

Diophantine Invariants in Dessins d'Enfants: An Example

Alexander K. Zvonkin*

November 7, 2013

Abstract

We consider a particular pair of dessins which, generically, forms a Galois orbit defined over a real quadratic field, and ask whether it can split into two orbits defined over \mathbb{Q} . This question is reduced to the classical Pell equation.

1. Introduction. The theory of dessins d'enfants (see Ch. 2 of [2]) studies the action of the absolute Galois group $\text{Aut}(\overline{\mathbb{Q}}|\mathbb{Q})$ on bicolored maps, with a particular interest in the search of invariants of this action. In a vast majority of cases, such invariants are of combinatorial and/or group-theoretic nature. There are, however, 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 the degrees of their vertices and faces. See in this respect Sections 2.2.4.2 and 2.2.4.3 of [2], and also Ex. 2.2.27, Prop. 2.2.28, and Ex. 2.2.31 there. We call such relations *diophantine invariants*. In this note we present a particularly beautiful example of this phenomenon.

2. Combinatorial orbit. We consider the dessins with the following characteristics:

- the black partition is $\alpha = m^3$, that is, there are three black vertices of degree m ;
- the white partition is $\beta = 5^1 1^{3m-5}$, that is, there is one white vertex of degree 5, 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.

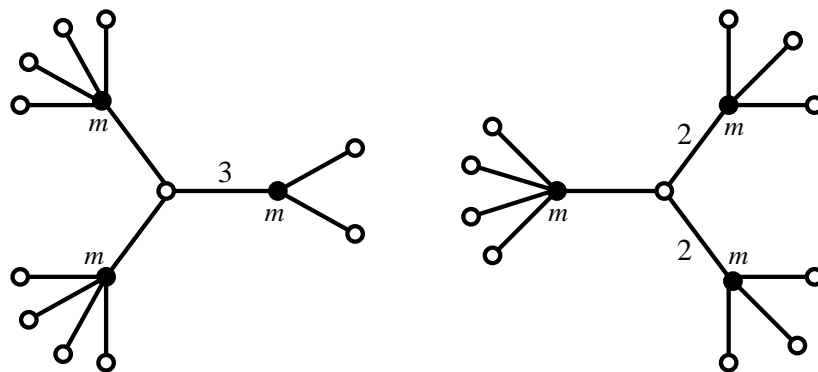


Figure 1: A real quadratic orbit ($m \geq 3$).

For $m = 2$ the corresponding dessin is unique and therefore defined over \mathbb{Q} . For $m \geq 3$ there are two dessins with the above face and vertex degrees. They look as is shown in Fig. 1 (for $m = 5$);

*LaBRI, Université Bordeaux I, 351 cours de la Libération, F-33405 Talence Cedex FRANCE; e-mail: zvonkin@labri.fr

according to the conventions of [3], an “edge of weight 3” represents three parallel edges, and an “edge of weight 2” represents two parallel edges. By merely looking at the dessins we see that the orbit is quadratic and real.

Note that, according to Jordan’s theorem, a primitive permutation group of degree n which contains a cycle of order p prime and $p < n - 2$ is either S_n or A_n . In our example, the monodromy group is of degree $n = 3m$, and contains a cycle of order 5. Thus, for $m \geq 3$ it satisfies the conditions of Jordan’s theorem. It is easy to see that for m even the group is odd, thus S_{3m} , and for m odd the group is even, thus A_{3m} . (For $m = 2$ the monodromy group of the unique dessin is $\text{PGL}_2(5)$.) We see that the monodromy group of both dessins is the same and therefore cannot explain an eventual splitting of this combinatorial orbit into two Galois orbits.

3. Belyi function and field of definition. The computation of the Belyi 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 Belyi function takes the following form:

$$f = K \cdot \frac{(x^3 + ax^2 + bx + c)^m}{x^2 - x + d}. \quad (1)$$

Computing f' we get

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

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 for the field of definition, we get indeed a real quadratic field $\mathbb{Q}(\sqrt{\Delta})$, where

$$\Delta = 3(2m - 1)(3m - 2). \quad (3)$$

4. Main question: when Δ is a perfect square? When this is the case, our quadratic orbit splits into two orbits, both defined over \mathbb{Q} .

Two remarks are in order. First, the numbers $2m - 1$ and $3m - 2$ are coprime. Indeed, a direct application of Euclid’s algorithm gives

$$\begin{aligned} 3m - 2 &= 1 \cdot (2m - 1) + (m - 1), \\ 2m - 1 &= 2 \cdot (m - 1) + 1. \end{aligned}$$

Second, $3m - 2$ cannot be divisible by 3; only $2m - 1$ can. We conclude that, in order to get Δ a perfect square, its two factors $3(2m - 1) = 6m - 3$ and $3m - 2$ should both be made perfect squares.

Then, writing down

$$6m - 3 = a^2, \quad 3m - 2 = b^2, \quad (4)$$

we observe that

$$a^2 - 2b^2 = 1, \quad (5)$$

that is, we get the classical Pell equation! Note however that in order to fit into our scheme the parameter a must be divisible by 3.

5. Basic facts about Pell equation. Recall two basic facts about Eq. (5).

1. If (a, b) and (c, d) are two solutions of (5) then their composition

$$(a, b) * (c, d) = (ac + 2bd, ad + bc) \quad (6)$$

is also a solution of this equation.

2. All solutions of (5) are “composition powers” of the smallest solution (3, 2). That is, all of them can be obtained from (3, 2) by successively applying the operation (6). For example, the “second” solution is $(3, 2) * (3, 2) = (17, 12)$.

Finally, if (a, b) is a solution and a is divisible by 3 while b is not, then “the next” solution is

$$(a, b) * (3, 2) = (3a + 4b, 2a + 3b), \quad (7)$$

and we see that $3a + 4b$ is not divisible by 3. However, the “one after the next” solution is

$$(a, b) * (17, 12) = (17a + 24b, 12a + 17b), \quad (8)$$

and this time $17a + 24b$ is divisible by 3.

6. Conclusion. Let us summarize the results we have obtained.

(A) All solutions (a, b) of the Pell equation for which a is divisible by 3 are obtained, starting from the pair (3, 2), by successive application of the operation

$$(a, b) \mapsto (17a + 24b, 12a + 17b). \quad (9)$$

(B) Since $6m - 3 = a^2$ (see (4)) the degree m is obtained as

$$m = \frac{a^2 + 3}{6}. \quad (10)$$

(C) Since $a \approx b\sqrt{2}$ the growth exponent of the parameter a is $17 + \frac{24}{\sqrt{2}}$, and that of m is

$$\left(17 + \frac{24}{\sqrt{2}}\right)^2 \approx 1154. \quad (11)$$

7. Numerical data. First eight values of a divisible by 3 are

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

First four values of m are

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

Thus, the smallest degree m for which the quadratic orbit splits into two orbits over \mathbb{Q} is $m = 1634$.

8. Acknowledgements. The author is grateful to Gareth A. Jones for valuable remarks.

References

- [1] **Jacobson M. J., Jr., Williams H. C.** Solving the Pell Equation. – Canad. Math. Soc. Books in Mathematics, 2009, XX+495 pp.
- [2] **Lando S. K., Zvonkin A. K.** Graphs on Surfaces and Their Applications. – Springer-Verlag, 2004, XVI+455 pp.
- [3] **Pakovich F., Zvonkin A. K.** Minimum Degree of the Difference of Two Polynomials over \mathbb{Q} , and Weighted Plane Trees. – arXiv:1306.4141v1, June 2013, 54 pp.