Pell's equation and Diophantine invariants of dessins d'enfants

Alexander K. Zvonkin

June 9, 2019

Abstract

We consider a pair of *dessins d'enfants* which almost always form a Galois orbit defined over a quadratic number field. However, from time to time this pair splits into two Galois orbits, both defined over $\mathbb{Q}$. We show that this splitting takes its origin in a solution of a Diophantine equation, namely, in this particular case, of the Pell equation. A general conclusion which follows from this example is that, beside usual and well-known combinatorial and group-theoretic invariants of the Galois action on dessins d'enfants, there also exist invariants of a Diophantine nature.

The theory of dessins d'enfants studies the action of the absolute Galois group $\mathrm{Aut}(\overline{\mathbb{Q}}|\mathbb{Q})$ on bicolored maps, with a particular interest in the search of invariants of this action. In the vast majority of cases, such invariants are of a combinatorial and/or of group-theoretic nature. Sweet dreams are sometimes expressed in the dessins d'enfants community that it would be desirable to find a *complete* set of such invariants, a sort of "two dessins belong to the same Galois orbit *if and only if* all their invariants are equal". One of the goals of this paper is to show that such a system of invariants cannot exist. Namely, there are certain cases when the dessins in question do not present any particular combinatorial or group-theoretic properties, and the Galois splitting is explained by some Diophantine relations between certain numerical characteristics of the dessins in question. We call such relations *Diophantine invariants*. Thus, the statement that a complete set of combinatorial or group-theoretic invariants cannot exist is not entirely negative since the Diophantine equations are a remarkable subject in itself. In this paper we present a particularly beautiful example of this phenomenon, when the question of splitting of a combinatorial orbit of size 2 into two Galois orbits over $\mathbb{Q}$ is reduced to the famous Pell equation.

1 Pell's equation: preliminaries

Definition 1.1 (Pell's equation) Let $D > 0$ be an integer which is not a perfect square. Then the Diophantine equation

$$x^2 - Dy^2 = 1 \tag{1}$$

is called *Pell's equation*.

The word Diophantine means that we look for solutions in $\mathbb{N}$ or in $\mathbb{Z}$. The name of the British mathematician John Pell was erroneously attributed to this equation by Euler: Pell never worked on it.

1.1 A brief history of the Pell equation

This innocently looking and inconspicuous equation is a real mathematical jewel. It is studied for more than two thousand years, and people still find something new to say about it. Among the recent publications we may mention the monograph [5] (of more than 500 pages!) by Jacobson and Williams (2009); a problem book [2] by Barbeau (2003); and a scientific-popular brochure [3] by Bugaenko (2010). One of the proofs of the algorithmic undecidability of Hilbert's Tenth problem is based on the properties of Pell's equations: see a short announcement in [4] and a detailed exposition in [6].

The first name mentioned in relation to the Pell equation is that of Pithagoras (VI$^{\text{th}}$ century before n. e.). The books on the history of mathematics do not say what exactly was his contribution to the subject but we can advance a plausible conjecture: since the equation $x^2 - 2y^2 = 0$ does not have a solution in integers then let us try the closest one: $x^2 - 2y^2 = 1$.

The next appearance of this equation is in a letter by Archimedes to Eratosthenes (III$^{\text{rd}}$ century before n. e.) concerning the cattle of the god Helios. The full text of the letter, as well as a relevant discussion, may be found in [5], pages 19–24. In order to establish the number of bulls of Helios one must write down a system of algebraic equations which is reduced to the Pell equation with $D = 410\,286\,423\,278\,424$. It may well be that the whole story is a pure legend. At that time, the positional system was not yet invented, and without its apparatus it is close to impossible to work with huge numbers. Therefore, it is highly improbable that Archimedes was himself able to solve an equation with such an enormous coefficient. But maybe he proceeded in the opposite direction: from a solution to the equation.

The next step was made by Indian mathematicians: Brahmagupta (VII$^{\text{th}}$ century), Bhaskara II (XII$^{\text{th}}$ century), Narayana Pandit (XIV$^{\text{th}}$ century), and we return to Europe with the British mathematician Brouncker (XVII$^{\text{th}}$ century).

Then comes the omnipresent platoon of Fermat, Euler, Lagrange, Abel, Dirichlet... Lagrange was the first to prove that equation (1) always has infinitely many solutions. Abel considered the case where x, y and D are one variable polynomials; it turned out later that this problem is related to elliptic curves. Dirichlet, while studying the ring

$$\mathbb{Z}(\sqrt{D}) = \{x + y\sqrt{D} \mid x, y \in \mathbb{Z}\},$$

reinterpreted Lagrange's theorem as the existence, in this ring, of infinitely many divisors of unity. Indeed, if (x, y) is a solution of (1) then both $x+y\sqrt{D}$ and $x - y\sqrt{D}$ are divisors of unity since their product is equal to one. It is also interesting to know that all the divisors of unity can be obtained as powers of a single one, as we will see in the next section.

Then come modern times... And the Pell equation is still a subject of interest of many contemporary researches.

1.2 Solutions

It is known that the Pell equation has infinitely many solutions. All solutions in $\mathbb{N}$ lie on a quarter of hyperbola $\{(x, y) \in \mathbb{R}_+^2 \mid x^2 - Dy^2 = 1\}$; therefore, it is possible to order them from left to right. There always exists the trivial solution $(x_0, y_0) = (1, 0)$; the next one, the solution (x_1, y_1), is called the *fundamental solution*.

Proposition 1.2 (Solutions of Pell's equation) *Consider the matrix*

$$A = \begin{pmatrix} x_1 & Dy_1 \\ y_1 & x_1 \end{pmatrix} \tag{2}$$

where (x_1, y_1) is the fundamental solution of (1)*. Then all the solutions of* (1) *are given by the formula*

$$\begin{pmatrix} x_n \\ y_n \end{pmatrix} = A^n \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}. \tag{3}$$

Proof. If (x_n, y_n) is a solution then the multiplication by the matrix A gives another solution: this fact is established by a trivial verification. Why there are no other solutions? Notice that $\det A = 1$; therefore, the entries

of the inverse matrix A^{-1} are integers. Suppose that there is a solution which lies between the nth and $(n+1)$st solutions obtained by the above formulas. Multiplying it by A^{-1} we get a solution lying between $(n-1)$st and nth ones. Repeating this procedure we will finally find a solution between (x_0, y_0) and (x_1, y_1). But the existence of such a solution contradicts the definition of the fundamental solution. □

Pell-*like* equation is the equation

$$x^2 - Dy^2 = k, \quad k \neq 1.$$

This equation may have either no solutions at all, or infinitely many of them. For example, the equation $x^2 - 7y^2 = 3$ has no solutions. Indeed, taking it modulo 7 we get the equation $x^2 = 3 \bmod 7$, but 3 is not a quadratic residue in $\mathbb{Z}_7$. If, however, we find at least one solution then we get infinitely many of them by multiplying this one by the matrix (2) with the same D and with (x_1, y_1) being the fundamental solution of the corresponding Pell equation (that is, the one with $k = 1$). In general, algorithms to verify if a given Pell-like equation has a solution or not are rather sophisticated: see in this respect Section 16.3 of [5].

We see that the most important step in solving Pell's equation is to find the fundamental solution. A great difficulty is that even for moderate values of D the fundamental solution may be very large. For example, for $D = 991$ the smallest solution after $(1, 0)$ is

$$\begin{aligned} x_1 &= 379\,516\,400\,906\,811\,930\,638\,014\,896\,080, \\ y_1 &= 12\,055\,735\,790\,331\,359\,447\,442\,538\,767. \end{aligned}$$

Another example: for $D = 410\,286\,423\,278\,424$ the fundamental solution contains 206 545 decimal digits (this information is taken from [5]). It is hardly possible to find the solution for the first example (with $D = 991$) by a brute force search; the second example needs no commentary. Many sophisticated and efficient algorithms are known, but an algorithm proposed by Bhaskara II in 1150 is still in use today.

For those who are interested in concrete results we may recommend Pell's equation solver [10].

We are lucky: in the example that follows $D = 2$ and the fundamental solution is $(x_1, y_1) = (3, 2)$: indeed, $3^2 - 2 \cdot 2^2 = 1$.

2 Dessins, Belyĭ function, field of moduli

2.1 Combinatorial orbit

By a *combinatorial orbit* we mean the set of all the dessins with a given *passport* (that is, with a given set of degrees of the black vertices, of the white vertices, and of the faces).

We consider the dessins with the following passport (see Fig. 1): the black vertex partition is $\alpha = m^3$, that is, there are three black vertices, each of them of degree m; the white vertex partition is $\beta = 5^1 1^{3m-5}$, that is, there is one white vertex of degree 5 (the "center"), while all the other white vertices are of degree 1; the face partition is $\gamma = (3m-2)^1 1^2$, that is, there is an outer face of degree $3m-2$ and two faces of degree 1. (Note that for bicolored maps the degree of a face is, by definition, *the half* of the number of the edges surrounding this face.) Bicolored plane maps with all their faces except the outer one being of degree 1 are also known under the name of *weighted trees* and are thoroughly studied in [1].

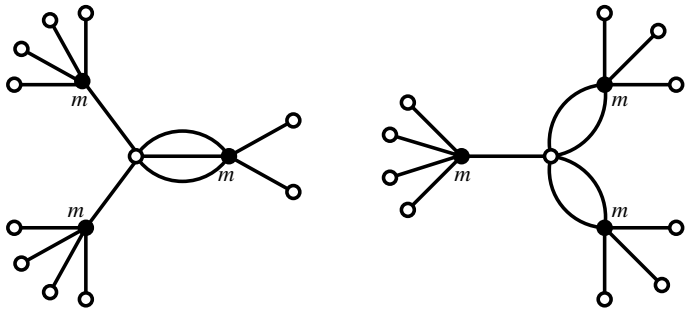

Figure 1: A combinatorial obit consisting of two dessins: black vertex degrees are equal to $m \geq 3$ (in the figure, $m = 5$).

There are two dessins with the above passport. They look as is shown in Fig. 1. Both of them are symmetric with respect to the real axis; therefore they are defined over a real field. They may constitute a single orbit defined over a real quadratic field, or two separate orbits both defined over $\mathbb{Q}$.

Combinatorially, these dessins don't have any particular features which would permit to distinguish them and to put them in separate Galois orbits. From the group-theoretic point of view, there is nothing to say either, as the following proposition shows.

Proposition 2.1 (Monodromy groups) *The monodromy groups of the dessins of the above figure are the same. Namely, they are* S_{3m} *for* m *even, and* A_{3m} *for* m *odd.*

PROOF. Let us first prove that the groups in question are primitive. We will use the following Lemma:

Lemma 2.2 (Ritt's theorem) *The monodromy group of a dessin is imprimitive if and only if the corresponding Belyĭ function* F *is decomposable, that is,* $F = g \circ f$ *where* $\deg(f) > 1$, $\deg(g) > 1$.

A proof of this Lemma may be found in [8]; a better proof is given in the ERRATA AND COMMENTS file to this book.

Let F be a Belyĭ function, and M_F the corresponding dessin. Suppose that F is decomposable, that is, $F = g \circ f$. Here g must be a Belyĭ function while f is not necessarily Belyĭ but its critical values must be either vertices or face centers of the map M_g corresponding to g.

Let A be a face of M_g and $\deg(A) = k$. Then $f^{-1}(A)$ is a set of faces of M_F whose degrees are multiples of k, and the sum of these degrees is equal to $k \cdot \deg(f)$. In our case, both dessins of Figure 1 have two faces of degree 1. Therefore, the only possibility for a composition would be to have $\deg(f) = 2$ and thus f (and, hence, also $F = g \circ f$) would be invariant under a central symmetry of order 2. But our dessins are not centrally symmetric. Hence, the function F cannot be a composition, and the monodromy groups of both dessins are primitive. □

What remains in order to prove Proposition 2.1 is to apply the classical Jordan's "symmetric group theorem" (see [7]): it states that a primitive permutation group of degree n which contains a cycle of a prime order $p < n - 2$ is either S_n or A_n. In our example, the monodromy group is of degree $n = 3m$, and it contains a cycle of order 5 (the permutation corresponding to the white vertices). Thus, for $m \geq 3$ it satisfies the conditions of Jordan's theorem. □

We conclude that the monodromy group is the same for both dessins, hence it does not permit to separate them. What comes to the rescue is the Pell equation. It permits to find a *complete* list of splitting combinatorial orbits.

2.2 Belyĭ function and the field of moduli

The computation of the Belyĭ function proceeds as follows. We put the center of the outer face to $x = \infty$; the white vertex of degree 5, to $x = 0$; and let the sum of the positions of the centers of two small faces be equal to 1. Then the Belyĭ function takes the following form:

$$f \;=\; K \cdot \frac{(x^3 + ax^2 + bx + c)^m}{x^2 - x + d}.$$

Computing f' we get

$$f' \;=\; K \cdot \frac{(x^3 + ax^2 + bx + c)^{m-1} \cdot q(x)}{(x^2 - x + d)^2},$$

where $q(x)$ is a polynomial of degree 4. What remains is to make $q(x)$ proportional to x^4, that is, to equate all the coefficients of $q(x)$, except the leading one, to zero. This gives us four equations for the unknowns a, b, c, d. The factor K is then determined by the condition $f(0) = 1$.

As a result of the computation we find out that all the coefficients of Belyĭ function belong to the real quadratic field $\mathbb{Q}(\sqrt{\Delta})$, where

$$\Delta \;=\; 3\,(2m-1)\,(3m-2). \tag{4}$$

Thus, our combinatorial orbit splits into two Galois orbits when, and only when the parameter Δ in (4) is a perfect square.

3 When the discriminant is a perfect square

Two remarks are in order. First, the numbers $2m-1$ and $3m-2$ are coprime, which can be verified by a direct application of Euclid's algorithm. Second, $3m-2$ cannot be divisible by 3; only $2m-1$ can. We conclude that, in order to make Δ a perfect square, its two factors $3\,(2m-1) = 6m-3$ and $3m-2$ should both be made perfect squares. Then, writing down

$$6m - 3 = a^2, \qquad 3m - 2 = b^2, \tag{5}$$

we observe that

$$a^2 - 2b^2 = 1, \tag{6}$$

that is, the pair (a, b) must be a solution of the Pell equation with $D = 2$.

The equalities (5) imply that the parameter m is found as

$$m \,=\, \frac{a^2+3}{6}, \qquad \text{and also} \qquad m \,=\, \frac{b^2+2}{3}.$$

Therefore, in order to fit into our scheme, the parameter a must be odd and divisible by 3 while b should not be divisible by 3.

It is easy to verify that every other solution of the Pell equation satisfies both conditions. Indeed, the main recurrence

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix}, \quad \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix},$$

being taken modulo 3 gives the following sequence:

$$(1,0) \to (0,2) \to (1,0) \to (0,2) \to \dots$$

The congruence

$$(a,b) = (0,2) \bmod 3$$

means that a is divisible by 3 while b is not. Also, a is always odd since $a^2 = 2b^2 + 1$.

4 Numerical data

The matrix A of Proposition 1.2 is in our case equal to

$$A \,=\, \begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix} \qquad \text{hence} \qquad A^2 \,=\, \begin{pmatrix} 17 & 24 \\ 12 & 17 \end{pmatrix}.$$

The greater eigenvalue of A is $3+2\sqrt{2}$; that of A^2 is $(3+2\sqrt{2})^2 = 17+12\sqrt{2}$. Thus, the growth exponent for the parameter a is $17 + 12\sqrt{2} \approx 33.97$. The parameter m is proportional to a^2, hence its growth exponent is

$$(3 + 2\sqrt{2})^4 \,=\, (17 + 12\sqrt{2})^2 \,\approx\, 1153.999133\dots \tag{7}$$

First eight values of a divisible by 3 are

$$3,\ 99,\ 3363,\ 114\,243,\ 3\,880\,899,\ 131\,836\,323,\ 4\,478\,554\,083,\ 152\,139\,002\,499.$$

First four values of m are

$$\begin{array}{lcl} a = 3 & \Rightarrow & m = 2, \\ a = 99 & \Rightarrow & m = 1634, \\ a = 3363 & \Rightarrow & m = 1\,884\,962, \\ a = 114\,243 & \Rightarrow & m = 2\,175\,243\,842. \end{array}$$

The value $m = 2$ does not fit in our construction; or, if you prefer, for $m = 2$ there exists only one tree, namely, the one the right in Fig. 1, so it is obviously defined over $\mathbb{Q}$. By the way, its monodromy group is not S_6 but $PGL_2(5)$. Therefore, the smallest degree m for which we have a quadratic combinatorial orbit which splits into two Galois orbits over $\mathbb{Q}$ is $m = 1634$. For $a = 152\,139\,002\,499$ we have $m \approx 3.86 \cdot 10^{21}$.

Exercise 4.1 (One more example) *Consider the following passport:*

$$(m^2, 5^1 1^{2m-5}, (2m-3)^1 1^3), \quad m \geq 5.$$

1. *Draw the dessins having this passport. Make sure that there are two of them, and that the corresponding field is real.*

2. *Compute the Belyĭ function. The corresponding field is* $\mathbb{Q}(\sqrt{\Delta})$ *where* $\Delta = 3(m-2)(2m-3)$.

3. *This time both* $m-2$ *and* $2m-3$ *can be divisible by* 3*, hence we must consider two cases:*

$$\text{(A)} \qquad 2m - 3 = a^2, \quad m - 2 = 3b^2,$$

and

$$\text{(B)} \qquad m - 2 = a^2, \quad 2m - 3 = 3b^2.$$

4. *Show that the system of equations* (A) *is reduced to the Pell equation*

$$a^2 - 6b^2 = 1.$$

Find the fundamental solution and the general formula giving all solutions. Find several numerical values of (a, b) *and the corresponding values of* m.

5. *Show that the system of equations* (B) *is reduced to the Pell-like equation*

$$c^2 - 6b^2 = -2$$

where $c = 2a$*. Find the fundamental solution and, using the results for equation* (A)*, find the general formula giving all solutions. Show that the value of the variable* c *for all the solutions is even. Find several numerical values of* (c, b) *and the corresponding values of* m.

6. *Find the growth exponents for the values of* m *obtained from the solutions of* (A) *and* (B).

References

[1] N. M. Adrianov, F. Pakovich, A. K. Zvonkin, Davenport–Zannier Polynomials and Weighted Trees, A monograph, 2019, submitted. Available at `https://www.labri.fr/perso/zvonkin/Books/WT-Book.pdf`.

[2] E. J. Barbeau, Pell's Equation, Problem Books in Mathematics, Springer-Verlag, 2003.

[3] V. O. Bugaenko, Pell's Equation (in Russian), Moscow, MCCME, 2010.

[4] G. V. Chudnovskii, *Diophantine predicates* (in Russian), Uspekhi Matematicheskikh Nauk, vol. **25** (1970), 185–186.

[5] M. J. Jacobson, Jr., H. C. Williams, Solving the Pell Equation, Springer-Verlag, 2009.

[6] J. P. Jones, Yu. V. Matiyasevich, *Proof of recursive unsolvability of Hilbert's tenth problem*, Amer. Math. Monthly, vol. **98** (1991), no. 8, 689–709.

[7] C. Jordan, Traité des substitutions et des équations algébriques, Paris, Gauthier-Villars, 1870. (Reprinted by Gauthier-Villars in 1957.)

[8] S. Lando, A. K. Zvonkin, Graphs on Surfaces and Their Applications, Springer-Verlag, 2004 (second printing 2013). See also Errata and comments to this book: `https://www.labri.fr/perso/zvonkin/Books/errata.pdf`.

[9] "Pell's equation", an article in Wikipedia: `https://en.wikipedia.org/wiki/Pell%27s_equation`.

[10] Pell's equation solver, `http://www.jakebakermaths.org.uk/maths/jshtmlpellsolverbigintegerv10.html`.