ARCHIVUM MATHEMATICUM (BRNO)
Tomus 59 (2023), 339–349

RATIONAL BÉZIER CURVES WITH INFINITELY MANY INTEGRAL POINTS

Petroula Dospra

Abstract. In this paper we consider rational Bézier curves with control points having rational coordinates and rational weights, and we give necessary and sufficient conditions for such a curve to have infinitely many points with integer coefficients. Furthermore, we give algorithms for the construction of these curves and the computation of theirs points with integer coefficients.

1. Introduction

Let $P_0, \dots, P_n$ be points of the affine space $\mathbb{A}^3$ over $\mathbb{R}$ and $w_0, \dots, w_n$ are nonzero real numbers. We recall that the Bernstein polynomials of degree n are defined by

$$B_i^n(t) = \binom{n}{i}(1-t)^{n-i}t^i \quad (i = 0, \dots, n)\,.$$

A *rational Bézier curve* of degree n is defined by a map of the form

$$F\colon \mathbb{A} \longrightarrow \mathbb{A}^3,\ t \longmapsto \frac{w_0 P_0 B_0^n(t) + \dots + w_n P_n B_n^n(t)}{w_0 B_0^n(t) + \dots + w_n B_n^n(t)}\,.$$

The numbers $w_0, \dots, w_n$ are called *weights* of F and the set $F(\mathbb{A})$ is called the *trace of* F. For $w_0 = \ldots = w_n$, we obtain the classical (integral) Bézier curves. Rational Bézier curves provide a curve fitting tool and are widely used in Computer Aided Geometric Design, Computer Aided Design and Geometric Modelling [1, 2, 3].

In this paper, we study the integral points of rational Bézier curves, i.e., the points having integer coordinates. Often, the manipulation of rational Bézier curves uses some auxiliary points of the curve (see for instance [7] where some points of the curve are used for interpolation). By knowing the integral points of such a curve and using them for its manipulation, the necessary computations will be simplified. Thus, we will deal with the cases where these curves have infinitely many integral points. More precisely, we give necessary and sufficient conditions on their weights to have infinitely many integral points which permit us to give algorithms for the construction of such rational Bézier curves. Furthermore, we present algorithms

2020 *Mathematics Subject Classification*: primary 65D17; secondary 14Q05, 14H25, 14H45, 14H50.

Key words and phrases: Bézier curve, rational Bézier curve, curve of genus 0, integral point.
Received April 19, 2022, revised October 2022. Editor C. Greither.
DOI: 10.5817/AM2023-4-339

for the computation of all the integral points of parametric space curves in cases where these curves have infinitely many integral points.

The paper is organised as follows. In Section 2, we give necessary and sufficient conditions for a parametric curve to have infinitely many integral points. In Section 3, we specialize these conditions for the rational Bézier curves in terms of theirs weights. Finally, Section 4 is devoted in the presentation of an algorithm for the computation of integral points of parametric space curves in these cases.

2. Curves with infinitely many integral points

Let $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$, and C an irreducible affine curve of (geometric) genus 0 in the affine space $\mathbb{A}^n_{\overline{\mathbb{Q}}}$ defined by a finite family of polynomials having integer coefficients. The points $(x_1, \dots, x_n)$ of C with $x_i \in \mathbb{Z}$ $(i = 1, \dots, n)$ are called *integral points* of C. We denote by $C(\mathbb{Z})$ the set of integral points on C. We denote by $\overline{\mathbb{Q}}(C)$ the function field of C, by $\overline{C}$ the Zariski closure of C in the projective space $\mathbb{P}^n$ and we set $C_\infty = (\overline{C} \setminus C)(\overline{\mathbb{Q}})$. We say that a discrete valuation ring U of $\overline{\mathbb{Q}}(C)$ *lies at infinity* if there is a point $P \in C_\infty$ such that U contains the local ring $O_P(C)$ of C at P and the maximal ideal of U contains the maximal ideal of $O_P(C)$. We denote by Σ_∞ the set of all the discrete valuation rings of $\overline{\mathbb{Q}}(C)$ at infinity. We call an element V of Σ_∞ *defined over a subfield* k of $\overline{\mathbb{Q}}(C)$, if $\tau(V) = V$ for every $\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/k)$. Furthermore, two elements V and W of Σ_∞ are said to be conjugate over a quadratic field k if V and W are defined over k and there is $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ which is not the identity on k such that $\sigma(V) = W$. By [4], we have the following result:

Theorem 1. *The set $C(\mathbb{Z})$ is infinite if and only if one of the following two conditions is satisfied:*

(a) *The set Σ_∞ consists of one element and $C(\mathbb{Z})$ contains at least one non-singular point.*

(b) *The set Σ_∞ consists of two elements which are conjugate over a real quadratic field and $C(\mathbb{Z})$ contains at least one non-singular point*

Suppose that C has a rational parametrization over $\mathbb{Q}$. Then, there are coprime homogeneous polynomials, $\phi_i(S,T)$ $(i = 0, \dots, n)$, of the same degree and with integer coefficients such that the map

$$\phi\colon \mathbb{P}^1 \longrightarrow \overline{C},\ (s:t) \longmapsto (\phi_0(s,t) : \dots : \phi_n(s,t))$$

is a birational isomorphism. The correspondence $f \mapsto f \circ \phi$ induces an isomorphism $\tilde{\phi}$ defined over $\mathbb{Q}$ from $\overline{\mathbb{Q}}(C)$ onto $\overline{\mathbb{Q}}(\mathbb{P}^1)$. If $f(s,t)$ is a homogeneous polynomial, then we set

$$Z(f) = \{(s:t) \in \mathbb{P}^1 /\ f(s,t) = 0\}.$$

Lemma 1. *The correspondence $P \mapsto \tilde{\phi}^{-1}(O_P(\mathbb{P}^1))$ defines a bijection from $Z(\phi_0)$ onto Σ_∞.*

Proof. The proof is an easy generalization of [5, Lemma 2.2]. □

The restriction of ϕ to $\mathbb{A}^1$ gives the map

$$\phi_a\colon \mathbb{A}^1 \longrightarrow C,\ t \longmapsto \left(\frac{\phi_1(1,t)}{\phi_0(1,t)} : \ldots : \frac{\phi_n(1,t)}{\phi_0(1,t)}\right).$$

Let $\mathcal{U}$ be the subset of $t \in \mathbb{A}^1$ with $\phi_0(1,t) \neq 0$. Combining Theorem 1 and Lemma 1, we deduce immediately the following result:

Theorem 2. *The set $C(\mathbb{Z}) \cap \phi_a(\mathcal{U})$ is infinite if and only if one of the following two conditions is satisfied:*

(a) *The set $\phi_a(\mathcal{U})$ contains an integral non-singular point, and $Z(\phi_0)$ has exactly one element.*

(b) *The set $\phi_a(\mathbb{Q})$ contains an integral non-singular point, and $Z(\phi_0) = \{(1 : a + b\sqrt{d}), (1 : a - b\sqrt{d})\}$, where $a, b, d \in \mathbb{Q}$, $b \neq 0$, and d is a square free integer > 1.*

3. Rational Bézier curves

In this section we specialize Theorem 2 for the case of rational Bézier curves. Let $F\colon \mathbb{A} \longrightarrow \mathbb{A}^3$ be a map defining a rational Bézier curve as in the Introduction. Set $\Pi_n(t) = w_0 B_0^n(t) + \cdots + w_n B_n^n(t)$. We have:

$$\Pi_n(t) = A_0 t^n + \cdots + A_n\,,$$

where

$$A_{n-k} = \sum_{j=0}^{k} w_j (-1)^{k-j} \binom{n}{j} \binom{n-j}{k-j}.$$

Lemma 2. *We have the following:*

a) *The polynomial $\Pi_n(t)$ has the form*

$$\Pi_n(t) = c(t-\alpha)^n\,,$$

where $c, \alpha \in \mathbb{Q} \setminus \{0\}$ if and only if we have

$$w_k = c(-1)^{n-k} \alpha^{n-k} (1-\alpha)^k \quad (k = 0, \ldots, n)\,.$$

b) *Let $u = \alpha + \beta\sqrt{d}$, where $\alpha, \beta \in \mathbb{Q}$ and d is a square-free positive integer, and $\bar{u} = \alpha - \beta\sqrt{d}$ the conjugate of u. The polynomial $\Pi_n(t)$ has the form*

$$\Pi_n(t) = c(t-u)^m (t-\bar{u})^m$$

if and only if $(w_0, \ldots, w_m)$ is the solution of the lower triangular linear system

$$\sum_{j=0}^{2m-l} w_j \binom{2m}{j} \binom{2m-j}{2m-l-j} (-1)^{2m-l-j} = \sum_{\substack{i+j=l \\ 0 \le i,j \le m}} \binom{m}{i} \binom{m}{j} u^i \bar{u}^j\,,$$

where $l = 2m, 2m-1, \ldots, 0\,.$

Proof. a) Setting
$$\Pi_n(t) = c(t-\alpha)^n\,,$$
where c, $\alpha \in \mathbb{Z}\setminus\{0\}$, we obtain the following linear system in unknowns $w_0,\dots,w_n$:
$$\sum_{j=0}^{k} w_j(-1)^{k-j}\binom{n}{j}\binom{n-j}{k-j} = c(-1)^{n-k}\alpha^{n-k}\binom{n}{k} \quad (k=0,\dots,n)\,.$$
We have $w_0 = c(-1)^n\alpha^n$ and $w_1 = c\alpha^{n-1}(-1)^{n-1}(1-\alpha)$. Suppose that $w_s = c(-1)^{n-s}\alpha^{n-s}(1-\alpha)^s$ $(s=2,\dots,k-1)$. Then, we get:
$$\begin{aligned}
w_k &= c(-1)^{n-k}\alpha^{n-k} - \binom{n}{k}^{-1}\sum_{j=0}^{k-1} w_j(-1)^{k-j}\binom{n}{j}\binom{n-j}{k-j}\\
&= c(-1)^{n-k}\alpha^{n-k} - c\sum_{j=0}^{k-1}(-1)^{n-j}\alpha^{n-j}(1-\alpha)^j(-1)^{k-j}\binom{k}{j}\\
&= c(-1)^{n-k}\alpha^{n-k}\left(1-\sum_{j=0}^{k-1}\alpha^{k-j}(1-\alpha)^j\binom{k}{j}\right)\\
&= c(-1)^{n-k}\alpha^{n-k}\left((1-\alpha)^k + 1 - \sum_{j=0}^{k}\alpha^{k-j}(1-\alpha)^j\binom{k}{j}\right)\\
&= c(-1)^{n-k}\alpha^{n-k}\left((1-\alpha)^k + 1 - (\alpha+1-\alpha)^k\right)\\
&= c(-1)^{n-k}\alpha^{n-k}(1-\alpha)^k\,.
\end{aligned}$$
Hence, we deduce that $w_k = c(-1)^{n-k}\alpha^{n-k}(1-\alpha)^k$ $(k=0,\dots,n)$.

b) Setting
$$\Pi_n(t) = c(t-u)^m(t-\bar{u})^m$$
we deduce the following linear system in unknowns $w_0,\dots,w_n$:
$$\sum_{j=0}^{2m-l} w_j\binom{2m}{j}\binom{2m-j}{2m-l-j}(-1)^{2m-l-j} = c\sum_{\substack{i+j=l\\0\le i,j\le m}}\binom{m}{i}\binom{m}{j}(-u)^i(-\bar{u})^j\,,$$
where $l = 2m, 2m-1,\dots,0$. This system is a lower triangular linear system with nonzero determinant, and so it has a unique solution which is easily computable. □

Thus we have the following result:

Theorem 3. *The rational Bézier curve given by F has infinitely many integral points if and only if the trace of F contains an integral non-singular point and one of the following two conditions is satisfied:*

(a) *We have $w_k = c(-1)^{n-k}\alpha^{n-k}(1-\alpha)^k$ $(k=0,\dots,n)$.*

(b) *The vector $(w_0,\dots,w_m)$ is the solution of the linear system*
$$\sum_{j=0}^{2m-l} w_j\binom{2m}{j}\binom{2m-j}{2m-l-j}(-1)^{2m-l-j} = \sum_{\substack{i+j=l\\0\le i,j\le m}}\binom{m}{i}\binom{m}{j}u^i\bar{u}^j\,,$$

where $l = 2m, 2m-1, \ldots, 0$.

We shall use the above Theorem 3 for the presentation of two algorithms which provide rational Bézier curves having infinitely many integral points.

Algorithm 1. Construction of a rational Bézier curve of degree n having infinitely many integral points and $\Pi_n(t)$ has only one root.

1. Select $c, \alpha \in \mathbb{Z} \setminus \{0,1\}$ and compute $w_k = c(-1)^{n-k}\alpha^{n-k}(1-\alpha)^k$ $(k = 0, \ldots, n)$.
2. Select $n+1$ distinct points $P_i \in \mathbb{A}^n$ $(i = 0, \ldots, n)$ such that the coordinates of P_0 are integers.
3. Output the rational Bézier curve defined by

$$F(t) = \frac{w_0 P_0 B_0^n(t) + \cdots + w_n P_n B_n^n(t)}{c(t-\alpha)^n}.$$

Proof of correctness of Algorithm 1. By Lemma 2(a), we deduce that

$$\Pi_n(t) = c(t-\alpha)^n\,.$$

On the other hand, we have $F(0) = P_0$ and so, the curve F has an integral point. Furthermore, by [1, Section 4.3] the derivative of F at P_0 is

$$F'(0) = \frac{nw_1}{w_0}\ \overrightarrow{P_0P_1} \neq 0\,,$$

where $\overrightarrow{P_0P_1}$ denotes the vector that points from P_0 to P_1. Then, P_0 is a non-singular point of F. □

Example 1. We shall construct a rational Bézier curve of degree 3 with infinitely many integral points using Algorithm 1. We take $c = 1$, $\alpha = -1$ and we compute

$$w_0 = 1\,, \quad w_1 = 2\,, \quad w_2 = 4\,, \quad w_3 = 8\,.$$

Next, we select the points

$$P_0 = (1,0,1)\,, \quad P_1 = (0,1,2/3)\,, \quad P_2 = (1,1/4,0)\,, \quad P_3 = (2,0,1/2)\,.$$

Thus, we obtain the curve

$$\begin{aligned} F(t) &= \frac{P_0B_0^3(t) + 2P_1B_1^3(t) + 4P_2B_2^3(t) + 8P_3B_3^3(t)}{(t+1)^3} \\ &= \frac{1}{(t+1)^3}\ (3t^3 + 15t^2 - 3t + 1, 3t^3 - 9t^2 + 6t, 7t^3 - 5t^2 + t + 1) \end{aligned}$$

which is a rational Bézier curve having infinitely many integral points.

Algorithm 2. Construction of a rational Bézier curve of degree $2m$ having infinitely many integral points and $\Pi_{2m}(t)$ has only two roots of the form $\alpha \pm \beta\sqrt{d}$, where $\alpha, \beta, d \in \mathbb{Z}$, $\beta \neq 0$ and d square free > 1.

1. Select $\alpha, \beta, c, d \in \mathbb{Z}$, $\beta c \neq 0$ and d square free > 1. Put $u = \alpha + \beta\sqrt{d}$ and $\bar{u} = \alpha - \beta\sqrt{d}$ and find the unique solution of the lower triangular linear system:

$$\sum_{j=0}^{2m-l} w_j \binom{2m}{j}\binom{2m-j}{2m-l-j}(-1)^{2m-l-j} = c \sum_{\substack{i+j=l \\ 0\le i,j\le m}} \binom{m}{i}\binom{m}{j}(-u)^i(-\bar{u})^j\,,$$

where $l = 2m, 2m-1, \ldots, 0$.

2. Select $2m+1$ distinct points $P_i \in \mathbb{A}^n$ $(i = 0, \ldots, 2m)$ such that the coordinates of P_0 are integers.

3. Output the rational Bézier curve defined by

$$F(t) = \frac{w_0 P_0 B_0^{2m}(t) + \cdots + w_{2m} P_{2m} B_{2m}^{2m}(t)}{c(t-u)^m (t-\bar{u})^m}\,.$$

Proof of correctness of Algorithm 2. By Lemma 2(b), we deduce that

$$\Pi_n(t) = c(t-u)^m(t-\bar{u})^m\,.$$

Since we have $F(0) = P_0$, the curve F has an integral point. Further, by [1, Section 4.3] the derivative of F at P_0 is

$$F'(0) = \frac{nw_1}{w_0}\ \overrightarrow{P_0P_1} \neq 0\,,$$

and, so, P_0 is a non-singular point of F. $\square$

Example 2. We shall construct a rational Bézier curve of degree 4 with infinitely many integral points using Algorithm 2. We take $c = 1$, $\alpha = 5$, $\beta = 3$ and $d = 2$. For the computation of the appropriate weights $w_0, \ldots, w_4$ we have the following linear system:

$$\begin{aligned} w_0 &= 49 \\ -w_0 + w_1 &= -35 \\ w_0 + 3w_1 - 3w_2 + w_3 &= -5 \\ w_0 - 4w_1 + 6w_2 - 4w_3 &= 1\,. \end{aligned}$$

Thus, we have:

$$w_0 = 49\,,\quad w_1 = 14\,,\quad w_2 = -2\,,\quad w_3 = -4\,,\quad w_4 = 4\,.$$

Next, we select the points

$$\begin{aligned} &P_0 = (0,1,1)\,, \qquad P_1 = (1,1,0)\,, \quad P_2 = (1/2,0,0)\,, \\ &P_3 = (1,1,-1/2)\,, \quad P_4 = (2,1/2,-1)\,. \end{aligned}$$

Thus, we obtain the curve

$$\begin{aligned} F(t) &= \frac{49P_0B_0^4(t) + 14P_1B_1^4(t) - 2P_2B_2^4(t) - 4P_3B_3^4(t) + 4P_4B_4^4(t)}{(t-(5+3\sqrt{2}))^2\ (t-(5-3\sqrt{2}))^2} \\ &= \frac{1}{t^4 - 20t^3 + 114t^2 - 140t + 49}(f_1(t), f_2(t), f_3(t))\,, \end{aligned}$$

where

$$f_1(t) = -38t^4 + 164t^3 - 174t^2 + 56t\,, \quad f_2(t) = 11t^4 - 44t^3 + 126t^2 - 140t + 49$$

and

$$f_3(t) = 45t^4 - 188t^3 + 294t^2 - 196t + 49\,.$$

4. Computation of integral points

Consider the rational map

$$\phi\colon \mathbb{A}^1 \longrightarrow \mathbb{A}^3,\ t \longmapsto \left(\frac{\phi_1(t)}{\phi_0(t)}, \frac{\phi_2(t)}{\phi_0(t)}, \frac{\phi_3(t)}{\phi_0(t)}\right)\,,$$

where $\phi_i(t) \in \mathbb{Z}[t]$ $(0,1,2,3)$ and $\gcd(\phi_0(t), \phi_1(t), \phi_2(t), \phi_3(t)) = 1$. The Zariski closure of $\phi(\mathbb{A}^1)$ in $\mathbb{A}^3$ is an affine curve $\mathcal{K}$ of genus 0. Consider the set:

$$I_{\mathcal{K}} = \phi(\mathbb{Q}) \cap \mathbb{Z}^3\,.$$

Let N be the maximum of the degrees of the polynomials $\phi_i(t)$ $(i = 0,1,2,3)$. We put $\psi_i(s,t) = s^{N-\deg\phi_i}\phi_{h,i}(s,t)$ $(i = 0,1,2,3)$, where $\phi_{h,i}(s,t)$ is the homogenization of $\phi_i(t)$. Thus the correspondence

$$(s : t) \longmapsto \big(\psi_0(s,t) : \psi_1(s,t) : \psi_2(s,t) : \psi_3(s,t)\big)$$

defines a rational map $\psi\colon \mathbb{P}^1 \to \mathbb{P}^3$ whose restriction on $\mathbb{A}^1$ is ϕ, and its image is the projective closure $\bar{\mathcal{K}}$ of $\mathcal{K}$. We shall give two algorithms for the computation of the elements of $I_{\mathcal{K}}$ in cases where this set is infinite (see Theorem 2). They are variants of the algorithms presented in [6].

Algorithm 3.
Input: A rational map $F\colon \mathbb{A}^1 \to \mathbb{A}^3$, as above.
Output: The elements of the set $I_{\mathcal{K}}$.

1. Factorize over $\mathbb{Q}$ the polynomial $\psi_0(s,t)$. If $\psi_0(s,t) = a(bs+ct)^N$, where $a \neq 0$ and $\gcd(b,c) = 1$, go to the next step, else output “FAIL”.

2. If $bc \neq 0$, then we set $s = v$, $t = (u - bv)c^{-1}$. Otherwise, we set $s = u$, $t = v$ if $(b,c) = (1,0)$, and $t = u$, $s = v$ if $(b,c) = (0,1)$. Thus we obtain a birational map

$$\omega\colon \mathbb{P}^1 \longrightarrow \bar{\mathcal{K}},\ (u : v) \longmapsto (p_1(u,v) : p_2(u,v) : p_3(u,v) : du^N)\,,$$

where d is a nonzero integer (with $d|ac^N$) and $p_i(u,v)$ have integer coefficients.

3. Let a_i be the coefficient of v^N in $p_i(u,v)$. Compute $\delta = \gcd(a_1,a_2,a_3)$.

4. Determine the set Σ of integers η such that

$$p_i(\delta,\eta) \equiv 0 \pmod{d\delta^N} \quad (i = 1,2,3)\,.$$

5. For every $\eta \in \Sigma$, compute the values

$$x_i = \frac{p_i(\delta,\eta)}{d\delta^N} \quad (i = 1,2,3)\,.$$

6. Output the points (x_1,x_2,x_3) computed in the previous step.

Proof of correctness of Algorithm 3. Suppose that $(x_1, x_2, x_3) \in I_{\mathcal{K}}$. Then, there are coprime integers u_0, v_0 such that $u_0 \neq 0$ and

$$x_i = \frac{p_i(u_0, v_0)}{du_0^N} \quad (i = 1, 2, 3)\,.$$

Since $\phi_0(t)$, $\phi_1(t)$, $\phi_2(t)$, $\phi_3(t))$ are coprime, it follows that $p_0(t)$, $p_1(t)$, $p_2(t)$, $p_3(t)$ are coprime, and so $(a_1, a_2, a_3) \neq (0, 0, 0)$. Let $\delta = \gcd(a_1, a_2, a_3)$. Thus, u_0 divides δ. Setting $\eta = v_0\delta/u_0$, we obtain

$$x_i = \frac{p_i(\delta, \eta)}{d\delta^N} \quad (i = 1, 2, 3)$$

and hence $\eta \in \Sigma$. Conversely, every point of this form belongs to $I_{\mathcal{K}}$. $\square$

Example 3. We shall compute the integral points of the rational Bézier curve of Example 1 defined by the rational map:

$$\begin{aligned} F(t) &= \frac{P_0B_0^3(t) + 2P_1B_1^3(t) + 4P_2B_2^3(t) + 8P_3B_3^3(t)}{(t+1)^3} \\ &= \left(\frac{3t^3 + 15t^2 - 3t + 1}{(t+1)^3}, \frac{3t^3 - 9t^2 + 6t}{(t+1)^3}, \frac{7t^3 - 5t^2 + t + 1}{(t+1)^3}\right)\,. \end{aligned}$$

We apply Algorithm 3. Thus, the corresponding projective map $\tilde{F}\colon \mathbb{P}^1 \mapsto \mathbb{P}^3$ is defined by

$$\tilde{F}(s:t) = (p_1(s,t) : p_2(s,t) : p_3(s,t) : (t+s)^3)\,,$$

where

$$p_1(s,t) = 3t^3 + 15t^2s - 3ts^2 + s^3, \quad p_2(s,t) = 3t^3 - 9t^2s + 6ts^2\,,$$
$$p_3(s,t) = 7t^3 - 5t^2s + ts^2 + s^3\,.$$

Setting $s = v$, $t = u - v$, we obtain the polynomials:

$$\begin{aligned} q_1(u,v) &= p_1(v, u-v) = 3u^3 + 6u^2v - 24uv^2 + 16v^3\,, \\ q_2(u,v) &= p_2(v, u-v) = 3u^3 - 18u^2v + 33uv^2 - 18v^3\,, \\ q_3(u,v) &= p_3(v, u-v) = 7u^3 - 26u^2v + 32uv^2 - 12v^3\,. \end{aligned}$$

Next, we compute $\delta = \gcd(16, 18, 12) = 2$, and consider the polynomial congruences

$$q_i(2, \eta) \equiv 0 \pmod 8 \quad (i = 1, 2, 3)\,.$$

For $i = 1$, we have the congruence $6\eta^3 \equiv 0 \pmod 8$, whence $3\eta^3 \equiv 0 \pmod 4$, and so $\eta \equiv 0, 2 \pmod 4$. For $i = 2$, we have $-2\eta^3 + 2\eta^2 \equiv 0 \pmod 8$, whence $-\eta^3 + \eta^2 \equiv 0 \pmod 4$, and so, we have $\eta \equiv 0, 1, 2 \pmod 4$. For $i = 3$, we get $4\eta^3 \equiv 0 \pmod 8$, and so $\eta \equiv 0 \pmod 2$. The common solutions of the above congruences are:

$$\eta \equiv 0, 2 \pmod 4\,.$$

Thus, we have

$$\eta = 4k, 2 + 4k\,, \quad k \in \mathbb{Z}\,.$$

For $\eta = 4k$, we get:

$$x_{k,1} = \frac{q_1(2,4k)}{8} = 128k^3 - 96k^2 + 12k + 3\,,$$

$$x_{k,2} = \frac{q_2(2,4k)}{8} = -144k^3 + 132k^2 - 36k + 3\,,$$

$$x_{k,3} = \frac{q_3(2,4k)}{8} = -96k^3 + 128k^2 - 52k + 7\,.$$

Therefore, we obtain the integral points $P_k = (x_{k,1}, x_{k,2}, x_{k,3})$, $k \in \mathbb{Z}$. For $\eta = 2+4k$, we have:

$$y_{k,1} = \frac{q_1(2,2+4k)}{128} = 128k^3 + 96k^2 + 12k + 1\,,$$

$$y_{k,2} = \frac{q_2(2,2+4k)}{128} = -144k^3 - 84k^2 - 12k\,,$$

$$y_{k,3} = \frac{q_3(2,2+4k)}{128} = -96k^3 - 16k^2 + 4k + 1\,.$$

Thus, we obtain the integral points $Q_k = (y_{k,1}, y_{k,2}, y_{k,3})$, $k \in \mathbb{Z}$. It follows that the integral points of F are P_k and Q_k, $k \in \mathbb{Z}$.

Algorithm 4.
Input: A rational map $F\colon \mathbb{A}^1 \longrightarrow \mathbb{A}^3$, as above.
Output: The elements of the set $I_{\mathcal{K}}$.

1. Factorize over $\mathbb{Q}$ the polynomial $\psi_0(s,t)$. If

$$\psi_0(s,t) = k(as^2 + bst + ct^2)^{N/2}\,,$$

with $\delta = b^2 - 4ac > 0$, then go to the next step, else output "FAIL".

2. Setting $u = 2as + bt$ and $v = t$, we compute a birational morphism

$$\omega\colon \mathbb{P}^1 \longrightarrow \bar{\mathcal{K}},\ (u:v) \longmapsto (p_1(u,v) : p_2(u,v) : p_3(u,v) : m(u^2 - \delta v^2)^{N/2})\,,$$

where $p_i(u,v)$ $(i = 1,2,3)$ are homogeneous polynomials in $\mathbb{Z}[u,v]$ of degree N and m a non-zero integer.

3. For $i = 1,2,3$, compute the resultant R_i of $p_i(u,1)$ and $u^2 - \delta$.
4. Compute $D = \gcd(R_1, R_2, R_3)$.
5. Determine the set

$$\Sigma = \{(u,v) \in \mathbb{Z}^2 /\ \gcd(u,v) = 1\,,\ u \geq 0\,,\ u^2 - \delta v^2 | D\}\,.$$

6. For every $(u,v) \in \Sigma$, compute the values

$$x_i = \frac{p_i(u,v)}{m(u^2 - \delta v^2)^{N/2}} \quad (i = 1,2,3)\,.$$

7. Output the triples (x_1, x_2, x_3), where $x_1, x_2, x_3 \in \mathbb{Z}$, computed in the previous step.

Proof of correctness of Algorithm 4. Suppose that $(x_1, x_2, x_3) \in I_{\mathcal{K}}$. Then, there are coprime integers u_0, v_0 such that $u \neq 0$ and

$$x_i = \frac{p_i(u_0, v_0)}{m(u_0^2 - \delta v_0^2)^{N/2}} \quad (i = 1, 2, 3)\,.$$

Since the polynomials $p_i(u, v)$ $(i = 1, 2, 3)$ and $u^2 - \delta v^2$ have no common non-constant factor, it follows that one of the resultants R_i is not zero, and so $D \neq 0$. Suppose that $R_i \neq 0$. There are polynomials $B(u)$ and $C(u)$ with integer coefficients such that

$$R_i = B(u)p_i(u, 1) + C(u)(u^2 - \delta)\,.$$

Homogenizing this equation, we obtain

$$R_i v^r = p_i(u, v)B(u, v) + C(u, v)(u^2 - \delta v^2)\,,$$

where r is a positive integer and $B(u, v)$, $C(u, v)$ are homogeneous polynomials such that their dehomogenizations with respect to v are $B(u)$ and $C(u)$, respectively. If $(u_0, v_0) \neq (1, 0)$, then $u_0^2 - \delta v_0^2$ divides $R_1 v_0^r$. Since $\gcd(u_0^2 - \delta v_0^2, v_0) = 1$, we deduce that $u_0^2 - \delta v_0^2$ divides R_i, and so, $u_0^2 - \delta v_0^2$ divides D. Hence $(u, v) \in \Sigma$. Thus, (x_1, x_2, x_3) is given by the algorithm. $\square$

Example 4. We shall compute the integral points of the rational Bézier curve of Example 2 defined by the rational map:

$$F(t) = \frac{1}{t^4 - 20t^3 + 114t^2 - 140t + 49}(f_1(t), f_2(t), f_3(t))\,,$$

where

$$\begin{aligned} f_1(t) &= -38t^4 + 164t^3 - 174t^2 + 56t\,, \\ f_2(t) &= 11t^4 - 44t^3 + 126t^2 - 140t + 49\,, \\ f_3(t) &= 45t^4 - 188t^3 + 294t^2 - 196t + 49\,. \end{aligned}$$

The Zariski closure of $F(\mathbb{A}^1)$ in $\mathbb{A}^3$ is an affine curve $\mathcal{K}$. We denote by $\bar{\mathcal{K}}$ its projective closure. We have the birational morphism

$$\psi \colon \mathbb{P}^1 \longrightarrow \bar{\mathcal{K}}, (s : t) \longmapsto ((7s^2 - 10ts + t^2)^2 : \psi_1(s, t) : \psi_2(s, t) : \psi_3(s, t))\,,$$

where $\psi_i(s, t)$ is the homogenization of $f_i(t)$ $(i = 1, 2, 3)$. Setting $u = 14s - 10t$, $v = t$, we have $s = (u + 10v)/14$ and $t = v$. Thus, we obtain the birational morphism

$$\omega \colon \mathbb{P}^1 \longrightarrow \bar{\mathcal{K}},\ (u : v) \longmapsto ((u^2 - 72v^2)^2 : p_1(u, v) : p_2(u, v) : p_3(u, v))\,,$$

where

$$p_1(u, v) = 8(2u^3 v - 27u^2 v^2 + 8uv^3 + 1056v^4)\,,$$

$$p_2(u, v) = u^4 - 96u^2 v^2 - 384uv^3 + 4384v^4\,,$$

$$p_3(u, v) = u^4 - 16u^3 v + 96u^2 v^2 + 192uv^3 + 1600v^4\,.$$

Now, we compute the resultant R_i of $p_i(u,1)$ and u^2-72 $(i=1,2,3)$. We have $R_1=R_2=R_3=1$, and so, $D=\gcd(R_1,R_2,R_3)=1$. Next, we shall compute the set

$$\Sigma=\{(u,v)\in\mathbb{Z}^2/\ u\geq 0,\ u^2-72v^2=\pm 1\}.$$

If $u^2-72v^2=-1$, then $u^2\equiv -1 \pmod 4$ which is a contradiction. Further, the integer solutions of the Pell equation $u^2-72v^2=1$, with $u\geq 0$, are given by

$$u_n+v_n\sqrt{72}=(17\pm 2\sqrt{72})^n,\quad (n=1,2,\ldots),$$

whence we get:

$$u_n=\sum_{l=0}^{\lfloor n/2\rfloor}\binom{n}{2l}17^{n-2l}2^{2l}72^l,\quad v_n=\pm\sum_{l=0}^{\lfloor (n-1)/2\rfloor}\binom{n}{2l+1}17^{n-2l-1}2^{2l+1}72^l,$$

where $n=1,2,\ldots$. Therefore, the integral points of F are given by the following triples:

$$(p_1(u_n,v_n),p_2(u_n,v_n),p_3(u_n,v_n)),\quad (n=1,2,\ldots).$$

Acknowledgement. The author wishes to thank Professor Dimitrios Poulakis for helpful suggestions and beneficial conversations, and the anonymous referee for useful remarks and comments.

References

[1] Farine, G., *Curves and Surfaces for CAGD. A Practical Guide*, fifth ed., Academic Press, 2002.

[2] Hoschek, J., Lasser, D., *Fundamentals of Computer Aided Geometric Design*, AK Peters, 1993.

[3] Mortenson, M.E., *Geometric Modelling*, Industrial Press Inc., 2006.

[4] Poulakis, D., *Affine curves with infinitely many integral points*, Proc. Amer. Math. Soc. **131** (2) (2002), 1357–1359.

[5] Poulakis, D., Voskos, E., *On the practical solution of genus zero Diophantine equations*, J. Symbolic Comput. **30** (2000), 573–582.

[6] Poulakis, D., Voskos, E., *Solving genus zero Diophantine equations with at most two infinite valuations*, J. Symbolic Comput. **33** (2002), 479–491.

[7] Ramanantoanina, A., Hormann, K., *New shape control tools for rational Bézier curve design*, Comput. Aided Geom. Design **88** (2021), 11 pp., 102003.

Department of Chemical Engineering,
University of West Macedonia,
Kila, 501 50, Kozani, Greece
E-mail: petroula.dospra@gmail.com