Galois Orbits of Plane Trees: A Case Study

A. Zvonkin

March 13, 1996

1 A cubic family

We consider the family of trees

- of diameter 4;
- with the central vertex of valency 7;
- with the 7 vertices around the center having the valencies m, m and n, n, n, n, n, with m and n being *different* positive integers;
- and with all other vertices being leaves (i.e. of valency 1).

The number of edges is thus equal to $N = 2m + 5n$. See Example 5.3 in [2].

There are 3 plane trees with this set of valencies, therefore in general we must get a cubic field of definition. Indeed, we look for a Shabat polynomial of the form

$$P(z) = p_1(z)^m p_2(z)^n,$$

where

$$p_1(z) = z^2 - z + a$$

and

$$p_2(z) = z^5 + b_4 z^4 + b_3 z^3 + b_2 z^2 + b_1 z + b_0.$$

We compute the derivative $P'(z)$, which is equal to

$$P'(z) = p_(z)^{m-1} p_2(z)^{n-1} Q(z),$$

where $Q(z)$ is a polynomial of degree 6,

$$Q(z) = (2m + 5n)z^6 + \dots .$$

Equating

$$Q(z) = (2m + 5n)z^6,$$

that is, making all the coeffitients of Q but first equal to zero, we get a system of 6 equations on 6 unknowns $a, b_4, \dots, b_0$. Eliminating step by step all the b_i, we finally get a cubic equation on a:

$$15n^3a^3 - 45n^2(m + 3n)a^2 + 15n(m + 3n)(m + 4n)a - (m + 3n)(m + 4n)(m + 5n) = 0. \qquad (1)$$

(The equation given in Example 5.3 [2] is written for the parameter $2a$ instead of a.)

The roots of the last equation *usually* generate a cubic number field. But *sometimes* the equation might have one or even three rational roots; then the corresponding family of trees splits into two or three Galois orbits. This is exactly the situation we want to study.

Problem: Find numbers m and n such that equation (1) would have a rational root.

2 Reduction of the problem

First of all, we may note that the polynomial (1) is homogenious in m and n. Hence one may divide it by n^3 and introduce a new variable

$$b = \frac{m}{n},$$

thus having

$$f(a, b) = 15a^3 - 45a^2(b + 3) + 15a(b + 3)(b + 4) - (b + 3)(b + 4)(b + 5) = 0. \qquad (2)$$

We may reformulate our problem as follows:

Problem (reformulation): Find all the *rational* points (a, b) on the cubic $f(a, b) = 0$, satisfying two additional conditions: (1) $b \neq 1$, and (2) $b > 0$.

The first condition is very easy to satisfy: the substitution of $b = 1$ reduces the equation to $a^3 - 12a^2 + 20a - 8 = 0$, which does not have any rational roots. The second condition is rather nasty and causes some trouble.

Anyway, we are in front of a problem of finding the rational points on a plane cubic. We may mention two basic facts:

(A) Any plane cubic reduces to an elliptic curve (see, for example, [1] or any other source).

(B) The problem of finding the rational points on an elliptic curve is more than classic (see, for example, [3]), but it is also notoriously difficult, and many questions remain open.

An algorithm of reducing a cubic to one of the standard forms is described in [1], Section 7.4.2. To start with, it needs at least one rational point on the cubic. One may use one of the following:

$$(a, b) = (0, -3),\ (0, -4),\ (0, -5),\ (1, 0); \tag{3}$$

in our computations we have used the point $(1, 0)$.

Then, after a series of rather tedious transformations involving cumbersome fractions we finally get a surprisingly simple elliptic curve equivalent to (2):

$$y^2 = x^3 - 2475x - 5850. \tag{4}$$

Some additional information concerning this curve may be useful. First, the coefficients are $2475 = 3^2 \cdot 5^2 \cdot 11$ and $5850 = 2 \cdot 3^2 \cdot 5^2 \cdot 13$. The polynomial

$$P(x) = x^3 - 2475x - 5850$$

does not have rational roots. It has three real roots:

$$x_1 = -48.52254620, \quad x_2 = -2.36900822, \quad x_3 = 50.89155442.$$

The discriminant of P is equal to

$$D = 59719680000 = 2^{17} \cdot 3^6 \cdot 5^4. \tag{5}$$

The J-invariant of the curve is equal to

$$J = \frac{898425}{512} = \frac{3^3 \cdot 5^2 \cdot 11^3}{2^9}.$$

Now starts the hunting for rational points.

3 Rational points

In looking for rational points we have used three methods:

- the Nagell–Lutz algorithm for enumerating the torsion points (see [1], Theorem 7.5.4);
- transformation of the points (3) to new coordinates (and also taking their multiples);
- a trial and error method.

The results are summed up below.

3.1 Torsion points

The polynomial $P(x)$ not having rational roots, there are no rational points of order 2.

Recall the Nagell–Lutz theorem mentioned above: all rational points of finite order $k > 2$ have integral coordinates x and y, and y^2 divides the discriminant D, given by (5). This gives a finite number of possibilities to check, and we come out with two points of order 3, namely,

$$Q = (75, 480) \quad \text{and} \quad -Q = (75, -480).$$

The torsion group is isomorphic to $\mathbf{Z}/3\mathbf{Z}$.

3.2 Rank

The point

$$P = (-21, 192)$$

is not of a finite order, as, for example, the point $3P$ has fractional coordinates. Thus, the rank of the curve is positive, and the curve contains infinitely many rational points.

All the other rational points found up to now turn out to be of the form $pP + qQ$, with $p \in \mathbf{Z}$, $q \in \mathbf{Z}/3\mathbf{Z}$. It seems reasonable to believe that the rank of the curve is 1, and the generator of the non-torsion part is P.

(We remind the reader that there are no systematic procedures known to determine the rank of an elliptic curve, though in particular cases the results may be found by means of various clever tricks; see [3].)

4 Positivity of b

To each point (x, y) on the curve (4) there corresponds a unique point (a, b) on the curve (2). The parameter a does not interest us very much. As to b, it may be found by the following formula:

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

An elementary, though rather tedious analysis of this expression produces the domains of its positivity on the real plane (x, y); they are shaded in Figure 1.

There are three segments of the real part of the curve (4) that lie inside the positive regions. Let c_1, c_2, c_3 be the roots of the polynomial

$$Q(x) = x^3 - 1305x^2 + 63675x + 299925,$$

their numerical values being

$$c_1 = -4.32551841, \quad c_2 = 55.29240881, \quad c_3 = 1254.033109.$$

Let d_1, d_2 be the roots of the polynomial

$$q(x) = 9x^2 - 582x - 2879,$$

i.e.,

$$d_{1,2} = \frac{97 \pm 64\sqrt{3}}{3},$$

their numerical values being

$$d_1 = -4.61708390, \quad d_2 = 69.28375056.$$

Then the segments of the curve (4) which produce positive values of b are the following:

$$d_1 < x < c_1, \quad y < 0; \tag{6}$$

$$c_2 < x < d_2, \quad y > 0; \tag{7}$$

$$x > c_3, \quad y < 0. \tag{8}$$

Anyway, the rank of the curve being positive, rational points are dense in its real part, and hence infintely many examples may be found, in which the "combinatorially cubic" family of trees splits into one or even three Galois orbits without any "visible" reason.

5 Computations

The "smallest" example found is the point

$$-4P + Q = \left(\frac{8155}{121}, \frac{486280}{1331}\right).$$

Here $\frac{8155}{121} = 67.39669421$, thus the point itself belongs to segment (7). The corresponding value of b is $\frac{33}{124}$, therefore the vertex degrees are $m = 33$ and $n = 124$.

The next point is

$$4P = (12219, -1350672),$$

which obviously belongs to segment (8). It gives us

$$b = \frac{2008145}{1653242}.$$

Thus, the vertex degrees of the trees in question are

$$m = 2008145, \quad n = 1653242.$$

We have verified that equation (1) indeed has a rational root.

It is interesting to mention that the number of edges is

$$N = 2m + 5n = 12282500 = 2^2 \cdot 5^4 \cdot 17^3,$$

while

$$m = 5 \cdot 401629, \quad \text{and} \quad n = 2 \cdot 826621.$$

In the same manner, we computed all the points $pP + qQ$, $|p| \leq 25$, $q = 0, 1, 2$, i.e., the total of over 150 rational points on the curve. Among them, 11 points belong to one of the regions (6), (7) or (8). (In fact, segment (6) is so small that we did not find points belonging to it even for greater values of p.) Here is the list of resulting vertex degrees m and n and numbers of edges N:

$p = -4$, $q = 1$: segment (7)
$m = 33$
$n = 124$
$N = 686 = 2 \cdot 7^3$

$p = 4$, $q = 0$: segment (8)
$m = 2008145$
$n = 1653242$
$N = 12282500 = 2^2 \cdot 5^4 \cdot 17^3$

$p = -8$, $q = 1$: segment (7)
$m = 1317156026567$
$n = 649800344821$
$N = 5883313777239 = 3 \cdot 12517^3$

$p = 8$, $q = 0$: segment (8)
$m = 487834953714776556005$
$n = 104793834699948131134$
$N = 1499639080929293767680 = 2^{10} \cdot 3^7 \cdot 5 \cdot 7^3 \cdot 7309^3$

$p = -12$, $q = 1$: segment (7)
$m = 19992975580199268981768219085 16$
$n = 208841813498019535906845150263$
$N = 5042804183529951475887869568347 = 5483^3 \cdot 3127561^3$

$p = 12$, $q = 0$: segment (8)
$m = 437850945102575176061421040201 1206419586020$
$n = 67325256969855198242822530593450569436743$
$N = 5 \cdot 2557^3 \cdot 135601^3 \cdot 352043^3$

$p = 14$, $q = 0$: segment (7)
$m = 736968638710363146558449063198029837892542443037937548205$
$n = 421052670229760905387145078331669085402155581277988045 93$
$N = 3^4 \cdot 5^4 \cdot 17^3 \cdot 73^3 \cdot 191^3 \cdot 6163^3 \cdot 220175107^3$

$p = -18$, $q = 1$: segment (8)
$m = 3023891033812208125766826808891800838271747754929805457892116714643880474 1$
$n = 4516545280972262137491008912167324424939495969666716640564907223707253558$
$N = 2^3 \cdot 41^3 \cdot 2503^3 \cdot 212580566684382812 53^3$

$p = 18$, $q = 0$: segment (7)
$N = 5 \cdot 16787^3 \cdot 927497^3 \cdot 49047517^3 \cdot 2893480568837^3$

$p = -22$, $q = 1$: segment (8)
$N = 2 \cdot 7^6 \cdot 256942247^3 \cdot 167323173560473489509266865 1^3$

$p = 22$, $q = 0$: segment (7)
$N = 2^2 \cdot 5 \cdot 25844161968412127441324475850568111544007667 9^3$.

In the last three examples we do not give the values of m and n anymore, because they do not fit into the A4 page format even with the smallest font.

It is interesting to note that the number of edges N is, up to a small factor, a cube. Such a prime as

$$258441619684121274413244758505681115440076679$$

may well show up "by chance". But to find it by chance *three times* is highly unprobable.

References

[1] **Cohen H.** A Course in Computational Algebraic Number Theory. – Springer-Verlag (Graduate Texts in Mathematics, vol. 138), 1993, XXII+534 pp.

[2] **Shabat G. B., Zvonkin A. K.** Plane trees and algebraic numbers. – In "Jerusalem Combinatorics '93" (H. Barcelo, G. Kalai eds.), AMS, Contemporary Mathematics series, vol. **178**, 1994, 233–275.

[3] **Silverman J. H., Tate J.** Rational Points on Elliptic Curves. – Springer, 1992, X+281 pp. ("Undergraduate Texts in Mathematics")