Gen. Math. Notes, Vol. 28, No. 2, June 2015, pp.1-8
ISSN 2219-7184;
www.i-csrs.org
Available free online at http://www.geman.in

An Algorithm to Solve a Pell Equation

Alexandre Junod

Lycée Denis-de-Rougemont
2000 Neuchâtel, Switzerland
E-mail: alexandre.junod@rpn.ch

(Received: 9-4-15 / Accepted: 28-5-15)

Abstract

Given a non-square positive integer n, we want to find two integers x and y such that $x^2 - ny^2 = \pm 1$. We present an elementary method to do this and we make the well-known link with the continued fraction of $\sqrt{n}$ with a new pedagogical point of view. Finally we give a generalization to deal with equations $mx^2 - ny^2 = \pm 1$ when m and n are positive integers whose product is not a perfect square.

Keywords: *Pell equation, Continued fractions.*

1 Introduction

The equations $x^2 - ny^2 = \pm 1$ (where n is a non-square positive integer) have been studied by several Indian mathematicians. From a solution $(x; y)$ of an equation $x^2 - ny^2 = \varepsilon$ with $\varepsilon \in \{\pm 1, \pm 2, \pm 4\}$, Brahmagupta (598−668) could find a solution $(x'; y')$ with $x' > x$ for the case $\varepsilon = 1$ and could deduce infinitely many solutions for this case. Later, Bhāskara II (1114−1185) developed a cyclic algorithm (called *chakravala method*) to produce a solution of an equation $x^2 - ny^2 = 1$. The topic interessed the European mathematicians (ignorant of the Indians' work) after a challenge given in 1657 by Pierre de Fermat (1601−1665). William Brouncker (1620−1684) found an empirical method related to the continued fractions

$$[a_0; a_1, \ldots, a_n] \;=\; a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots \; \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}$$

John Wallis (1616−1703) published and completed the work of Brouncker. Leonhard Euler (1707−1783) named the equation after John Pell by mistake, studied the infinite continued fractions and proved that a finally periodic continued fraction describes an irrational quadratic. Joseph-Louis Lagrange (1736−1813) proved the reciprocal : every irrational zero of a quadratic polynomial has a finally periodic continued fraction $[a_0; a_1, \ldots, a_m, \overline{a_{m+1}, \ldots, a_n}]$. He published a rigorous version of the continued fractions approach to solve an equation $x^2 - ny^2 = 1$ and proved the infinity of solutions $(x; y)$ for every n. Evariste Galois (1811−1832) described the irrational quadratics whose continued fractions are purely periodic ($m = 0$ in the above continued fraction) and Adrien-Marie Legendre (1752−1833) found the continued fraction of $\sqrt{n}$ for a non-square integer $n > 1$. The solutions of a Pell equation depend on this expansion. In fact, the relation $x^2 - ny^2 = \pm 1$ (where x and y are positive integers) implies that $\left|\sqrt{n} - \frac{x}{y}\right| < \frac{1}{2y^2}$ and this inequality allows to say that x/y has a (finite) continued fraction which coincides with the beginning of that of $\sqrt{n}$.

2 Algorithm

Given a non-square integer n, we consider the following algorithm :

$$\text{Initialization : } \boxed{\begin{matrix} a_{i-1} & b_{i-1} & c_{i-1} \\ a_i & b_i & c_i \end{matrix}} = \boxed{\begin{matrix} 0 & 1 & n \\ 1 & 0 & 1 \end{matrix}} \text{ for } i = 0.$$

$$\text{Iteration : } \Downarrow$$

$$\boxed{q_i a_i + a_{i-1} \quad q_i b_i + b_{i-1} \quad c_{i+1}} \text{ with } q_i = \left\lfloor \frac{\sqrt{n - c_{i-1}c_i} + \sqrt{n}}{c_i} \right\rfloor$$

$$\text{and } c_{i+1} = 2q_i\sqrt{n - c_{i-1}c_i} + c_{i-1} - q_i^2 c_i.$$

In this paper, we first prove the theorem of Legendre :

Theorem 1. *There exists an index m such that $q_m = 2q_0$. Then we have the periodic continued fraction*

$$\sqrt{n} = [q_0; q_1, q_2, \ldots] = [q_0; \overline{q_1, \ldots, q_m}] = [q_0; \overline{\underbrace{q_1, \ldots, q_1}_{palindrome}, 2q_0}].$$

Then we make the link with Pell's equations $x^2 - ny^2 = \pm 1$:

Theorem 2. *For each $i \geqslant 0$, we have the relation $a_i^2 - nb_i^2 = (-1)^i c_i$ and the continued fraction $\frac{a_{i+1}}{b_{i+1}} = [q_0; q_1, \ldots, q_i]$.*

Example : Let us consider $n = 23$

	i	a_i	b_i	c_i	q_i
Initialization	-1	0	1	23	
	0	1	0	1	$q_0 = \lfloor (0+\sqrt{23})/1 \rfloor = 4$
	1	4	1	7	$q_1 = \lfloor (4+\sqrt{23})/7 \rfloor = 1$
	2	5	1	2	$q_2 = \lfloor (3+\sqrt{23})/2 \rfloor = 3$
	3	19	4	7	$q_3 = \lfloor (3+\sqrt{23})/7 \rfloor = 1$
	4	24	5	1	$q_4 = \lfloor (4+\sqrt{23})/1 \rfloor = 8$
	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

The continued fraction of $\sqrt{23}$ is $[4; \overline{1, 3, 1, 8}]$ and the equation $x^2 - 23y^2 = 1$ has the solution $x = 24$, $y = 5$.

Shortcuts. To solve an equation $x^2 - ny^2 = 1$, we can stop the algorithm as soon as c_i divides $2a_i$: the relation $a_i^2 - nb_i^2 = (-1)^i c_i$ implies that

$$(a_i^2 - nb_i^2)^2 = (a_i^2 + nb_i^2)^2 - n(2a_ib_i)^2 = (2a_i^2 + (-1)^{i+1}c_i)^2 - n(2a_ib_i)^2$$

is eqal to c_i^2, hence we get the solution $x = \dfrac{2a_i^2}{c_i} + (-1)^{i+1}$ and $y = \dfrac{2a_ib_i}{c_i}$. The condition is automatic for $c_i \in \{1, 2\}$ and for $c_i = 4$ if a_i is even. The case where a_i is odd (and $c_i = 4$) can also be solved : the numbers $\alpha = \frac{1}{2}a_i(a_i^2 - 3(-1)^i)$ and $\beta = \frac{1}{2}b_i(a_i^2 - (-1)^i)$ are integers and we can check that $\alpha^2 - n\beta^2 = (-1)^i$, getting a previous case.

3 Relevance

At first, we have to show that the algorithm is well-defined.

Proposition 1. *The numbers c_{i-1}, c_i, q_i are strictly positive integers and $\sqrt{n - c_{i-1}c_i}$ is also an integer (i.e. $n - c_{i-1}c_i$ is a perfect square).*

Proof. The assertion is true for $i = 0$. Proceeding by induction, let us suppose that it is true for an index i and let us prove its validity for the index $i + 1$.

• $\sqrt{n - c_i c_{i+1}}$ *is an integer*: The equation $c_i x^2 - 2\sqrt{n - c_{i-1}c_i}\,x + c_{i+1} - c_{i-1} = 0$ has integral coefficients and admits a solution ($x = q_i$). Then its discriminant $\Delta = 4(n - c_i c_{i+1})$ is non-negative and the number $\sqrt{n - c_i c_{i+1}}$ is well-defined. We can check that

$$|c_i q_i - \sqrt{n - c_{i-1}c_i}| = \sqrt{n - c_i c_{i+1}}$$

because both members of the equality have the same square (independently of the definition of the numbers q_i). We deduce that $\sqrt{n - c_i c_{i+1}}$ is an integer.

• c_{i+1} *is a positive integer*: The obvious relation $0 < \dfrac{\sqrt{n - c_{i-1}c_i} + \sqrt{n}}{c_i} - q_i < 1$ can be written in the form

$$-\sqrt{n} < \underbrace{\sqrt{n - c_{i-1}c_i} - c_i q_i}_{\pm\sqrt{n - c_i c_{i+1}}} < c_i - \sqrt{n} \qquad (*)$$

because $c_i > 0$. As $q_i \geqslant 1$ and $c_i c_{i-1} > 0$, we have $c_i < \sqrt{n - c_{i-1}c_i} + \sqrt{n} < 2\sqrt{n}$. Hence $c_i - \sqrt{n} < \sqrt{n}$ and the relation $(*)$ implies $\sqrt{n - c_i c_{i+1}} < \sqrt{n}$. We deduce that $c_i c_{i+1} > 0$ and thus the number c_{i+1} is a positive integer.

• q_{i+1} *is a positive integer* : The map $x \longmapsto x^2 - c_i x - n$ is decreasing on the interval $]-\infty; \frac{1}{2}c_i]$. We can apply it to $(*)$ by inversing the inequalities (because $c_i - \sqrt{n} < c_i - \frac{1}{2}c_i = \frac{1}{2}c_i$). We get

$$c_i\sqrt{n} > -c_i c_{i+1} + c_i^2 q_i - c_i\sqrt{n - c_{i-1}c_i} > -c_i\sqrt{n},$$

that is $|c_{i+1} + \sqrt{n - c_{i-1}c_i} - c_i q_i| < \sqrt{n}$. Using the triangular inequality, we deduce

$$|c_{i+1}| \leqslant \underbrace{|c_{i+1} + \sqrt{n - c_{i-1}c_i} - c_i q_i|}_{<\sqrt{n}} + \underbrace{|c_i q_i - \sqrt{n - c_{i-1}c_i}|}_{=\sqrt{n - c_i c_{i+1}}}.$$

We have $c_{i+1} < \sqrt{n} + \sqrt{n - c_i c_{i+1}}$, hence the obviously integer q_{i+1} is $\geqslant 1$. $\square$

We have seen that the integers $c_i q_i - \sqrt{n - c_{i-1}c_i}$ and $\sqrt{n - c_i c_{i+1}}$ are equal or opposite. We can now show that they are really the same :

- If $c_i > \sqrt{n}$, then $c_i q_i - \sqrt{n - c_i c_{i+1}} > \sqrt{n} - \sqrt{n - c_i c_{i+1}} > 0$.

- If $c_i < \sqrt{n}$, then $(*)$ shows that $c_i q_i - \sqrt{n - c_{i-1}c_i} > \sqrt{n} - c_i > 0$.

4 Continued Fraction of $\sqrt{n}$

Theorem 1. *There exists an index m such that $q_m = 2q_0$. Then the sequence $(q_i)_{i\geqslant 1}$ is m-periodic and we have the periodic continued fraction*

$$\sqrt{n} = [q_0; q_1, q_2, \ldots] = [q_0; \overline{q_1, \ldots, q_m}] = [q_0; \overline{\underbrace{q_1, \ldots, q_1}_{palindrome}, 2q_0}]$$

Proof. Let us consider the positive real numbers $\theta_i = \dfrac{\sqrt{n - c_{i-1}c_i} + \sqrt{n}}{c_i}$ present in the definition of q_i. As $\sqrt{n - c_{i-1}c_i} = c_i q_i - \sqrt{n - c_i c_{i+1}}$, we have

$$\theta_i = \frac{c_i q_i - \sqrt{n - c_i c_{i+1}} + \sqrt{n}}{c_i} = q_i + \frac{\sqrt{n} - \sqrt{n - c_i c_{i+1}}}{c_i}$$

and amplifying the last fraction by $\sqrt{n} + \sqrt{n - c_i c_{i+1}}$, we get

$$\theta_i = q_i + \frac{c_i c_{i+1}}{c_i(\sqrt{n} + \sqrt{n - c_i c_{i+1}})} = q_i + \frac{c_{i+1}}{\sqrt{n} + \sqrt{n - c_i c_{i+1}}} = q_i + \frac{1}{\theta_{i+1}}$$

As all q_i's are strictly positive integers, we then have $\theta_i = [q_i; q_{i+1}, q_{i+2}, \ldots]$.

In the same way, the numbers $\theta'_i = \dfrac{\sqrt{n - c_{i-1}c_i} + \sqrt{n}}{c_{i-1}}$ satisfy

$$\theta'_{i+1} = \frac{\sqrt{n - c_i c_{i+1}} + \sqrt{n}}{c_i} = q_i + \frac{\sqrt{n} - \sqrt{n - c_{i-1}c_i}}{c_i} = q_i + \frac{1}{\theta'_i}$$

hence $\theta'_{i+1} = [q_i, q_{i-1}, \ldots, q_0, \theta'_0]$ with $\theta'_0 = \sqrt{n}$. We can also deduce that $q_i = \lfloor \theta'_{i+1} \rfloor$.

• *Periodicity* : As the sequence $(c_i)_{i\geqslant 0}$ of integers is bounded, we can find two indices $m > i \geqslant 0$ with i minimal, such that $c_m = c_i$ and $c_{m+1} = c_{i+1}$. Then we have $\theta'_{m+1} = \theta'_{i+1}$, $q_m = \lfloor \theta'_{m+1} \rfloor = \lfloor \theta'_{i+1} \rfloor = q_i$ and $c_{m-1} = q_m^2 c_m - 2q_m\sqrt{n - c_m c_{m+1}} + c_{m+1}$ coincides with c_{i-1}. To respect the minimality of i, we deduce that $i = 0$, $c_m = c_0 = 1$ and $c_{m+1} = c_1 = n - q_0^2$. We also have the continued fraction

$$\theta_{m+1} = \theta_1 = [q_1, q_2 \ldots, q_m, \theta_{m+1}] = [\overline{q_1, q_2, \ldots, q_m}].$$

• *Palindromy* : Let us remark that $\theta_1 = \dfrac{\sqrt{n} + q_0}{n - q_0^2} = \dfrac{1}{\sqrt{n} - q_0} = \dfrac{1}{\theta'_1 - 2q_0}$. With the above continued fraction, we have

$$\theta'_1 - 2q_0 = [0, \overline{q_1, q_2, \ldots, q_m}], \qquad \theta'_1 = [2q_0, \overline{q_1, q_2, \ldots, q_m}].$$

Comparing with $\theta'_1 = \theta'_{m+1} = [q_m, q_{m-1}, \ldots, q_1, \theta'_1] = [\overline{q_m, q_{m-1}, \ldots, q_1}]$, we get $q_m = 2q_0$, $q_{m-1} = q_1$, $q_{m-2} = q_2$, and so on. □

5 The Pell Equation

Theorem 3. *For each index $i \geqslant 0$, we have the relation $a_i^2 - nb_i^2 = (-1)^i c_i$ and the continued fraction $\frac{a_{i+1}}{b_{i+1}} = [q_0; q_1, \ldots, q_i]$.*

Proof. With the relations $a_{i+1} = q_i a_i + a_{i-1}$ and $\theta_{i+1} = 1/(\theta_i - q_i)$, we get

$$a_{i+1}\theta_{i+1} + a_i = \theta_{i+1}(q_i a_i + a_{i-1} + a_i(\theta_i - q_i)) = \theta_{i+1}(a_i\theta_i + a_{i-1})$$

and a similar relation is valid for the b_i's. By iteration and using the initial values $a_0\theta_0 + a_{-1} = \theta_0 = \sqrt{n}$, resp. $b_0\theta_0 + b_{-1} = 1$, we can write

$$a_{i+1}\theta_{i+1} + a_i = \theta_{i+1}\theta_i \cdots \theta_2\theta_1\sqrt{n} \quad \text{and} \quad b_{i+1}\theta_{i+1} + b_i = \theta_{i+1}\theta_i \cdots \theta_2\theta_1$$

We deduce that $a_i\theta_i + a_{i-1} = (b_i\theta_i + b_{i-1})\sqrt{n}$. Let us explicit θ_i and multiply this last relation by c_i :

$$a_i\sqrt{n - c_{i-1}c_i} + a_i\sqrt{n} + c_i a_{i-1} = (b_i\sqrt{n - c_{i-1}c_i} + c_i b_{i-1})\sqrt{n} + b_i n.$$

Let us now compare the integer parts and the irrational parts :

$$\begin{cases} a_i = b_i\sqrt{n - c_{i-1}c_i} + c_i b_{i-1} \\ nb_i = a_i\sqrt{n - c_{i-1}c_i} + c_i a_{i-1} \end{cases}$$

Multiplying the first equation by a_i, the second one by b_i and substracting the obtained relations, we get $a_i^2 - nb_i^2 = c_i(a_i b_{i-1} - a_{i-1}b_i)$. The first part of the theorem is then proved if we remark that

$$\begin{aligned} a_{i+1}b_i - a_i b_{i+1} &= (q_i a_i + a_{i-1})b_i - a_i(q_i b_i + b_{i-1}) = a_{i-1}b_i - a_i b_{i-1} \\ &= -(a_i b_{i-1} - a_{i-1}b_i) = \ldots = (-1)^{i+1}(a_0 b_{-1} - a_{-1}b_0) = (-1)^{i+1}. \end{aligned}$$

We can also find this relation by considering the determinant in the matrix relation

$$\begin{pmatrix} a_{i+1} & a_i \\ b_{i+1} & b_i \end{pmatrix} = \begin{pmatrix} a_i & a_{i-1} \\ b_i & b_{i-1} \end{pmatrix}\begin{pmatrix} q_i & 1 \\ 1 & 0 \end{pmatrix} = \cdots = \underbrace{\begin{pmatrix} a_0 & a_{-1} \\ b_0 & b_{-1} \end{pmatrix}}_{\text{Identity matrix}}\begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} q_i & 1 \\ 1 & 0 \end{pmatrix}.$$

Given a matrix $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and a number x, we define $M * x = \dfrac{ax+b}{cx+d}$. We have for example $\begin{pmatrix} q & 1 \\ 1 & 0 \end{pmatrix} * x = q + \dfrac{1}{x}$ and we can check that $M_1 * (M_2 * x) = M_1M_2 * x$. Let us apply the map $M \longmapsto M * x$ to the above matrix relation :

$$\frac{a_{i+1}x + a_i}{b_{i+1}x + b_i} = [q_0; q_1, \ldots, q_i, x].$$

If we take the limit as x tends to infinity, we get $\frac{a_{i+1}}{b_{i+1}} = [q_0; q_1, \ldots, q_i]$ and the proof is complete. $\square$

Corollary. *Let m be the period of the continued fraction of $\sqrt{n}$ as defined in theorem 1. We then have $c_{km} = c_0 = 1$ and $a_{km}^2 - nb_{km}^2 = (-1)^{km}$ for every integer $k \geqslant 0$. Hence, the Pell equation $x^2 - ny^2 = -1$ can be solved only if m is odd (by considering odd values of k) whereas the equation $x^2 - ny^2 = 1$ can always be solved (by choosing even values of k if m is odd).*

Remark. *The number $\theta_i = [q_i; q_{i+1}, q_{i+2}, \ldots]$ is called the i-th complete quotient of $\sqrt{n} = [q_0; q_1, q_2, \ldots]$. The expression $\theta_i = (P_i + \sqrt{n})/Q_i$ for some integers P_i and Q_i is well-known and this paper gives a more precise connection between P_i and Q_i.*

6 The Generalized Pell Equation

1. We consider a quadratic irrational $\theta_0 = \dfrac{\gamma + \sqrt{\beta}}{\alpha}$ with positive integers α, β and γ. With the previous notations, the number θ_0 is obtained with $n = \beta\alpha^2$, $c_{-1} = \beta - \gamma^2$ and $c_0 = \alpha^2$. If $c_{-1} > 0$ and $\theta_0 > 1$, then the previous results about the continued fractions are all valid because the inductive proof of the proposition is well-initialized. We get the continued fraction of θ_0 (instead of $\sqrt{n}$) and we can check that the Pell relation becomes

$$(\alpha a_i - \gamma b_i)^2 - \beta b_i^2 = (-1)^i c_i.$$

Replacing β with $\gamma^2 + \beta\alpha > 0$ leads to the relation $\alpha a_i^2 - 2\gamma a_i b_i - \beta b_i^2 = (-1)^i \dfrac{c_i}{\alpha}$.

2. In the same way, the continued fraction of a number $\theta_0 = \sqrt{\alpha/\beta}$ with $\alpha > \beta \geqslant 1$ can be found with $n = \alpha\beta$, $c_{-1} = \alpha$ and $c_0 = \beta$. If n is a non-square integer, the previous results about the continued fractions (of θ_0 instead of $\sqrt{n}$) are all valid and the Pell relation becomes

$$\beta a_i^2 - \alpha b_i^2 = (-1)^i c_i.$$

Example. Can we find two integers x and y such that $11x^2 - 7y^2 = 1$?

If we consider the equation $11X - 7Y = 1$, the usual extended euclidean algorithm (connected with the continued fraction of $11/7$) gives the general solution $X = 2 + 7k$ and $Y = 3 + 11k$ with $k \in \mathbb{Z}$ but it is not easy to find some values of k for which X and Y are both perfect squares. So we use the continued fraction of $\theta_0 = \sqrt{11/7} = \sqrt{77}/7$. We consider $n = 77$, $c_{-1} = 11$ and $c_0 = 7$ in the algorithm :

i	a_i	b_i	c_i	q_i
-1	0	1	11	
0	1	0	7	1
1	1	1	4	3
2	4	3	13	1
3	5	4	$\boxed{1}$	16
4	84	67	13	1

i	a_i	b_i	c_i	q_i
5	89	71	4	3
6	351	280	7	2
7	791	631	4	3
8	2724	2173	13	1
9	3515	2804	$\boxed{1}$	16
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

We get the continued fraction $\sqrt{11/7} = [1; \overline{3, 1, 16, 1, 3, 2}]$ and the considered equation has the solutions $(4; 5)$ and $(2804; 3515)$ corresponding to the values $k = 2$ and $k = 1'123'202$. There is no other solution for $k < 1'123'202$ and the next one is $(1968404; 2467525)$, corresponding to $k = 553'516'329'602$.

References

[1] M.G. Duman, Positive integer solutions of some Pell equations, *Matematika*, 30(1) (2014), 97-108.

[2] H.W. Lenstra Jr., Solving the Pell equation, *Notices of the AMS*, 49(2) (2002), 182-192.

[3] K.R. Matthews, The diophantine equation $x^2 - Dy^2 = N$, $D > 1$, in integers, *Expositiones Mathematicae*, 18(2000), 323-331.

[4] R.A. Mollin, Simple continued fraction solutions for Diophantine equations, *Expositiones Mathematicae*, 19(2001), 55-73.