An elementary approach to Hessian curves with torsion group $\mathbb{Z}/6\mathbb{Z}$

Lorenz Halbeisen[1], Norbert Hungerbühler[2]

[1]Department of Mathematics, ETH Zentrum, Rämistrasse 101
8092 Zürich, SWITZERLAND
lorenz.halbeisen@math.ethz.ch

[2] Department of Mathematics, ETH Zentrum, Rämistrasse 101
8092 Zürich, SWITZERLAND
norbert.hungerbuehler@math.ethz.ch

key-words: Hessian curves, diophantine equations, elliptic curves

2010 Mathematics Subject Classification: **14H52** 11D25 10B15 14E05

Abstract

We investigate the geometry of Hessian curves $H_c : x^3+y^3+z^3+cxyz=0$. In particular, we present an elementary characterisation of Hessian curves with torsion group $\mathbb{Z}/\mathbf{6}\mathbb{Z}$. As an application we show, for example, that a result of Mordell's implies that the equation $7m^4-26m^2e^2-49e^4-n^2=0$ does not have a solution in positive integers.

1 Introduction

One can show that every non-singular, irreducible cubic curve C in the real projective plane has a point of inflection $\mathscr{O}$ (see Bix [1, Theorem 12.7]), and with respect to $\mathscr{O}$, one can define a commutative, binary, associative operation "+" on the points of C, where $\mathscr{O}$ is the neutral element. In fact, if P and Q are two points of C, then let $P\#Q$ be the third intersection point of the line through P and Q with the curve C. If $P=Q$, the line trough P and Q is replaced by the tangent in P. Then $P+Q$ is defined by stipulating

$$P+Q \ := \ \mathscr{O}\#(P\#Q).$$

In particular, $-P := \mathscr{O}\#P$. With this definition, $(C,+)$ is an abelian group with neutral element $\mathscr{O}$. Let $C(\mathbb{Q})$ be the set of rational points on C. Then one can show that $\big(C(\mathbb{Q}),+\big).$ is a subgroup of $(C,+)$. Now, Mordell's Theorem states that the group $\big(C(\mathbb{Q}),+\big)$ is finitely generated. For the proof of Mordell's Theorem, one usually works with the Weierstrass normal form

$$y^2 = x^3+ax^2+bx \tag{1}$$

or

$$y^2 = x^3 + bx + c. \tag{2}$$

For group calculations in the Weierstrass normal form, the inflection point $\mathscr{O} = (0, 1, 0)$ at infinity is used. For example, the Weierstrass normal form (1) is used in Silverman and Tate [11, Section 3.5], and form (2) is used by Mordell in [8, Chapter 16]. The two Weierstrass normal forms (1) and (2) are very well investigated. However, there are also other normal forms of cubic curves, for example the Hesse normal form

$$x^3 + y^3 + 1 + cxy = 0 \quad \text{for some } c \in \mathbb{R},$$

which reads in homogeneous coordinates as

$$X^3 + Y^3 + Z^3 + cXYZ = 0.$$

These so-called Hessian curves play a key-role in the proof that every non-singular, irreducible cubic curve in the real projective plane has a point of inflection (see Bix [1, Theorem 12.7]), and Hessian curves are also used in cryptography (see Doche and Lange [2]). For integral points on Hessian curves $X^3 + Y^3 + Z^3 = nXYZ$ see for example Dofs [3].

Below we will translate some results known for cubic curves in Weierstrass normal form (1) to curves in Hesse normal form. For this, we first summarise some facts about curves in Weierstrass normal form, and then we transform these curves into Hessian curves. Then, we give a characterisation of Hessian curves with torsion group $\mathbb{Z}/6\mathbb{Z}$. As a byproduct we give a complete list of rational or integral solutions of following equations:

- $1 + 8x^3 = y^2$
- $1 + 2x + x^2 + x^3 + 2x^4 + x^5 = y^2$
- $x^2y^2 + x^3 + y^3 - 9xy + 54 = 0$
- $x^4 + 13x^2e^2 + 128y^4 = z^2$
- $2x^4 + 13x^2y^2 + 64y^4 = z^2$
- $x^4 - 26x^2y^2 - 343y^4 = z^2$
- $7x^4 - 26x^2y^2 - 49y^4 = z^2$

2 Some facts about Weierstrassian curves

We say that a cubic curve $W_{a,b}$ (with parameters $a, b \in \mathbb{R}$) in the real plane $\mathbb{R}^2$ is a **Weierstrassian curve** if

$$W_{a,b}: \; y^2 = x^3 + ax^2 + bx \quad \text{for some } a, b \in \mathbb{R},$$

i.e., if $W_{a,b}$ is in Weierstrass normal form. Furthermore, we say that two Weierstrassian curves $W_{a,b}$ and $W_{a',b'}$ are **equivalent**, denoted $W_{a,b} \sim W_{a',b'}$, if there exists a non-zero real α, such that $a' = \alpha^2 a$ and $b' = \alpha^4 b$. Since $\alpha \neq 0$, the relation "$\sim$" is obviously an equivalence relation. For example, all Weierstrassian curves of the form $y^2 = x^3 - n^2 x$, where n is a non-zero integer, belong to the same equivalence class (*i.e.*, are pairwise equivalent). Notice that if $W_{a,b} \sim W_{a',b'}$ and $(x, y) \in \mathbb{R}^2$ is a point on $W_{a,b}$, then $(\alpha^2 x, \alpha^3 y)$ is a point on $W_{a',b'}$; and vice versa, if $(x', y') \in \mathbb{R}^2$ is a point on $W_{a',b'}$, then $(\alpha^{-2} x', \alpha^{-3} y')$ is a point on $W_{a,b}$. So, the transformation $(x, y) \mapsto (\alpha^2 x, \alpha^3 y)$ maps $W_{a,b}$ to $W_{a',b'}$ and is a homomorphism of the groups on $W_{a,b}$ and $W_{a',b'}$. In particular, if $\alpha \in \mathbb{Q}$, then each rational point on $W_{a,b}$ corresponds to a rational point on $W_{a',b'}$, and vice versa. Finally, we say that a Weierstrassian curve $W_{a,b}$ is **normalised** if at least one of its inflection points has x-coordinate equal to 1.

Before we show that every Weierstrassian curve $W_{a,b}$ with an inflection point in $\mathbb{R}^2$ is equivalent to a normalised Weierstrassian curve, we recall the following

FACT 2.1. *The x-coordinate of an inflection point in $\mathbb{R}^2$ of a Weierstrassian curve $W_{a,b}$ is always a positive root of the polynomial*

$$3x^4 + 4ax^3 + 6bx^2 - b^2 .$$

Proof. Let $P = (\tilde{x}, \tilde{y}) \in \mathbb{R}^2$ be an inflection point of the Weierstrassian curve $W_{a,b}$. First we show that $\tilde{x}$ is a root of $3x^4 + 4ax^3 + 6bx^2 - b^2$. We have the following equations:

$$\begin{aligned} y^2 &= x^3 + ax^2 + bx \\ (y^2)' = 2yy' &= 3x^2 + 2ax + b \\ (y^2)'' = 2y'^2 + 2yy'' &= 6x + 2a \end{aligned}$$

Since y'' at P is zero, we obtain $2y'^2 = 6x + 2a$. Furthermore, we have

$$(2yy')^2 = 2 \cdot (2y'^2) \cdot y^2,$$

which gives us

$$(3x^2 + 2ax + b)^2 = 2(6x + 2a)(x^3 + ax^2 + bx)\,,$$

and therefore we obtain

$$3x^4 + 4ax^3 + 6bx^2 - b^2 = 0\,.$$

Now, we show that $\tilde{x} > 0$. Let $p(x) := x(x^2 + ax + b)$ and notice that $y^2 = p(x)$. In the case when $a^2 \geq 4b$, the roots of $p(x)$ are $x_0 = 0$ and

$$x_\pm = \tfrac{1}{2}\big(-a \pm \sqrt{a^2 - 4b}\big)\,.$$

In the case when $a^2 < 4b$, the only root of $p(x)$ is $x_0 = 0$. In the latter case, $p(x) \geq 0$ implies $x \geq 0$, and therefore, all points in $\mathbb{R}^2$ on the Weierstrassian curve $W_{a,b}$, in particular points of inflection, have a non-negative x-coordinate. In the former case, notice that $x_- \leq x_+$. We consider the following sub-cases.

(a) $0 \leq x_-$. The curve $y^2 = p(x)$ is defined just on the intervals $[x_0, x_-]$ and $[x_+, \infty)$. In particular, points of inflection have a non-negative x-coordinate.

(b) $x_- < 0$. We know that the x-coordinate of the inflection point P is a root of

$$s(x) := 3x^4 + 4ax^3 + 6bx^2 - b^2\,.$$

Notice that

- $s(x)' = 12p(x)$,
- $s(0) = -b^2 \leq 0$, and
- $s(x_+) = -\frac{1}{2}\big(\underbrace{a^2 - a\sqrt{a^2 - 4b} - 2b}_{=:\,r(a,b)}\big)\big(\underbrace{a^2 - 4b}_{\geq 0}\big)$,

Furthermore, $r(a,b) \geq 0$ and $r(a,b) = 0$ if and only if $b = 0$ and $a \geq 0$. To see this, notice first that $r(a,b) = 0$ implies $4b^2 = 0$, and therefore $b = 0$. Now, for $b = 0$, $r(a,b) = 0$ implies $a^2 = a\sqrt{a^2}$, and therefore $a \geq 0$. Finally,

$$0 \leq \big(a - \sqrt{a^2 - 4b}\big)^2 = 2 \cdot r(a,b)\,.$$

We consider the following cases:

(i) $x_- < 0 \leq x_+$. Since $p(x) \leq 0$ for every $x \in (-\infty, x_-]$, we have $p(x), s(x)' \geq 0$ for all $x \in [x_-, 0]$. So, $s(x)$ is increasing on the interval $[x_-, 0]$, and since $s(0) = -b^2 \leq 0$, s has no root in the interval $[x_-, 0)$. Hence, the Weierstrassian curve $W_{a,b}$ (*i.e.*, $y^2 = p(x)$) has no point of inflection with negative x-coordinate.

(ii) $x_- < x_+ < 0$. This implies that for all $x \in [x_-, x_+]$, $p(x), s(x)' \geq 0$. Furthermore, since $x_+ < 0$, we get $a^2 - 4b < a^2$ which implies $b > 0$, and therefore $r(a,b) > 0$. Furthermore, since $x_- < x_+$, we have $a^2 - 4b > 0$. Thus, since

$s(x_+) = -\frac{1}{2} \cdot r(a,b) \cdot (a^2 - 4b) < 0$ and s is increasing on $[x_-, x_+]$, s has no root in the interval $[x_-, x_+]$. Hence, the Weierstrassian curve $W_{a,b}$ (*i.e.*, $y^2 = p(x)$) has no point of inflection with negative x-coordinate.

(*iii*) $x_- = x_+ < 0$. This implies $a^2 = 4b$, and since $x_+ < 0$, we have $a > 0$. Now, for all $x < 0$ we have $p(x) \leq 0$, where $p(x) = 0$ implies $x = x_+$. Thus, $(x_+, 0)$ is a singular point on the Weierstrassian curve $W_{a,b}$ and no point with negative x-coordinate can be a point of inflection of $W_{a,b}$, which completes the proof.

q.e.d.

Now, we are ready to prove the following

FACT 2.2. *For each Weierstrassian curve with an inflection point in* $\mathbb{R}^2$ *there exists a unique normalised Weierstrassian curve which is equivalent to the given curve.*

Proof. Let $W_{a,b}$ be a Weierstrassian curve with an inflection point $(x_0, y_0) \in \mathbb{R}^2$. By FACT 2.1, $x_0 > 0$, and we can choose $\alpha := \frac{1}{\sqrt{x_0}}$. Then the point $(\alpha^2 x_0, \alpha^3 y_0) = (1, \alpha^3 y_0)$ is an inflection point of $W_{a',b'}$ where $a' := \alpha^2 a$ and $b' := \alpha^4 b$. Obviously, $W_{a',b'}$ is normalised, the curves $W_{a,b}$ and $W_{a',b'}$ are equivalent, and no other normalised curve is equivalent to $W_{a,b}$.

q.e.d.

The following result characterizes normalised curves.

FACT 2.3. *A Weierstrassian curve* $W_{a,b}$ *is normalised if and only if*

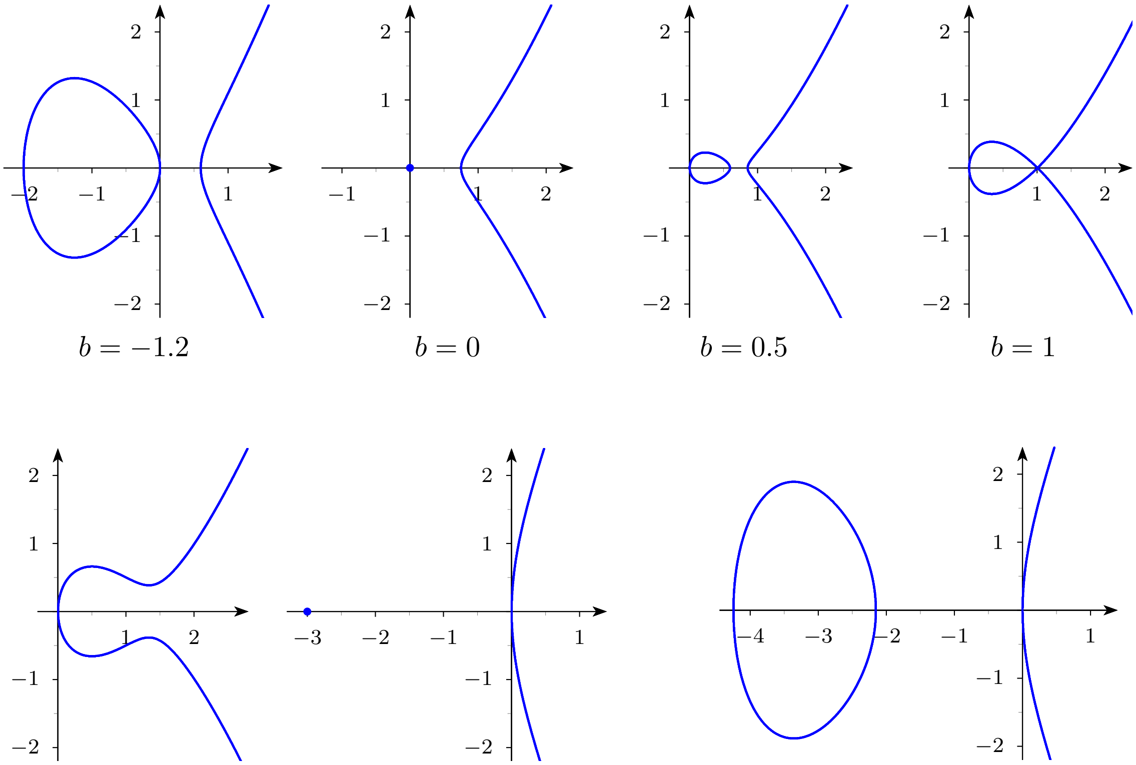
$$b \neq 1 \quad \textit{and} \quad a = \frac{b^2 - 6b - 3}{4}.$$

Proof. If $x = 1$ is a root of $3x^4 + 4ax^3 + 6bx^2 - b^2$, then

$$3 + 4a + 6b - b^2 = 0,$$

which implies that $a = \frac{b^2-6b-3}{4}$. On the other hand, if $a = \frac{b^2-6b-3}{4}$, then $3 + 4a + 6b - b^2 = 0$ and $x = 1$ is a root of $3x^4 + 4ax^3 + 6bx^2 - b^2$. Now, if $b = 1$, then $a = -2$ and $x^3 - 2x^2 + x = x(x-1)^2$, which shows that $W_{-2,1}$ has a singularity at $x = 1$, and it is easy to check directly that $W_{-2,1}$ does not have an inflection point in $\mathbb{R}^2$. *q.e.d.*

By FACT 2.3 we obtain that a normalised Weierstrassian curve is determined by the value of b. So, we shall denote normalised Weierstrassian curves by W_b instead of $W_{a,b}$. The following figures show a few normalised Weierstrassian curves together with the curve for $b = 1$:



$b = -1.2$ $b = 0$ $b = 0.5$ $b = 1$

$b = 2$ $b = 9$ $b = 9.13$

It is straightforward to compute the y-coordinate of an inflection point of a normalised Weierstrassian curve.

FACT 2.4. *If W_b is a normalised Weierstrassian curve (in particular, $b \neq 1$), then the inflection points in $\mathbb{R}^2$ of W_b are*

$$\Big(1, \pm\frac{b-1}{2}\Big).$$

Proof. Let W_b be a normalised Weierstrassian curve with $b \neq 1$ and let $(1, w)$ be an inflection point of W_b. Then, since $(1, w)$ is a point on W_b, $w = \pm\sqrt{a+b+1}$. Now, by FACT 2.3, $a = \frac{b^2-6b-3}{4}$, and therefore

$$w = \pm\sqrt{\frac{b^2-6b-3+4b+4}{4}} = \frac{\pm\sqrt{b^2-2b+1}}{2} = \pm\frac{b-1}{2}.$$

q.e.d.

In order to prove MORDELL'S THEOREM for elliptic curves one defines for every Weierstrassian curve $W_{a,b}$ a **dual curve** $W_{a',b'}$ by stipulating $a' := -2a$ and $b' := a^2 - 4b$. Since the dual of a normalised curve is in general no longer normalised, and since we are mainly interested in normalised Weierstrassian curves, we have to modify this dualization in order to get normalised dual curves.

Let W_{a_0,b_0} be a normalised Weierstrassian curve. Then the **normalised dual curve** W_{a_1,b_1} is defined by stipulating

$$b_1 := \frac{b_0 - 9}{b_0 - 1} \quad \text{and} \quad a_1 := \frac{b_1^2 - 6b_1 - 3}{4}.$$

By definition, W_{a_1,b_1} is a normalised Weierstrassian curve. Moreover, we get the following

FACT 2.5. *If W_{a_0,b_0} is a normalised Weierstrassian curve. Then the dual $W_{a_0',b_0'}$ is equivalent to the normalised dual W_{a_1,b_1}.*

Proof. It is enough to find an $\alpha \in \mathbb{R}$ such that $a_1 = \alpha^2 a_0'$ and $b_1 = \alpha^4 b_0'$. First notice that since W_{a_0,b_0} is normalised,

$$a_0 = \frac{b_0^2 - 6b_0 - 3}{4}.$$

Let

$$\alpha := \frac{2}{b_0 - 1}.$$

On the one hand we have

$$\alpha^2 \cdot a_0' = \alpha^2 \cdot (-2a_0) = \frac{4}{(b_0-1)^2} \cdot \frac{-2b_0^2 + 12b_0 + 6}{4} = \frac{-2b_0^2 + 12b_0 + 6}{(b_0-1)^2},$$

and on the other hand we have

$$a_1 = \frac{b_1^2 - 6b_1 - 3}{4} = \frac{(b_0-9)^2 - 6(b_0-9)(b_0-1) - 3(b_0-1)^2}{4(b_0-1)^2} = \frac{-2b_0^2 + 12b_0 + 6}{(b_0-1)^2},$$

which shows that $a_1 = \alpha^2 a_0'$.

Similarly, we have

$$\alpha^4 \cdot b_0' = \alpha^4 \cdot (a_0^2 - 4b_0) = \frac{16}{(b_0-1)^4} \cdot \Big(\frac{(b_0^2 - 6b_0 - 3)^2}{16} - 4b_0 \Big) =$$

$$\frac{(b_0^2 - 6b_0 - 3)^2 - 64b_0}{(b_0-1)^4} = \frac{b_0^4 - 12b_0^3 + 30b_0^2 - 28b_0 + 9}{(b_0-1)^4} =$$

$$\frac{(b_0-1)^3 \cdot (b_0 - 9)}{(b_0-1)^4} = \frac{b_0 - 9}{b_0 - 1} = b_1.$$

q.e.d.

It is easy to verify that the bidual curve $W_{a'',b''}$ of a Weierstrassian curve $W_{a,b}$ is equivalent to $W_{a,b}$. With respect to the normalised dual we get slightly more.

FACT 2.6. *If W_{b_0} is a normalised Weierstrassian curve and W_{b_2} is the normalised bidual of W_{b_0}, then $b_2 = b_0$.*

Proof. We have that

$$b_2 = \frac{b_1 - 9}{b_1 - 1} = \frac{\frac{b_0-9}{b_0-1} - 9}{\frac{b_0-9}{b_0-1} - 1} = \frac{\frac{b_0-9-9b_0+9}{b_0-1}}{\frac{b_0-9-b_0+1}{b_0-1}} = \frac{-8b_0}{-8} = b_0,$$

which completes the proof. *q.e.d.*

As a further fact, we would like to mention that for every Weierstrassian curve $W_{a,b}$, there is a homomorphism ϕ from $W_{a,b}$ to its dual $W_{a',b'}$, *i.e.*, $\phi(P+Q) = \phi(P)+'\phi(Q)$, where $+'$ denotes addition on $W_{a'.b'}$. If ϕ' is the corresponding homomorphism from the dual $W_{a',b'}$ of $W_{a,b}$ to its bidual (which is equivalent to $W_{a,b}$, but in general not identical with $W_{a,b}$) then $\phi' \circ \phi$ is essentially doubling points. The homomorphism ϕ is given by

$$\phi(x,y) := \left(\frac{y^2}{x^2} \,,\; y \cdot \frac{x^2 - b}{x^2} \right).$$

To get homomorphisms between a normalised Weierstrassian curve and its dual, we have to slightly modify ϕ:

PROPOSITION 2.7. *For $x \neq 0$, let*

$$\phi_i(x,y) := \left(\alpha_i^2 \cdot \frac{y^2}{x^2} \,,\; \alpha_i^3\, y \cdot \frac{x^2 - b_i}{x^2} \right), \quad \textit{where} \quad \alpha_i := \frac{2}{b_i - 1}.$$

If we extend ϕ_i by $\phi_i(0,0) := \mathscr{O}$ and $\phi_i(\mathscr{O}) := (0,0)$, then $\phi_0 : W_{b_0} \to W_{b_1}$ and $\phi_1 : W_{b_1} \to W_{b_0}$ are homomorphisms between the dual normalised Weierstrassian curves W_{b_0} and W_{b_1}. There holds

$$\begin{array}{rccc} \phi_1 \circ \phi_0 : & W_{b_0} & \to & W_{b_0} \\ & P & \mapsto & P \# P. \end{array}$$

Proof. The proof is an easy calculation. *q.e.d.*

We conclude this section with points of order 6 on a normalised Weierstrassian curve W_b. For this, let $T := (0,0)$, which is a point of order 2 on W_b. Now, by FACT 2.4, for $w = \frac{b-1}{2}$, the points $W_\pm := (1, \pm w)$ are inflection points, *i.e.*, $W_\pm$ is a point of order 3. Hence, $S_\pm := T \# W_\pm$ is a point of order 6. It is straightforward to compute the coordinates of $S_\pm$.

FACT 2.8. *The two points*

$$\left(b, \pm \frac{b(b-1)}{2} \right)$$

on the normalised Weierstrassian curve W_b are both points of order 6.

Proof. Let T and $W_\pm$ be as above. Then the line through T and $W_\pm$ is given by $y = \pm w \cdot x$, and the x-coordinates of the intersection points of the line $TW_\pm$ with the curve W_b are the zeros of the polynomial $x^3 + ax^2 + bx - w^2x^2$. Since $a = \frac{b^2-6b-3}{4}$, and $w^2 = \frac{(b-1)^2}{4}$ we get the factorisation

$$x^3 + ax^2 + bx - w^2x^2 = x(x-1)(x-b).$$

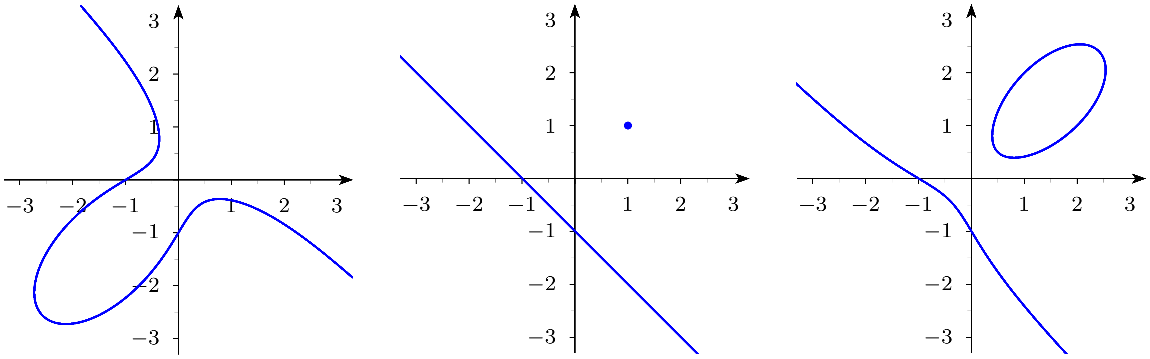
Hence, we obtain $S_\pm = (b, \pm bw)$, as claimed. *q.e.d.*

3 From Weierstrass to Hesse and back

In this section, we transform normalised Weierstrassian curves into **Hessian curves**, which are, in homogeneous coordinates, cubic curves of the form

$$H_c: \ X^3 + Y^3 + Z^3 + cXYZ = 0 \quad \text{for some } c \in \mathbb{R}.$$

Notice that if (X, Y, Z) is a point on H_c, then also $(X, Y, Z), (Y, X, Z), (Z, Y, X), \ldots$ are points on H_c.



$c = 5$ $c = -3$ $c = -5$

We now construct a projective transformation Φ_{WH} which maps a normalised Weierstrassian curve W_b to a Hessian curve H_c. In order to construct this transformation, we first map four points on W_b to four points in the projective plane, and then modify the transformation so that the four points in the projective plane belong to the same Hessian curve.

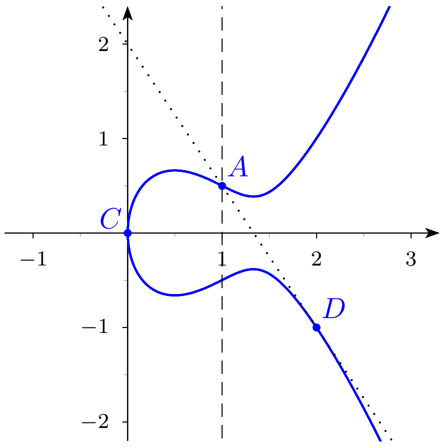
Let W_b be a normalised Weierstrassian curve, *i.e.*, $b \neq 1$ and $a = \frac{b^2-6b-3}{4}$. In the projective plane, W_b has three points of inflection, namely $\mathscr{O} := (0, 1, 0)$ (at infinity) and $(1, \pm w, 1)$, where $w = \frac{b-1}{2}$. Furthermore, W_b has a point of order 2, namely $(0, 0, 1)$, and at least two points of order 6, namely $(b, \pm bw, 1)$. Now, the four points on W_b which we map are

$$A = (1, w, 1), \quad B = (0, 1, 0), \quad C = (0, 0, 1), \quad D = (b, -bw, 1).$$

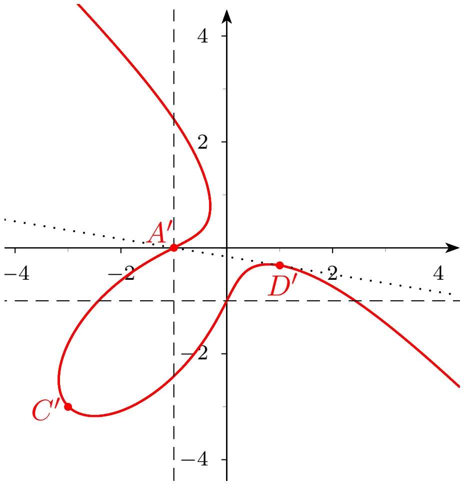
These points are not collinear and can therefore be projectively mapped to the four points

$$A' = (-1,0,1), \quad B' = (-1,1,0), \quad C' = (q,q,1), \quad D' = (1,\tfrac{1}{q},1)$$

for some $q \in \mathbb{R} \setminus \{0, -\frac{1}{2}, 1\}$. Notice that A' and B' are on every Hessian curve, and by Fact 4.4 we know that if C' is a point on some Hessian curve H_c, then so is D'. The projective transformation Φ_{WH} is illustrated by the following figure:



$b = 2$

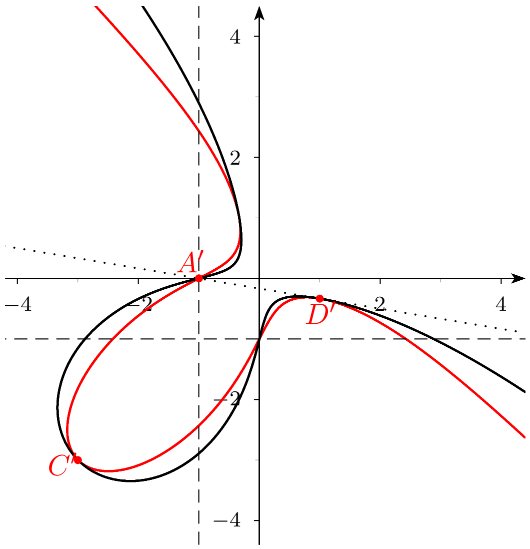


$q = -3$

The projective transformation which maps $A \mapsto A'$, $B \mapsto B'$, $C \mapsto C'$, $D \mapsto D'$, can be given by the matrix

$$\Phi_{\mathrm{WH}} := \begin{pmatrix} \frac{1}{2}\big(b-1+q(b+1)\big) & 1-q & -bq \\ \frac{1}{2}\big(b-1+q(b+1)\big) & -(1-q) & -bq \\ 1+q(b-1) & 0 & -b \end{pmatrix}.$$

Let Γ be the image of W_b under the projective transformation Φ_{WH}. Then Γ goes through the points A', B', C', D'. The following figure shows the curve Γ (black) together with the Hessian curve (red) through the same points:



In order to obtain the equation for Γ, we have to compute Φ_{WH}^{-1}, which corresponds to the matrix

$$\Phi_{\mathrm{HW}} := \begin{pmatrix} b & b & -2bq \\ \frac{1}{2}b(b-1)(1+2q) & -\frac{1}{2}b(b-1)(1+2q) & 0 \\ 1+q(b-1) & 1+q(b-1) & -(b-1)-q(b+1) \end{pmatrix}.$$

Now, a point (X,Y,Z) is on Γ if and only if the point $(x,y,z)^{\top} := \Phi_{\mathrm{HW}} \cdot (X,Y,Z)^{\top}$ is on W_b, or in other words, if x,y,z satisfy the equation

$$y^2z = x^3 + ax^2z + bxz^2$$

where $a = \frac{b^2-6b-3}{4}$. This is equivalent to saying that X,Y,Z satisfy the following equation:

$$\begin{aligned} 0 &= \Big(X^3+Y^3+Z^3\Big) \cdot \Big(-2q+(1-b)q^2+(1-b)q^3\Big) \\ &+ \; XYZ \cdot \Big((3-b)-(3+3b)q+(6-6b)q^2-(6+2b)q^3\Big) \\ &+ \; \Big(X^2Y+Y^2Z+Z^2X+X^2Z+Y^2X+Z^2Y\Big) \cdot \Big(1+(b-3)q+(b+3)q^2+(b-1)q^3\Big) \end{aligned}$$

Thus, Γ is a Hessian curve if and only if

$$1+(b-3)q+(b+3)q^2+(b-1)q^3 = 0,$$

which is satisfied if and only if

$$b = \frac{(q-1)^3}{q+q^2+q^3}.$$

Now, starting with a Hessian curve H_c, we get that $(q, q, 1)$ is on H_c, if and only if

$$1 + cq^2 + 2q^3 = 0,$$

i.e., if and only if

$$c = -\frac{2q^3 + 1}{q^2}.$$

So, the parameter b of the normalised Weierstrassian curve W_b which corresponds to H_c is given by $b = \frac{(q-1)^3}{q+q^2+q^3}$. We summarise the result as follows:

THEOREM 3.1. *For $q \in \mathbb{R} \setminus \{0, -\frac{1}{2}, 1\}$ let $b = \frac{(q-1)^3}{q+q^2+q^3}$ and $c = -\frac{2q^3+1}{q^2}$. Then*

$$\Phi_{bc} : W_b \to H_c, \begin{pmatrix} x \\ y \\ z \end{pmatrix} \mapsto \begin{pmatrix} X \\ Y \\ Z \end{pmatrix} = \begin{pmatrix} \frac{1}{2}\big(b - 1 + q(b+1)\big) & 1 - q & -bq \\ \frac{1}{2}\big(b - 1 + q(b+1)\big) & -(1-q) & -bq \\ 1 + q(b-1) & 0 & -b \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

is an isomorphism between the normalised Weierstrassian curve

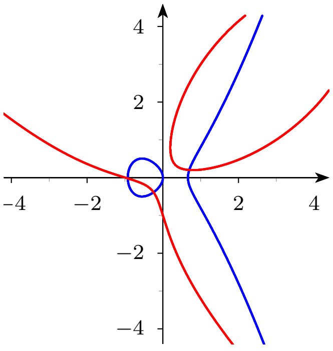
$$W_b : y^2 z = x^3 + ax^2 z + bxz^2 \quad \text{with } a = \frac{b^2 - 6b - 3}{4}$$

and the corresponding Hessian curve

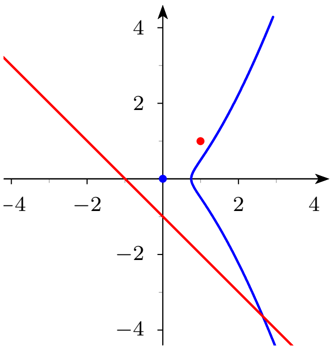
$$H_c : X^3 + Y^3 + Z^3 + cXYZ = 0.$$

In particular, if q is rational, then both b and c are rational.

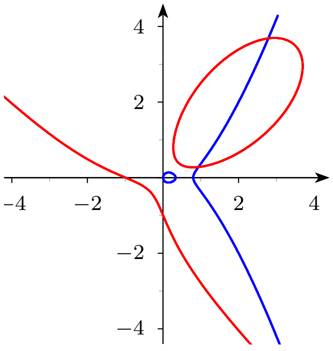
The following figures show some Hessian curves (red) together with the corresponding normalised Weierstrassian curves (blue):



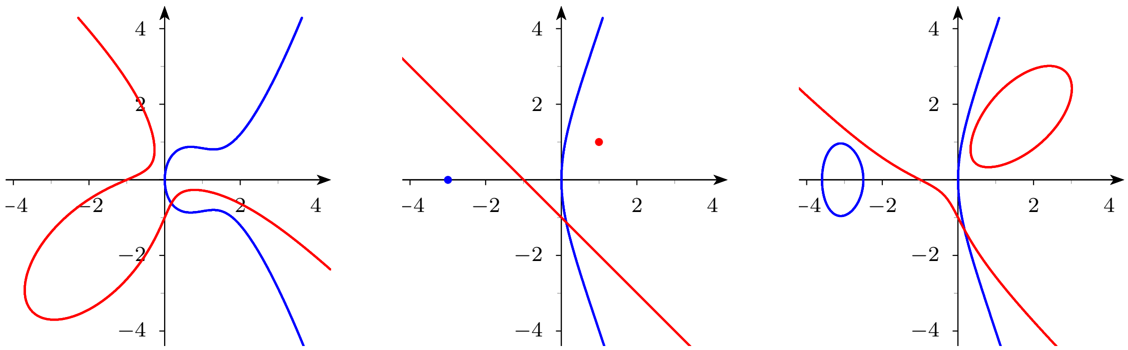
$q = \frac{1}{3} \qquad b = -\frac{8}{13}$



$q = 1 \qquad b = 0$



$q = \frac{7}{2} \qquad b = \frac{125}{469}$



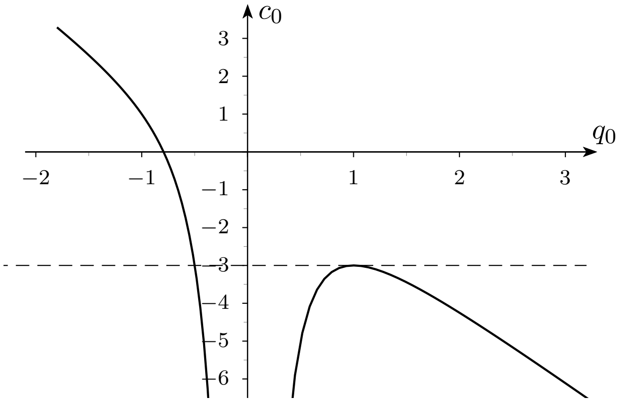
$q = -\frac{7}{2}$ $b = \frac{243}{91}$ $q = -\frac{1}{2}$ $b = 9$ $q = -\frac{7}{18}$ $b = \frac{15625}{1729}$

4 The dual of a Hessian curve

We now want to define the dual of a Hessian curve H_{c_0}. First, observe that the equation $c_0 = -\frac{2q_0^3+1}{q_0^2}$ has

$$\begin{array}{rcl} \text{one solution } q_0 \text{ and } q_0 < 0 & \iff & c_0 > -3, \\ \text{two solutions } q_0, \text{ namely } q_0 = 1 \text{ and } q_0 = -\dfrac{1}{2} & \iff & c_0 = -3, \\ \text{a negative and two positive solutions} & \iff & c_0 < -3. \end{array}$$

The relation between q_0 and c_0 is illustrated by the following figure:



Later, in LEMMA 5.1, we shall see that if $c_0 < -3$ is rational, then at most one of the three possible solutions for q_0 is rational.

Now, we fix one of the possible values q_0 in the cases where we have a choice (*i.e.*, when $c_0 \leq -3$). Then we consider for $b_0 = \frac{(q_0-1)^3}{q_0+q_0^2+q_0^3}$ the normalised Weierstrassian curve W_{b_0}. Let W_{b_1} be the normalised dual of W_{b_0}. Recall that $b_1 = \frac{b_0-9}{b_0-1}$. This value defines a unique q_1 via the equation $b_1 = \frac{(q_1-1)^3}{q_1+q_1^2+q_1^3}$, which in turn yields a Hessian curve H_{c_1} for $c_1 = -\frac{2q_1^3+1}{q_1^2}$. We call H_{c_1} a dual of H_{c_0}. The following lemma relates the values q_0 and q_1.

LEMMA 4.1. *If H_{c_1} is a dual of a Hessian curve H_{c_0} and $c_0 = -\frac{2q_0^3+1}{q_0^2}$, then*

$$q_1 = -\frac{1}{2q_0} \quad \textit{and} \quad c_1 = \frac{1-4q_0^3}{q_0}\,.$$

Proof. We know that $b_0 = \frac{(q_0-1)^3}{q_0+q_0^2+q_0^3}$ and that $b_1 = \frac{b_0-9}{b_0-1}$. Further we infer from the previous section that

$$1 + (b_1-3)q_1 + (b_1+3)q_1^2 + (b_1-1)q_1^3 = 0.$$

The combination of these three equations yields

$$\big(1+2q_0q_1\big)\Big(1-2q_1+4q_1^2+4q_0^2(1+q_1+q_1^2)+2q_0\big(q_1(5+2q_1)-1\big)\Big) = 0\,.$$

This is the case when $1+2q_0q_1 = 0$, or when

$$1-2q_1+4q_1^2+4q_0^2(1+q_1+q_1^2)+2q_0\big(q_1(5+2q_1)-1\big) = 0.$$

If $1+2q_0q_1 = 0$, then

$$q_1 = -\frac{1}{2q_0}.$$

In the other case, we have

$$(1-2q_0+4q_0^2) + (-2+10q_0+4q_0^2)q_1 + (4+4q_0+4q_0^2)q_1^2 = 0,$$

and the discriminant of this quadratic equation for q_1 is $D_{q_0} := -3(1+q_0-2q_0^2)^2 \leq 0$. $D_{q_0} = 0$ if and only if $q_0 = -\frac{1}{2}$ or $q_0 = 0$. So, the only real solutions for q_1 are when $q_0 = -\frac{1}{2}$, which gives us $q_1 = 1$, and when $q_0 = 1$, which gives us $q_1 = -\frac{1}{2}$, and in both cases we get again

$$q_1 = -\frac{1}{2q_0}.$$

Finally, since $c_1 = -\frac{2q_1^3+1}{q_1^2}$, we obtain

$$c_1 = \frac{1-4q_0^3}{q_0}\,.$$

q.e.d.

Now, for $q_0 \in \mathbb{R} \setminus \{0, -\frac{1}{2}, 1\}$ and $q_1 = -\frac{1}{2q_0}$ let

$$b_i = \frac{(q_i-1)^3}{q_i+q_i^2+q_i^3}, \qquad a_i = \frac{b_i^2-6b_i-3}{4}, \qquad c_i = -\frac{2q_i^3+1}{q_i^2}$$

for $i \in \{0,1\}$. Hence, $W_{b_i} : y^2z = x^3 + a_ix^2z + b_ixz^2$ are normalised Weierstrassian curves and W_{b_1} is the normalised dual of W_{b_0} and vice versa. Moreover, $H_{c_i} : X^3 + Y^3 + Z^3 + c_iXYZ = 0$ are the Hessian curves which are isomorphic to the curves W_{b_i} in the sense of Theorem 3.1 via projective maps $\Phi_{b_ic_i}$. We consider the homomorphisms $\phi_0 : W_{b_0} \to W_{b_1}$ and $\phi_1 : W_{b_1} \to W_{b_0}$ from Section 2 which are in homogeneous coordinates given by

$$\phi_i : \begin{pmatrix} x \\ y \\ z \end{pmatrix} \mapsto \begin{pmatrix} \alpha_i^2y^2z \\ \alpha_i^3y(x^2 - b_iz^2) \\ x^2z \end{pmatrix}$$

where $\alpha_i = \frac{2}{b_i-1}$. We can now push the homomorphisms between the normalised Weierstrassian curves to the Hessian curves by letting the following diagram commute:

$$\begin{tikzcd}
W_{b_0} \arrow[r, "\phi_0"] \arrow[d, "\Phi_{b_0c_0}"] & W_{b_1} \arrow[r, "\phi_1"] \arrow[d, "\Phi_{b_1c_1}"] & W_{b_0} \arrow[d, "\Phi_{b_0c_0}"] \\
H_{c_0} \arrow[r, "\psi_0"] & H_{c_1} \arrow[r, "\psi_1"] & H_{c_0}
\end{tikzcd}$$

Observe that by construction $\psi_1 \circ \psi_0 : P \mapsto P\#P$.

For (X_0, Y_0, Z_0) on the Hessian curve H_{c_0} we can explicitly compute $(X_1, Y_1, Z_1) := \psi_0(X_0, Y_0, Z_0)$. Reducing the occurring polynomials by $X_0^3 + Y_0^3 + Z_0^3 + c_0X_0Y_0Z_0$ one finds:

Theorem 4.2. *If H_{c_1} is the dual of the Hessian curve H_{c_0}, then the map*

$$\begin{array}{ccccc} H_{c_0} & \to & H_{c_1} & & \\ \begin{pmatrix} X_0 \\ Y_0 \\ Z_0 \end{pmatrix} & \mapsto & \begin{pmatrix} X_1 \\ Y_1 \\ Z_1 \end{pmatrix} & = & \begin{pmatrix} 2q_0^2X_0(X_0+Y_0)Z_0 + X_0Z_0^2 - q_0\big(Y_0(X_0+Y_0)^2 + Z_0^3\big) \\ 2q_0^2Y_0(X_0+Y_0)Z_0 + Y_0Z_0^2 - q_0\big(X_0(X_0+Y_0)^2 + Z_0^3\big) \\ Z_0(X_0+Y_0-2q_0Z_0)(X_0+Y_0+q_0Z_0) \end{pmatrix} \end{array}$$

is an homomorphism.

The resulting exression for $(X_2, Y_2, Z_2) := \psi_1 \circ \psi_0(X_0, Y_0, Z_0)$ is rather long, but

$$\begin{pmatrix} X_2 \\ Y_2 \\ Z_2 \end{pmatrix} \times \begin{pmatrix} X_0(Y_0^3 - Z_0^3) \\ Y_0(Z_0^3 - X_0^3) \\ Z_0(X_0^3 - Y_0^3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \quad \bmod (X_0^3 + Y_0^3 + Z_0^3 + c_0X_0Y_0Z_0)$$

which shows:

Proposition 4.3 ([8, Chapter 10]). *On a Hessian curve H_{c_0} there holds*

$$(X_0, Y_0, Z_0)\#(X_0, Y_0, Z_0) = \big(X_0(Y_0^3 - Z_0^3)\,, Y_0(Z_0^3 - X_0^3)\,, Z_0(X_0^3 - Y_0^3)\big).$$

If $c \neq -3$, then the Hessian curve H_c has the three points of inflection $\mathscr{O} := (-1,1,0), (0,-1,1), (-1,0,1)$, which are points of order 3. Notice that $\mathscr{O}\#(X,Y,Z) = (Y,X,Z)$. Furthermore, H_c has either 1 or 3 points of order 2, which are all of the form $(q,q,1)$ for some $q \in \mathbb{R} \setminus \{0\}$. Concerning points of order 6, we have the following

Lemma 4.4. *If $(q,q,1)$ is a point on a Hessian curve H_c, i.e., $c = -\frac{2q^3+1}{q}^2$, then $(1,\frac{1}{q},1)$ and $(\frac{1}{q},1,1)$ are points on H_c of order* 6.

Proof. First notice that if $(q,q,1)$ is a point on H_c, then also $\frac{1}{q}(q,q,1) = (1,1,\frac{1}{q})$ is a point on H_c, and consequently also $(1,\frac{1}{q},1)$ and $(\frac{1}{q},1,1)$ are points on H_c. To see that $S = (1,\frac{1}{q},1)$ is a point of order 6, notice that

$$S\#S = \Big(\frac{1}{q^3} - 1\,,\ 0\,,\ 1 - \frac{1}{q^3}\Big)$$

which is the same point (in the projective plane) as $(-1,0,1)$. So, $S\#S$ is a point of order 3, and since $S + S = \mathscr{O}\#(S\#S) = (0,-1,1)$, which is also a point of order 3, we obtain that S is of order 6. The proof for $(\frac{1}{q},1,1)$ is similar. *q.e.d.*

5 Rational Hessian curves

If c_0 is rational, then H_{c_0} is called a **rational Hessian curve**.

Notice that for example for $q_0 = -\big(1 + \sqrt[3]{2} + \frac{1}{\sqrt[3]{2}}\big)$, $c_0 = -\frac{2q_0^3+1}{q_0^2} = 6$ is rational, which shows that a rational Hessian curve H_{c_0} does not necessarily come from a rational q_0. However, if $c_0 < -3$ is rational (where $c_0 = -\frac{2q_0^3+1}{q_0^2}$), then at most one of the three possible values for q_0 is rational. In order to show this, we first prove the following

Lemma 5.1. *If $x_0, y_0 \in \mathbb{Q}$ are rational solutions of*

$$1 + 8x^3 = y^2,$$

then $x_0 = 0$ and $y_0 = 1$, $x_0 = -\frac{1}{2}$ and $y_0 = 0$, or $x_0 = 1$ and $y_0 = \pm 3$.

Proof. Let $x_0 = \frac{r}{s}$ and $y_0 = \frac{u}{v}$ be rational solutions, where $r,s,u,v \in \mathbb{Z}$, $s,v > 0$, $r,u \neq 0$, and $(r,s) = 1 = (u,v)$. In the case when $u = 0$ we obtain $x_0 = -\frac{1}{2}$ and $y_0 = 0$, and in the case when $r = 0$ we obtain $x_0 = 0$ and $y_0 = 1$. So, we have to show that the only other solution is $x_0 = 1$ and $y_0 = \pm 3$. Now,

$$1 + \frac{8r^3}{s^3} = \frac{u^2}{v^2}$$

and we obtain

$$1-\frac{u^2}{v^2}=\frac{(v-u)(v+u)}{v^2}=\frac{-(2r)^3}{s^3}. \tag{3}$$

We conclude that $v^2=s^3$, which implies that there exists a positive integer t such that $v=t^3$ and $\bar{s}=t^2$, where $(t,u)=1$. This gives us

$$-(2r)^3=t^6-u^2=(t^3-u)(t^3+u).$$

Since $2r$ is even, at least one of the factors $t^3\pm u$ is even, which implies that t^3 and u are both even or both odd, and since $(t,u)=1$, we obtain that both t^3 and u are odd. Now, let $d:=(t^3-u,t^3+u)$. Then $d\geq 2$ and $d\mid 2u$, and since $(t^3,u)=1$, we have $d\nmid u$ (otherwise, $d\mid t^3$), and therefore, $d=2$. Since t^3-u is even, we have *either* $t^3-u\equiv 0 \mod 4$, in which case $t^3+u\equiv 2 \mod 4$, *or* $t^3-u\equiv 2 \mod 4$, in which case $t^3+u\equiv 0 \mod 4$. This shows that one of the factors $t^3\pm u$ is four times a cube and the other is twice a cube. So, we find non-zero integers a,b such that $(a,b)=1$ and

$$4a^3+2b^3=(t^3-u)+(t^3+u)=2t^3,$$

or in other words,

$$t^3+(-b)^3=2a^3.$$

So, we arrive at an equation of the form

$$C^3+B^3=2A^3,$$

which has only the trivial integral solutions $C=B=A$ and $C=-B$, $A=0$ (see Euler [4, p. 520, §247]).

If $A=0$, then $t^3=\pm u$, which is impossible since $(t^3,u)=1$. So, assume $C=B$ (*i.e.*, $t=-b$), and that $t^3-u=2b^3$ (the case when $t^3+u=2b^3$ is similar). This gives us $t^3-u=-2t^3$, and since $(t,u)=1$, we finally obtain $t=\pm 1$ and $u=\pm 3$. Thus, $y_0=\pm 3$ and $x_0=1$, which completes the proof. *q.e.d.*

Now we are ready to prove the following

PROPOSITION 5.2. *If H_{c_0} is a rational Hessian curve and $c_0\neq -3$, then there exists at most one rational $q_0\in\mathbb{Q}$ such that $c_0=-\frac{2q_0^3+1}{q_0^2}$. In the case when $c_0=-3$, we get two rational values for q_0, namely $q_0=1$ and $q_0=-\frac{1}{2}$.*

Proof. Let $q_0\in\mathbb{Q}$ be a solution of

$$2x^3+c_0x^2+1=0. \tag{4}$$

$$(2x^3+c_0x^2+1):(x-q_0)=2x^2+x(c_0+2q_0)+q_0(c_0+2q_0).$$

Hence, the other two solutions of (4) are

$$\begin{aligned} q_{1,2} &= -\frac{1}{4}\Big(c_0 + 2q_0 \pm \sqrt{c_0^2 - 4c_0q_0 - 12q_0^2}\Big) \\ &= \frac{1}{4q_0}\Big(1 \pm \sqrt{1+8q_0^3}\Big) \end{aligned}$$

where we have used that $c_0 = -\frac{2q_0^3+1}{q_0^2}$. Therefore, $q_{1,2} \in \mathbb{Q}$ if and only if $1 + 8q_0^3 = \left(\frac{u}{v}\right)^2$ where $u, v \in \mathbb{Z}$, $v > 0$, and $(u, v) = 1$. Now, by Lemma 5.1, we obtain $q_0 \in \{-\frac{1}{2}, 0, 1\}$. The case when $q_0 = 0$ is impossible, and $q_0 = -\frac{1}{2}$ or $q_0 = 1$ both imply $c_0 = -3$. *q.e.d.*

With Lemma 5.1 we can show that the cubic curve $y^2 = x^3 + 1$ contains only six rational projective points.

Proposition 5.3. *The cubic curve $y^2z = x^3 + z^3$ contains only the following six rational projective points:* $(0, 1, 0)$, $(-1, 0, 1)$, $(0, \pm1, 1)$, $(2, \pm3, 1)$.

Proof. It is easy to verify that the six projective points given above belong to the curve $y^2z = x^3 + z^3$. Furthermore, by replacing x with $2x$, it is enough to show that $(0, 1, 0)$, $(-\frac{1}{2}, 0, 1)$, $(0, \pm1, 1)$, $(1, \pm3, 1)$ are the only rational points on the curve

$$C: \; y^2z = 8x^3 + z^3.$$

For this, assume that (x_0, y_0) is a rational point on the curve $y^2 = x^3 + 1$, or equivalently, (x_0, y_0) is a solution of

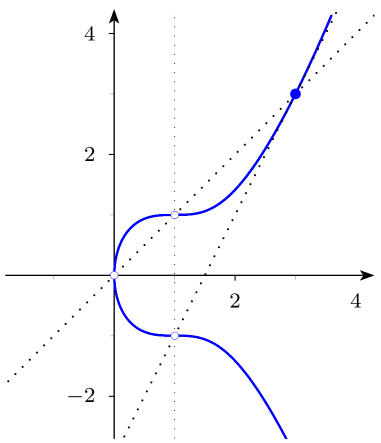
$$1 + (2x_0)^3 = y_0^2.$$

Now, in the proof of Lemma 5.1 we have seen that the only rational solutions of this equations are when $x_0 \in \{-\frac{1}{2}, 0, 1\}$, which gives us the six rational projective points $(0, 1, 0)$, $(-\frac{1}{2}, 0, 1)$, $(0, \pm1, 1)$, $(1, \pm3, 1)$ on the cubic curve $y^2z = x^3 + z^3$. *q.e.d.*

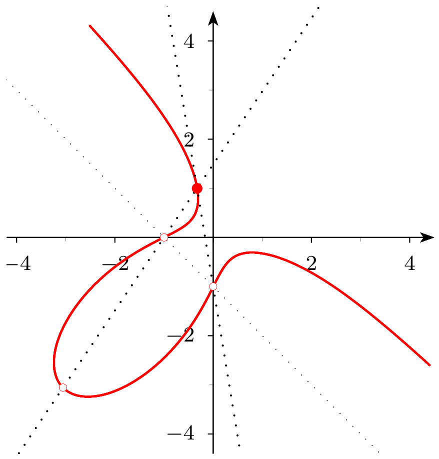
By replacing x with $x - 1$, the curve $y^2 = x^3 + 1$ becomes the normalised Weierstrassian curve

$$y^2 = x^3 - 3x^2 + 3x\,,$$

which corresponds to the Hessian curve H_{c_0} with $c_0 = 6$ and $q_0 = -\big(1 + \sqrt[3]{2} + \frac{1}{\sqrt[3]{2}}\big)$. Notice that by Hurwitz [5] (see also Mordell [8, Chapter 10]), the Hessian curve H_{c_0} with $c_0 = 6$ has either exactly three or infinitely many rational points. The two curves together with a point of order 6 are illustrated by the following figures:



$b_0 = 3$



$c_0 = 6$

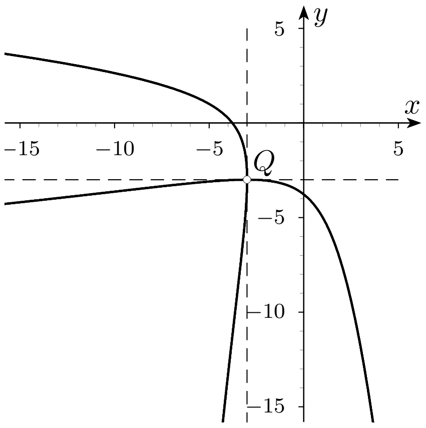
6 Pairs of dual rational Hessian curves

If, for some non-zero real q_0, $c_0 = -\frac{2q_0^3+1}{q_0^2}$ and $c_1 = \frac{1-4q_0^3}{q_0}$, then H_{c_0} and H_{c_1} are **dual Hessian curves** (see Lemma 4.1). If H_{c_0} and H_{c_1} is a pair of dual Hessian curves and both c_0 and c_1 are rational, then the pair H_{c_0} and H_{c_1} is called a **pair of dual rational Hessian curves**. If a curve H_c belongs to a pair of dual rational Hessian curves, then we say that H_c is a **dual rational Hessian curve**.

We have seen that for $q_0 = -\bigl(1 + \sqrt[3]{2} + \frac{1}{\sqrt[3]{2}}\bigr)$, $c_0 = -\frac{2q_0^3+1}{q_0^2} = 6$ is rational, which shows that a rational Hessian curve H_{c_0} does not necessarily come from a rational q_0. However, for dual rational Hessian curves, this is always the case; but before we show this, we give a parametrisation of the quartic curve

$$x^2y^2 + x^3 + y^3 - 9xy + 54 = 0, \tag{5}$$

which is illustrated in the following figure:



Proposition 6.1. *The map*

$$\begin{aligned}\gamma : \mathbb{R} \setminus \left\{0, 1, -\tfrac{1}{2}\right\} &\rightarrow \Big\{(x,y) \in \mathbb{R}^2 \setminus \{(-3,-3)\} : x^2y^2 + x^3 + y^3 - 9xy + 54 = 0\Big\} \\ q &\mapsto \Big(-\frac{2q^3+1}{q^2}, \frac{1-4q^3}{q}\Big)\end{aligned}$$

is bijective. The point $\gamma(1) = \gamma(-\frac{1}{2}) = (-3,-3)$ *corresponds to the double point* Q *on the quartic (5).*

Proof. First of all, it is easy to check that each point $(x,y) = \gamma(q)$ satisfies (5).

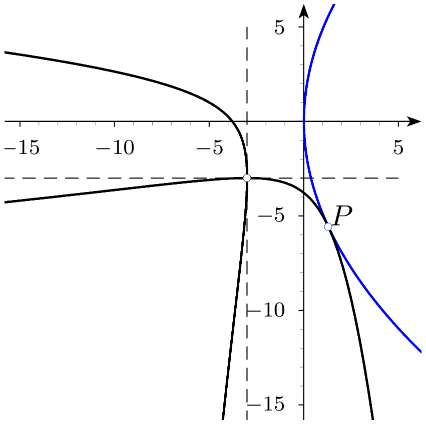
γ is injective: Let $(x,y) := \gamma(q)$ for some $q \in \mathbb{R} \setminus \left\{0, 1, -\frac{1}{2}\right\}$. *i.e.*, $(x,y) \neq (-3,-3)$. We need to show that only one q can have this property. By eliminating q^3 from

$$2q^3 + xq^2 + 1 = 0 \quad \text{and} \quad 4q^3 + yq - 1 = 0$$

we obtain $2xq^2 - yq + 3 = 0$. For $x = 0$ it follows that $q = 3/y$ and we are done. For $x \neq 0$ only two values

$$q_{\pm} = \frac{y \pm \sqrt{y^2 - 24x}}{4x} \tag{6}$$

are possible for q. Observe that $y^2 - 24x = \frac{(5+4q^3)^2}{q^2} \geq 0$ and $y^2 - 24x = 0$ *iff* $q = -\sqrt[3]{\frac{5}{4}}$, corresponding to the point $P = \big(3\sqrt[3]{\frac{2}{5^2}}, -6\sqrt[3]{\frac{2^2}{5}}\big)$ on the quartic. So, for $(x,y) = P$ we are done. The following figure shows the quartic (5) together with the parabola $y^2 - 24x = 0$ (blue) and the point P.



Otherwise, we have

$$\gamma(q_+) - \gamma(q_-) = \frac{\sqrt{y^2 - 24x}}{3x}\Big(\frac{xy - 9}{3}, -\frac{x^2 + 3y}{x}\Big)$$

which vanishes only for $(x,y) = (-3,-3)$. In particular, this means that for only one value $q = q_{\pm}$ we have $(x,y) = \gamma(q)$.

It is instructive to determine the sign of the root in (6): For a concrete point $\gamma(q)$ on the quartic, one can just check which sign is the correct one. Then, by continuity, this sign is valid for all points on the corresponding branch of the curve until one reaches P (see the figure above).

γ *is surjective*: Let $(x, y) \neq (-3, -3)$ be a point on the quartic (5). If $x > -3$ there is a unique q such that $x = -\frac{2q^3+1}{q^2}$, and $q < -\frac{1}{2}$. If we replace x in (5) with this expression, we are left with an equation in y and q which has, for $q < -\frac{1}{2}$, only one real solution, namely $y = \frac{1-4q^3}{q}$, and hence, $(x, y) = \gamma(q)$. If $x < -3$, there are three different values $q_i \notin \{-\frac{1}{2}, 1\}$ for q such that $x = -\frac{2q^3+1}{q^2}$. In this case, the resulting equation in y and q has three real solutions y in terms of q. On the other hand, each of the three different points $\gamma(q_i)$ is a point on (5). Hence, $\gamma(q) = (x, y)$ for one of the three values $q = q_i$. *q.e.d.*

We get a somewhat nicer picture when we transform the quartic (5) projectively to an "8-shaped" curve and the parabola to a hyperbola:

$$\Phi : \begin{pmatrix} x \\ y \\ z \end{pmatrix} \mapsto \begin{pmatrix} X \\ Y \\ Z \end{pmatrix} = \begin{pmatrix} -3 & 0 & 0 \\ 0 & -3 & 0 \\ 1 & 1 & -3 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} .$$

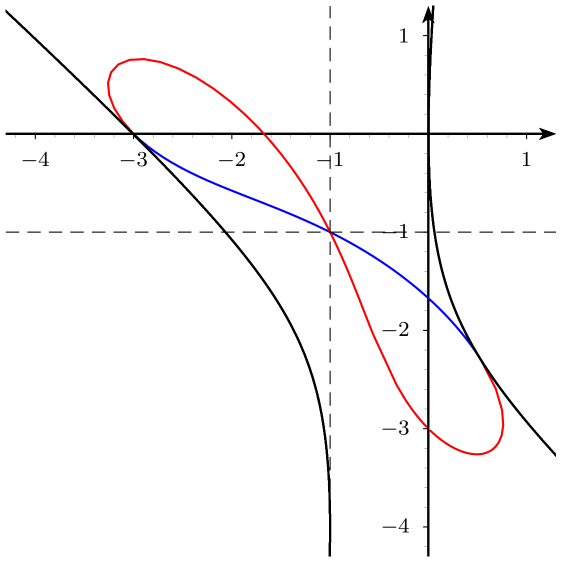
The following figure shows the transformed quartic (in the plane $Z = 1$)

$$\begin{aligned} 54 + 72X + 36X^2 + 9X^3 + X^4 + 72Y + 63XY \\ + 18X^2Y + 2X^3Y + 36Y^2 + 18XY^2 + 3X^2Y^2 + 9Y^3 + 2XY^3 + Y^4 = 0 \end{aligned}$$

which is parametrised by

$$\left(-\frac{3(1+2q^3)}{(1+q+q^2)(1-2q+4q^2)} , \frac{3q(1-4q^3)}{(1+q+q^2)(1-2q+4q^2)} \right),$$

together with the hyperbola, where the red part of the quartic shows where we have to take the negative root to compute the original q:



With the parametrisation given in Proposition 6.1 of the quartic (5), we obtain that for each $q \in \mathbb{Q} \setminus \{0\}$, $\gamma(q)$ is a rational point on (5). As a consequence of the following result, which characterises dual rational Hessian curves, we get that each rational point on (5) is the image under γ of some $q \in \mathbb{Q}$.

Theorem 6.2. *If H_{c_0} and H_{c_1} is a pair of dual rational Hessian curves, i.e., if c_0 and c_1 are both rational, then there exists a unique rational $q_0 \in \mathbb{Q}$ such that*

$$c_0 = -\frac{2q_0^3 + 1}{q_0^2} \quad \textit{and} \quad c_1 = \frac{1 - 4q_0^3}{q_0}\,.$$

Proof. Since H_{c_0} and H_{c_1} is a pair of dual rational Hessian curves, c_0 and c_1 are both rational, say $c_0 = \frac{r}{s}$ and $c_1 = \frac{u}{v}$, and there is a $q \in \mathbb{R}$ such that $c_0 = -\frac{2q^3+1}{q^2}$ and $c_1 = \frac{1-4q^3}{q}$. Notice that by Lemma 5.1, if $q \in \mathbb{Q}$, then q is unique. By eliminating q^3 from the two equations

$$c_0 = -\frac{2q^3 + 1}{q^2} = \frac{r}{s} \qquad\qquad c_1 = \frac{1 - 4q^3}{q} = \frac{u}{v}$$

we get

$$2q^2rv - qsu + 3sv = 0\,.$$

Since q is a root of $2q^2rv - qsu + 3sv$, the minimal polynomial of q over $\mathbb{Q}$ must divide this polynomial. Let

$$m_q := q^2 - \tfrac{su}{2rv}q + \tfrac{3s}{2r}.$$

Then m_q is the minimal polynomial of q over $\mathbb{Q}$ if and only if $q \notin \mathbb{Q}$. So, in order to show that q is rational, it is enough to prove that m_q is not the minimal polynomial of q over $\mathbb{Q}$.

So, assume that m_q is the minimal polynomial of q over $\mathbb{Q}$. Then, from the equation $c_0 = -\frac{2q^3+1}{q^2}$ we obtain

$$2q^3 + c_0 q^2 + 1 = 0,$$

and since m_q is the minimal polynomial of q, there exists a polynomial $p(x) = kx + l$ with rational coefficients such that

$$p(q) \cdot m_q = 2q^3 + c_0 q^2 + 1.$$

Since $c_0 = \frac{r}{s}$, we have

$$p(q) \cdot m_q = (kq + l)(q^2 - \tfrac{su}{2rv} q + \tfrac{3s}{2r}) = (2q^3 + \tfrac{r}{s} q^2 + 1)$$

and equating the coefficients yields $k = 2$, $l = \frac{2r}{3s}$ and

$$\frac{3s}{r} - \frac{u}{3v} = 0\,.$$

Hence, since $c_0 = \frac{r}{s}$ and $c_1 = \frac{u}{v}$, we get from this

$$-\frac{3q^2}{2q^3+1} = \frac{1-4q^3}{3q}\,,$$

which is equivalent to $8q^6 - 7q^3 - 1 = 0$. Thus, we have either $q^3 = 1$ or $q^3 = -\frac{1}{8}$ and, in both cases, $q \in \mathbb{Q}$. This shows that m_q is not the minimal polynomial of q over $\mathbb{Q}$ which completes the proof. *q.e.d.*

As a consequence we get the following

COROLLARY 6.3. *A point* (x_0, y_0) *on the quartic curve*

$$x^2y^2 + x^3 + y^3 - 9xy + 54 = 0$$

is rational if and only if there is a $q \in \mathbb{Q}$ *such that*

$$x_0 = -\frac{2q^3+1}{q^2} \quad \textit{and} \quad y_0 = \frac{1-4q^3}{q}\,.$$

7 Pairs of dual integral Hessian curves

Let H_{c_0} be a dual rational Hessian curve with $c_0 \in \mathbb{Z}$. What are the possible values for c_0? The answer to this question is given by the following

THEOREM 7.1. *If* H_{c_0} *is a dual rational Hessian curve and* $c_0 \in \mathbb{Z}$*, then* $c_0 \in \{1, -3, -5\}$.

Proof. Let $c_0 = k$ for some integer k. Then

$$k = -\frac{2q^3+1}{q^2}$$

for some rational $q = \frac{u}{v}$, where $u > 0$ (since $q \neq 0$), $v \neq 0$, and $(u,v) = 1$. We therefore have

$$\begin{aligned} 2q^3 + kq^2 + 1 &= 0, \\ 2\frac{u^3}{v^3} + k\frac{u^2}{v^2} + 1 &= 0, \\ 2u + kv + \frac{v^3}{u^2} &= 0. \end{aligned}$$

Since $2u + kv \in \mathbb{Z}$, $u > 0$, and $(u,v) = 1$, we must have $u = 1$. Hence, $q = \frac{1}{v}$ for some $v \in \mathbb{Z}$ with $v \neq 0$ and $v^3 + kv + 2 = 0$. We consider the following cases:

$v > 0$: In this case, we have $v^3 \geq 1$ and $v^3 + 2 = -kv$ for some $k < 0$. The only possible values for v are $v = 1$ and $v = 2$, which give us $k = -3$ and $k = -5$, respectively.

$v < 0$: In this case, the only possible values for v are $v = -1$ and $v = -2$, which give us $k = 1$ and $k = -3$, respectively.

So, the only possible values for k (*i.e.*, for c_0) are $1, -3, -5$. *q.e.d.*

8 The torsion group of dual rational Hessian curves

In this section, we give a characterization of rational Hessian curves. For this, we first prove the following

THEOREM 8.1. *A Hessian curve H_c with $c \neq -3$ is a dual rational Hessian curve if and only if H_c has a rational point of order* 6.

Proof. ($\Rightarrow$) Let H_c be a dual rational Hessian curve. Then $c = -\frac{2q^3+1}{q^2}$ for some $q \in \mathbb{Q}$. We already have seen that the rational point $(\frac{1}{q}, 1, 1)$ is a point of order 6 on H_c, hence, every dual rational Hessian curve has a rational point of order 6.

($\Leftarrow$) Let $P = (X_0, Y_0, Z_0)$ be a rational point of order 6 on the Hessian curve H_c. Then $2P$ is a rational point on H_c of order 3, *i.e.*, $2P$ is a point of inflection. Therefore, either $2P$ or $P\#P$ is the point $(0,-1,1)$. Without loss of generality, let us assume that $P\#P = (0,-1,1)$, *i.e.*,

$$P\#P = \Big(X_0(Y_0^3 - Z_0^3)\,,\, Y_0(Z_0^3 - X_0^3)\,,\, Z_0(X_0^3 - Y_0^3)\Big) = \big(0,-1,1\big)\,.$$

Since $X_0(Y_0^3 - Z_0^3) = 0$, we have either $X_0 = 0$ or $Y_0 = Z_0 \neq 0$. If $X_0 = 0$, then P is a point of inflection which contradicts the fact that P is a point of order 6. So, we must have $Y_0 = Z_0 \neq 0$, but then,

$$P = \Big(\frac{X_0}{Z_0}\,,\,1\,,\,1\Big).$$

Now, since $\frac{1}{q} := \frac{X_0}{Z_0}$ is rational and $(\frac{1}{q}, 1, 1)$ is on H_c, we have $\frac{1}{q^3} + 2 + \frac{c}{q} = 0$, which implies that

$$c = -\frac{2q^3+1}{q^2},$$

hence, H_c is a dual rational Hessian curve. *q.e.d.*

The question is now, whether a rational Hessian curve H_c with $c = -\frac{2q^3+1}{q^2}$ can have rational points beside the six points $(-1, 1, 0)$, $(0, -1, 1)$, $(-1, 0, 1)$, $(q, q, 1)$, $(\frac{1}{q}, 1, 1)$, $(1, \frac{1}{q}, 1)$. We will see that this is not the case, but before we have to recall some facts: As mentioned above, MORDELL'S THEOREM states that the rational points of an elliptic curve form a finitely generated abelian group (see Mordell [8, Ch. 16]). Therefore, by the FUNDAMENTAL THEOREM OF FINITELY GENERATED ABELIAN GROUPS, the group of rational points on an elliptic curve is isomorphic to some group of the form

$$\underbrace{\mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_k\mathbb{Z}}_{\text{torsion group}} \times \mathbb{Z}^r,$$

where $n_1, \ldots, n_k$ are positive integers with $n_i \mid n_{i+1}$, and r is a non-negative integer. The group $\mathbb{Z}/\mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}/\mathbb{Z}_{n_k}$, which is generated by rational points of finite order, is the so-called *torsion group*, and r is called the *rank* of the curve. Now, by MAZUR'S THEOREM (see Mazur [6]) the torsion group of an elliptic curve is isomorphic to one of the following fifteen groups:

$$\mathbb{Z}/m\mathbb{Z} \quad \text{for } m \in \{1,2,3,4,5,6,7,8,9,10,12\}, \quad \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2n\mathbb{Z} \quad \text{for } n \in \{1,2,3,4\}.$$

By THEOREM 8.1 we know that every dual rational Hessian curve H_c with $c \neq -3$ has a rational point of order 6. Hence, the torsion group of a dual rational Hessian curve is isomorphic to one of the following three groups:

$$\mathbb{Z}/6\mathbb{Z}\,, \quad \mathbb{Z}/12\mathbb{Z}\,, \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}\,.$$

With the method at hand we are now able to give a short proof for the following Theorem. See Papadopoulos [9] and Rubin and Silverberg [10] for similar results.

THEOREM 8.2. *If H_c is a dual rational Hessian curve with $c \neq -3$, then the torsion group of H_c is isomorphic to $\mathbb{Z}/6\mathbb{Z}$.*

Proof. Let H_{c_0} be a dual rational Hessian curve with $c_0 = -\frac{2q_0^3+1}{q_0^2}$ for some $q_0 \in \mathbb{Q}$. By Mazur's Theorem it is enough to show that the torsion group of H_{c_0} is neither $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ nor $\mathbb{Z}/12\mathbb{Z}$.

Assume towards a contradiction that the torsion group of H_{c_0} is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. Then, since $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, there are three rational points on H_{c_0} of order 2, where one of these rational points is $(q_0, q_0, 1)$. Now, the existence of three rational points on H_{c_0} is equivalent to the existence of three rational solutions of $2q^3 + c_0q^2 + 1 = 0$, which, by Proposition 5.2 (and since $c_0 \neq -3$), is impossible.

Now, assume towards a contradiction that the torsion group of H_{c_0} is $\mathbb{Z}/12\mathbb{Z}$. Then there is a rational point Q_0 on H_{c_0} of order 12, which implies that $P_0 := Q_0 \# Q_0$ is a rational point on H_{c_0} of order 6. In particular, the line through P_0 and Q_0 is tangent to the curve H_{c_0} at Q_0, and since the tangent to the curve H_{c_0} at P_0 meets H_{c_0} at an inflection point, this implies that $q_0 < 0$ (*i.e.*, H_{c_0} is connected), and since H_{c_0} has just two points of order 6, $P_0 = (1, \frac{1}{q_0}, 1)$ or $P_0 = (\frac{1}{q_0}, 1, 1)$. Without loss of generality, we may assume that $P_0 = (1, \frac{1}{q_0}, 1)$; the case when $P_0 = (\frac{1}{q_0}, 1, 1)$ is similar. We now apply the homomorphisms $\psi_0 : H_{c_0} \to H_{c_1}$ and $\psi_1 : H_{c_1} \to H_{c_0}$ given in Section 4, where H_{c_1} is the dual of H_{c_0}. Let $Q_1 := \psi_0(Q_0)$. By the properties of ψ_0 and ψ_1, we obtain $P_0 = \psi_1(Q_1)$ and $\psi_0(P_0) = Q_1 \# Q_1$. Now, an easy calculation shows that $\psi_0(P_0) = (-1, 0, 1)$, which implies that $Q_1 \# Q_1 = (-1, 0, 1)$. If $Q_1 = (-1, 0, 1)$, then $\psi_1(Q_1) = (-1, 0, 1)$, which contradicts the fact that $\psi_1(Q_1) = P_0$. Therefore, Q_1 is a rational point of order 6 such that $Q_1 \# Q_1 = (-1, 0, 1)$. If $Q_1 = (1, \frac{1}{q_1}, 1)$ (where $q_1 = -\frac{1}{2q_0}$), then $\psi_1(Q_1) = (-1, 0, 1)$, which contradicts again the fact that $P_0 = \psi_1(Q_1)$. Hence, Q_1 is a rational point of order 6, $Q_1 \# Q_1 = (-1, 0, 1)$, but Q_1 is neither $(1, \frac{1}{q_1}, 1)$ nor $(\frac{1}{q_1}, 1, 1)$; notice that $(\frac{1}{q_1}, 1, 1) \# (\frac{1}{q_1}, 1, 1) = (0, -1, 1)$. So, we find at least three points of order 6 on H_{c_0}, which shows that the torsion group of H_{c_0} cannot be $\mathbb{Z}/12\mathbb{Z}$. *q.e.d.*

Transforming the dual rational Hessian curve H_{c_0} to the corresponding Weierstrassian curve W_{b_0}, we obtain the following

Corollary 8.3. *The rational solutions* (x_0, y_0) *of the equation*

$$1 + 2x + x^2 + x^3 + 2x^4 + x^5 = y^2$$

are $(-1, 0)$*,* $(0, 1)$*,* $(2, 9)$*.*

Proof. Let W_{b_0} be a normalized Weierstrassian curve where $b_0 = \frac{(q_0-1)^3}{q_0+q_0^2+q_0^3}$ for some rational $q_0 \neq 0$, and let W_{b_1} be its dual (*i.e.*, $b_1 = \frac{b_0-9}{b_0-1}$). We apply the homomorphisms $\phi_0 : W_{b_0} \to W_{b_1}$ and $\phi_1 : W_{b_1} \to H_{b_0}$ given in Section 2. Let $(x_0, y_0, 1)$ with $y_0 \neq 0$ be a rational point on W_{b_0} and let

$$x_2 := \frac{(b_0 - x_0^2)^2}{4y_0^2}\,.$$

Then, for some rational y_2,

$$\phi_1 \circ \phi_0(x_0, y_0, 1) = (x_2, y_2, 1).$$

Now, since $y_0^2 = x_0^3 + a_0 x_0^2 + b_0 x_0$, where $a_0 = \frac{b_0^2 - 6b_0 - 3}{4}$, x_2 depends only on x_0 and b_0. Let us assume that $(x_2, y_2, 1)$ is an inflection point, then $x_2 = 1$. Hence, $x_2 - 1 = 0$, and the solutions for x_0 are

$$x_0 \in \left\{1,\ b_0,\ \tfrac{1}{2}\big(3 - b_0 \pm \sqrt{(b_0 - 9)(b_0 - 1)}\,\big)\right\}.$$

If $x_0 = 1$, then (x_0, y_0) is an inflection point, and if $x_0 = b_0$, then (x_0, y_0) is a point of order 6. As a consequence of THEOREM 8.2 we know that there are no other rational values for x_0 such that $x_2 - 1 = 0$. Let us consider $\sqrt{(b_0 - 9)\,(b_0 - 1)}$: By replacing b_0 with $\frac{(q_0 - 1)^3}{q_0 + q_0^2 + q_0^3}$ we get

$$\sqrt{(b_0 - 9)\,(b_0 - 1)} = \sqrt{\frac{(1 + 2q_0)^3 (1 - 2q_0 + 4q_0^2)}{q_0^2 (1 + q_0 + q_0^2)^2}} = \frac{\sqrt{(1 + 2q_0)^3 (1 - 2q_0 + 4q_0^2)}}{q_0 (1 + q_0 + q_0^2)},$$

which shows that $\sqrt{(b_0 - 9)\,(b_0 - 1)} \in \mathbb{Q}$ if and only if $\sqrt{(1 + 2q_0)^3 (1 - 2q_0 + 4q_0^2)} \in \mathbb{Q}$. In other words, $\sqrt{(b_0 - 9)\,(b_0 - 1)} \in \mathbb{Q}$ if and only if

$$1 + 4q_0 + 4q_0^2 + 8q_0^3 + 32q_0^4 + 32q_0^5 = p^2 \quad \text{for some } p \in \mathbb{Q}, \tag{7}$$

and since x_0 can take no other rational values than 1 and b_0, we obtain that the only possible values for the rational q_0 are when the corresponding b_0 is not defined or the corresponding curve is singular. So, the only rational solutions (q_0, p) of (7) are $(-\frac{1}{2}, 0)$, $(0, 1)$,$(1, 9)$, and multiplying q_0 by 2 leads to the equation

$$1 + 2x + x^2 + x^3 + 2x^4 + x^5 = y^2,$$

which has no other solutions than $(-1, 0)$, $(0, 1)$, and $(2, 9)$. *q.e.d.*

9 The rank of H_{c_0} for $c_0 = 1, -5$

Hurwitz showed in [5] (see also Mordell [8, Chapter 10]) that for every integer $c \neq 1, -5$, the Hessian curve H_c has either exactly three or infinitely many rational points. Now, since the only dual integral Hessian curves H_{c_0} are when $c_0 = 1, -5, -3$, and since $c_0 = -3$ corresponds to the line $x + y + z = 0$ together with the point $(1, 1, 1)$, Hurwitz' result does not tell us something new about dual rational Hessian curves. However, Mordell showed in [7] that for $c_0 = 1, -5$, the dual integral Hessian curve H_{c_0} has exactly six rational points. Therefore, all rational points on H_{c_0} (for

$c_0 = 1, -5$) have finite order, which implies that the rank of both curves is zero—recall that the rank of an elliptic curve is the number of generators of rational points of infinite order and notice that the rank of H_{c_0} is the same as the rank of its dual H_{c_1}.

In order to compute the rank of a dual rational Hessian curve H_{c_0}, we first transform H_{c_0} to the corresponding normalised Weierstrassian curve W_{a_0,b_0}, and then multiply the coefficients a_0 and b_0 by α^2 and α^4, respectively, in order to get integer coefficients a and b, respectively. Then, we apply the technique described in Silverman and Tate [11, Chapter III.6.] to "compute" the rank. To illustrate this procedure, we consider the case when $c_0 = 1$, *i.e.*, when $q_0 = -1$.

First we get $b_0 = 8$ and $a_0 = \frac{13}{4}$. For $\alpha = 2$, we obtain $a = 13$ and $b = 128$, so,

$$W_{a,b} : \quad y^2 = x^3 + 13x^2 + 128x \,.$$

In order to compute the rank of $W_{a,b}$, which is the same as the rank of H_{c_0} (for $c_0 = 1$), we have to find out how many of the following equations have solutions in positive integers:

$$\begin{array}{rcrcrcrl}
n^2 & = & m^4 & + & 13\,m^2e^2 & + & 128\,e^4 & \qquad (1)\\
n^2 & = & -m^4 & + & 13\,m^2e^2 & - & 128\,e^4 & \qquad (2)\\
n^2 & = & 2\,m^4 & + & 13\,m^2e^2 & + & 64\,e^4 & \qquad (3)\\
n^2 & = & -2\,m^4 & + & 13\,m^2e^2 & - & 64\,e^4 & \qquad (4)\\[6pt]
n^2 & = & m^4 & - & 26\,m^2e^2 & - & 343\,e^4 & \qquad (1')\\
n^2 & = & -m^4 & - & 26\,m^2e^2 & + & 343\,e^4 & \qquad (2')\\
n^2 & = & 7\,m^4 & - & 26\,m^2e^2 & - & 49\,e^4 & \qquad (3')\\
n^2 & = & -7\,m^4 & - & 26\,m^2e^2 & + & 49\,e^4 & \qquad (4')
\end{array}$$

The first four equations (1)–(4) are obtained from the curve $W_{a,b}$, and the second four equations (1′)–(4′) are obtained from the dual curve $W_{a',b'}$, where $a' = -2a$ and $b' = a^2 - 4b$. The equations (1)–(4) are of the form

$$n^2 \;=\; b_1\,m^4 \;+\; a\,m^2e^2 \;+\; b_2\,e^4$$

where b_1 and b_2 are integers, $b_1b_2 = b$, and b_1 is square-free. The equations (1′)–(4′) are obtained similarly by a' and b'. So, for $b = 128$, $b_1 \in \{1, -1, 2, -2\}$, and for $b' = -343$, $b'_1 \in \{1, -1, 7, -7\}$.

Let k be the number of equations (1)–(4) for which we find solutions in positive integers, let k' be the corresponding number with respect to equations (1′)–(4′), and let r be the rank of $W_{a,b}$ (*i.e.*, of H_{c_0}). Then, if $r > 0$,

$$2^r = \frac{k \cdot k'}{4}.$$

Now, since by Mordell's result the rank of H_{c_0} for $c_0 = 1, -5$ is zero, we must have $k \cdot k' \leq 4$. In fact, $k = k' = 2$, *i.e.*, exactly four equations have solutions in positive integers. These four equations are:

$$\begin{array}{ll} (1) & \text{with solution} \quad n = 14\,, \quad m = 2\,, \quad e = 1\,. \\ (3) & \text{with solution} \quad n = 28\,, \quad m = 4\,, \quad e = 1\,. \\ (1') & \text{with solution} \quad n = 28\,, \quad m = 7\,, \quad e = 1\,. \\ (4') & \text{with solution} \quad n = 4\,, \quad m = 1\,, \quad e = 1\,. \end{array}$$

In particular, we obtain that the other four equations do not have solutions in positive integers:

PROPOSITION 9.1. *None of the four equations* $(2), (4), (2'), (3')$ *has a solution in positive integers.*

We may ask whether the rank of a dual rational Hessian curve is always zero. This is not the case. For example $(8, 31, -14)$ is a point of infinite order on the curve H_{c_0}, where $c_0 = \frac{127}{16}$ with corresponding $q_0 = -4$, and for $q_0 = 4$ we have $c_0 = -\frac{129}{16}$ with the points of infinite order $(8, 5, 2)$ and $(8, -13, 2)$ on H_{c_0}.

References

[1] ROBERT BIX, ***Conics and Cubics***, 2nd ed., Springer-Verlag, New York, 2006.

[2] CHRISTOPHE DOCHE AND TANJA LANGE, *Arithmetic of elliptic curves*, *in* ***Handbook of Elliptic and Hyperelliptic Curve Cryptography*** (Henri Cohen and Gerhard Frey, eds.), Discrete Mathematics and its Applications, Chapman & Hall/CRC, Boca Raton, 2006, pp. 267–302.

[3] ERIK DOFS, *Solutions of* $x^3 + y^3 + z^3 = nxyz$, ***Acta Arithmetica***, vol. 73 (1995), 201–213.

[4] LEONHARD EULER, ***Vollständige Anleitung zur Algebra,*** *Zweyter Theil: Von Auflösung algebraischer Gleichungen und der unbestimmten Analytic*, Kays. Acad. der Wissenschaften, St. Petersburg, 1770.

[5] ADOLF HURWITZ, *Über ternäre diophantische Gleichungen dritten Grades*, ***Vierteljahrsschrift der Naturforschenden Gesellschaft in Zürich***, vol. 62 (1917), 207–229, [***Mathematische Werke von Adolf Hurwitz II***, Birkhäuser, Basel (1933), pp. 446–468].

[6] BARRY MAZUR, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, ***Inventiones Mathematicae***, vol. 44 (1978), 129–162.

[7] Louis Joel Mordell, *The Diophantine Equation* $x^3 + y^3 + z^3 + kxyz = 0$, ***Colloque sur la Théorie des Nombres,*** *Tenu à Bruxelles les 19, 20 et 21 décembre 1955*, 67–76.

[8] ______, ***Diophantine Equations***, Academic Press, London · New York, 1969.

[9] Ioannis Papadopoulos, *Courbes elliptiques ayant même 6-torsion qu'une courbe elliptique donnée*, ***Journal of Number Theory***, vol. 79 (1999), 103–114.

[10] Karl Rubin and Alice Silverberg, *Mod* 6 *representations of elliptic curves*, Automorphic forms, automorphic representations, and arithmetic (Fort Worth, TX, 1996), Proceedings of Symposia in Pure Mathematics, vol. 66, American Mathematical Society, Providence, RI, 1999, pp. 213–220.

[11] Joseph H. Silverman and John Tate, ***Rational Points on Elliptic Curves***, 2nd ed., Springer-Verlag, New York, 2015.