PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 1, *Number* 1, *March* 2016, *pages* 43–48

Leonardo Zapponi

Parametric Solutions of Pell's Equation

written by Pietro Mercuri

1 Introduction

An *ordinary Pell's equation* is an equation of the form

$$x^2 - ny^2 = 1, \tag{1}$$

where n is a positive integer that is not a square. It is well known that a pair of integers (x, y) is a solution for (1) if and only if $x + y\sqrt{n}$ is a unit with norm 1 of the ring $\mathbb{Z}[\sqrt{n}]$. It is also known that the integer solutions of (1) form an abelian group V isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$. Moreover, $V \cap \mathbb{R}_{>0} \cong \mathbb{Z}$ is cyclic and a generator of this group is called a fundamental solution of (1).

A *polynomial Pell's equation* is an equation of the form

$$P^2 - DQ^2 = 1, \tag{2}$$

where $D \in \mathbb{Z}[X]$ is not a square. We are interested in solutions $P, Q \in \mathbb{Z}[X]$. Now, we define what a parametric solution of a Pell's equation is. Let the pair (a, b) be a fundamental solution of the ordinary Pell's equation (1). A pair (P, Q), with $P, Q \in \mathbb{Z}[X]$, is a *parametric solution* associated to (a, b) if there is a polynomial $D \in \mathbb{Z}[X]$ that is not a square and $\deg(D) = 2$ such that (P, Q) is a solution of (2) and there is an integer k such that

$$\begin{cases} P(k) = a, \\ Q(k) = b, \\ D(k) = n. \end{cases}$$

The *degree* of a parametric solution (P, Q) associated to (a, b) is $\deg(P)$. Without loss of generality we can assume that $k = 0$. With this assumption, if the polynomials $P, Q, D \in \mathbb{Z}[X]$ form a parametric solution, then $P(mX), Q(mX), D(mX)$ form a parametric solution for every nonzero integer m. From now on, we also assume that $\deg(D) = 2$.

The solutions of a Pell's equation are strictly related to Chebyshev polynomials. Let V be the $\mathbb{C}(X)$-vector space of sequences $\{u_n\}_{n \in \mathbb{N}}$, with $u_n \in \mathbb{C}(X)$ such that

$$u_{n+1} = 2Xu_n - u_{n-1}.$$

We know that V has dimension 2 and a basis is $\{T_n, U_n\}$, where $T_n, U_n \in \mathbb{Z}[X]$ are the *Chebyshev polynomials of first and second kind of degree n* respectively. They are defined by

$$\begin{cases} T_0(X) = 1 \\ T_1(X) = X, \end{cases} \quad \text{and} \quad \begin{cases} U_0(X) = 1 \\ U_1(X) = 2X. \end{cases}$$

Explicitly they can be expressed as

$$T_n(X) = \frac{1}{2}\left[\left(X - \sqrt{X^2 - 1}\right)^n + \left(X + \sqrt{X^2 - 1}\right)^n\right],$$
$$U_n(X) = \frac{1}{2\sqrt{X^2 - 1}}\left[\left(X - \sqrt{X^2 - 1}\right)^{n+1} - \left(X + \sqrt{X^2 - 1}\right)^{n+1}\right],$$

and, in the field $\mathbb{C}(X)\left[\sqrt{X^2 - 1}\right]$, they satisfy the identity

$$\left(X + \sqrt{X^2 - 1}\right)^n = T_n(X) + U_{n-1}(X)\sqrt{X^2 - 1}.$$

Hence (T_n, U_{n-1}) is a solution of the Pell's equation with $D(X) = X^2 - 1$, i.e.

$$T_n^2(X) - (X^2 - 1)U_{n-1}^2(X) = 1.$$

Theorem 1. *Let* $P, Q, D \in \mathbb{C}[X]$ *with* $\deg(D) = 2$ *and* $\deg(P) = d$. *The following conditions are equivalent:*

1. *P, Q, D satisfy the identity $P^2 - DQ^2 = 1$;*

2. *there are $\lambda, \mu \in \mathbb{C}^*$ and $\nu \in \mathbb{C}$ such that*

$$\begin{cases} P(X) = \pm T_d(\lambda X + \nu) \\ Q(X) = \mu U_{d-1}(\lambda X + \nu) \\ D(X) = \frac{(\lambda X + \nu)^2 - 1}{\mu^2}. \end{cases}$$

Remark 2. If d is odd, then T_d is an odd function and we can remove the sign $\pm$.

2 Parametric solutions

Now, we study the possible degrees of a parametric solution. We start giving an explicit description in the cases $\deg(P) = 1, 2$.

Proposition 3. *Let (a, b) be a solution of the Pell's equation (1) and let $P, Q, D \in \mathbb{Z}[X]$ with* $\deg(D) = 2$ *and* $\deg(P) = 1$. *Let*

$$c = \begin{cases} 1 & \text{if } b \text{ is odd} \\ 2 & \text{if } b \text{ is even.} \end{cases}$$

The following conditions are equivalent:

1. *P, Q, D satisfy*

$$\begin{cases} P^2 - DQ^2 = 1 \\ P(0) = a \\ Q(0) = b \\ D(0) = n; \end{cases}$$

2. *there is a nonzero integer m such that*

$$\begin{cases} P(X) = \frac{b^2 m}{c} X + a \\ Q(X) = b \\ D(X) = \frac{b^2 m^2}{c^2} X^2 + \frac{2am}{c} X + n. \end{cases}$$

Proposition 4. *Let (a, b) be a solution of the Pell's equation (1) and let $P, Q, D \in \mathbb{Z}[X]$ with $\deg(D) = 2$ and $\deg(P) = 2$. The following conditions are equivalent:*

1. *P, Q, D satisfy*

$$\begin{cases} P^2 - DQ^2 = 1 \\ P(0) = a \\ Q(0) = b \\ D(0) = n; \end{cases}$$

2. *there are two integers $m \neq 0$ and $\varepsilon \in \{\pm 1\}$ such that, if*

$$c = \gcd(b^3, (a+\varepsilon)b, 2(a+\varepsilon)^2),$$

then we have

$$\begin{cases} P(X) = \frac{b^4(a+\varepsilon)m}{c} X^2 + \frac{2b^2(a+\varepsilon)m}{c} X + a \\ Q(X) = \frac{b^3 m}{c} X + b \\ D(X) = \frac{b^2(a+\varepsilon)^2 m^2}{c^2} X^2 + \frac{2(a+\varepsilon)^2 m}{c} X + n. \end{cases}$$

Let n be a positive integer that is not a square and let $K = \mathbb{Q}(\sqrt{n})$ a quadratic real number field. Let $\mathcal{O}_K$ the ring of integers of K and let U the subgroup of $\mathcal{O}_K^\times$ consisting of the units with norm 1. We have that U is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$. We also know that the elements of the subgroup $V = U \cap \mathbb{Z}[\sqrt{n}]$ correspond bijectively to the solutions of Pell's equation (1). We denote by $V(a, b)$ the subgroup of V generated by -1 and $a + b\sqrt{n}$. If (a, b) is a fundamental solution of Pell's equation (1) we have that $V(a, b) = V$. The quotient U/V is a finite cyclic group. The following theorem states that the degree of a parametric solution is bounded.

Theorem 5. *Let n be a positive integer that is not a square and let (a, b) a solution of Pell's equation (1). The following conditions are equivalent:*

1. *there is a parametric solution $P, Q, D \in \mathbb{Z}[X]$ of degree d associated to (a, b);*
2. *we have that $d \mid 2[U : V(a, b)]$.*

Without other assumptions on n this bound is not uniform, in fact for any positive integer d there are $a, b \in \mathbb{Z}$ such that

$$\left(2 + \sqrt{3}\right)^d = a + b\sqrt{3}.$$

Now, taking $n = 3b^2$ we have that $(a, 1)$ is a fundamental solution of $x^2 - ny^2 = 1$ and $d \mid [U : V(a, 1)]$. Hence, by Theorem 5 above, there is a parametric solution of degree d.

If we restrict to n squarefree, we have that if $n \equiv 2, 3 \pmod 4$ then U/V is trivial, else U/V is a subgroup of $\mathbb{Z}/3\mathbb{Z}$. Hence, d must divide 6. More precisely, if $n \equiv 2, 3 \pmod 4$ then $d = 1, 2$, else $d = 1, 2, 3, 6$.

References

[1] L. Zapponi, *Parametric solutions of Pell equations*, available at the URL http://arxiv.org/abs/1503.00637.

[2] *Parametric solutions of Pell's equations*, Discussion on the mathematical forum Mathoverflow, available at the URL http://mathoverflow.net/questions/194910/.

[3] *The Grothendieck theory of dessins d'enfants*, papers from the Conference on dessins d'enfant held in Luminy, April 1924, 1993. Edited by Leila Schneps. London Mathematical Society Lecture Note Series, **200**, Cambridge University Press, Cambridge, 1994.

Pietro Mercuri
Dipartimento di Matematica
Sapienza Università di Roma
Piazzale Aldo Moro 5
00185 Roma, Italy
email: mercuri.ptr@gmail.com