Mathematische Zeitschrift (2022) 301:3609–3616
https://doi.org/10.1007/s00209-022-03030-7

Mathematische Zeitschrift

Integral points on curves $\frac{f(X)-f(Y)}{X-Y}$

Umberto Zannier[1]

Received: 14 February 2022 / Accepted: 5 March 2022 / Published online: 28 April 2022

Abstract
The following short article first arose as an Appendix to the paper *Counting points of bounded height in monoid orbits*, by WADE HINDES, which appears just above in this journal. Subsequently, due to the general nature of the underlying problem, we thought that the result could have further applications, and could be easily overlooked if it appeared as an appendix. So, with the welcome kind help of the Editors, we decided to publish the result separately.

1 Introduction

The general issue treated here concerns the *values attained more than once* by a polynomial f over a given ring. This issue may be translated into the equation $f(X) = f(Y)$, to be solved with X, Y over the ring in question, and where we prescribe that X, Y should be in fact *distinct*. In turn, this corresponds to seeking the points, defined over the said ring, of the plane curve defined by the polynomial

$$F(X, Y) = \frac{f(X) - f(Y)}{X - Y}. \tag{1}$$

A very natural case arises when f has coefficients in $\mathbb{Q}$ and the ring is $\mathbb{Z}$ or a ring of S-integers in a number field.[1] But let us proceed more generally, restricting merely to zero characteristic.

So, let $f \in \mathbb{C}[X]$ be a complex polynomial of degree $d \geq 2$ and let $\mathcal{O}$ be a finitely generated subring of $\mathbb{C}$. We seek conditions for the curve defined by $F(X, Y) = 0$ to have infinitely many points with $X, Y \in \mathcal{O}$.

Before stating the results, recall that the *cyclic polynomial* of degree n is simply X^n, whereas the *Chebyshev polynomial* of degree n is the unique polynomial T_n satisfying the identity $T_n(Z+Z^{-1}) = Z^n+Z^{-n}$. One can check that it has integer coefficients (for instance by induction).

These polynomials are quite remarkable, in particular in the theory of *composition* of rational functions (see e.g., A. SCHINZEL's book [7]). For instance, if S_n is either the cyclic

[1] Recall that the S-integers of a number field K are those elements of K whose denominator is divisible only by prime ideals in the set S, usually assumed to be finite.

✉ Umberto Zannier
umberto.zannier@sns.it

[1] Scuola Normale Superiore, Piazza dei Cavalieri, 7, 56126 Pisa, Italy

or the Chebyshev polynomial of degree n, then for integers $n, m \geq 0$ we have the identities $S_{nm}(x) = (S_n \circ S_m)(x) =: S_n(S_m(x))$.

A purpose of the present note is to prove, in particular, the following

Theorem 1.1 *Assume that the plane curve defined by $F(X, Y)$ has infinitely many points in $\mathcal{O}^2$. Then there are an integer $n > 1$ and polynomials $g, l \in \mathbb{C}[X]$, with $\deg l = 1$, such that $f = g \circ S_n \circ l$, where S_n is either the cyclic or the Chebyshev polynomial of degree n.*

Below we shall give more precise results, in particular about the identities in the statement, which allow a full description of the solutions (for instance as in (iii) of next subsection).

1.1 Some converse results

In this short subsection we shall very briefly discuss some conclusions in the converse direction. Indeed, the theorem has an easy converse, at any rate as soon as we allow a bit of freedom on $\mathcal{O}$, as we are going to illustrate. Note that some conditions on $\mathcal{O}$ are indeed necessary for the infinitude of integral points arising from a general decompositions as in the statement. For instance, we shall see in Remark 1.2 that in the most natural case $\mathcal{O} = \mathbb{Z}$ it turns out (moreover with a simple argument) that in the theorem we can limit to $n \leq 2$ and that all but finitely many solutions lie on a fixed line $X + Y = c$.

Let us briefly see what can happen in general, where we assume, on applying first l^{-1}, that the linear polynomial l is the identity.

(i) `Cyclic case`. When we may take $S_n(X) = X^n$ in the theorem, we obtain factors (after applying l^{-1}) $X - \zeta Y$ ($\zeta^n = 1, \zeta \neq 1$) for our polynomial $F(X, Y)$, i.e. components of the curve which are lines through the origin, defined over $\mathbb{Q}(\zeta)$. Therefore we obtain infinitely many points in $\mathcal{O}^2$ corresponding to that factor if and only if the field of quotients of $\mathcal{O}$ contains ζ.

(ii) `Chebyshev case`. In the case $S_n = T_n$, from the defining property of T_n we easily obtain the complete factorisation of $(T_n(X) - T_n(Y))/(X - Y)$ given by the (well-known) factors $X^2 - (\zeta + \zeta^{-1})XY + Y^2 + (\zeta - \zeta^{-1})^2$, for $\zeta \neq \pm 1$ an n-th root of unity.

If the equation corresponding to such factor has infinitely many solutions in $\mathcal{O}$, then the field of quotients of $\mathcal{O}$ must contain $\sigma := \zeta + \zeta^{-1}$, and then it contains automatically $(\zeta - \zeta^{-1})^2 = \sigma^2 - 4 =: \Delta$. Note that if e.g. $\mathcal{O}$ is integrally closed then actually $\mathcal{O}$ must contain σ. Let us then assume that $\mathcal{O}$ itself contains σ.

We may write the equation in the Pell shape $(2X - \sigma Y)^2 - \Delta Y^2 = -4\Delta$. We are going to show that this has infinitely many solutions in $\mathcal{O}$ as soon as $\mathcal{O}$ contains σ.

For this, we also use the Chebyshev polynomials of the second kind U_n defined by the identity $U_n(Z + Z^{-1}) = \frac{Z^n - Z^{-n}}{Z - Z^{-1}}$. Like the T_n, they have integer coefficients.

Let t_n, u_n be defined formally by

$$\frac{t_n \pm u_n\sqrt{\Delta}}{2} = \left(\frac{\sigma \pm \sqrt{\Delta}}{2}\right)^n, \qquad n = 1, 2, \ldots.$$

(This corresponds to working in the algebra $\mathcal{O}[X]/(X^2 - \Delta)$, even if Δ is a square in $\mathcal{O}$.) Then, on setting $Z = (\sigma + \sqrt{\Delta})/2$ in the defining identities for T_n, U_n and noting that $Z^{-1} = (\sigma - \sqrt{\Delta})/2$, we find that

$$t_n^2 - \Delta u_n^2 = 4, \qquad t_n = T_n(\sigma), \quad u_n = U_n(\sigma).$$

The last two equations imply that $t_n, u_n \in \mathcal{O}$. The first equation yields, after multiplication by $-\Delta$, $(\Delta u_n)^2 - \Delta t_n^2 = -4\Delta$. We may now put $Y_n := t_n$, $2X_n := \sigma Y_n + \Delta u_n = \sigma t_n + \Delta u_n$ and obtain a solution of the original equation $X^2 - (\zeta + \zeta^{-1})XY + Y^2 + (\zeta - \zeta^{-1})^2 = 0$.

We have still to check that $X_n \in \mathcal{O}$. For this, observe that the definition yields $2X_n + 4u_n = \sigma(t_n + \sigma u_n) = \sigma(T_n(\sigma) + \sigma U_n(\sigma))$. However the defining identities easily give

$$T_n(X) + XU_n(X) = 2U_{n+1}(X).$$

Hence we eventually find $X_n = \sigma U_{n+1}(\sigma) - 2u_n = \sigma u_{n+1} - 2u_n$, which indeed lies in $\mathcal{O}$. This yields an infinity of solutions in $\mathbb{Z}[\sigma]$, hence in $\mathcal{O}$.

Similarly , we also obtain quadratic factors of $T_n(X) + T_n(Y)$, which are relevant when $g(X) = h(X^2)$ is even. These factors divide also $T_{2n}(X) - T_{2n}(Y)$, since $T_{2n} = T_2 \circ T_n = T_n^2 - 2$. We omit the corresponding discussion of the integer solutions, which is similar to the former.

This analysis does not take the polynomial g into consideration. However, if n is maximal for the conclusion of the theorem, all but finitely many solutions may arise only from the factors that we have taken into account; see also next point (iii). In any case, we do not expand the analysis here, we consider the above discussion as sufficient for our purposes.

(iii) `Full description of solutions`. In the next version of the result, i.e. Theorem 1.3 below, we shall add a further conclusion which implies that all but finitely many integral points arise in this way, i.e. from some decomposition as in Theorem 1.1. More precisely, saying that an integral point (u, v) (such that $f(u) = f(v)$) 'comes' from a decomposition $F = g \circ S_n \circ l$, we mean that $S_n(l(u)) = S_n(l(v))$, so in turn the point $(l(u), l(v))$ is a zero of an irreducible factor of $S_n(X) - S_n(Y)$.

We also note that, since the factors which arise from the various components appear as factors of $F(X, Y)$, it follows that these decompositions are finite in number. In a sense, this allows to answer completely the question of the infinitude of the integral points, once the ring is given, in view of the factorisations and the analysis given in (i) and (ii).

1.2 Integral points on curves

Let us now comment on the nature of Theorem 1.1. We recall at once that in virtue of SIEGEL's Theorem (extended suitably to finitely generated subrings) an *irreducible* `affine` curve can have can have infinitely many (integral) points defined over $\mathcal{O}$ only if

(i) it has genus 0

and

(ii) it has at most two points at infinity.

Here by *points at infinity* we mean the missing points with respect to the closure of the curve in some projective space. This number may increase by passing to a smooth model, but the theorem applies to any model.

The original version by C.L. SIEGEL was over $\mathbb{Z}$, and was extended later by K. MAHLER to the rings of S-integers in a number field. See any of the books [2], [5], or [8] for proofs of this result, which is of deep nature. See also the paper [3] for a proof by P. CORVAJA and the author, depending on the SCHMIDT's *Subspace Theorem*. See further the booklet [9] for SIEGEL's original 1929 article and a translation of it in English, together with a commentary by C. FUCHS and the present author.

In general, the deep result of SIEGEL reduces our problem to investigate when the (possibly reducible) curve defined by $F(X, Y)$ has a component satisfying the above 'SIEGEL conditions' (i) and (ii) (which cannot generally be avoided or improved).

Remark 1.2 We pause to note that in the natural case when f has coefficients in $\mathbb{Q}$ and the ring $\mathcal{O}$ is $\mathbb{Z}$, there is an easy argument for our main problem, avoiding completely SIEGEL's theorem and leading to a simple conclusion for our basic question. For completeness we give this self-contained argument here.

We are interested in the infinitude of the solutions $m \neq n$ in $\mathbb{Z}$ of the equation $f(m) = f(n)$, where $f \in \mathbb{Q}[X]$. By a translation in $\mathbb{Q}$ we may assume that f has vanishing second coefficient, at the cost of allowing m, n to be rationals with a bounded denominator. Under this normalisation (performed also in the proof below), the equation immediately leads to the estimate $|m^d - n^d| = O(\max(|m|, |n|)^{d-2})$, where $d := \deg f$. On the other hand, on factoring the left-hand side as $\prod_{\zeta^d=1} |m - \zeta n|$, we see that it is $\gg |m \pm n| \max(|m|, |n|)^{d-1}$ for some choice of the sign (where the minus sign may occur only if d is even). For large enough $\max(|m|, |n|)$ this implies that $m = \pm n$, so, since we assume $m \neq n$, we have eventually $m = -n$ and an identity $f(X) = f(-X)$, i.e. f is even. Taking into account that we have performed a translation, we see that all but finitely many solutions are given by $m + n = -2b/(ad)$, where a, b are the first two coefficients of f.

1.3 Irreducible factors of $F(X, Y)$

In the general case, in turn, the issue of the *components* of the curve $F(X, Y) = 0$ leads in the first place to the need to establish *when the defining polynomial F can be reducible*, which itself is an interesting and subtle problem. If f is *indecomposable* (i.e. not of the shape $g \circ h$ for polynomials g, h of degree > 1) then the correct condition was found by M. FRIED [4]: namely, *F is irreducible unless $f(X)$ is either a cyclic or a Chebyshev polynomial up to a linear change of variable*, which of course corresponds to our conclusion. (See also SCHINZEL's book [7], especially 1.5, where fields of definitions are considered as well, which instead we disregard here.) An application of FRIED's result would then directly yield the present theorem in the indecomposable cases.

However, if f is decomposable, say $f = g \circ h$, then certainly $F(X, Y)$ is anyway reducible (with a factor $(h(X) - h(Y))/(X - Y)$), and the issue leads to more delicate problems concerning the nature of all the irreducible factors. In the paper [1] of R. AVANZI with the present author, a laborious classification is obtained for all the cases when there is a factor defining a curve of genus 0. The results of [1] depend on some finite-group theory, which is used to an even much heavier extent in P. MUELLER's paper [6], which again obtains certain complete and even more laborious classifications relevant for suitable applications of SIEGEL's theorem.

Now, an application of the paper [1] would suffice for the present purposes of proving Theorem 1.1, even using only SIEGEL's condition (i) and forgetting about (ii). But in fact it turns out that looking at such condition (ii) not only makes the former (i) automatic, but also leads to a much simpler and self-contained elementary proof, which can be hopefully useful for some readers and for other applications. Moreover the resulting proof yields with little effort a slightly more precise conclusion, as in the last phrase of the statement below (which allows to describe all but finitely many integral points).

To present such a proof is the main scope of this note.

Summing up, by the foregoing discussion, all but finitely many integral points of the (possibly reducible) curve $F(X, Y) = 0$ correspond to a component of such curve with at most two points at infinity, defined by a corresponding factor of F. In particular, for Theorem 1.1 it will suffice to prove the following result (even disregarding the last conclusion):

Theorem 1.3 *Assume that the polynomial $F(X, Y)$ has an irreducible factor Φ defining a curve with at most two points at infinity (in a closure in $\mathbb{P}_2$). Then* $\deg \Phi \leq 2$ *and there are an integer $n > 1$ and polynomials $g, l \in \mathbb{C}[X]$, with* $\deg l = 1$, *such that $f = g \circ S_n \circ l$, where S_n is the cyclic (if* $\deg \Phi = 1$*) or the Chebyshev (if* $\deg \Phi = 2$*) polynomial of degree n.*

Further, if $\deg \Phi = 1$, *then Φ divides $l(X)^n - l(Y)^n$. If* $\deg \Phi = 2$, *then Φ is symmetric and either it divides $S_n(l(X)) - S_n(l(Y))$, or g is even and Φ divides $S_n(l(X)) + S_n(l(Y))$.*

2 Proofs

We have already remarked in the discussion above that, in view of SIEGEL's theorem, Theorem 1.1 follows from Theorem 1.3. Therefore it suffices to prove the latter.

Proof of Theorem 1.3 To start with, we normalise f by assuming, after multiplication by a nonzero constant and a translation on X, that it is monic and with vanishing second coefficient: $f(X) = X^d + f_2X^{d-2} + \ldots + f_d$, $f_i \in \mathbb{C}$. This does not affect the results on taking into account the linear polynomial $l(X)$ in the statement.

Remark 2.1 We stress that this normalisation is very helpful in simplifying calculations. We also note that it holds for a (composite) polynomial f of the shape $g \circ h$ where $\deg h > 1$, if and only if holds for the polynomial h, as is very easy to check. In turn, this entails that if f has been likewise normalised, then the polynomial $l(X)$ of degree 1 in the statements will have no constant term, which further simplifies the relevant shapes.

Our affine (possibly reducible) curve $C_F : F(X, Y) = 0$ has degree $d - 1$. Note that the points at infinity in $\mathbb{P}_2$ of (the closure of) this curve are given in homogenous coordinates $(x : y : z)$ by $z = 0$, $x^d = y^d$, $x \neq y$, so they form a set of $d - 1$ pairwise distinct points.[2]

Let $\Phi(X, Y) \in \mathbb{C}[X, Y]$ be an irreducible factor of $F(X, Y)$, defining an irreducible curve C_Φ with at most two points at infinity. The homogeneous part of Φ of highest degree must be a factor of $(X^d - Y^d)/(X - Y)$, and the points at infinity correspond to linear factors of this homogeneous part. Since this has no multiple factors, we deduce that C_Φ has $\deg \Phi$ points at infinity. Hence, if C_Φ satisfies SIEGEL's condition (ii), we must have $\deg \Phi \leq 2$.

From these considerations it also follows that, on multiplying by a nonzero constant, we may assume that Φ is monic in Y.

We have two cases, leading to the corresponding pair of conclusions.

Case A. Suppose first that $\deg \Phi = 1$, so $\Phi(X, Y) = Y - aX - b$; hence we must have $f(aX + b) = f(X)$ identically. Since however f has vanishing second coefficient, this entails $b = 0$, hence $f(aX) = f(X)$. This implies, as by the way we already knew, that a is a d-th root of unity, $a \neq 1$.

If n is the exact order of a, then $n > 1$ divides d and f must be a polynomial in X^n, i.e. $f(X) = g(X^n)$ and we fall into one of the cases of the conclusion.

Note that $Y - aX$ divides indeed $X^n - Y^n$ so the last assertion holds as well. This completes the first (simpler) half of the verification.

Case B. Suppose now that $\deg \Phi = 2$. The two points at infinity of C_Φ correspond to two Puiseux expansions $Y = P_\pm(X) := a_\pm X + b_{0\pm} + b_{1\pm}X^{-1} + \ldots$ in descending powers of

[2] They are smooth points, which simplifies things as we do not need to refer to smooth models.

X, where $b_{i\pm}$ are complex numbers and $a_\pm$ are two distinct d-th roots of 1, both different from 1.

We have $\Phi(X, P_\pm(X)) = 0$ hence $F(X, P_\pm(X)) = 0$, so $f(X) = f(P_\pm(X))$ identically. As before, since f has vanishing second coefficient this yields $b_{0\pm} = 0$. We may write

$$\Phi(X, Y) = (Y - a_+X)(Y - a_-X) + L(X, Y) - k,$$

where L is linear homogeneous and $k \in \mathbb{C}$. We have that $P_\pm(X) - a_\pm X = O(X^{-1})$, in the sense that it is a Puiseux series where no non-negative power of X appears. Since $\Phi(X, P_\pm(X)) = 0$ we get that $L(X, P_\pm(X)) = O(1)$ for both choices of the sign. But then, since $a_\pm$ are distinct this implies $L = 0$, and since Φ is irreducible we have $k \neq 0$. Hence, setting $s := a_+ + a_-$, $p := a_+a_-$, we have $pk \neq 0$ and

$$\Phi(X, Y) = (Y - a_+X)(Y - a_-X) - k = Y^2 - sXY + pX^2 - k.$$

Let now x be a variable over $\mathbb{C}$ and let y be a solution of $\Phi(x, y) = 0$ in an extension of $\mathbb{C}(x)$, so $\mathbb{F} := \mathbb{C}(x, y)$ is the function field of C_Φ. Note that $\mathbb{F}$ is a quadratic extension of both $\mathbb{C}(x)$ and $\mathbb{C}(y)$; looking at the equation we find that the Galois groups of $\mathbb{F}$ over these two fields are generated respectively by the automorphisms σ, τ of $\mathbb{F}$ (of order 2) given by

$$\sigma(x) = x, \quad \sigma(y) = sx - y, \qquad \tau(x) = (\frac{s}{p})y - x, \quad \tau(y) = y.$$

It will be notationally convenient to have another expression for $\mathbb{F}$. Define the linear forms $Z_\pm := Y - a_\pm X$, so $\Phi = Z_+Z_- - k$. Letting $z_\pm = y - a_\pm x$ we thus have $z_+z_- = k$ and

$$x = \frac{z_+ - z_-}{a_- - a_+} = \gamma(z_+ - z_-), \qquad y = \gamma(a_-z_+ - a_+z_-),$$

where we have put $\gamma := (a_- - a_+)^{-1}$. So in particular we have $\mathbb{F} = \mathbb{C}(z_+)$ and by an easy computation one finds that the above automorphisms are expressed by

$$\sigma(z_+) = -z_- = \frac{\alpha}{z_+}, \qquad \tau(z_+) = -\frac{a_+}{a_-}z_- = \frac{\beta}{z_+}, \tag{2}$$

where $\alpha = -k$, $\beta = -ka_+/a_-$.

Now, since $\Phi(x, y) = 0$ we have $F(x, y) = 0$ whence $f(x) = f(y)$, so the field $K := \mathbb{C}(x) \cap \mathbb{C}(y)$ contains $\mathbb{C}(f(x))$ and thus the degree $[\mathbb{F} : K]$ is finite. The field K is left fixed by both σ, τ, and thus by the group G that they generate inside $\mathrm{Aut}(\mathbb{F}/\mathbb{C}) = \mathrm{PGL}_2(\mathbb{C})$. By basic Galois theory actually the fixed field of G is precisely the intersection $\mathbb{C}(x) \cap \mathbb{C}(y) = K$.

We have $\sigma(\tau(z_+)) = (\beta/\alpha)z_+$, hence $\beta/\alpha = a_+/a_-$ is a root of unity of a certain order n: actually, we already knew that a_+, a_- are d-th roots of unity, and they are distinct, so $n > 1$ is a divisor of d.

The group G is generated by σ and $\xi := \sigma\tau$. On looking at the action on z_+ it is now easily seen that $\sigma^{-1}\xi\sigma = \xi^{-1}$, so G is a dihedral group of order $2n$.

Now, the rational function of z_+ given by $w := z_+^n + \alpha^n z_+^{-n}$ of degree $2n$ is plainly invariant by both σ and ξ, hence by G. Again by simple Galois theory, we have $\mathbb{C}(w) = K$. Therefore $f(x)$, which lies in K, is a rational function of w, $f(x) = g(w)$. (On comparing degrees we find $\deg g = d/n$.)

Recall that $x = \gamma(z_+ - z_-) = \gamma(z_+ + (-k)z_+^{-1}) = \gamma(z_+ + \alpha z_+^{-1})$. Hence x has only the poles $z_+ = 0, \infty$, and the same holds for $f(x)$ (as functions of z_+). It follows at once that g must be a polynomial, of degree d/n.

The proof is now easily completed by a simple change of variables. We have $w \in K \subset \mathbb{C}(x)$, so we may write $w = S(x)$ with S a rational function of degree n, which as above must be a polynomial.

Set $z = \delta z_+$ where $\delta^2\alpha = 1$. Hence $x = \gamma\delta^{-1}(z+z^{-1})$. Also, $w = \delta^{-n}(z^n+z^{-n})$. Hence $\delta^n S(\gamma\delta^{-1}(z+z^{-1})) = z^n + z^{-n}$, and by uniqueness it follows that $\delta^n S(\gamma\delta^{-1}X) = T_n(X)$ is the Chebyshev polynomial of degree n. Hence in conclusion we find

$$f(X) = g(\delta^{-n}T_n(\gamma^{-1}\delta X)),$$

as required.

To check the last assertion of Theorem 1.3, for notational simplification we slightly change conventions and replace $g(\delta^{-n}X)$ with $g(X)$ and $f(X)$ with $f(\gamma\delta^{-1}X)$, so as to suppose $f(X) = g(T_n(X))$.

With these substitutions, in the above notation x then becomes $z + z^{-1}$ and $y = a_-z + a_+z^{-1}$. (Note that these substitutions leave unchanged the set $\{a_+, a_-\}$.)

Also, let $\mu^2 = a_+/a_-$, so $\mu^{2n} = 1$ and $\mu^n =: \epsilon \in \{\pm 1\}$.

We have $y = \mu a_-((z/\mu)+(z/\mu)^{-1})$, so $T_n((\mu a_-)^{-1}y) = \epsilon(z^n+z^{-n}) = \epsilon T_n(x)$. Hence, setting $\nu := (\mu a_-)^{-1}$, we have

$$T_n(\nu y) = \epsilon T_n(x), \qquad g(T_n(y)) = f(y) = f(x) = g(T_n(x)) = g(\epsilon T_n(\nu y)).$$

Denoting $b := \deg g = d/n$, we then deduce that $\deg(T_n(y)^b - (\epsilon T_n(\nu y))^b) \le (b-1)n$. But on factoring the left side and noting that all factors but at most one have degree $\ge n$, this implies that in fact one of the factors is constant, hence

$$T_n(y) = \theta\epsilon T_n(\nu y) + c, \qquad g(\theta X + c) = g(X), \tag{3}$$

for some b-th root of unity θ, where we note that this argument is fairly standard in this type of theory. Note that all of these equalities hold identically.

Now, the Chebyshev polynomial $T_n(X)$ starts with $X^n - nX^{n-2} + \ldots$, whence the first of the equations gives $\theta\epsilon\nu^n = \nu^2 = 1$. Also, if n is odd then $T_n(0) = 0$ whence $c = 0$; if n is even then $\nu^n = 1$ so $\theta\epsilon = 1$ and again setting $y = 0$ we find $c = 0$ anyway. Conversely, if these equalities hold it is easy to check that the equation holds, since T_n has the same parity of n.

So we may suppose in the sequel that $\theta\epsilon\nu^n = \nu^2 = 1$ and that $g(\theta X) = g(X)$.

Now, consider again the equation $T_n(\nu y) = \epsilon T_n(x)$, i.e. $\nu^n T_n(y) = \epsilon T_n(x)$.

If $\nu^n = \epsilon$ we have $T_n(x) = T_n(y)$ so $\Phi(X, Y)$ divides $(T_n(X) - T_n(Y))/(X - Y)$, and we are in the first case of the conclusion.

If $\nu^n \neq \epsilon$, then $T_n(x) = -T_n(y)$ hence $\Phi(X, Y)$ divides $T_n(X) + T_n(Y)$. Also, we have already observed that $\theta = \epsilon\nu^n$ which in this case equals -1 so g is an even polynomial by the second equation in (3) (since $c = 0$), again as in the sough conclusion.

Finally, from the above equations we derive $p = a_+a_- = (a_+/a_-)(a_-)^2 = (\mu a_-)^2 = \nu^{-2} = 1$, hence $\Phi(X, Y)$ is symmetric.

This concludes the proof of Theorem 1.3. □

Remark 2.2 We note that the last conclusion could have been stated as follows: *if nis maximal such that the decomposition holds, then the quadratic factor anyway divides* $S_n(l(X)) - S_n(l(Y))$. Indeed, if g is even, then since $T_2(X) = X^2 - 2$, g can be written as $h \circ T_2$ and now we use that $T_2 \circ T_n = T_{2n}$ (a special case of the formulae recalled above).

Also, the same proof-arguments (especially on using Remark 2.1) show that if n is maximal such that *a* decomposition holds as in the conclusion, then all the factors Φ of F of degree

1 or 2 arise from *that* decomposition. We omit a complete verification, which would lead us too far from the main purpose of the article.

Acknowledgements We thank the Editors of this journal, in particular OLIVIER WITTENBERG, for the help and positivity in handling this note, and we thank an anonymous referee for several relevant and helpful comments. We warmly thank WADE HINDES for posing the question which led to the note, and for kind help in the editorial process.

Funding Open access funding provided by Scuola Normale Superiore within the CRUI-CARE Agreement.

References

1. Avanzi, R., Zannier, U.: The equation f(X)=f(Y) in rational functions X=X(t), Y=Y(t). Compos. Math. **139**(3), 263–295 (2003)
2. Bombieri, E., Gubler, W.: Heights in diophantine geometry. In: New Mathematics Monographs, vol. 4. Cambridge University Press, Cambridge (2006)
3. Corvaja, P., Zannier, U.: A subspace theorem approach to integral points on curves. C.R. Acad. Sci. Paris **334**, 267–271 (2002)
4. Fried, M.: On a conjecture of Schur. Michigan Math. J. **17**, 41–50 (1970)
5. Lang, S.: Diophantine Geometry. Springer, New York (1982)
6. Mueller, P.: Permutation groups with a cyclic two-orbits subgroup and monodromy groups of Laurent polynomials. Ann. Sc. Norm. Super. Pisa Cl. Sci. (5) **12**(2), 369–398 (2013)
7. Schinzel, A.: Polynomials with Special Regard to Reducibility. Cambridge University Press, Cambridge (2000)
8. Serre, J.-P.: Lectures on the Mordell-Weil Theorem, 2nd edn. Vieweg, Braunschweig (1990)
9. Siegel, C.L.: On some applications of diophantine approximations (a translation of Siegel's Über einige Anwendungen diophantischer Approximationed by Clemens Fuchs). In: Zannier, U. (ed.) Quaderni, No. 2, Edizioni della Normale. Scuola Normale Superiore, Pisa (2014)