark 1.** In recent papers by K.R. Matthews [1] and R.A. Mollin [4], it is shown that each integer solution of  $x^2 - Dy^2 = N$  with  $\gcd(x, y) = 1$ , will arise from some  $P_0$  in the above manner.

**Remark 2.** The theorem similarly shows that the solutions produced in the paper by K.R. Matthews [2] for the equation  $ax^2 + bxy + cy^2 = N$ , where  $D = b^2 - 4ac > 1$  is not a perfect square and  $\gcd(a, b, c) = 1 = \gcd(a, N)$ , also satisfy  $\gcd(x, y) = 1$ .

## 2. Standard continued fraction properties

We remind the reader of some properties of  $A_n, B_n, P_n$  and  $Q_n$ .

First,  $a_n = [\omega_n]$  denotes the  $n$ -th partial quotient to  $\omega$  (see [6, Chapter 12.4]).

$$A_{-1} = 1, A_0 = a_0, B_{-1} = 0, B_0 = 1, B_1 = a_1,$$

while for  $n \geq 1$ :

$$\begin{aligned} \text{(i)} \quad A_n &= a_n A_{n-1} + A_{n-2}, \\ \text{(ii)} \quad B_n &= a_n B_{n-1} + B_{n-2}, \\ \text{(iii)} \quad P_n &= a_{n-1} Q_{n-1} - P_{n-1}, \\ \text{(iv)} \quad Q_n &= (D - P_n^2) / Q_{n-1}. \end{aligned}$$

## 3. A lemma

*Definition 1.* We define a sequence  $R_0, R_1, \dots$  by  $R_0 = 0, R_1 = 1$  and for  $i \geq 2$ ,

$$R_i = a_i R_{i-1} + R_{i-2}.$$

In particular,  $R_2 = a_2$ .

LEMMA 1 For  $i \geq 0$  we have

$$B_{i+1} R_i - B_i R_{i+1} = (-1)^{i+1}. \quad (2)$$

**Proof:** (By induction on  $i \geq 0$ .) Equation (2) holds when  $i = 0$ , as

$$B_1 R_0 - B_0 R_1 = a_1 \times 0 - 1 \times 1 = -1.$$

Now assume (2) holds. Then substituting for  $B_i$  and  $R_i$  gives

$$\begin{aligned} B_{i+1}(R_{i+2} - a_{i+2} R_{i+1}) - (B_{i+2} - a_{i+2} B_{i+1}) R_{i+1} &= (-1)^{i+1} \\ B_{i+1} R_{i+2} - B_{i+2} R_{i+1} &= (-1)^{i+1} \\ B_{i+2} R_{i+1} - B_{i+1} R_{i+2} &= (-1)^{i+2}, \end{aligned}$$

as required. ■

#### 4. Recurrence congruences

Our Theorem is a consequence of the following congruences:

LEMMA 2 *Modulo  $Q_0$ , the following identities hold for  $N \geq 1$ :*

$$\begin{aligned} \text{(a)} \quad P_N &= (-1)^N B_{N-1} B_{N-2} Q_1 + (-1)^{N+1} (2B_{S_N} R_{T_N} + 1) P_1 \\ \text{(b)} \quad Q_N &= (-1)^{N+1} B_{N-1}^2 Q_1 + (-1)^N 2B_{N-1} R_{N-1} P_1, \end{aligned}$$

where  $S_N = 2\lfloor \frac{N-1}{2} \rfloor + (-1)^N$  and  $T_N = 2\lfloor \frac{N-1}{2} \rfloor$ .

**Proof:** (By induction on  $N$ .)

When  $N = 1$  and  $2$ , equation (a) becomes an equality, as does (b) when  $N = 1$  (recall  $B_{-1} = 0, B_0 = 1$  and  $B_1 = a_1$ ). When  $N = 2$ , (b) reduces to

$$Q_2 = -B_1^2 Q_1 + 2B_1 R_1 P_1 = -a_1^2 Q_1 + 2a_1 P_1.$$

However

$$\begin{aligned} Q_2 &= \frac{D - P_2^2}{Q_1} = \frac{D - (a_1 Q_1 - P_1)^2}{Q_1} \\ &= \frac{D - P_1^2}{Q_1} - a_1^2 Q_1 + 2a_1 P_1 \\ &= Q_0 - a_1^2 Q_1 + 2a_1 P_1, \end{aligned}$$

as required.

Now let  $N \geq 2$  and assume equations (a) and (b) hold for  $N$  and  $N - 1$ . The following values of  $S_N, T_N, S_{N+1}$  and  $T_{N+1}$  are needed:

$N$	$S_N$	$T_N$	$S_{N+1}$	$T_{N+1}$
$2n - 1$	$N - 2$	$N - 1$	$N$	$N - 1$
$2n$	$N - 1$	$N - 2$	$N - 1$	$N$

Case (a):

$$\begin{aligned} P_{N+1} &= a_N Q_N - P_N \\ &= a_N ((-1)^{N+1} B_{N-1}^2 Q_1 + (-1)^N 2B_{N-1} R_{N-1} P_1) \\ &\quad - ((-1)^N B_{N-1} B_{N-2} Q_1 + (-1)^{N+1} (2B_{S_N} R_{T_N} + 1) P_1) \\ &= (-1)^{N+1} (a_N B_{N-1}^2 + B_{N-1} B_{N-2}) Q_1 \\ &\quad + (-1)^N (2a_N B_{N-1} R_{N-1} + 2B_{S_N} R_{T_N} + 1) P_1 \\ &= (-1)^{N+1} \alpha_N Q_1 + (-1)^N \beta_N P_1, \text{ say.} \end{aligned} \tag{3}$$

Then

$$\begin{aligned} \alpha_N &= (a_N B_{N-1} + B_{N-2}) B_{N-1} \\ &= B_N B_{N-1}. \end{aligned} \tag{4}$$

Case (i):  $N = 2n - 1$ . Then

$$\begin{aligned}\beta_N &= 2a_N B_{N-1} R_{N-1} + 2B_{N-2} R_{N-1} + 1 \\ &= 2(a_N B_{N-1} + B_{N-2}) R_{N-1} + 1 \\ &= 2B_N R_{N-1} + 1.\end{aligned}\tag{5}$$

Case (ii):  $N = 2n$ . Then

$$\begin{aligned}\beta_N &= 2a_N B_{N-1} R_{N-1} + 2B_{N-1} R_{N-2} + 1 \\ &= 2B_{N-1} (a_N R_{N-1} + R_{N-2}) + 1 \\ &= 2B_{N-1} R_N + 1.\end{aligned}\tag{6}$$

Equations (3), (4), (5), (6) and the table entries for  $S_{N+1}$  and  $T_{N+1}$  then give

$$P_{N+1} = (-1)^{N+1} B_N B_{N-1} Q_1 + (-1)^{N+2} (2B_{S_{N+1}} R_{T_{N+1}} + 1) P_1,$$

completing part (a) of the induction.

Case (b):

$$\begin{aligned}Q_{N+1} &= \frac{D - P_{N+1}^2}{Q_N} = \frac{D - (a_N Q_N - P_N)^2}{Q_N} \\ &= \frac{D - P_N^2}{Q_N} - a_N^2 Q_N + 2a_N P_N \\ &= Q_{N-1} - a_N^2 Q_N + 2a_N P_N \\ &= (-1)^N B_{N-2}^2 Q_1 + (-1)^{N-1} 2B_{N-2} R_{N-2} P_1 \\ &\quad - a_N^2 ((-1)^{N+1} B_{N-1}^2 Q_1 + (-1)^N 2B_{N-1} R_{N-1} P_1) \\ &\quad + 2a_N ((-1)^N B_{N-1} B_{N-2} Q_1 + (-1)^{N+1} (2B_{S_N} R_{T_N} + 1) P_1) \\ &= (-1)^N (B_{N-2}^2 + a_N^2 B_{N-1}^2 + 2a_N B_{N-1} B_{N-2}) Q_1 \\ &\quad + (-1)^{N+1} 2(B_{N-2} R_{N-2} + a_N^2 B_{N-1} R_{N-1} + a_N (2B_{S_N} R_{T_N} + 1)) P_1 \\ &= (-1)^N \gamma_N Q_1 + (-1)^{N+1} 2\delta_N P_1, \text{ say.}\end{aligned}\tag{7}$$

Now

$$\gamma_N = (B_{N-2} + a_N B_{N-1})^2 = B_N^2.\tag{8}$$

Case (i):  $N = 2n - 1$ . Then

$$\begin{aligned}\delta_N &= B_{N-2} R_{N-2} + a_N^2 B_{N-1} R_{N-1} + a_N (2B_{N-2} R_{N-1} + 1) \\ &= B_{N-2} (R_{N-2} + a_N R_{N-1}) + a_N^2 B_{N-1} R_{N-1} + a_N B_{N-2} R_{N-1} + a_N \\ &= B_{N-2} R_N + a_N R_{N-1} (a_N B_{N-1} + B_{N-2}) + a_N \\ &= B_{N-2} R_N + a_N R_{N-1} B_N + a_N \\ &= B_{N-2} R_N + a_N (R_{N-1} B_N + 1) \\ &= B_{N-2} R_N + a_N B_{N-1} R_N \text{ (by Lemma 1 with } i = N - 1) \\ &= (B_{N-2} + a_N B_{N-1}) R_N \\ &= B_N R_N.\end{aligned}\tag{9}$$

Case (ii):  $N = 2n$ . Then

$$\begin{aligned}
\delta_N &= B_{N-2}R_{N-2} + a_N^2 B_{N-1}R_{N-1} + a_N(2B_{N-1}R_{N-2} + 1) \\
&= (B_{N-2} + a_N B_{N-1})R_{N-2} + a_N^2 B_{N-1}R_{N-1} + a_N B_{N-1}R_{N-2} + a_N \\
&= B_N R_{N-2} + a_N B_{N-1}(a_N R_{N-1} + R_{N-2}) + a_N \\
&= B_N R_{N-2} + a_N B_{N-1}R_N + a_N \\
&= B_N R_{N-2} + a_N(B_{N-1}R_N + 1) \\
&= B_N R_{N-2} + a_N B_N R_{N-1} \text{ (by Lemma 1 with } i = N - 1) \\
&= B_N(R_{N-2} + a_N R_{N-1}) \\
&= B_N R_N.
\end{aligned} \tag{10}$$

Equations (7), (8), (9) and (10) then give

$$Q_{N+1} = (-1)^{N+2} B_N^2 Q_1 + (-1)^{N+1} 2B_N R_N P_1,$$

completing part (b) of the induction. ■

### Acknowledgments

The first author would like to thank the School of Mathematical Sciences, Australian National University, for its hospitality.

### References

1. Matthews, K.R., "The diophantine equation  $x^2 - Dy^2 = N, D > 0$ ," Expo. Math. 18, 2000, pp. 323–331.
2. Matthews, K.R., "The diophantine equation  $ax^2 + bxy + cy^2 = N, D = b^2 - 4ac > 0$ ," J. Théor. Nombres Bordeaux, to appear.
3. Mollin, R.A., "Fundamental Number Theory with Applications," CRC Press, NY, 1998.
4. Mollin, R.A. "Simple continued fraction solutions for Diophantine equations," Expo. Math. 19, 2001, pp. 55–73.
5. Patz, W., "Über die Gleichung  $X^2 - DY^2 = \pm c \cdot (2^{31} - 1)$ ," Bayer. Akad. Wiss. Math-Natur. Kl. S.-B., 1948, pp. 21–30.
6. Rosen, K.H., "Elementary Number Theory and its Applications," 4th edition, Addison-Wesley, Reading, Massachusetts, 2000.