Eidgenössische Technische Hochschule Zürich

a characterisation of quadratic rational maps with a preperiodic first critical point

a Bachelor Thesis

written by

Jennifer-Jayne Jakob

supervised by

Prof. Richard Pink

Abstract

The moduli space of critically marked quadratic rational maps from the Riemann sphere to itself is essentially an algebraic surface. The subset where the first critical point is preperiodic of type (m, k) is a curve inside the moduli space. We describe these curves by explicit polynomials. The main result is the factorisation of these polynomials in a fashion similar to that of $x^n - 1$ into cyclotomic polynomials. The zero loci of these factors contain the Zariski closure of the curves.

Summer 2014

Introduction

Our moduli space $\mathcal{M}$ consists of triples $\langle f, \omega_1, \omega_2 \rangle$, where f is a quadratic rational map from the Riemann sphere $\hat{\mathbb{C}}$ to itself and ω_1, ω_2 are the critical points of f. A point ω in $\hat{\mathbb{C}}$ has exact preperiod (m, k) under f if there exist integers $m \geq 0$ and $k \geq 1$ which are minimal such that $f_{m+k}(\omega) = f_m(\omega)$. Here f_n denotes the n^{th} iterate of f.
The moduli space is essentially an affine surface. The subset $\mathcal{M}_{m,k}$ of triples $\langle f, \omega_1, \omega_2 \rangle$ where ω_1 has exact preperiod (m, k) under f is an algebraic curve inside $\mathcal{M}$.

Conjecture (Pink)**.** *The curves $\mathcal{M}_{m,k}$ are irreducible and given by explicit polynomials which are irreducible.*

Our aim is to find these explicit polynomials. For technical reasons, we work with an open set $\mathcal{N}_{m,k}$ inside $\mathcal{M}_{m,k}$ obtained by removing the finitely many triples which additionally satisfy $f(\omega_2) \in \{\omega_1, \omega_2\}$. The definition of preperiodicity gives one closed and finitely many open conditions. Using this we derive a recursive formula for polynomials $C_{m,k}$ that describe $\mathcal{N}_{m,k}$. Due to the open conditions, the zero locus of each $C_{m,k}$ contains certain curves $\mathcal{N}_{m',k'}$ for smaller integers $m' \leq m$ and $k' \leq k$. The polynomial that defines the Zariski closure of one of these curves by a single closed condition is the unique factor of $C_{m,k}$ which is not a factor of any other $C_{m',k'}$. This property is analogous to that of cyclotomic polynomials as factors of $x^n - 1$. Our main result is the existence of a similar unique factorisation. In preparation for this result, we determine all greatest common divisors and certain divisibility relations. These are key to the proof that the explicit decomposition does indeed yield polynomial factors. We also briefly discuss the relations between these factors and give a condition under which their zero loci are equal to the Zariski closure of the curves.

The principal prerequisite for this bachelor thesis is elementary algebra as covered in an undergraduate course. In addition, some familiarity with very basic notions of algebraic geometry may be helpful.

1 Basic Notions and Notation

We will often identify the Riemann sphere $\hat{\mathbb{C}} := \mathbb{C} \cup \{\infty\}$ with the *complex projective line* $\mathbb{P}^1 := \mathbb{CP}^1$. This is the subset of $\mathbb{C}^2$ consisting of all pairs of complex numbers $(\alpha, \beta) \neq (0, 0)$ modulo the equivalence relation $(\alpha, \beta) \sim (\lambda\alpha, \lambda\beta)$ for any $\lambda \in \mathbb{C}^\times$. We denote elements of $\mathbb{P}^1$ by $[\alpha : \beta]$. Following standard conventions, the points 0 and ∞ in $\hat{\mathbb{C}}$ are identified with the points $[0 : 1]$ and $[1 : 0]$ respectively, and for $\beta \neq 0$, we identify $[\alpha : \beta]$ in $\mathbb{P}^1$ with $\frac{\alpha}{\beta}$ in $\hat{\mathbb{C}}$. The following vocabulary is that used by Silverman in [4].
A *quadratic rational map* from the Riemann sphere to itself is a map

$$f : \hat{\mathbb{C}} \to \hat{\mathbb{C}},\ x \mapsto \frac{\alpha_1 x^2 + \beta_1 x + \gamma_1}{\alpha_2 x^2 + \beta_2 x + \gamma_2}$$

with coefficients $\alpha_1, \alpha_2, \beta_1, \beta_2, \gamma_1, \gamma_2$ in $\mathbb{C}$ such that (i) α_1 and α_2 are not both zero and (ii) numerator and denominator have no nontrivial common factors as polynomials. This gives rise to a holomorphic map from the projective line to itself:

$$f : \mathbb{P}^1 \to \mathbb{P}^1,\ [x : y] \mapsto [\alpha_1 x^2 + \beta_1 xy + \gamma_1 y^2 : \alpha_2 x^2 + \beta_2 xy + \gamma_2 y^2].$$

By setting $f_0 := \mathrm{id}$ and $f_{n+1} := f \circ f_n$ for nonnegative integers n, we let f_n denote the n^{th} iterate of f.

The *(forward) orbit* of a point ω in $\hat{\mathbb{C}}$ under f is the set $\mathcal{O}_f(\omega) := \{f_n(\omega) \mid n \geq 1\}$. For integers $m \geq 0$ and $k \geq 1$, we call ω a *preperiodic point* under f with *preperiod* (m, k) if ω satisfies the equation $f_{m+k}(\omega) = f_m(\omega)$. In this case, the orbit $\mathcal{O}_f(\omega)$ is finite. If m and k are minimal with respect to this equation, then we say that ω has *exact preperiod* (m, k). When ω has preperiod $(0, k)$, i.e. when ω satisfies $f_k(\omega) = \omega$, we say ω is *k-periodic.* If k is minimal with this property, then ω has *exact period* k.
A *critical point of* f is a point $\omega \in \hat{\mathbb{C}}$ at which the derivative of f vanishes. Every quadratic rational map has precisely two critical points[1], which we denote by ω_1 and ω_2.
The *(strictly) postcritical orbit of* f is the union $\mathcal{O}_f(\omega_1) \cup \mathcal{O}_f(\omega_2)$ of the orbits of the two critical points of f. We say f is *postcritically finite* if this set is finite.
The map f is a 2-to-1 branched covering with exactly one nontrivial *covering automorphism*, which we denote by σ_f. This is a Möbius transformation with the following properties:

(1.1) (i) $\sigma_f^2 = \mathrm{id}$ (ii) $f \circ \sigma_f = f$ (iii) $\sigma_f(\omega) = \omega \iff \omega \in \{\omega_1, \omega_2\}$

Since f is branched at its two critical points, the postcritical orbit contains at least two distinct elements $f(\omega_1)$ and $f(\omega_2)$. Our aim is to determine for which quadratic rational maps the orbit of the first critical point is finite. In order to do so, we first need an appropriate moduli space.

[1] This can be shown, for example, by using the Riemann-Hurwitz formula, cf. Silverman [4, Cor. 1.2.]

2 The Moduli Space $\mathcal{M}$

Let us first look at triples (f, ω_1, ω_2) consisting of a quadratic rational map f together with an ordered list of its critical points. The group $\mathrm{PSL}_2(\mathbb{C})$ of Möbius transformations acts on the space of these triples via conjugation:

$$\forall \varphi \in \mathrm{PSL}_2(\mathbb{C}) : \varphi.(f, \omega_1, \omega_2) = (\varphi \circ f \circ \varphi^{-1}, \varphi(\omega_1), \varphi(\omega_2)).$$

We define as our moduli space the set of all such conjugacy classes. We denote this set by $\mathcal{M}$ and its elements by $\langle f, \omega_1, \omega_2 \rangle$. We now want to find a more specific description of $\mathcal{M}$.

Proposition 2.1. *Every conjugacy class in $\mathcal{M}$ contains a representative of the form $(f, 0, \infty)$. For every such triple, the nontrivial covering automorphism σ_f of f is given by*

$$\sigma_f(x) = -x$$

and f is of the form

$$f(x) = \frac{\alpha x^2 + \beta}{\gamma x^2 + \delta}, \quad \textit{where } \alpha\delta - \beta\gamma \neq 0.$$

Conversely, any f of this form yields an element $\langle f, 0, \infty \rangle \in \mathcal{M}$.

Proof. The action of $\mathrm{PSL}_2(\mathbb{C})$ on $\mathbb{P}^1$ is sharply 3-transitive. This implies that, in particular, for any triple $(\tilde{f}, \omega_1, \omega_2)$ there exists a Möbius transformation φ such that $\varphi(\omega_1) = 0$ and $\varphi(\omega_2) = \infty$. Thus, each conjugacy class in $\mathcal{M}$ contains a representative of the form $(f, 0, \infty)$. The critical points 0 and ∞ of f are precisely the fixed points of the nontrivial covering automorphism σ_f, which is a Möbius transformation. Therefore, it must be of the form $\sigma_f(x) = \lambda x$ for some $\lambda \in \mathbb{C}^\times$. But $\sigma_f^2 = \mathrm{id}$ is only satisfied if $\lambda = \pm 1$. Since σ_f is nontrivial, we thus conclude that $\sigma_f(x) = -x$.
We have that $f(x) = f(\sigma_f(x)) = f(-x)$. This identity can only hold if f has no linear terms in x. Thus f is of the form $\frac{\alpha x^2+\beta}{\gamma x^2+\delta}$. Furthermore, (α, β) is not a multiple of (γ, δ) by definition of a quadratic rational map. Thus, $\alpha\delta - \beta\gamma$ cannot vanish.
For the converse, let f be given by $f(x) = \frac{\alpha x^2+\beta}{\gamma x^2+\delta}$ with $\alpha\delta - \beta\gamma \neq 0$. Considering the derivative $df(x) = \frac{2x(\alpha\delta-\gamma\beta)}{(\gamma x^2+\delta)^2}$, we see that $df(x) = 0$ if and only if $x = 0$ or $x = \infty$. In other words, the points 0 and ∞ are the two critical points of f. $\square$

Let $\mathcal{N}$ denote the set of conjugacy classes $\langle f, \omega_1, \omega_2 \rangle$ that satisfy $f(\omega_2) \neq \omega_1, \omega_2$ and let $\mathcal{N}'$ denote that of all $\langle f, \omega_1, \omega_2 \rangle$ satisfying $f(\omega_1) \neq \omega_1, \omega_2$. Then $\mathcal{M} \setminus (\mathcal{N} \cup \mathcal{N}')$ is the set of $\langle f, \omega_1, \omega_2 \rangle$ with $\{f(\omega_1), f(\omega_2)\} = \{\omega_1, \omega_2\}$.

Statements (i),(ii) and (v) of the next proposition are mentioned in a more general setting in the proof of [2, Prop. 1.8] and in [2, Prop. 1.4].

Proposition 2.2. *The subsets $\mathcal{N}$ and $\mathcal{N}'$ of the moduli space are characterised as follows:*

(i) *Every pair $(a,b) \in \mathbb{C}^2 \setminus \operatorname{diag}(\mathbb{C})$ defines an element $\langle \frac{x^2+a}{x^2+b}, 0, \infty\rangle$ in $\mathcal{N}$ and an element $\langle \frac{ax^2+1}{bx^2+1}, 0, \infty\rangle$ in $\mathcal{N}'$.*

(ii) *Conversely, every conjugacy class in $\mathcal{N}$ contains a representative $(\frac{x^2+a}{x^2+b}, 0, \infty)$ and every element of $\mathcal{N}'$ admits a representative $(\frac{ax^2+1}{bx^2+1}, 0, \infty)$, each for a unique pair (a,b) in $\mathbb{C}^2 \setminus \operatorname{diag}(\mathbb{C})$.*

(iii) *The intersection $\mathcal{N} \cap \mathcal{N}'$ is the set of conjugacy classes $\langle \frac{x^2+a}{x^2+b}, 0, \infty\rangle$ with $ab \neq 0$.*

(iv) *Every element of the complement of $\mathcal{N}$ in $\mathcal{N}'$ is of the form $\langle (cx^2+1)^{\pm 1}, 0, \infty\rangle$ for a unique $c \in \mathbb{C}^\times$ and some sign. Conversely, every $c \in \mathbb{C}^\times$ defines an element of this set.*

(v) *The set $\mathcal{M} \setminus (\mathcal{N} \cup \mathcal{N}')$ consists of precisely the two conjugacy classes $\langle x^{\pm 2}, 0, \infty\rangle$.*

Proof. We will prove (i) and (ii) for $\mathcal{N}$. The proofs for $\mathcal{N}'$ are analogous.
(i) Let f be given by $f(x) = \frac{x^2+a}{x^2+b}$ with $a \neq b$ in $\mathbb{C}$. By Proposition 2.1, this yields an element $\langle f, 0, \infty\rangle \in \mathcal{M}$. Furthermore, we have that $f(\infty) = 1$. Thus, the pair $(a,b) \in \mathbb{C}^2 \setminus \operatorname{diag}(\mathbb{C})$ defines a conjugacy class $\langle f, 0, \infty\rangle$ in $\mathcal{N}$.

(ii) For any conjugacy class $\langle \tilde{f}, \omega_1, \omega_2\rangle \in \mathcal{N}$, the points ω_1, ω_2 and $\tilde{f}(\omega_2)$ are distinct. Thus, we can uniquely define a Möbius transformation φ by requiring that $\varphi(\omega_1) = 0$ and $\varphi(\omega_2) = \infty$ and $\varphi(\tilde{f}(\omega_2)) = 1$. This yields a representative $(f, 0, \infty)$ with $f(\infty) = \varphi(\tilde{f}(\omega_2)) = 1$. By Proposition 2.1, this f is of the form $f(x) = \frac{\alpha x^2+\beta}{\gamma x^2+\delta}$ with $\alpha\delta - \beta\gamma$ nonzero. Since φ is unique, so are the coefficients of f. Furthermore, we have $1 = f(\infty) = \alpha/\gamma$, and thus $\alpha = \gamma$. This implies that $f(x) = \frac{\alpha x^2+\beta}{\alpha x^2+\delta} = \frac{x^2+\beta/\alpha}{x^2+\delta/\alpha}$ with $\beta/\alpha \neq \delta/\alpha$, as claimed.

(iii) Using (i),(ii) and the fact that $\tilde{f}(\omega_1) \neq \omega_1, \omega_2$ for any element $\langle \tilde{f}, \omega_1, \omega_2\rangle$ of $\mathcal{N}'$, we find that $\langle \tilde{f}, \omega_1, \omega_2\rangle$ lies in $\mathcal{N} \cap \mathcal{N}'$ if and only if $\langle \tilde{f}, \omega_1, \omega_2\rangle = \langle f(x) {=} \frac{x^2+a}{x^2+b}, 0, \infty\rangle$ for a pair $(a,b) \in \mathbb{C}^2 \setminus \operatorname{diag}(\mathbb{C})$ and $f(0) = a/b \neq 0, \infty$. The last equation is equivalent to $ab \neq 0$.

(iv) The complement of $\mathcal{N}$ in $\mathcal{N}'$ consists of all $\langle \tilde{f}, \omega_1, \omega_2\rangle$ that satisfy $\tilde{f}(\omega_2) \in \{\omega_1, \omega_2\}$ and $\tilde{f}(\omega_1) \neq \omega_1, \omega_2$. By (ii), we have $\langle \tilde{f}, \omega_1, \omega_2\rangle = \langle f(x) {=} \frac{ax^2+1}{bx^2+1}, 0, \infty\rangle$ for unique a and b. Moreover, $f(\infty) = a/b \in \{0, \infty\}$. From this we deduce that $f(x) = (ax^2+1)$ or $(bx^2+1)^{-1}$ with $a, b \in \mathbb{C}^\times$. Conversely, for any $c \in \mathbb{C}^\times$, the maps $f_\pm(x) = (cx^2+1)^{\pm 1}$ clearly satisfy $f_\pm(\infty) \in \{0, \infty\}$ and $f_\pm(0) \neq 0, \infty$. Thus c yields elements $\langle f_\pm, 0, \infty\rangle$ in $\mathcal{N}' \setminus \mathcal{N}$.

(v) The elements of $\mathcal{M} \setminus (\mathcal{N} \cup \mathcal{N}')$ are precisely the conjugacy classes $\langle \tilde{f}, \omega_1, \omega_2\rangle$ such that $\{\tilde{f}(\omega_1), \tilde{f}(\omega_2)\} = \{\omega_1, \omega_2\}$. By Proposition 2.1, the map $\tilde{f}$ is conjugate to $f(x) = \frac{\alpha x^2+\beta}{\gamma x^2+\delta}$ with $\alpha\delta - \beta\gamma \neq 0$. Moreover f satisfies $f(\infty) = \alpha/\gamma$ and $f(0) = \beta/\delta$. From these properties we conclude that $f(x) = \frac{\alpha}{\delta}x^2$ or $\frac{\beta}{\gamma}x^{-2}$. Thus, $\langle \tilde{f}, \omega_1, \omega_2\rangle = \langle x^{\pm 2}, 0, \infty\rangle$ for some sign. $\square$

Remark 2.3. Statements (i) and (ii) of Proposition 2.2 give bijections $\mathcal{N} \leftrightarrow \mathbb{C}^2 \setminus \operatorname{diag}(\mathbb{C})$ and $\mathcal{N}' \leftrightarrow \mathbb{C}^2 \setminus \operatorname{diag}(\mathbb{C})$.
Statement (iv) tells us that the complement of $\mathcal{N}$ in $\mathcal{M}$ is in bijection with two copies of $\mathbb{C}$, if we additionally assign 0 to $\langle x^{\pm 2}, 0, \infty \rangle$.
From Statement (v), we see that $\mathcal{M}$ is equal to the union of $\mathcal{N}$, $\mathcal{N}'$ and the two points $\langle x^{\pm 2}, 0, \infty \rangle$. Thus, we find that $\mathcal{M}$ is essentially an affine surface. This can be made precise, see for example [1, Lemma 6.1].

We now want to describe subsets of $\mathcal{M}$ consisting of $\langle f, \omega_1, \omega_2 \rangle$ such that the forward orbit of the first critical point under f is finite of a given form.

3 The Curves in $\mathcal{M}$

Let (f, ω_1, ω_2) represent an element of $\mathcal{M}$, with covering automorphism σ_f. Consider the orbit $\mathcal{O}_f(\omega_1) = \mathcal{O}(\omega_1)$ of the first critical point under f. This is a finite set when ω_1 is preperiodic. More specifically, if ω_1 has exact preperiod $(m+1, k)$ for $m, k \geq 1$, then the orbit $\mathcal{O}(\omega_1)$ has cardinality $m + k$. Since $f^{-1}(f(\omega_1)) = \{\omega_1\}$, the equation $f_{k+1}(\omega_1) = f(\omega_1)$ is equivalent to $f_k(\omega_1) = \omega_1$. In other words, ω_1 has preperiod $(1, k)$ if and only if it is k-periodic.
We define $M_{0,k}$ as the subset of $\mathcal{M}$ of all conjugacy classes whose first critical point has exact period k. For all $m, k \geq 1$, we denote by $\mathcal{M}_{m,k}$ the subsets consisting of all conjugacy classes with a first critical point of exact preperiod $(m+1, k)$.

Claim 3.1. *For all $m \geq 0$ and $k \geq 1$:*

$$\mathcal{M}_{m,k} = \{\langle f, \omega_1, \omega_2 \rangle \in \mathcal{M} \mid f_{m+k}(\omega_1) = \sigma_f(f_m(\omega_1)) \textit{ and } f(\omega_1), \ldots, f_{m+k}(\omega_1) \textit{ all distinct}\}.$$

Proof. A direct computation using the properties of σ_f shows that $\sigma_{(\varphi \circ f \circ \varphi^{-1})} = \varphi \circ \sigma_f \circ \varphi^{-1}$. Thus, if the equation $f_{m+k}(\omega_1) = \sigma_f(f_m(\omega_1))$ holds for f, then it also holds for any conjugate. The claim now follows from the equivalence:

$$f_{m+k+1}(\omega_1) = f_{m+1}(\omega_1) \iff f_{m+k}(\omega_1) = \sigma_f(f_m(\omega_1)) \text{ or } f_{m+k}(\omega_1) = f_m(\omega_1).$$

The first direction is due to the fact that $f^{-1}(f(\omega)) = \{\omega, \sigma_f(\omega)\}$ for any point $\omega \in \hat{\mathbb{C}}$. The converse follows by applying f to both sides of each equation and using Properties (1.1.ii) and (1.1.iii) of the covering automorphism. □

For all $m \geq 0$ and $k \geq 1$, define

$$\mathcal{N}_{m,k} := \mathcal{M}_{m,k} \cap \mathcal{N}. \tag{3.2}$$

This is the subset of $\mathcal{M}_{m,k}$ of elements $\langle f, \omega_1, \omega_2 \rangle$ that additionally satisfy $f(\omega_2) \neq \omega_1, \omega_2$.

Claim 3.3. *For each $m \geq 0$ and $k \geq 1$, the complement of $\mathcal{N}$ in $\mathcal{M}_{m,k}$ is a finite set.*

Proof. By Proposition 2.2 (iv) and (v), the complement of $\mathcal{N}$ in $\mathcal{M}$ is the set of conjugacy classes of the form $\langle (cx^2+1)^{\pm 1}, 0, \infty \rangle$ for $c \in \mathbb{C}^\times$ or of the form $\langle x^{\pm 2}, 0, \infty \rangle$. By Proposition 2.1, the associated covering automorphism is $x \mapsto -x$. For $f(x) = cx^2 + 1$, the iterate f_n evaluated at 0 is a polynomial in c of degree $2^n - 1$, with leading coefficient 1 and constant term 1. Therefore, the expression $F_{m,k}(c) := f_{m+k}(0) + f_m(0)$ is a polynomial in c of degree $2^{m+k} - 1$, with vanishing constant term. Thus, assigning $0 \in \mathbb{C}$ to $\langle x^2, 0, \infty \rangle$, we get a bijection between the set

$$\{\langle x^2, 0, \infty \rangle\} \cup \{\langle cx^2 + 1, 0, \infty \rangle \mid c \in \mathbb{C}^\times \text{ and } f_{m+k}(0) = -f_m(0)\}$$

and the zero locus of $F_{m,k}$ in $\mathbb{C}$, where c is now an abstract variable. But $F_{m,k}$ is a univariate polynomial which cannot vanish identically due to its degree. Thus $F_{m,k}$ has only finitely many zeros, which implies that the above set is finite. A similar argument shows that for $g(x) = (cx^2+1)^{-1}$, the analogous set is also finite. Since $\mathcal{M}_{m,k}$ is contained in the set $\{\langle f, \omega_1, \omega_2 \rangle \in \mathcal{M} \mid f_{m+k}(\omega_1) = \sigma_f(f_m(\omega_1))\}$, it follows that $\mathcal{M}_{m,k} \setminus \mathcal{N}$ is a finite union of finite sets and thus itself finite. $\square$

Claim 3.3 implies that any findings we make regarding $\mathcal{N}_{m,k}$ hold for all but finitely many points in $\mathcal{M}_{m,k}$, namely the conjugacy classes of maps that satisfy $f(\omega_2) \in \{\omega_1, \omega_2\}$. Since each $\mathcal{M}_{m,k}$ is defined by one closed and finitely many open conditions, using the fact that $\mathcal{M}$ is essentially an affine surface as discussed in Remark 2.3, we can identify each set $\mathcal{N}_{m,k}$ with an algebraic curve in $\mathbb{C}^2 \setminus \mathrm{diag}(\mathbb{C})$. From here on, we will work with representatives $(f, 0, \infty)$ of elements in $\mathcal{N}$, where $f(x) = \frac{x^2+a}{x^2+b}$ and $\sigma_f(x) = -x$.
The set of curves $\mathcal{N}_{m,k}$ contains information on how the preperiodicity of a first critical point varies as a function of a and b. So we will consider a and b as abstract variables and search for polynomials $P_{m,k}$ in $\mathbb{Z}[a,b]$ whose zero locus in $\mathbb{C}^2 \setminus \mathrm{diag}(\mathbb{C})$ is equal to the Zariski closure of the curve $\mathcal{N}_{m,k}$.

4 The defining Polynomials

Let $R := \mathbb{Z}[a,b]$ denote a polynomial ring over the integers, and set $\tilde{R} := \mathbb{Z}\left[a, b, \frac{1}{b-a}\right]$. The *projective line* $\mathbb{P}^1(S)$ over an $\tilde{R}$-algebra S consists of pairs of relatively prime elements $(x,y) \in S \times S$ modulo the relation $(x,y) \sim (ux, uy)$ for any $u \in S^\times$.

Consider any ring homomorphism $\varphi : \tilde{R} \to S, f \mapsto {}^\varphi f$. We obtain a quadratic morphism

$$^\varphi f : \mathbb{P}^1(S) \to \mathbb{P}^1(S)\,,\ [x:y] \mapsto \left[x^2 + {}^\varphi a\, y^2 : x^2 + {}^\varphi b\, y^2\right].$$

This is well-defined, because $a \neq b$ everywhere in $\tilde{R}$. We define polynomials in R by the recursion

$$\begin{aligned} p_0 &:= 0, & p_{n+1} &:= p_n^2 + a q_n^2 \\ q_0 &:= 1, & q_{n+1} &:= p_n^2 + b q_n^2. \end{aligned} \tag{4.1}$$

By identification, we have $f_n([0:1]) = [p_n : q_n] = \frac{p_n}{q_n} = f_n(0)$. Therefore, the following equivalence holds:

$$f_{m+k}(0) = \sigma_f(f_m(0)) = -f_m(0) \iff p_{m+k}q_m + p_m q_{m+k} = 0. \tag{4.2}$$

For all $m \geq 0$ and $k \geq 1$, we define the polynomial

$$C_{m,k} := p_{m+k}q_m + p_m q_{m+k}. \tag{4.3}$$

This leads to the identity

(4.4)
$$\mathcal{N}_{m,k} = \{(a,b) \in \mathbb{C}^2 \setminus \mathrm{diag}(\mathbb{C}) \mid C_{m,k} = 0 \text{ and } \forall m' \leq m, \forall k' \leq k,\, (m',k') \neq (m,k) : C_{m',k'} \neq 0\}.$$

As we can see from this description of $\mathcal{N}_{m,k}$, the curve is a subset of the zero locus of $C_{m,k}$ in $\mathbb{C}^2 \setminus \mathrm{diag}(\mathbb{C})$. The next step is to find the common divisors of any two $C_{m,k}$ and $C_{m',k'}$. Then we can define a new polynomial cleared of all common divisors, and the zero locus of this new polynomial will still contain the curve $\mathcal{N}_{m,k}$.

5 The Divisibility Relations

In this rather technical section, we will determine the greatest common divisor of any two polynomials $C_{m,k}$ and $C_{m',k'}$. In order to do so, we first establish certain divisibility relations. Unless otherwise specified, all such relations and greatest common divisors [gcd] will be in R. First, note that every ring homomorphism φ from $\tilde{R}$ to an arbitrary ring S induces a map

$$\varphi : \mathbb{P}^1(\tilde{R}) \to \mathbb{P}^1(S), [x : y] \mapsto [\varphi(x) : \varphi(y)].$$

Using the same notation as in the previous section, for any such φ the definition of $C_{m,k}$ yields

$$\forall m \geq 0,\ k \geq 1 : \quad {}^{\varphi}C_{m,k} = 0 \iff {}^{\varphi}f_{m+k}(0) = -{}^{\varphi}f_m(0). \tag{5.1}$$

To start with, we will concentrate on the case $m = 0$. Here, we have

$$\forall k \geq 1 : \quad C_{0,k} = p_k q_0 + p_0 q_k = p_k$$

and hence,

$$\forall k \geq 1 : \quad {}^{\varphi}p_k = 0 \iff {}^{\varphi}f_k(0) = 0. \tag{5.2}$$

Claim 5.3. *For all $k \geq 1$, the polynomials p_k and q_k are congruent modulo $(b - a)$.*

Proof. Since $a \equiv b \bmod (b - a)$, we have $p_1 \equiv q_1 \bmod (b - a)$. By induction on k we find that $p_{k+1} = p_k^2 + aq_k^2 \equiv p_k^2 + bq_k^2 \equiv q_{k+1} \bmod (b - a)$. □

Claim 5.4. *For all $k \geq 1$, neither p_k nor q_k is a multiple of $b - a$.*

Proof. By Claim 5.3, it is sufficient to prove this claim for p_k. We proceed by induction. The statement is clearly true for $p_1 = a$. Claim 5.3 implies that

$$p_{k+1} = p_k^2 + aq_k^2 \equiv (1 + a)p_k^2 \bmod (b - a).$$

Thus $p_{k+1} \not\equiv 0 \bmod (b - a)$ by induction hypothesis. □

Claim 5.5. *For all $k \geq 1$, both $\gcd(p_k, q_k)$ and $\gcd(p_k \bmod 2, q_k \bmod 2)$ are equal to 1.*

Proof. For $k = 1$, we have the identity $\gcd(p_1, q_1) = \gcd(a, b) = 1$. For $k > 1$, note that $q_k - p_k = (b - a)q_{k-1}^2$. Therefore,

$$\begin{aligned}\gcd(p_k, q_k) &= \gcd(p_k, q_k - p_k) = \gcd(p_k, (b - a)q_{k-1}^2) \overset{(b-a)\nmid p_k}{=} \gcd(p_k, q_{k-1}^2)\\ &= \gcd(p_{k-1}^2 + aq_{k-1}^2, q_{k-1}^2) = \gcd(p_{k-1}^2, q_{k-1}^2) = \gcd(p_{k-1}, q_{k-1})^2 = 1,\end{aligned}$$

by induction. The proof of the second part of the statement is analogous. □

Claim 5.6. *For all divisors ℓ of $k \geq 1$, the polynomial p_ℓ divides p_k.*

Proof. Let $\varphi : \tilde{R} \to \tilde{R}/(p_\ell)$ be the projection map. Using Equivalence (5.2), we know that ${}^\varphi p_\ell = 0$ implies ${}^\varphi f_\ell(0) = 0$. Since ℓ divides k, this in turn implies that ${}^\varphi f_k(0) = 0$. Therefore ${}^\varphi p_k = 0$, again using Equivalence (5.2). Thus p_k lies in the ideal $\tilde{R}p_\ell$ and Claim 5.4 implies that p_k lies in Rp_ℓ, so p_ℓ divides p_k in R. $\square$

Lemma 5.7. *For all $k, k' \geq 1$, the greatest common divisor of p_k and $p_{k'}$ is $p_{\gcd(k,k')}$.*

Proof. Set $h := \gcd(p_k, p_{k'})$ in R and $\ell := \gcd(k, k')$. From Claim 5.6 we know that p_ℓ divides h. For the converse, that h divides p_ℓ, we proceed by induction on $\max\{k, k'\}$. The statement is clear for $k = k'$. For $k \neq k'$, let $\varphi : \tilde{R} \to \tilde{R}/(h)$ be the projection map and without loss of generality, assume $k > k'$. Suppose that the claim holds for all $\tilde{k} < k$. Since p_k and $p_{k'}$ both lie in $\tilde{R}h$, we have that ${}^\varphi f_k(0) = 0$ and ${}^\varphi f_{k'}(0) = 0$. From this we deduce

$$0 = {}^\varphi f_k(0) = {}^\varphi f_{k-k'}({}^\varphi f_{k'}(0)) = {}^\varphi f_{k-k'}(0),$$

which implies that ${}^\varphi p_{k-k'} = 0$. Therefore $p_{k-k'}$ lies in $\tilde{R}h$ and thus in Rh, again by Claim 5.4. So h divides $p_{k-k'}$ in R. But $\gcd(k - k', k') = \gcd(k, k')$, and $k - k' < k$, so by induction hypothesis we have $p_\ell = \gcd(p_{k-k'}, p_{k'})$. Hence h divides p_ℓ and we conclude that $h = p_\ell$. $\square$

Now that we have found the greatest common divisor for the case $m = 0$, we can move on to the general case $m \geq 0$. This will take a little more effort, because the results differ for the three cases $\gcd(C_{m,k}, p_{k'})$, $\gcd(C_{m,k}, C_{m,k'})$ and $\gcd(C_{m,k}, C_{m',k'})$.

Claim 5.8. *The polynomial $C_{m,k}$ is not a multiple of $b - a$ for any $m, k \geq 1$.*

Proof. We proceed by induction on m. Recall that $q_k \equiv p_k \not\equiv 0 \bmod (b - a)$ by Claims 5.3 and 5.4. Therefore,

$$C_{1,k} = p_{k+1}q_1 + p_1 q_{k+1} \equiv 2p_1 p_{k+1} \equiv 2a p_{k+1} \not\equiv 0 \bmod (b - a).$$

For $m > 1$, suppose that $C_{m-1,k} \equiv 2p_{m-1}p_{m+k-1} \not\equiv 0 \bmod (b - a)$. Recall from the proof of Claim 5.4 that $p_k \equiv (1 + a)p_{k-1}^2 \bmod (b - a)$. Thus,

$$\begin{aligned} 2C_{m,k} = 2(p_{m+k}q_m + p_m q_{m+k}) &\equiv 4p_m p_{m+k} \equiv 4(1 + a)p_{m-1}^2 (1 + a)p_{m+k-1}^2 \\ &\equiv (1 + a)^2\, 4\, p_{m-1}^2 p_{m+k-1}^2 \equiv (1 + a)^2 C_{m-1,k}^2 \not\equiv 0 \bmod (b - a). \end{aligned}$$ $\square$

Claim 5.9. *For all $m, k \geq 1$, the polynomial $p_{\gcd(m,k)}$ divides $C_{m,k}$.*

Proof. Using Lemma 5.7 and the identity $\gcd(m, m + k) = \gcd(m, k)$, we see that

$$p_{\gcd(m,k)} = p_{\gcd(m+k,k)} = \gcd(p_{m+k}, p_m).$$

Therefore $p_{\gcd(m,k)}$ divides $p_{m+k}q_m + p_m q_{m+k} = C_{m,k}$. $\square$

Lemma 5.10. *For all $m, k, k' \geq 1$, the greatest common divisor of $C_{m,k}$ and $p_{k'}$ is $p_{\gcd(m,k,k')}$.*

Proof. Set $\ell := \gcd(m, k, k')$ and $h := \gcd(C_{m,k}, p_{k'})$. Let $\varphi : \tilde{R} \to \tilde{R}/(h)$ be the projection map. We know that p_ℓ divides both $p_{\gcd(m,k)}$ and $p_{k'}$ by Claim 5.6 and that $p_{\gcd(m,k)}$ divides $C_{m,k}$ by Claim 5.9. Therefore p_ℓ divides both $C_{m,k}$ and $p_{k'}$ and thus also h. To prove the converse, that h divides p_ℓ, we proceed by induction on $\max\{k, k'\}$.

If $k = k'$, then $\ell = gcd(m, k)$ and $h = \gcd(C_{m,k}, p_k)$. Using Equivalences (5.1) and (5.2), we know that

$$\begin{aligned} {}^{\varphi}C_{m,k} = 0 &\implies {}^{\varphi}f_{m+k}(0) = -{}^{\varphi}f_m(0) \\ {}^{\varphi}p_k = 0 &\implies {}^{\varphi}f_k(0) = 0. \end{aligned}$$

Together this implies

$${}^{\varphi}f_m(0) = {}^{\varphi}f_m({}^{\varphi}f_k(0)) = {}^{\varphi}f_{m+k}(0) = -{}^{\varphi}f_m(0),$$

hence ${}^{\varphi}f_m(0) = 0$ or ∞.
If ${}^{\varphi}f_m(0) = \infty$, then ${}^{\varphi}q_m = 0$ and thus q_m lies in $\tilde{R}h$. Since $b - a$ does not divide q_m by Claim 5.4, we find that h divides q_m in R. It follows that p_ℓ also divides q_m. Moreover p_ℓ divides p_m by Claim 5.6, since ℓ is a divisor of m. Hence p_ℓ divides $\gcd(p_m, q_m)$ in R. But $\gcd(p_m, q_m) = 1$ by Claim 5.5, so this is not possible. Therefore, ${}^{\varphi}f_m(0) = 0$ and equivalently ${}^{\varphi}p_m = 0$. So p_m lies in $\tilde{R}h$ and thus in Rh by Claim 5.4. Hence h divides $\gcd(p_m, p_k) = p_\ell$.

For the case $k > k'$, suppose the claim is true for any $\tilde{k} < k$. We know that

$${}^{\varphi}C_{m,k} = 0 \text{ and } {}^{\varphi}p_{k'} = 0 \implies {}^{\varphi}f_{m+k}(0) = -{}^{\varphi}f_m(0) \text{ and } {}^{\varphi}f_{k'}(0) = 0.$$

It follows that

$$-{}^{\varphi}f_m(0) = {}^{\varphi}f_{m+k}(0) = {}^{\varphi}f_{m+k-k'}({}^{\varphi}f_{k'}(0)) = {}^{\varphi}f_{m+k-k'}(0).$$

This implies that ${}^{\varphi}C_{m,k-k'} = 0$. So $C_{m,k-k'}$ lies in $\tilde{R}h$ and thus in Rh using Claim 5.8. Therefore h divides $\gcd(C_{m,k-k'}, p_{k'})$ and by induction hypothesis $\gcd(C_{m,k-k'}, p_{k'}) = p_{\gcd(m,k-k',k')}$. Since $\gcd(m, k - k', k') = \gcd(m, k, k') = \ell$, we conclude that h divides p_ℓ.

For the case $k' > k$, note that

$${}^{\varphi}p_{k'} = 0 \text{ and } {}^{\varphi}C_{m,k} = 0 \implies {}^{\varphi}f_{m+k+k'}(0) = {}^{\varphi}f_{m+k}({}^{\varphi}f_{k'}(0)) = {}^{\varphi}f_{m+k}(0) = -{}^{\varphi}f_m(0).$$

Therefore ${}^{\varphi}C_{m,k+k'} = 0$. Since $k + k' > k'$, we can reduce to the previous case, which yields that $\gcd(C_{m,k+k'}, p_{k'}) = p_{\gcd(m,k+k',k')} = p_\ell$ in R. Moreover h divides both $C_{m,k+k'}$ and $p_{k'}$. Therefore h divides p_ℓ and we conclude that $h = p_\ell$. □

Lemma 5.11. *For all $m, k, k' \geq 1$, the greatest common divisor of $C_{m,k}$ and $C_{m,k'}$ is given by $C_{m,\gcd(k,k')}$. In particular $C_{m,\ell}$ divides $C_{m,k}$ for any divisor ℓ of k.*

Proof. Set $\ell := \gcd(k, k')$ and consider the projection map $\psi : \tilde{R} \to \tilde{R}/(C_{m,\ell})$. We know that ${}^{\psi}C_{m,\ell} = 0$ implies ${}^{\psi}f_{m+\ell}(0) = -{}^{\psi}f_m(0)$, and since ℓ divides both k and k', this implies both

$$\begin{aligned} {}^{\psi}f_{m+k}(0) &= {}^{\psi}f_{m+\ell}(0) = -{}^{\psi}f_m(0) \\ {}^{\psi}f_{m+k'}(0) &= {}^{\psi}f_{m+\ell}(0) = -{}^{\psi}f_m(0). \end{aligned}$$

Therefore ${}^{\psi}C_{m,k} = 0$ and ${}^{\psi}C_{m,k'} = 0$. So $C_{m,\ell}$ divides both $C_{m,k}$ and $C_{m,k'}$ in $\tilde{R}$, and thus in R by Claim 5.8. Hence $C_{m,\ell}$ divides $\gcd(C_{m,k}, C_{m,k'})$ in R.

For the converse, set $h := \gcd(C_{m,k}, C_{m,k'})$ and let $\varphi : \tilde{R} \to \tilde{R}/(h)$ be the projection map. Then

$$\begin{aligned} {}^{\varphi}C_{m,k} = {}^{\varphi}C_{m,k'} = 0 &\implies {}^{\varphi}f_{m+k}(0) = {}^{\varphi}f_{m+k'}(0) = -{}^{\varphi}f_m(0) \\ &\implies {}^{\varphi}f_{m+k+1}(0) = {}^{\varphi}f_{m+k'+1}(0) = {}^{\varphi}f_{m+1}(0). \end{aligned}$$

So ${}^{\varphi}f_{m+1}(0)$ is both k- and k'-periodic. But then ${}^{\varphi}f_{m+1}(0)$ must also be ℓ-periodic. Therefore,

$$\begin{aligned} {}^{\varphi}f_{m+\ell+1}(0)) = {}^{\varphi}f_{m+1}(0) &\implies {}^{\varphi}f_{m+k+\ell}(0) = {}^{\varphi}f_{m+k}(0) = -{}^{\varphi}f_m(0) \\ {}^{\varphi}f_{m+k+\ell}(0) = {}^{\varphi}f_{m+\ell}(0) &\implies {}^{\varphi}f_{m+\ell}(0) = -{}^{\varphi}f_m(0). \end{aligned}$$

Hence ${}^{\varphi}C_{m,\ell} = 0$. So $C_{m,\ell}$ lies in $\tilde{R}h$ and thus in Rh, again by Claim 5.8. We conclude that $h = C_{m,\ell}$. $\square$

Lemma 5.12. *For all $m, m', k, k' \geq 1$ with $m \neq m'$, the greatest common divisor of $C_{m,k}$ and $C_{m',k'}$ is equal to $p_{gcd(m,m',k,k')}$.*

Proof. Without loss of generality, let $m' > m$ (otherwise switch (m, k) and (m', k')). Set $h := \gcd(C_{m,k}, C_{m',k'})$ and $\ell := \gcd(m, m', k, k')$. Recall that $p_{\gcd(m,k)}$ divides $C_{m,k}$ and $p_{\gcd(m',k')}$ divides $C_{m',k'}$, both by Claim 5.9, and $p_\ell = \gcd(p_{\gcd(m,k)}, p_{\gcd(m',k')})$ by Lemma 5.7. This implies that p_ℓ divides h.

For the converse, let $\varphi : \tilde{R} \to \tilde{R}/(h)$ be the projection map. Then

$$\begin{aligned} &{}^{\varphi}C_{m,k} = 0 \implies {}^{\varphi}f_{m+k}(0) = -{}^{\varphi}f_m(0) \\ &\quad \implies {}^{\varphi}f_{m'+k}(0) = {}^{\varphi}f_{m'-m}({}^{\varphi}f_{m+k}(0)) = {}^{\varphi}f_{m'-m}(-{}^{\varphi}f_m(0)) = {}^{\varphi}f_{m'-m}({}^{\varphi}f_m(0)) = {}^{\varphi}f_{m'}(0). \end{aligned}$$

From this we see that $f_{m'}$ is k-periodic and thus ${}^{\varphi}f_{m'+kk'}(0) = {}^{\varphi}f_{m'}(0)$.

But we also have

$$\begin{aligned} {}^{\varphi}C_{m',k'} = 0 &\implies {}^{\varphi}f_{m'+k'}(0) = -{}^{\varphi}f_{m'}(0) \\ &\implies {}^{\varphi}f_{m'+k'+1}(0) = {}^{\varphi}f_{m'+1}(0) \\ &\implies {}^{\varphi}f_{m'+kk'}(0) = {}^{\varphi}f_{m'+k'}(0) = -{}^{\varphi}f_{m'}(0). \end{aligned}$$

So ${}^{\varphi}f_{m'}(0) = -{}^{\varphi}f_{m'}(0)$, which means that ${}^{\varphi}f_{m'}(0) = 0$ or ∞.
If ${}^{\varphi}f_{m'}(0) = \infty$, then ${}^{\varphi}q_{m'} = 0$, so $q_{m'}$ lies in $\tilde{R}h$ and thus in Rh by Claim 5.4. But now p_ℓ divides both $q_{m'}$ and $p_{m'}$, so p_ℓ divides $\gcd(p_{m'}, q_{m'}) = 1$, which is not possible. Therefore ${}^{\varphi}f_{m'}(0) = 0$ and we deduce that $p_{m'}$ lies in Rh.
Consequently, using Lemma 5.10, we find that $h = \gcd(h, p_{m'}) = \gcd(C_{m,k}, C_{m',k'}, p_{m'}) = \gcd(C_{m,k}, \gcd(C_{m',k'}, p_{m'})) = \gcd(C_{m,k}, p_{\gcd(m',k')}) = p_{\gcd(m,k,\gcd(m',k'))} = p_\ell$. □

Now that we have determined all relevant divisiblity relations, we can define new polynomials by clearing the polynomials $C_{m,k}$ of their common divisors with each p_k: For $k \geq 1$, define

$$D_{0,k} := C_{0,k} \qquad \text{and for } m \geq 1: \quad D_{m,k} := \frac{C_{m,k}}{p_{\gcd(m,k)}}, \tag{5.13}$$

which are again polynomials in R by Claim 5.9. This construction ensures that $D_{m,k}$ and $D_{m',k'}$ no longer share nontrivial divisors for $m \neq m'$, whereas the divisibility relation found in Lemma 5.11 is maintained:

Claim 5.14. *For all $m \geq 0$ and $k, k' \geq 1$, the greatest common divisor of $D_{m,k}$ and $D_{m,k'}$ is given by $D_{m,\gcd(k,k')}$.*

Proof. For $m = 0$, this is Lemma 5.7. For $m > 0$, set $\ell := \gcd(m, k, k')$ and $h_k := \frac{p_{\gcd(m,k)}}{p_\ell}$. Recall that by Lemma 5.11 we have $C_{m,\gcd(k,k')} = \gcd(C_{m,k}, C_{m,k'})$. We also know that p_ℓ divides $C_{m,\gcd(k,k')}$ by Claim 5.9. Thus,

$$D_{m,\gcd(k,k')} = \frac{C_{m,\gcd(k,k')}}{p_\ell} = \gcd\left(\frac{C_{m,k}}{p_\ell}, \frac{C_{m,k'}}{p_\ell}\right) = \gcd\left(D_{m,k}h_k, D_{m,k'}h_{k'}\right).$$

Furthermore, note that

$$\gcd\left(D_{m,\gcd(k,k')}, h_k\right) = \frac{\gcd\left(C_{m,\gcd(k,k')}, p_{\gcd(m,k)}\right)}{p_\ell} \overset{\text{Lemma}}{\underset{5.10}{=}} \frac{p_\ell}{p_\ell} = 1$$

and similarly for $h_{k'}$. Hence, $D_{m,\gcd(k,k')} = \gcd\left(D_{m,k}h_k, D_{m,k'}h_{k'}\right) = \gcd(D_{m,k}, D_{m,k'})$. □

6 The Factorisation

The zero loci of our new polynomials $D_{m,k}$ still each contain the corresponding curve $\mathcal{N}_{m,k}$. We want to find a decomposition of each $D_{m,k}$ into a product of polynomials $B_{m,d}$, where the index d ranges over all divisors of k, and such that the zero locus of $B_{m,k}$ is equal to the Zariski closure of $\mathcal{N}_{m,k}$. The following number theoretic facts will be useful for this factorisation.

Definition 6.1. The *Möbius function* $\mu(n)$ is defined for all integers $n \geq 1$ by

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ (-1)^k & \text{if } n = p_1 \cdots p_k, \text{ where } p_1, \dots, p_k \text{ are } k \text{ distinct primes} \\ 0 & \text{otherwise.} \end{cases}$$

The Möbius function has the following summation properties:

Lemma 6.2. *The following holds for all $n \geq 1$:*

(i) $$\sum_{d|n} \mu(n/d) = \sum_{d|n} \mu(d) = \begin{cases} 1 & \textit{if } n = 1 \\ 0 & \textit{if } n > 1, \end{cases}$$

(ii) *for any divisor k of n :*

$$\sum_{\{d\colon k|d|n\}} \mu(n/d) = \sum_{\{d\colon k|d|n\}} \mu(d/k) = \begin{cases} 1 & \textit{if } n = k \\ 0 & \textit{if } n > k. \end{cases}$$

The idea of the first part of the proof is taken from Rassias [3, Thm. 2.2.3].

Proof. (i) Since n/d is a divisor of n for each divisor d of n, the first equality is just a reordering of the summands. For the second equality, note that the statement is true for $n = 1$, because $\mu(1) = 1$. For $n > 1$, let $n = p_1^{e_1} \cdots p_k^{e_k}$ be the prime factorisation of n. By definition of the Möbius function, the only non-vanishing terms in the sum are the $\mu(d)$ for the squarefree divisors d of n, i.e. those of the form $d = p_1^{\ell_1} \cdots p_k^{\ell_k}$ with $\ell_1, \dots \ell_k \in \{0, 1\}$. Hence,

$$\sum_{d|n} \mu(d) = \sum_{i=0}^{k} \binom{k}{i} (-1)^i = (1-1)^k = 0.$$

(ii) If k divides d and d divides n, we can write $d = d'k$ and $n = n'k$ for some $d', n' \geq 1$. Thus, the equality follows applying (i) to

$$\sum_{\{d\colon k|d|n\}} \mu(n/d) = \sum_{d'|n'} \mu(n'/d') = \sum_{d'|n'} \mu(d') = \sum_{\{d\colon k|d|n\}} \mu(d/k). \qquad \square$$

Lemma 6.2 leads to the Möbius inversion formula, which we state in its multiplicative version.

Lemma 6.3 (Multiplicative Möbius Inversion Formula)**.** *Let f, g be maps from $\mathbb{Z}^{\geq 1}$ into a multiplicative abelian group. Then the following equivalence holds for any $n \geq 1$:*

$$g(n) = \prod_{d|n} f(d) \iff f(n) = \prod_{d|n} g(d)^{\mu(n/d)}.$$

Proof. The statement is clearly true for $n = 1$. For $n > 1$, suppose that the left-hand side of the equivalence holds. Then

$$\begin{aligned}\prod_{d|n} g(d)^{\mu(n/d)} &= \prod_{d|n} \Big(\prod_{k|d} f(k)\Big)^{\mu(n/d)} = \prod_{d|n}\prod_{k|d} f(k)^{\mu(n/d)} \\ &= \prod_{k|n}\prod_{\{d\colon k|d|n\}} f(k)^{\mu(n/d)} = \prod_{k|n} f(k)^{\sum_{\{d\colon k|d|n\}}\mu(n/d)} \overset{\substack{\text{Lemma}\\ 6.2\,(ii)}}{=} f(n).\end{aligned}$$

For the converse, we have

$$\prod_{d|n} f(d) = \prod_{d|n}\prod_{k|d} g(k)^{\mu(d/k)} = \prod_{k|n}\prod_{\{d\colon k|d|n\}} g(k)^{\mu(d/k)} = \prod_{k|n} g(k)^{\sum_{\{d\colon k|d|n\}}\mu(d/k)} = g(n),$$

again using Lemma 6.2 (ii) for the last equality. ☐

Lemma 6.4. *For every sequence $(a_k)_{k\geq 1}$ of nonnegative integers with the property*

$$a_{\gcd(k,k')} = \min\{a_k, a_{k'}\} \quad \textit{for all } k, k' \geq 1, \tag{6.5}$$

the following holds:

(i) *The index set $\{k \geq 1 \mid a_k > 0\}$ is either empty or of the form $\mathbb{Z}^{\geq 1}k_0$ for some $k_0 \geq 1$.*

(ii) *For k_0 from* (i)*, the sequence $(a_{\ell k_0} - a_{k_0})_{\ell \geq 1}$ is nonnegative and satisfies* (6.5)*.*

(iii) *For each $k \geq 1$, the sum $b_k := \sum_{k'|k} \mu(k/k')a_{k'}$ is nonnegative.*

(iv) *If each a_k only takes values in $\{0, 1\}$, then $b_{k_0} = 1$ and $b_k = 0$ for every $k \neq k_0$.*

Proof. (i) Set $S := \{k \geq 1 \mid a_k > 0\}$ and suppose S is nonempty. Property (6.5) implies that for all $k, k' \in S$ and all $\ell \geq 1$, both $k\ell$ and $\gcd(k, k')$ lie in S. Let $k_0 \geq 1$ be the smallest integer such that $a_{k_0} > 0$. Pick an element $s \in S$. Then $s \geq k_0$ and we can write $s = \ell k_0 + r$ for some $\ell \geq 1$ and $0 \leq r < k_0$. Then $\gcd(r, \ell k_0) = \gcd(s - \ell k_0, \ell k_0) = \gcd(s, \ell k_0) \in S$. By minimality of k_0, we conclude that $r = 0$. Therefore, each element of S is a multiple of k_0, i.e. $S = \mathbb{Z}^{\geq 1}k_0$.

(ii) Since (6.5) holds for the sequence $(a_k)_{k\geq 1}$, we have $a_{\ell k_0} \geq a_{k_0}$ for all $\ell \geq 1$ and

$$a_{\gcd(\ell,\ell')k_0} - a_{k_0} = a_{\gcd(\ell k_0,\ell' k_0)} - a_{k_0} = \min\{a_{\ell k_0}, a_{\ell' k_0}\} - a_{k_0} = \min\{a_{\ell k_0} - a_{k_0}, a_{\ell' k_0} - a_{k_0}\}.$$

(iii) We proceed by induction on k. If $k = 1$, we find that $b_1 = \mu(1)a_1 \geq 0$. Suppose that the claim holds for any $k' < k$ and any nonnegative sequence satisfying (6.5). Note that $a_{k'} = 0$ for all $k' \notin S$. Thus, $b_k = \sum_{\{k':k_0|k'|k\}} \mu(k/k')a_{k'}$ vanishes if $k \notin S$, and $b_{k_0} = \mu(1)a_{k_0} > 0$. If $k_0 < k \in S$, write $k = \ell k_0$ for some $\ell > 1$. For all $\ell' \geq 1$, set $\tilde{a}_{\ell'} := a_{\ell' k_0} - a_{k_0}$. By (ii), this defines a sequence of nonnegative integers satisfying (6.5). By Lemma 6.2 (i), the sum $\sum_{\ell'|\ell} \mu(\ell/\ell')$ vanishes. Therefore,

$$b_k = b_{\ell k_0} = \sum_{\ell'|\ell} \mu(\ell/\ell')a_{\ell' k_0} = \sum_{\ell'|\ell} \mu(\ell/\ell')a_{\ell' k_0} - a_{k_0} \sum_{\ell'|\ell} \mu(\ell/\ell') = \sum_{\ell'|\ell} \mu(\ell/\ell')\tilde{a}_{\ell'} = \tilde{b}_\ell.$$

We can thus assume without loss of generality that $k_0 > 1$ (otherwise replace the sequence $(a_k)_{k\geq 1}$ by $(a_k - a_1)_{k\geq 1}$). Then $\ell < k$, so we can apply the induction hypothesis to $\tilde{b}_\ell$ and conclude that $b_k = b_{\ell k_0} = \tilde{b}_\ell \geq 0$.

(iv) If $a_{k'} \in \{0, 1\}$ for each k', then $k' \in S$ if and only if $a_{k'} = 1$. Thus, using Lemma 6.2 (ii),

$$b_k = \sum_{k'|k} \mu(k/k')a_{k'} = \sum_{\{k':k_0|k'|k\}} \mu(k/k') \overset{\substack{\text{Lemma} \\ 6.2\,(ii)}}{=} \begin{cases} 1 & k = k_0, \\ 0 & k \neq k_0. \end{cases}$$

□

Proposition 6.6. *There exist unique polynomials $B_{m,d}$ for all $m \geq 0$ and $d \geq 1$ such that for each $k \geq 1$:*

$$D_{m,k} = \prod_{d|k} B_{m,d}.$$

Proof. Consider the rational functions $B_{m,d} := \prod_{k|d} D_{m,k}^{\mu(d/k)} \in \mathbb{Q}(a, b)$, which satisfy the stated equality by the Möbius inversion formula. We will show that they are in fact polynomials. Since R is a factorial ring, this is equivalent to $\mathrm{ord}_\pi(B_{m,d}) \geq 0$ for all primes $\pi \in R$. Let π be an irreducible polynomial in R, fix $m \geq 0$ and set $a_k := \mathrm{ord}_\pi(D_{m,k})$ for all $k \geq 1$. Since each $D_{m,k}$ is a polynomial, each a_k is nonnegative. Moreover, we have $D_{m,\gcd(k,k')} = \gcd(D_{m,k}, D_{m,k'})$ for all $k, k' \geq 1$ by Claim 5.14. This implies that the sequence $(a_k)_{k\geq 1}$ satisfies $a_{\gcd(k,k')} = \min\{a_k, a_{k'}\}$ for all $k, k' \geq 1$. Thus, we can apply Lemma 6.4 (iii) to find

$$\mathrm{ord}_\pi(B_{m,d}) = \sum_{k|d} \mathrm{ord}_\pi(D_{m,k})\mu(d/k) = \sum_{k|d} a_k \mu(d/k) \geq 0.$$ □

7 The Factors

In this section we will prove that, under certain conditions, the polynomials $B_{m,d}$ found in Proposition 6.6 are pairwise coprime. This implies that the zero locus of $B_{m,k}$ not only contains, but is in fact equal to the Zariski closure of $\mathcal{N}_{m,k}$.

Without any additional requirements on the polynomials, we already have:

Claim 7.1. *For all $m, m' \geq 0$ and $k, k' \geq 1$ the following holds:*

(i) *If $m \neq m'$, then $\gcd(B_{m,k}, B_{m',k'}) = 1$.*

(ii) *If $k \nmid k'$ and $k' \nmid k$, then $\gcd(B_{m,k}, B_{m,k'}) = 1$.*

Proof. (i) If $m \neq m'$, then $\gcd(C_{m,k}, C_{m',k'}) = p_{\gcd(m,m',k,k')} = \gcd(p_{\gcd(m,k)}, p_{\gcd(m',k')})$ for any $k, k' \geq 1$ by Lemmata 5.12 and 5.7. Therefore $\gcd(D_{m,k}, D_{m',k'}) = 1$ by construction and in particular, $\gcd(B_{m,d}, B_{m',d'}) = 1$ for all divisors d of k and d' of k'.
(ii) By Claim 5.14, we have $\gcd(D_{m,k}, D_{m',k'}) = D_{m,\gcd(k,k')}$, which by Proposition 6.6 is the same as

$$\gcd\Big(\prod_{d|k} B_{m,d}, \prod_{d'|k'} B_{m,d'}\Big) = \prod_{\ell|\gcd(k,k')} B_{m,\ell}.$$

Dividing both sides by the left-hand side yields

$$\gcd\Big(\prod_{\substack{d|k \\ d\nmid k'}} B_{m,d}, \prod_{\substack{d'|k' \\ d'\nmid k}} B_{m,d'}\Big) = 1.$$

Since k does not divide k' and vice versa, these products cannot be trivial. This implies in particular that $\gcd(B_{m,k}, B_{m,k'}) = 1$. $\square$

For the remaining case that $m = m'$ and either $k|k'$ or $k'|k$, we only get a conditional result.

In a factorial ring, we say a polynomial g is *reduced* if it is squarefree, i.e. if there is no irreducible polynomial whose square divides g.

Claim 7.2. *Let A be a factorial ring and $g \in A[x, y]$. If $\gcd\left(g, \frac{\partial g}{\partial x}\right) = 1$, then g is reduced.*

Proof. Suppose g is not reduced. Since A is factorial, so is $A[x, y]$, and there exist some $h, \pi \in A[x, y]$ such that π is irreducible and $g = h\pi^2$. Then we have $\frac{\partial g}{\partial x} = \pi^2 \frac{\partial h}{\partial x} + 2h\pi \frac{\partial \pi}{\partial x}$ and thus

$$\gcd\left(g, \frac{\partial g}{\partial x}\right) = \gcd\left(h\pi^2, \pi^2 \frac{\partial h}{\partial x} + 2h\pi \frac{\partial \pi}{\partial x}\right) = \pi \gcd\left(h\pi, \pi \frac{\partial h}{\partial x} + 2h \frac{\partial \pi}{\partial x}\right) \neq 1,$$

since π is not a unit in $A[x, y]$. $\square$

Claim 7.3. *Each p_k is reduced.*

Proof. Let $k \geq 1$ and note that $\frac{\partial p_k}{\partial a} = \frac{\partial}{\partial a}(p_{k-1}^2 + aq_{k-1}^2) \equiv q_{k-1}^2 \bmod 2$. Also, recall that $\gcd(p_k \bmod 2, q_k \bmod 2) = 1$ by Claim 5.5. Therefore,

$$\begin{aligned}\gcd\left(p_k \bmod 2, \frac{\partial p_k}{\partial a} \bmod 2\right) &= \gcd\left(p_{k-1}^2 + aq_{k-1}^2 \bmod 2, q_{k-1}^2 \bmod 2\right) \\ &= \gcd\left(p_{k-1}^2 \bmod 2, q_{k-1}^2 \bmod 2\right) = \gcd\left(p_{k-1} \bmod 2, q_{k-1} \bmod 2\right)^2 = 1.\end{aligned}$$

Since R is a factorial ring, we can apply Claim 7.2 and find that $p_k \bmod 2$ is reduced. Moreover, $\text{content}(p_k) = 1$ and the total degree of p_k is equal to that of $p_k \bmod 2$. Using Gauss' Lemma, we conclude that p_k is reduced. □

This leads to the following statement for $m = 0$:

Claim 7.4. *For all $d > d' \geq 1 : \gcd(B_{0,d}, B_{0,d'}) = 1$.*

Proof. Let π be prime in R. Recall from the proof of Proposition 6.6 that for $d \geq 1$, we can write $\text{ord}_\pi(B_{0,d})$ as the sum $\sum_{k|d} \text{ord}_\pi(p_k)\mu(d/k)$ and apply Lemma 6.4 to the sequence $(\text{ord}_\pi(p_k))_{k\geq 1}$. By Claim 7.3, each p_k is reduced, thus $\text{ord}_\pi(p_k)$ only takes values in $\{0, 1\}$. Using Lemma 6.4 (i) and (iv), we find that $\text{ord}_\pi(B_{0,k_0}) = 1$ if k_0 exists, and for all $d \neq k_0$, $\text{ord}_\pi(B_{0,d}) = 0$. From this we conclude that $\gcd(B_{0,d}, B_{0,d'}) = 1$ for all $d > d' \geq 1$. □

Claim 7.5. *If each $C_{m,k}$ is reduced, then the polynomials $B_{m,d}$ are pairwise coprime.*

Proof. We have already shown in Claim 7.1 that the gcd is trivial if $m \neq m'$. If each $C_{m,k}$ is reduced, then so is each $D_{m,k} = \frac{C_{m,k}}{p_{\gcd(m,k)}}$. Thus, by the same arguments as in the proof of Claim 7.4, we find that the statement is also true for $m = m'$. □

We believe that each $C_{m,k}$ is reduced and that the polynomials $B_{m,d}$ are all irreducible. We have found that both holds for the first 55 polynomials with indices $0 \leq m < 10$ and $1 \leq k \leq 10$ satisfying $m + k \leq 10$. For explicit calculations and results, consult the appendix.

Appendix - Maple calculations

Calculate the iterates f_n(0)=[p_n:q_n] of the critical point 0 by recursion.

```
> p := proc (n::nonnegint) option remember;
> if n = 0 then 0
> else p(n-1)^2+a*q(n-1)^2 fi;
> end proc:
> q := proc (n::nonnegint) option remember;
> if n = 0 then 1
> else p(n-1)^2+b*q(n-1)^2 fi;
> end proc:
```

The equation f_(m+k)(0) = sigma(f_m(0)) for any m,k$\geq$ 1 is equivalent to [p(m+k):q(m+k)] = - [p(m) : q(m)], which is equivalent to the vanishing of the polynomial C_(m,k):=p_(m+k)*q_m + p_m*q_(m+k)

```
> C := proc (m::nonnegint, k::nonnegint) option remember;
> if m = 0 then p(k)
> else p(m+k)*q(m)+p(m)*q(m+k) fi;
> end proc:
```

Define new polynomials D_(m,k) by clearing C_(m,k) of common factors with C_(0,k')

```
> DD := proc (m::nonnegint, k::nonnegint) option remember;
> if m = 0 then p(k)
> else if divide(C(m,k), C(0,gcd(m,k)), 'temp') then temp;
> else printf("problem at (%d,%d)",m,k); fi; fi; end proc:
```

The factorisation of D_(m,k) is given by D_(m,k)=$\prod_{d|k}$B_(m,d)

```
> with(numtheory):
> B := proc (m::nonnegint, k::nonnegint) option remember;
> if k = 1 then DD(m,k)
> else if
> divide(DD(m,k), mul( B(m,d), d in (divisors(k)\{k}) ),'temp')
> then B(m,k) := temp;
> else printf("problem at (%d,%d)",m,k); fi; fi;
> end proc:
```

This proc outputs true if the input polynomial is reduced, and otherwise false.

```
> IsSquareFree := proc(f)
> local fact,expo,i;
> fact := sqrfree(f)[2];
> expo := max(0,seq(fact[i][2],i=1..nops(fact)));
> if expo<=1 then true else false fi;
> end proc:
```

Check if the polynomials C_(m,k) are reduced for all indices with m+k $\leq$ nmax, k=1,...,nmax

```
> nmax := 10;
> seq(seq(print([m,k,IsSquareFree(C(m,k))]),m=0..nmax-k),k=1..nmax);
```

$[0,1,\mathit{true}]$	$[1,2,\mathit{true}]$	$[3,3,\mathit{true}]$	$[6,4,\mathit{true}]$	$[4,6,\mathit{true}]$
$[1,1,\mathit{true}]$	$[2,2,\mathit{true}]$	$[4,3,\mathit{true}]$	$[0,5,\mathit{true}]$	$[0,7,\mathit{true}]$
$[2,1,\mathit{true}]$	$[3,2,\mathit{true}]$	$[5,3,\mathit{true}]$	$[1,5,\mathit{true}]$	$[1,7,\mathit{true}]$
$[3,1,\mathit{true}]$	$[4,2,\mathit{true}]$	$[6,3,\mathit{true}]$	$[2,5,\mathit{true}]$	$[2,7,\mathit{true}]$
$[4,1,\mathit{true}]$	$[5,2,\mathit{true}]$	$[7,3,\mathit{true}]$	$[3,5,\mathit{true}]$	$[3,7,\mathit{true}]$
$[5,1,\mathit{true}]$	$[6,2,\mathit{true}]$	$[0,4,\mathit{true}]$	$[4,5,\mathit{true}]$	$[0,8,\mathit{true}]$
$[6,1,\mathit{true}]$	$[7,2,\mathit{true}]$	$[1,4,\mathit{true}]$	$[5,5,\mathit{true}]$	$[1,8,\mathit{true}]$
$[7,1,\mathit{true}]$	$[8,2,\mathit{true}]$	$[2,4,\mathit{true}]$	$[0,6,\mathit{true}]$	$[2,8,\mathit{true}]$
$[8,1,\mathit{true}]$	$[0,3,\mathit{true}]$	$[3,4,\mathit{true}]$	$[1,6,\mathit{true}]$	$[0,9,\mathit{true}]$
$[9,1,\mathit{true}]$	$[1,3,\mathit{true}]$	$[4,4,\mathit{true}]$	$[2,6,\mathit{true}]$	$[1,9,\mathit{true}]$
$[0,2,\mathit{true}]$	$[2,3,\mathit{true}]$	$[5,4,\mathit{true}]$	$[3,6,\mathit{true}]$	$[0,10,\mathit{true}]$

Output the factors B_(0,k) for k=1,...,nmax

```
> nmax := 6; K1 := seq(print([0,k,B(0,k)]), k=1..nmax);
```

$$[\mathbf{0{,}1}, a]$$

$$[\mathbf{0{,}2}, b^2 + a]$$

$$[\mathbf{0{,}3}, b^6 + 2\,a^2b^3 + ab^4 + a^4 + 2\,a^2b^2 + a^3]$$

$$\begin{aligned}[\mathbf{0{,}4}, &b^{12} + 6\,a^2b^9 + 11\,a^4b^6 + 2\,a^3b^7 + 2\,a^2b^8 + 6\,a^6b^3 + 7\,a^5b^4 + 4\,a^4b^5 + 3\,a^3b^6 \\ &+a^8 + 2\,a^7b + 5\,a^6b^2 + 4\,a^5b^3 + 3\,a^4b^4 + 3\,a^7 + 3\,a^5b^2 + a^6]\end{aligned}$$

$$\begin{aligned}[\mathbf{0{,}5}, &b^{30} + 14\,a^2b^{27} + ab^{28} + 79\,a^4b^{24} + 24\,a^3b^{25} + 2\,a^2b^{26} + 234\,a^6b^{21} + 174\,a^5b^{22} \\ &+42\,a^4b^{23} + 5\,a^3b^{24} + 403\,a^8b^{18} + 560\,a^7b^{19} + 324\,a^6b^{20} + 64\,a^5b^{21} + 14\,a^4b^{22} \\ &+432\,a^{10}b^{15} + 903\,a^9b^{16} + 1086\,a^8b^{17} + 424\,a^7b^{18} + 132\,a^6b^{19} + 26\,a^5b^{20} + 308\,a^{12}b^{12} + 768\,a^{11}b^{13} \\ &+1712\,a^{10}b^{14} + 1344\,a^9b^{15} + 621\,a^8b^{16} + 208\,a^7b^{17} + 44\,a^6b^{18} + 150\,a^{14}b^9 + 374\,a^{13}b^{10} + 1294\,a^{12}b^{11} \\ &+1962\,a^{11}b^{12} + 1510\,a^{10}b^{13} + 806\,a^9b^{14} + 270\,a^8b^{15} + 69\,a^7b^{16} + 49\,a^{16}b^6 + 104\,a^{15}b^7 + 528\,a^{14}b^8 \\ &+1224\,a^{13}b^9 + 1780\,a^{12}b^{10} + 1496\,a^{11}b^{11} + 848\,a^{10}b^{12} + 312\,a^9b^{13} + 94\,a^8b^{14} + 10\,a^{18}b^3 + 13\,a^{17}b^4 \\ &+124\,a^{16}b^5 + 360\,a^{15}b^6 + 848\,a^{14}b^7 + 1308\,a^{13}b^8 + 1152\,a^{12}b^9 + 792\,a^{11}b^{10} + 284\,a^{10}b^{11} + 114\,a^9b^{12} \\ &+a^{20} + 14\,a^{18}b^2 + 56\,a^{17}b^3 + 154\,a^{16}b^4 + 456\,a^{15}b^5 + 688\,a^{14}b^6 + 712\,a^{13}b^7 + 598\,a^{12}b^8 + 208\,a^{11}b^9 \\ &+116\,a^{10}b^{10} + 5\,a^{19} + 6\,a^{18}b + 58\,a^{17}b^2 + 142\,a^{16}b^3 + 272\,a^{15}b^4 + 324\,a^{14}b^5 + 340\,a^{13}b^6 + 124\,a^{12}b^7 \\ &+94\,a^{11}b^8 + 12\,a^{18} + 16\,a^{17}b + 87\,a^{16}b^2 + 80\,a^{15}b^3 + 152\,a^{14}b^4 + 48\,a^{13}b^5 + 60\,a^{12}b^6 + 15\,a^{17} \\ &+6\,a^{16}b + 48\,a^{15}b^2 + 8\,a^{14}b^3 + 28\,a^{13}b^4 + 7\,a^{16} + 8\,a^{14}b^2 + a^{15}]\end{aligned}$$

$$
\begin{aligned}
&[\mathbf{0,6}, b^{54} + 28a^2b^{51} - ab^{52} + 350a^4b^{48} + a^2b^{50} + 2586a^6b^{45} + 306a^5b^{46} + 30a^4b^{47} + 3a^3b^{48} \\
&+12613a^8b^{42} + 4176a^7b^{43} + 666a^6b^{44} + 88a^5b^{45} + 7a^4b^{46} + 42996a^{10}b^{39} + 27933a^9b^{40} \\
&+8130a^8b^{41} + 1444a^7b^{42} + 210a^6b^{43} + 17a^5b^{44} + 105927a^{12}b^{36} + 114698a^{11}b^{37} + 56559a^{10}b^{38} \\
&+15244a^9b^{39} + 3073a^8b^{40} + 474a^7b^{41} + 35a^6b^{42} + 192688a^{14}b^{33} + 314574a^{13}b^{34} + 243560a^{12}b^{35} \\
&+101456a^{11}b^{36} + 28486a^{10}b^{37} + 6268a^9b^{38} + 922a^8b^{39} + 76a^7b^{40} + 262700a^{16}b^{30} + 601160a^{15}b^{31} \\
&+687287a^{14}b^{32} + 430746a^{13}b^{33} + 173274a^{12}b^{34} + 51588a^{11}b^{35} + 11403a^{10}b^{36} + 1762a^9b^{37} \\
&+155a^8b^{38} + 271526a^{18}b^{27} + 820318a^{17}b^{28} + 1316432a^{16}b^{29} + 1196768a^{15}b^{30} + 690876a^{14}b^{31} \\
&+282037a^{13}b^{32} + 85702a^{12}b^{33} + 19688a^{11}b^{34} + 3180a^{10}b^{35} + 298a^9b^{36} + 214771a^{20}b^{24} \\
&+812000a^{19}b^{25} + 1749749a^{18}b^{26} + 2223320a^{17}b^{27} + 1814818a^{16}b^{28} + 1026624a^{15}b^{29} \\
&+423486a^{14}b^{30} + 133880a^{13}b^{31} + 31645a^{12}b^{32} + 5456a^{11}b^{33} + 536a^{10}b^{34} + 130948a^{22}b^{21} \\
&+589244a^{21}b^{22} + 1638336a^{20}b^{23} + 2803380a^{19}b^{24} + 3164208a^{18}b^{25} + 2475480a^{17}b^{26} \\
&+1391432a^{16}b^{27} + 594656a^{15}b^{28} + 192272a^{14}b^{29} + 48400a^{13}b^{30} + 8612a^{12}b^{31} + 927a^{11}b^{32} \\
&+61809a^{24}b^{18} + 315140a^{23}b^{19} + 1092212a^{22}b^{20} + 2425524a^{21}b^{21} + 3681233a^{20}b^{22} \\
&+3941328a^{19}b^{23} + 3019268a^{18}b^{24} + 1743096a^{17}b^{25} + 762649a^{16}b^{26} + 258780a^{15}b^{27} + 68636a^{14}b^{28} \\
&+12660a^{13}b^{29} + 1525a^{12}b^{30} + 22578a^{26}b^{15} + 124043a^{25}b^{16} + 520860a^{24}b^{17} + 1452522a^{23}b^{18} \\
&+2868864a^{22}b^{19} + 4128115a^{21}b^{20} + 4288488a^{20}b^{21} + 3338604a^{19}b^{22} + 1983642a^{18}b^{23} \\
&+897163a^{17}b^{24} + 324480a^{16}b^{25} + 89042a^{15}b^{26} + 17568a^{14}b^{27} + 2331a^{13}b^{28} + 6331a^{28}b^{12} \\
&+35532a^{27}b^{13} + 177023a^{26}b^{14} + 603264a^{25}b^{15} + 1503368a^{24}b^{16} + 2832796a^{23}b^{17} + 3946778a^{22}b^{18} \\
&+4126904a^{21}b^{19} + 3316469a^{20}b^{20} + 2033672a^{19}b^{21} + 972789a^{18}b^{22} + 370384a^{17}b^{23} \\
&+107112a^{16}b^{24} + 22568a^{15}b^{25} + 3310a^{14}b^{26} + 1334a^{30}b^9 + 7200a^{29}b^{10} + 42212a^{28}b^{11} + 172198a^{27}b^{12} \\
&+527290a^{26}b^{13} + 1270876a^{25}b^{14} + 2323064a^{24}b^{15} + 3251238a^{23}b^{16} + 3494178a^{22}b^{17} \\
&+2923140a^{21}b^{18} + 1881324a^{20}b^{19} + 955386a^{19}b^{20} + 385082a^{18}b^{21} + 118340a^{17}b^{22} + 26652a^{16}b^{23} \\
&+4346a^{15}b^{24} + 202a^{32}b^6 + 968a^{31}b^7 + 6821a^{30}b^8 + 32896a^{29}b^9 + 121303a^{28}b^{10} + 367336a^{27}b^{11} \\
&+866993a^{26}b^{12} + 1591376a^{25}b^{13} + 2302779a^{24}b^{14} + 2561136a^{23}b^{15} + 2280889a^{22}b^{16} \\
&+1545972a^{21}b^{17} + 845085a^{20}b^{18} + 360872a^{19}b^{19} + 119397a^{18}b^{20} + 28612a^{17}b^{21} + 5258a^{16}b^{22} \\
&+20a^{34}b^3 + 74a^{33}b^4 + 692a^{32}b^5 + 3984a^{31}b^6 + 17394a^{30}b^7 + 65928a^{29}b^8 + 199512a^{28}b^9 \\
&+474320a^{27}b^{10} + 912544a^{26}b^{11} + 1369182a^{25}b^{12} + 1620516a^{24}b^{13} + 1545072a^{23}b^{14} \\
&+1117458a^{22}b^{15} + 666150a^{21}b^{16} + 300492a^{20}b^{17} + 109664a^{19}b^{18} + 27440a^{18}b^{19} + 5843a^{17}b^{20} + a^{36} \\
&+2a^{35}b + 35a^{34}b^2 + 280a^{33}b^3 + 1361a^{32}b^4 + 6796a^{31}b^5 + 26533a^{30}b^6 + 81736a^{29}b^7 + 209508a^{28}b^8 \\
&+422192a^{27}b^9 + 678458a^{26}b^{10} + 866832a^{25}b^{11} + 892081a^{24}b^{12} + 702244a^{23}b^{13} + 458529a^{22}b^{14} \\
&+220896a^{21}b^{15} + 90139a^{20}b^{16} + 23310a^{19}b^{17} + 5892a^{18}b^{18} + 10a^{35} + 38a^{34}b + 320a^{33}b^2 + 1816a^{32}b^3 \\
&+7082a^{31}b^4 + 25678a^{30}b^5 + 70168a^{29}b^6 + 154292a^{28}b^7 + 274142a^{27}b^8 + 379354a^{26}b^9 + 433808a^{25}b^{10} \\
&+372712a^{24}b^{11} + 271958a^{23}b^{12} + 140724a^{22}b^{13} + 65346a^{21}b^{14} + 17314a^{20}b^{15} + 5313a^{19}b^{16} \\
&+51a^{34} + 208a^{33}b + 1304a^{32}b^2 + 5516a^{31}b^3 + 16563a^{30}b^4 + 43612a^{29}b^5 + 84972a^{28}b^6 \\
&+133296a^{27}b^7 + 171645a^{26}b^8 + 162632a^{25}b^9 + 136261a^{24}b^{10} + 75492a^{23}b^{11} + 41263a^{22}b^{12} \\
&+10996a^{21}b^{13} + 4219a^{20}b^{14} + 157a^{33} + 528a^{32}b + 2822a^{31}b^2 + 8182a^{30}b^3 + 19541a^{29}b^4 \\
&+35520a^{28}b^5 + 53012a^{27}b^6 + 56496a^{26}b^7 + 55792a^{25}b^8 + 33098a^{24}b^9 + 22138a^{23}b^{10} + 5832a^{22}b^{11} \\
&+2892a^{21}b^{12} + 295a^{32} + 688a^{31}b + 3337a^{30}b^2 + 6024a^{29}b^3 + 12669a^{28}b^4 + 14274a^{27}b^5 \\
&+18273a^{26}b^6 + 11204a^{25}b^7 + 9812a^{24}b^8 + 2482a^{23}b^9 + 1672a^{22}b^{10} + 332a^{31} + 440a^{30}b \\
&+2246a^{29}b^2 + 2160a^{28}b^3 + 4704a^{27}b^4 + 2598a^{26}b^5 + 3500a^{25}b^6 + 778a^{24}b^7 + 792a^{23}b^8 + 215a^{30} \\
&+130a^{29}b + 854a^{28}b^2 + 332a^{27}b^3 + 947a^{26}b^4 + 154a^{25}b^5 + 293a^{24}b^6 + 77a^{29} + 14a^{28}b + 168a^{27}b^2 \\
&+14a^{26}b^3 + 78a^{25}b^4 + 14a^{28} + 13a^{26}b^2 + a^{27}]
\end{aligned}
$$

This is an irreducibility test for a given factor B_(m,k)

```
> IrreducibilityTest := proc (m::nonnegint, k::nonnegint)
> if irreduc(B(m,k)) then printf("B(%d,%d) is irreducible",m,k)
> else printf("B(%d,%d) is not irreducible",m,k) fi;
> end proc:
```

Check if the polynomials B_(m,k) are irreducible for all indices with m+k $\leq$ nmax, k=1,...,nmax

```
> seq(seq(print(IrreducibilityTest(m,k)), m=0..nmax-k), k=1..nmax);
```

B(0,1) *is irreducible*
B(1,1) *is irreducible*
B(2,1) *is irreducible*
B(3,1) *is irreducible*
B(4,1) *is irreducible*
B(5,1) *is irreducible*
B(6,1) *is irreducible*
B(7,1) *is irreducible*
B(8,1) *is irreducible*
B(9,1) *is irreducible*
B(0,2) *is irreducible*
B(1,2) *is irreducible*
B(2,2) *is irreducible*
B(3,2) *is irreducible*
B(4,2) *is irreducible*
B(5,2) *is irreducible*
B(6,2) *is irreducible*
B(7,2) *is irreducible*
B(8,2) *is irreducible*
B(0,3) *is irreducible*
B(1,3) *is irreducible*
B(2,3) *is irreducible*
B(3,3) *is irreducible*
B(4,3) *is irreducible*
B(5,3) *is irreducible*
B(6,3) *is irreducible*
B(7,3) *is irreducible*
B(0,4) *is irreducible*
B(1,4) *is irreducible*
B(2,4) *is irreducible*
B(3,4) *is irreducible*
B(4,4) *is irreducible*
B(5,4) *is irreducible*
B(6,4) *is irreducible*
B(0,5) *is irreducible*
B(1,5) *is irreducible*
B(2,5) *is irreducible*
B(3,5) *is irreducible*
B(4,5) *is irreducible*
B(5,5) *is irreducible*
B(0,6) *is irreducible*
B(1,6) *is irreducible*
B(2,6) *is irreducible*
B(3,6) *is irreducible*
B(4,6) *is irreducible*
B(0,7) *is irreducible*
B(1,7) *is irreducible*
B(2,7) *is irreducible*
B(3,7) *is irreducible*
B(0,8) *is irreducible*
B(1,8) *is irreducible*
B(2,8) *is irreducible*
B(0,9) *is irreducible*
B(1,9) *is irreducible*
B(0,10) *is irreducible*

References

[1] Milnor, J.: Geometry and dynamics of quadratic rational maps. *Experiment. Math.* **2** (1993), no. 1, 37–83.

[2] Pink, R.: *Finiteness and liftability of postcritically finite quadratic morphisms in arbitrary characteristic.* Preprint (version 3, August 2013), 36p. `arXiv` : `1305.2841`[`math.AG`]

[3] Rassias, M.T.: *Problem-Solving and Selected Topics in Number Theory: In the Spirit of the Mathematical Olympiads.* Springer, 2011

[4] Silverman, J.H.: *The Arithmetic of Dynamical Systems.* Graduate Texts in Mathematics **241**. Springer, 2007