Primitive Pythagorean triples and the negative Pell equation

Keith Matthews

Abstract

Abstract. This paper uses continued fractions to give more explicit versions of results of A. Grytczuk, F. Luca and M. Wójtowicz and of K. Hardy and K.S. Williams relating the solvability of the negative Pell equation to the existence of primitive Pythagorean triples. These results were also obtained by P. Kaplan and K.S. Williams.

1 Introduction.

This note started on reading a short paper of Grytczuk, Luca and Wójtowicz (GLW) [2], which proved that the negative Pell equation $x^2 - Dy^2 = -1, D > 1$ and non-square, is solvable in positive integers x and y if and only if there exist a primitive Pythagorean triple (A, B, C) (ie. A, B, C are positive integers satisfying $A^2 + B^2 = C^2$ and $\gcd(A, B) = 1$) and positive integers a, b such that

$$D = a^2 + b^2 \text{ and } |aA - bB| = 1.$$

Sufficiency is immediate: If $x = |aB + bA|$ and $y = C$, then

$$Dy^2 = (a^2 + b^2)(A^2 + B^2) = (aB + bA)^2 + (aA - bB)^2 = x^2 + 1. \quad (1)$$

It is easy to see that D is not a perfect square.

Then earlier related papers of K. Hardy and K.S. Williams [3] and P. Kaplan and K.S. Williams [5] came to the attention of the author.

The primitive Pythagorean triples (A, B, C) with A even, are given by

$$A = 2uv, B = u^2 - v^2, C = u^2 + v^2, \quad (2)$$

where $u > v > 0$, $\gcd(u, v) = 1$ and u and v have different parity.

For example, $(u, v) = (2, 1)$ gives $(A, B, C) = (4, 3, 5)$ and $(a, b) = (2, 3)$ satisfies $aA - bB = -1$. Then with $D = 13$, $(x, y) = (18, 5) = \eta$, the least solution of $x^2 - Dy^2 = -1$.

Contrastingly, $u = 71, v = 38$ gives $(A, B, C) = (5396, 3597, 6485)$ and again $(a, b) = (2, 3)$ satisfies $aA - bB = -1$. Then with $D = 13$, we have $(x, y) = \eta^3$.

The condition $|aA - bB| = 1$ becomes $|2auv - b(u^2 - v^2)| = 1$. The solubility of this diophantine equation is equivalent to that of $bV^2 - 2aVW - bW^2 = 1$ and criteria for solubility of this last equation were discussed in [3] and [5].

The authors GLW gave two proofs of the necessity part, one of these proofs being in terms of gcd's in $Z[i]$. Hardy and Williams also use this approach in their Theorem 3, page 148.

Kaplan and Williams also give a proof, using continued fractions - see Lemma 3, [5, p. 174-176]. We give a slightly different proof in Theorem 2.1 and show that if the negative Pell equation $x^2 - Dy^2 = -1$ has a solution, then there are relatively prime positive integers a and b such that $D = a^2 + b^2$, with b odd and such that a primitive Pythagorean triple (A, B, C) exists with $|aA - bB| = 1$ and A even. In Theorem 4.1, we show that a and b are unique.

2 Producing primitive Pythagorean triples

The continued fraction expansion of $\sqrt{D}$ is $[a_0, \overline{a_1, \ldots, a_l}]$, with period-length l. Let $(P_i + \sqrt{D})/Q_i$ denote the i–th complete convergent and A_i/B_i the i-th convergent, where $P_0 = 0, Q_0 = 1, A_{-2} = 0, A_{-1} = 1, B_{-2} = 1, B_{-1} = 0, a_0 = \lfloor \sqrt{D} \rfloor$ and for $i \geq 1$,

(a) $P_i = a_{i-1}Q_{i-1} - P_{i-1}$,

(b) $Q_i = (D - P_i^2)/Q_{i-1}$,

(c) $a_i = \lfloor (P_i + \sqrt{D})/Q_i \rfloor$.

It is well-known ([8, page 93] that the negative Pell equation is soluble if and only if the continued fraction expansion of $\sqrt{D}$ has odd period-length l.

Suppose $l = 2n - 1$. Then the positive solutions (x, y) of $x^2 - Dy^2 = -1$ are given by $(x_t, y_t) = (A_{2N-2}, B_{2N-2})$, where $N = n + t(2n - 1), t \geq 0$. In

fact $x_t + y_t\sqrt{D} = (x_0 + y_0\sqrt{D})^{2t+1}$, where $(x_0, y_0) = (A_{2n-2}, B_{2n-2})$ is the smallest (*fundamental*) positive solution of the negative Pell equation.

THEOREM 2.1 Suppose $\sqrt{D} = [a_0, \overline{a_1, \ldots, a_l}]$, where the period-length $l = 2n-1$ is odd. Let $u = B_{n-1}$ and $v = B_{n-2}$. Also let

$$a = P_n, b = Q_n, A = 2uv, B = u^2 - v^2, C = u^2 + v^2.$$

Then

(a) $D = a^2 + b^2$, b odd.

(b) $aA - bB = (-1)^n$.

(c) $\gcd(u, v) = 1, u > v$ and one of u and v is even.

(d) $x_0 = aB + bA, y_0 = C$.

(e) $A = (bx_0 - \epsilon a)/D, B = (ax_0 + \epsilon b)/D$, where $\epsilon = (-1)^{n-1}$.

REMARK 2.1 (i) We have $A \geq 0, B > 0$. Also

$$A = 0 \Leftrightarrow n = 1 \Leftrightarrow D = \alpha^2 + 1,$$

for some $\alpha \geq 1$.

(ii) From (e), we get congruences

$$bx_0 \equiv \epsilon a \,(\mathrm{mod}\, D) \text{ and } ax_0 \equiv -\epsilon b \,(\mathrm{mod}\, D). \tag{3}$$

This result is also part of Theorem 5 [3, page 154] where it is stated that the congruence $x_0 e \equiv d \,(\mathrm{mod}\, D)$ has precisely four coprime integer solutions (e, d) satisfying $|d| < \sqrt{D}$ and $|e| < \sqrt{D}$. These are by (3) $\pm(\epsilon b, a)$ and $\pm(a, -\epsilon b)$.

EXAMPLE 2.1 $D = 13$. $\sqrt{13} = [3, \overline{1, 1, 1, 1, 6}]$, $l = 5, n = 3$. $a = P_3 = 2, b = Q_3 = 3$, $\eta = (18, 5)$. Then $(u, v) = (B_2, B_1) = (2, 1)$ and $(A, B, C) = (2uv, u^2 - v^2, u^2 + v^2) = (4, 3, 5)$.

3 Some lemmas

LEMMA 3.1 *Let $\sqrt{D}$ have period–length l. Then*

$$\begin{aligned} DB_{l-1} &= a_0 A_{l-1} + A_{l-2} \quad (4) \\ A_{l-1} &= a_0 B_{l-1} + B_{l-2}. \quad (5) \end{aligned}$$

Proof. See equations (16) and (17) [8, p. 70].

LEMMA 3.2 *Let $\sqrt{D}$ have period–length $l = 2n-1$. Then*

$$\begin{aligned} DB_{2n-2} &= A_{n-1}^2 + A_{n-2}^2 \quad (6) \\ A_{2n-2} &= A_{n-1}B_{n-1} + A_{n-2}B_{n-2} \quad (7) \\ B_{2n-2} &= B_{n-1}^2 + B_{n-2}^2. \quad (8) \end{aligned}$$

Proof of Lemma 3.2. We start from the matrix identity

$$\begin{bmatrix} a_0 & 1 \\ 1 & 0 \end{bmatrix} \cdots \begin{bmatrix} a_{2n-2} & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} A_{2n-2} & A_{2n-3} \\ B_{2n-2} & B_{2n-3} \end{bmatrix} \quad (9)$$

and partition the above matrix product as

$$\begin{bmatrix} a_0 & 1 \\ 1 & 0 \end{bmatrix} \cdots \begin{bmatrix} a_{n-1} & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a_n & 1 \\ 1 & 0 \end{bmatrix} \cdots \begin{bmatrix} a_{2n-2} & 1 \\ 1 & 0 \end{bmatrix}.$$

But $a_{n+i} = a_{n-i-1}$ for $i = 0, \ldots, n-2$, so (9) becomes

$$\begin{bmatrix} a_0 & 1 \\ 1 & 0 \end{bmatrix} \cdots \begin{bmatrix} a_{n-1} & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a_{n-1} & 1 \\ 1 & 0 \end{bmatrix} \cdots \begin{bmatrix} a_1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} A_{2n-2} & A_{2n-3} \\ B_{2n-2} & B_{2n-3} \end{bmatrix}.$$

Multiplying both sides of this equation on the right by $\begin{bmatrix} a_0 & 1 \\ 1 & 0 \end{bmatrix}$ then gives

$$\begin{aligned} \begin{bmatrix} A_{n-1} & A_{n-2} \\ B_{n-1} & B_{n-2} \end{bmatrix} \begin{bmatrix} A_{n-1} & A_{n-2} \\ B_{n-1} & B_{n-2} \end{bmatrix}^t &= \begin{bmatrix} a_0 A_{2n-2} + A_{2n-3} & A_{2n-2} \\ a_0 B_{2n-2} + B_{2n-3} & B_{2n-2} \end{bmatrix} \\ &= \begin{bmatrix} DB_{2n-2} & A_{2n-2} \\ A_{2n-2} & B_{2n-2} \end{bmatrix}, \quad (10) \end{aligned}$$

by Lemma 3.1. Hence

$$\begin{bmatrix} A_{n-1} & A_{n-2} \\ B_{n-1} & B_{n-2} \end{bmatrix} \begin{bmatrix} A_{n-1} & B_{n-1} \\ A_{n-2} & B_{n-2} \end{bmatrix} = \begin{bmatrix} DB_{2n-2} & A_{2n-2} \\ A_{2n-2} & B_{2n-2} \end{bmatrix}. \quad (11)$$

Finally, equation (11) implies equations (6), (7) and (8).

LEMMA 3.3

$$A_{i-1} = Q_i B_{i-2} + B_{i-1} P_i \text{ for } i \geq 0, \tag{12}$$

$$A_{n-2} = Q_n B_{n-1} - P_n B_{n-2}, \tag{13}$$

Proof. For (12) see [8, p. 70].

For (13), we note that $Q_n = Q_{n-1}$. Then

$$\begin{aligned} Q_n B_{n-1} - P_n B_{n-2} &= Q_n(a_{n-1} B_{n-2} + B_{n-3}) \\ &\quad - (a_{n-1} Q_{n-1} - P_{n-1}) B_{n-2} \\ &= Q_n B_{n-3} + P_{n-1} B_{n-2} \\ &= Q_{n-1} B_{n-3} + P_{n-1} B_{n-2} = A_{N-2}, \end{aligned}$$

by equation (12), with $i = n - 1$.

Proof of Theorem 2.1. (a) Part (a) is proved in [8, p. 95] and also in [11], where it is pointed out that b is odd.

(b)

$$\begin{aligned} aA - bB &= P_n(2B_{n-1}B_{n-2}) - Q_n(B_{n-1}^2 - B_{n-2}^2) \\ &= P_n(2B_{n-1}B_{n-2}) - Q_n(B_{n-1}^2 - B_{n-2}^2) \\ &= B_{n-1}(P_n B_{n-2} - B_{n-1} Q_n) + \\ &\quad + B_{n-2}(Q_n B_{n-2} + B_{n-1} P_n) \\ &= B_{n-1}(-A_{n-2}) + B_{n-2} A_{n-1} \\ &= (-1)^n. \end{aligned} \tag{14}$$

(c) $u = B_{n-1} \geq v = B_{n-2}$ always holds. However equality would imply $2auv = (-1)^n$. Also $\gcd(B_{n-1}, B_{n-2}) = 1$ follows from equation (14) above.

(d) Next,

$$\begin{aligned} aB + bA &= P_n(B_{n-1}^2 - B_{n-2}^2) + Q_n(2B_{n-1}B_{n-2}) \\ &= B_{n-1}(P_n B_{n-1} + Q_n B_{n-2}) + B_{n-2}(Q_n B_{n-1} - P_n B_{n-2}) \\ &= B_{n-1} A_{n-1} + B_{n-2} A_{n-2} = A_{2n-2} = x_0 \text{ by (7)}. \end{aligned}$$

(e)

$$\begin{aligned} b^2 y^2 &= b^2 B^2 + b^2 A^2 \\ &= b^2 B^2 + (x - aB)^2 \\ &= x^2 - 2aBx + DB^2. \end{aligned}$$

Hence $DB^2 - 2axB + x^2 - b^2y^2 = 0$.
But $x^2 = Dy^2 - 1$, so $DB^2 - 2axB + a^2y^2 - 1 = 0$. Hence

$$\begin{aligned} B &= \frac{ax \pm \sqrt{a^2x^2 - D(a^2y^2 - 1)}}{D} \\ &= \frac{ax \pm \sqrt{a^2(Dy^2 - 1) - D(a^2y^2 - 1)}}{D} \\ &= \frac{ax \pm \sqrt{b^2}}{D} = \frac{ax + \epsilon b}{D}, \epsilon = \pm 1. \end{aligned}$$

Next

$$A = \frac{x - a\left(\frac{ax+\epsilon b}{D}\right)}{b} = \frac{b^2x - \epsilon ab}{bD} = \frac{bx - \epsilon a}{D}.$$

Finally

$$\begin{aligned} aA - bB &= \frac{a(bx - \epsilon a)}{D} - \frac{b(ax + \epsilon b)}{D} \\ &= \frac{-\epsilon(a^2 + b^2)}{D} = (-1)^n. \end{aligned}$$

Hence $\epsilon = (-1)^{n-1}$.

4 Uniqueness of a and b

We give a version of the "only if" part of Theorem 3 of [3, p. 148] and Lemma 2 [5, pp. 171-174], which characterise a and b in terms of continued fractions.

THEOREM 4.1 . Suppose (A, B, C) is a primitive Pythagorean triple with A even and a and b are positive integers satisfying

$$|aA - bB| = 1. \tag{15}$$

Then with $D = a^2 + b^2$, we have

(a) D is not a perfect square.

(b) $a = P_n$ and $b = Q_n$, where $2n - 1$ is the period-length of the continued fraction expansion of $\sqrt{D}$.

REMARK 4.1 Hardy and Williams characterise a and b instead in terms of gcd's in Z[i] in Theorem 3 [3, p. 148].

Proof. (a) Let $x = aB + bA, y = C$. Then

$$\begin{aligned} x^2 - dy^2 &= (aB + bA)^2 - (a^2 + b^2)(A^2 + B^{@}) \\ &= (aA - bB)^2 = -1. \end{aligned}$$

However $D = d^2$ would imply $(x+dy)(x-dy) = -1$, giving the contradiction $x + dy = 1$. To prove (b) we need the following result, which is Theorem 172 of [4, pp. 140-141] in slightly more general form:

LEMMA 4.1 . Let $\omega = \frac{P\zeta+R}{Q\zeta+S}$, where $\zeta > 1$ and P, Q, R, S are integers such that $Q > 0, S > 0$ and $PS - QR = \pm 1$. Then P/Q is a convergent A_k/B_k to ω. Moreover, if $Q > S$, then $R/S = A_{k-1}/B_{k-1}, k \geq 0$. Also ζ is the $(k + 1)$-th complete convergent to ω.

In Lemma 4.1 take $P = (au + bv), R = bu - av, Q = u, S = v, \zeta = (a + \sqrt{D})/b$. Then

$$\sqrt{D} = (P\zeta + Q)/(R\zeta + S),$$

where $PS - QR = \pm 1$. Also $\zeta > 1$ and $Q > S > 0$.
For

$$\begin{aligned} (P\zeta + Q)/(R\zeta + S) &= \frac{(au + bv)\frac{(a+\sqrt{D})}{b} + (bu - av)}{u\frac{(a+\sqrt{D})}{b} + v} \\ &= \frac{(au + bv)(a + \sqrt{D}) + b(bu - av)}{u(a + \sqrt{D}) + bv} \\ &= \frac{(a^2u + b^2u + (au + bv)\sqrt{D})}{ua + bv + u\sqrt{D}} \\ &= \frac{(Du + (au + bv)\sqrt{D})}{ua + bv + u\sqrt{D}} \\ &= \sqrt{D}. \end{aligned}$$

Also

$$\begin{aligned} PS - QR &= (au + bv)v - u(bu - av) \\ &= (auv + bv^2) - (bu^2 - auv) \\ &= 2auv - b(u^2 - v^2) = \pm 1, \end{aligned}$$

from equation (15).

It follows from Lemma 4.1 that

$$\begin{aligned} P/Q &= (au+bv)/u = A_{N-1}/B_{N-1}, && (16)\\ R/S &= (bu-av)/v = A_{N-2}/B_{N-2}, && (17)\\ (a+\sqrt{D})/b &= (P_N+\sqrt{D})/Q_N, && (18) \end{aligned}$$

for some $N \geq 1$.

Hence as $\gcd(au+bv, u) = 1 = \gcd(bu-av)$, we have from (16) and (18)

$$\begin{aligned} au+bv &= A_{N-1}, \qquad u = B_{N-1}, && (19)\\ bu-av &= A_{N-2}, \qquad v = B_{N-2}. && (20) \end{aligned}$$

Also from (18) we have

$$P_N = a \text{ and } Q_N = b. \tag{21}$$

Then we also have

$$b = Q_{N-1}. \tag{22}$$

For

$$\begin{aligned} (-1)^{N-1} &= A_{N-2}B_{N-1} - A_{N-1}B_{N-2}\\ &= (bu-av)u - (au+bv)v\\ &= -2auv + b(u^2-v^2). \end{aligned}$$

Hence

$$\begin{aligned} (-1)^{N-1}Q_{N-1} &= A_{N-2}^2 - DB_{N-2}^2\\ &= (bu-av)^2 - (a^2+b^2)v^2\\ &= -2abuv + b^2(u^2-v^2) = (-1)^{N-1}b. \end{aligned}$$

Finally, let $2n-1$ be the period-length of $\sqrt{D}$. Then as $Q_{N-1} = Q_N$, it follows from Satz 3.11 [8, p. 82] that $N \equiv n \pmod{2n-1}$. Then by periodicity, $a = P_N = P_n$ and $b = Q_N = Q_n$.

5 Examples

EXAMPLE 5.1 The case $a = 1$ and $b > 1$ cannot occur. ie. the equation $|-bu^2 + 2uv + bv^2| = 1$ has no integer solutions if $b > 1$.

Proof. Assume $a = 1$ and $b > 1$. Then (15) becomes

$$| - bu^2 + 2uv + bv^2| = 1.$$

Consider the matrix

$$H = \begin{bmatrix} u & u + bv \\ v & bu - v \end{bmatrix}$$

Then $\det H = -\epsilon$ and all entries are positive.

Also if $D = b^2 + 1$,

$$\omega = \frac{1 + \sqrt{D}}{b} = \frac{u\sqrt{D} + u + bv}{v\sqrt{D} + bu - v}.$$

Hence by Lemma 4.1, u/v is a convergent A_{k-1}/B_{k-1} to ω.

Now $\omega = [\overline{1, b - 1, 1}]$.

Also by Theorem 5.3.4 [6, p. 246],

$$bA_{k-1}^2 - 2A_{k-1}B_{k-1} - bB_{k-1}^2 = (-1)^k Q_k,$$

where $(P_k + \sqrt{D})/Q_k$ is the k-th complete convergent to ω. Hence

$$\pm 1 = bu^2 - 2uv - bv^2 = (-1)^k Q_k, \tag{23}$$

But we readily verify that for $i \geq 0$,

1. (a) $(P_{3i} + \sqrt{D})/Q_{3i} = (1 + \sqrt{D})/b$,
2. (b) $(P_{3i+1} + \sqrt{D})/Q_{3i+1} = (b - 1 + \sqrt{D})/2$,
3. (c) $(P_{3i+2} + \sqrt{D})/Q_{3i+2} = (b - 1 + \sqrt{D})/b$.

Hence equation (23) gives a contradiction.

References

[1] P. Epstein, *Zur Auflosbarkeit der Gleichung* $x^2 - Dy^2 = -1$, J. Reine Angew. Math. 171 (1934) 243–252.

[2] A. Grytczuk, F. Luca, M. Wójtowicz, *The negative Pell equation and Pythagorean triples*, Proc. Japan Acad., Volume 76 (2000) 91–94.

[3] K. Hardy, K.S. Williams, *On the solvability of the diophantine equation* $dV^2 - 2eVW - dW^2 = 1$, Pacific Journal of Mathematics, Volume 124 (1986) 145–158.

[4] G.H. Hardy and E.M. Wright, *An Introduction to Theory of Numbers*, Oxford University Press, 1962.

[5] P. Kaplan, K.S. Williams, *Pell's Equations* $X^2 - mY^2 = -1, -4$ *and Continued Fractions*, J. Number Theory, Volume 23 (1986) 169–182.

[6] R.A. Mollin, *Fundamental Number Theory with Applications*, CRC Press, New York 1998.

[7] R.A. Mollin, B. Goddard, *A description of continued fraction expnasions of quadratic surds represented by polynomials*, J. Number Theory, Volume 107 (2004) 228–240.

[8] O. Perron, *Die Lehre von den Kettenbrüchen*, third edition, Teubner, Stuttgart, 1954.

[9] M. Pohst, H. Zassenhaus, *On unit computation in real quadratic fields*, *EUROSAM '79*, Springer Lecture Notes in Computer Science, Volume 72, (1979) 140–152.

[10] A.J. Van der Poorten, H.C. Williams, *On certain continued fraction expansions of fixed period length*, Acta Arith., Volume 89 (1999) 23–35.

[11] J.P. Robertson, K.R. Matthews, *A continued fractions approach to a result of Feit*, American Math. Monthly, Volume 115 (2008) 346–349.