Diophantine invariants

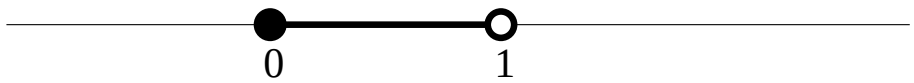
of dessins d'enfants

Alexander Zvonkin
(University of Bordeaux, France)

Symmetries of Surfaces, Maps and Dessins
Banff International Research Station, Canada
24–29 September 2017

What is a **dessin d'enfants:**

- A combinatorial map M with its vertices colored in black and white in a bipartite way
- A compact Rieamann surface X whose genus is that of M
- A meromorphic function $f : X \to \overline{\mathbb{C}}$, called **Belyi function**, such that M is a preimage of the segment $[0, 1]$ and each face contains a single pole of f



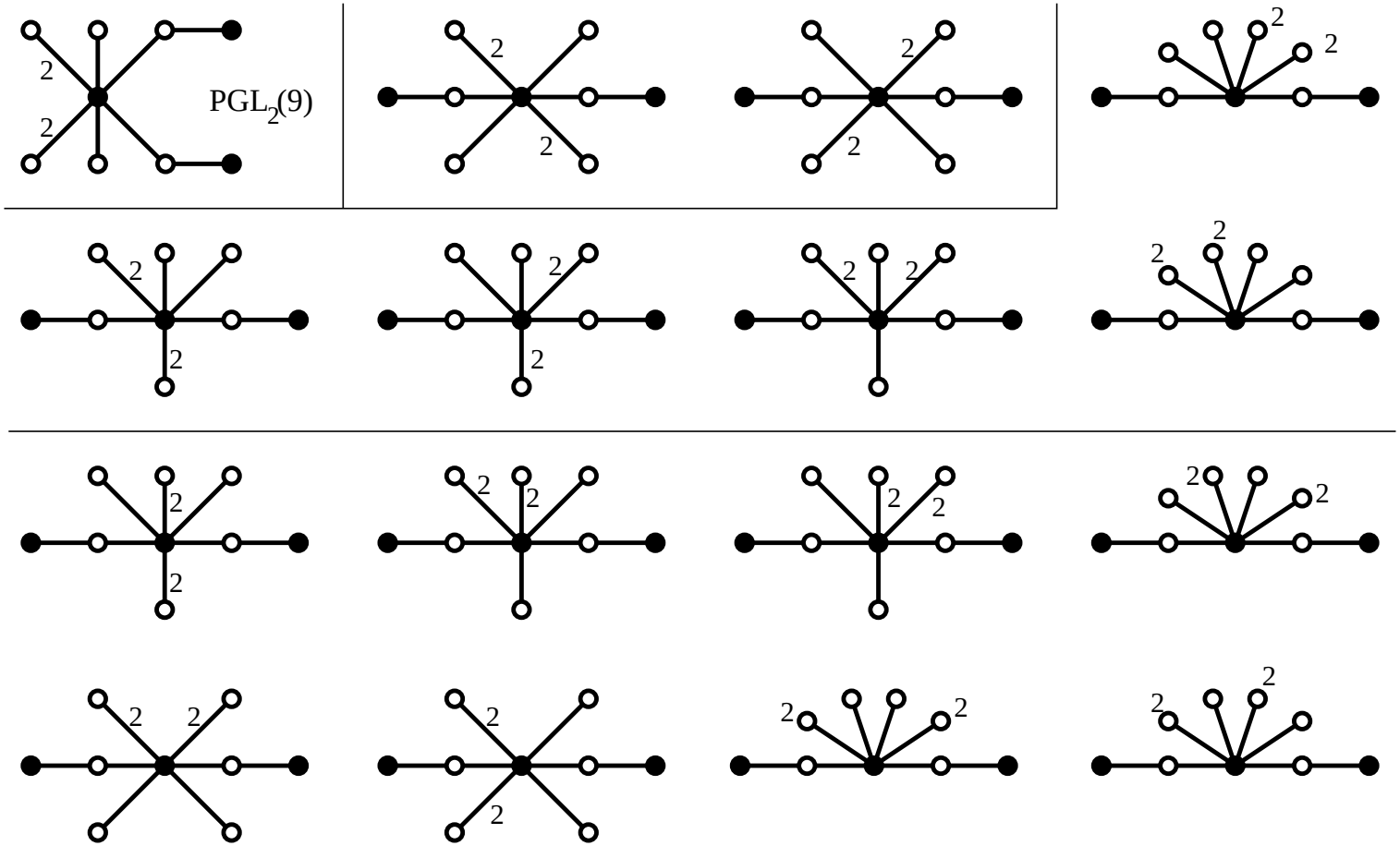
In this case both X and f are **defined** over the field $\overline{\mathbb{Q}}$ of algebraic numbers.

Acting simultaneously on X and f by an automorphism of $\overline{\mathbb{Q}}$ we get, in general, another dessin. This is a **Galois action** on dessins.

There are many combinatorial and group-theoretic invariants of the Galois action on dessins d'enfants:

- **Passport:** the triple of partitions of the degree n of f representing the degrees of the black and white vertices and of the faces
- **Symmetry** (that is, the automorphism group of M)
- **Self-duality**
- **Composition** (long to explain. . .)
- **Monodromy group:** the permutation group generated by the rotations of the edges around vertices
- **Refined passport:** the triple of conjugacy classes of black, white and face permutations in the monodromy group (when these conjugacy classes are not Galois conjugate)
- **etc.**

An example in which several invariants are involved



Dessins with 10 edges and with the passport $(8^1 1^2, 2^4 1^2, 8^1 1^2)$.
16 dessins split into four Galois orbits, of sizes 1, 2, 5 and 8.
Invariants: size **1**: monodromy group $\mathrm{PGL}_2(9)$;
size **2**: symmetry; size **5**: self-dual; size **8**: not self-dual.
The monodromy group of the latter $5 + 8 = 13$ dessins is S_{10}.

Not once, I have heard the following request (or, if you like, a dream):

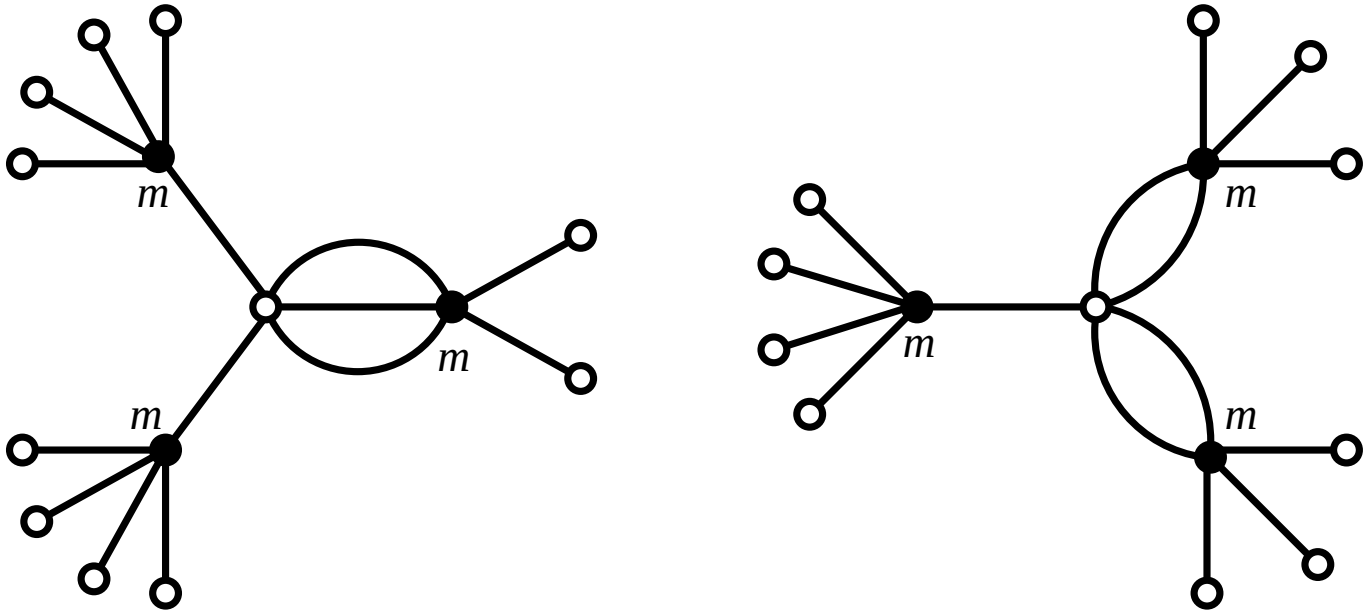
> It would be nice to find a **complete** set of such invariants.
>
> Here **complete** means that two dessins belong to distinct Galois orbits **IF AND ONLY IF** certain of their combinatorial or group theoretic invariants are distinct.
>
> The IF part is obvious, the ONLY IF part is far from being obvious.

The goal of this talk is to show that such a set of invariants cannot exist.

We will see that this is not an entirely bad news: there are also some positive moments in it.

Let us consider the following dessins with $3m$ edges: passport

$$\pi = [m^3, 5^1 1^{3m-5}, (3m-2)^1 1^2], \quad m \geq 3$$



We have:

– either a single orbit defined over a **real** quadratic field

$$\mathbb{Q}(\sqrt{\Delta}), \quad \Delta > 0,$$

– or two orbits, both defined over $\mathbb{Q}$.

Combinatorial invariants provide us with no hint. . .

As for the group-theoretic ones:

Theorem (C. Jordan, 1870): A primitive permutation group of degree n having a cycle of a prime length $p < n - 2$ is either S_n or A_n.

Here we have a cycle of length 5 corresponding to the central white vertex, while $n = 3m \geq 9$ (since $m \geq 3$).

Therefore, whatever is $m \geq 3$, the monodromy group for both maps is the same.

The computation of the Belyi function is an easy exercise:
– put the center of the outer face to $x = \infty$;
– put the white vertex of degree 5 to $x = 0$;
– let the sum of the positions of the centers of the two small faces be equal to 1.

Then the Belyi function takes the following form:

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

Computing f' we get

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

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

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

Main question: Can Δ be 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 a multiple of 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

$$6m-3 = a^2, \qquad 3m-2 = b^2, \tag{4}$$

we observe that

$$\boldsymbol{a^2 - 2b^2 = 1.} \tag{5}$$

We have got the classical

Pell equation!

Remark: a must be a multiple of 3.

Euler attributed Pell's name to this equation by error...

- Pythagoras (VI before J. C.): the equation $a^2 - 2b^2 = 0$ does not have integral solutions; then what about $a^2 - 2b^2 = 1$?
- A letter by Archimedes to Eratosthenes (III before J. C.): a problem about bulls of Helios
- Brahmagupta (VII)
- Bhaskara II (XII)
- Narayana Pandit (XIV)
- Brouncker (XVII)
- Fermat, Euler, Lagrange, Abel, ... (XVII–XIX)
- Dirichlet (XIX)
- etc.

Dirichlet: Any solution of the above equation provides us with two divisors of the unity in the ring $\mathbb{Z}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$:

$$(a + b\sqrt{2})(a - \sqrt{2}) = 1.$$

Classical Pell equation:

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

General (or generalized) Pell equation:

$$a^2 - d \cdot b^2 = 1,$$

where d is positive and without square factors; d is given, we look for a and b. There are always infinitely many solutions.

An equation of Pell type:

$$a^2 - d \cdot b^2 = k.$$

There are either infinitely many solutions or no solutions at all.

Example:

$$a^2 - 7b^2 = 3.$$

Consider this equation modulo 7: we get $a^2 = 3 \bmod 7$, but 3 is not a quadratic residue mod 7.

For an equation of Pell type, there is **no known algorithm** to distinguish between the two cases, no solution or infinitely many solutions.

There are only several *ad hoc* methods for particular cases, like in the example modulo 7 above. Sometimes there are known upper bounds for the smallest solution; there also exists a criterion for $k = -1$.

Remark: The set $\{(a, b) \in \mathbb{R}^2 \mid a, b \geq 0, a^2 - d \cdot b^2 = k\}$ is a half of a hyperbola on the plane of the coordinates (a, b). Therefore, all the solutions, if they exist, may be ordered from left to right. The smallest one not equal to $(1, 0)$ is called *fundamental solution*.

Example: $a^2 - 991b^2 = 1$ (i. e., $d = 991$)
The fundamental solution is

$$a = 379\,516\,400\,906\,811\,930\,638\,014\,896\,080$$

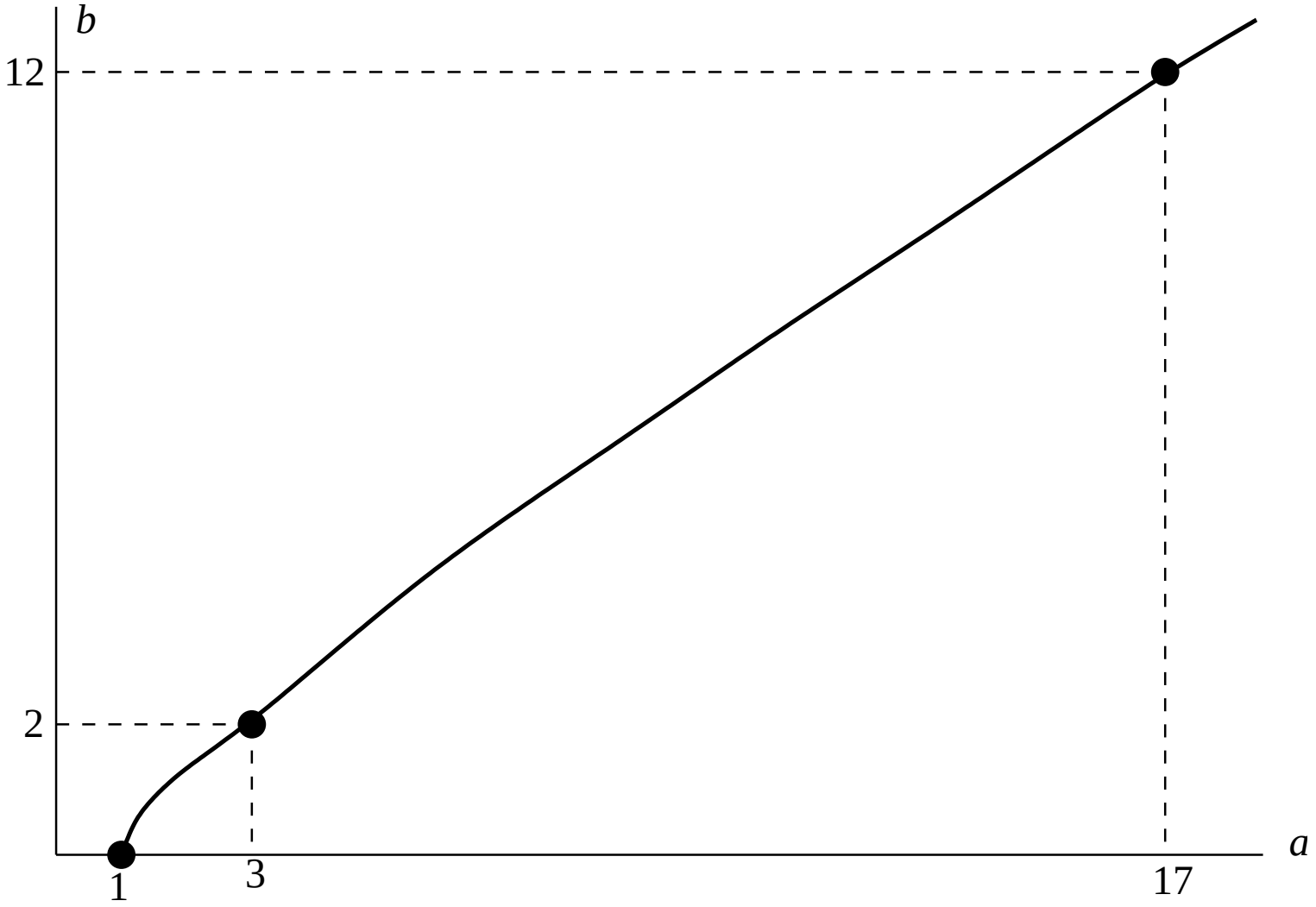
$$b = 12\,055\,735\,790\,331\,359\,447\,442\,538\,767$$

Example: $d = 410\,286\,423\,278\,424$
The fundamental solution contains 206 545 decimal digits.

An algorithm for their search involves the continued fraction for the $\sqrt{d}$.

In our case, $d = 2$ and the fundamental solution is $(3, 2)$:

$$3^2 - 2 \cdot 2^2 = 1.$$


b
12
2
1
3
17
a

The equation $a^2 - 2b^2 = 1$ has infinitely many solutions. The entire set of them is obtained as follows: take $(a_0, b_0) = (1, 0)$; then

$$\begin{pmatrix} a_n \\ b_n \end{pmatrix} = \begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix}^n \cdot \begin{pmatrix} a_0 \\ b_0 \end{pmatrix}, \qquad n = 0, 1, 2, \ldots$$

It turns out that for every other solution the parameter a is a multiple of 3: we may just consider the same recurrence mod 3:

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

Recall that $a^2 = 6m - 3$, so that $m = \dfrac{a^2 + 3}{6}$ where m is the degree of the three black vertices.

First values of the parameter m are

$$1\,634,\ 1\,884\,962,\ 2\,175\,243\,842,\ \ldots$$

Growth exponent: $(3 + 2\sqrt{2})^4 = 1153.999\ldots \approx 1154$.

I have a sample of other examples. . .

Intermediate conclusion (a good news to which I made an allusion at the beginning of the talk):

> The theory of Diophantine equations is a classical and beautiful mathematical subject. It is exciting to find out that dessins d'enfants are related to this theory.

Further questions

Is it possible to model **any** equation of Pell type by dessins d'enfants?

If yes, construct a series of orbits of degree 2 which **never** split into separate orbits.

A much more ambitious program...

In 1970, Yuri Matiyasevich solved the 10^{th} Hilbert's problem. Namely, he proved that there does not exist an algorithm which, for any given Diophantine equation, would say if this equation has a solution.

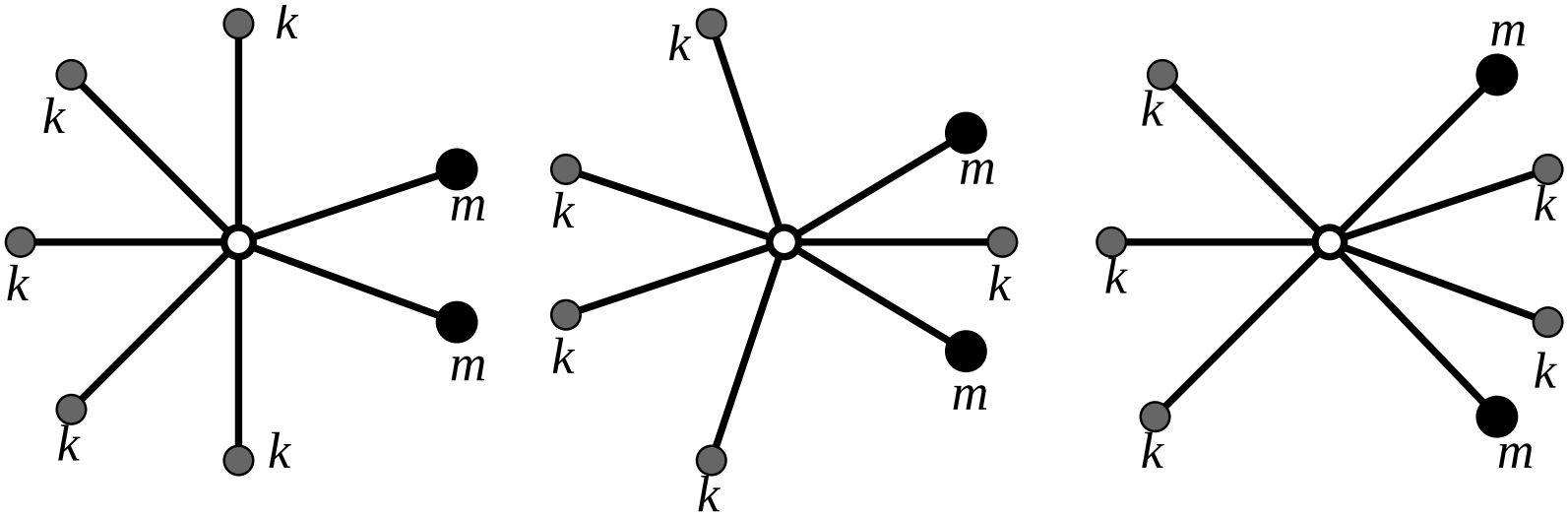
One of the proofs of this fact, due to Grigory Chudnovsky, reduces the problem to a solution of a **system** of Pell equations. How to model a **system** of Pell equations?

If we succeed then we will prove that certain aspects of the theory of dessins d'enfants are algorithmically undecidable.

Thank you!

A more advanced example: **rational points on an elliptic curve.** There are huge computations which I mainly omit, presenting only the final results.

Passport: $\pi = (m^2k^5, 7^1 1^{2m+5k-7}, 2m+5k)$



Field of definition: a totally real field which is the splitting field of the polynomial

$$15k^3a^3 - 45k^2(m+3k)a^2 + 15k(m+3k)(m+4k)a - (m+3k)(m+4k)(m+5k).$$

Question: Can this polynomial have a rational root?

$$15k^3a^3 - 45k^2(m+3k)a^2 + 15k(m+3k)(m+4k)a - (m+3k)(m+4k)(m+5k).$$

We notice that the expression is homogeneous in m and k, of degree 3. It is reasonable to divide it by k^3 and introduce a new variable $b = m/k$:

$$15a^3 - 45a^2(b+3) + 15a(b+3)(b+4) - (b+3)(b+4)(b+5).$$

This is a plane cubic and therefore an elliptic curve (which is a complex torus). After somewhat tedious computations it takes the following form:

$$\boxed{y^2 = x^3 - 2475x - 5850}$$

$$\boxed{y^2 = x^3 - 2475x - 5850}$$

We are interested in the parameter $b = m/k$ since it is related to the vertex degrees. Its expression as a function of x and y is as follows:

$$b = 30 \cdot \frac{111x^2 - 6090x - 29385 - 3xy + y}{x^3 - 1305x^2 + 63675x + 299925}.$$

We also need

$$b > 0 \quad \text{and} \quad b \neq 1.$$

(There are no rational solutions for a when $b = 1$; thus, the condition $b \neq 1$ is automatically satisfied.)

Thank you!