

AN ALGEBRAIC APPROACH TO CERTAIN CASES OF THURSTON RIGIDITY

JOSEPH H. SILVERMAN

(Communicated by Bryna Kra)

ABSTRACT. In the parameter space of monic centered polynomials of degree 3 with marked critical points c_1 and c_2 , let $C_{1,n}$ be the locus of maps for which c_1 has period n and let $C_{2,m}$ be the locus of maps for which c_2 has period m . A consequence of Thurston's rigidity theorem is that the curves $C_{1,n}$ and $C_{2,m}$ intersect transversally. We give a purely algebraic proof that the intersection points are 3-adically integral and use this to prove transversality. We also prove an analogous result when c_1 or c_2 or both are taken to be preperiodic with tail length exactly 1.

1. INTRODUCTION

The moduli space of polynomials of degree $d \geq 2$ is the space of polynomials modulo conjugation by the affine action $z \mapsto \alpha z + \beta$. Working over \mathbb{C} and choosing appropriate values for α and β , every degree d polynomial can be put into monic centered form

$$f(z) = z^d + a_2 z^{d-2} + \cdots + a_d.$$

We will work on $\mathcal{P}_d \cong \mathbb{C}^{d-1}$, the parameter space of monic centered polynomials. This space is a $(d-1)$ -fold branched cover of the associated moduli space, since $f \in \mathcal{P}_d$ is conjugate to $\zeta^{-1}f(\zeta z)$ for $\zeta \in \mu_{d-1}$. The polynomial f has $d-1$ critical points (counted with multiplicity), and we write $\mathcal{P}_d^{\text{crit}}$ for the space of monic centered polynomials f with marked critical point (c_1, \dots, c_{d-1}) . Imposing natural relations on these critical points gives subvarieties of $\mathcal{P}_d^{\text{crit}}$, and an important consequence of Thurston's rigidity theorem [2] is that in many cases these subvarieties have transversal intersection. For example, transversality holds if we require c_1, \dots, c_{d-1} to be periodic with respective periods n_1, \dots, n_{d-1} , or more generally if they are preperiodic with specified tail lengths and periods. Thurston's theorem also gives analogous results for rational functions.

The proof of Thurston's general theorem is quite difficult and requires deep tools; see [2]. Adam Epstein has asked if one might prove at least some cases of Thurston rigidity using p -adic and/or algebraic methods. In this paper we give an algebraic 3-adic proof of the following special case of Thurston rigidity for cubic polynomials.

Theorem 1. *Let $\mathcal{P}_3^{\text{crit}}$ be the parameter space of monic centered polynomials of degree 3 with marked critical points; i.e., points in $\mathcal{P}_3^{\text{crit}}$ are equivalence classes of*

Received by the editors October 21, 2010 and, in revised form, April 5, 2011.

2010 *Mathematics Subject Classification.* Primary 37F10; Secondary 37P05 37P45.

The author's research is supported by NSF DMS-0650017 and DMS-0854755.

©2012 American Mathematical Society
Reverts to public domain 28 years from publication

triples (f, c_1, c_2) , where $f \in \mathbb{C}[z]$ is a monic centered polynomial of degree 3 and c_1 and c_2 are the critical points of f .

For integers $n, m \geq 1$, let

$$C_{1,n} = \{(f, c_1, c_2) \in \mathcal{P}_3^{\text{crit}} : c_1 \text{ is periodic with } f^n(c_1) = c_1\},$$

$$C_{2,m} = \{(f, c_1, c_2) \in \mathcal{P}_3^{\text{crit}} : c_2 \text{ is periodic with } f^m(c_2) = c_2\}.$$

Then $C_{1,n}$ and $C_{2,m}$ intersect transversally at all of their points of intersection.

For a complex analytic proof of Theorem 1, see [6, Lemma 5.5 and Theorem 5.1]. (See also [4] for transversality results based on a formal identity.) Our 3-adic proof of Theorem 1 may be compared with the analogous 2-adic proof for quadratic polynomials that is due independently to Adler and Gleason; see [1, Lemma 19.1] and [5], and also [3, Appendix] for a generalization. Our proof of Theorem 1 may also be compared with the recent, independently discovered, 3-adic proof by Epstein [3]. (We note that Epstein's paper contains results stronger than our Theorem 1. The primary purpose of our paper is to provide a conceptually different proof.) Both our proof and Epstein's proof deduce the final conclusion, namely that a certain Jacobian determinant is nonzero, by showing that it does not vanish modulo 3. The most difficult part of the proof is to show that the critical points of suitably normalized post-critically finite cubic polynomials are 3-adically integral, and this is where the two proofs differ. Epstein's proof uses a detailed analysis of the sequence of 3-adic valuations $\text{ord}_3(f^n(c))$ of the points in the forward orbit of a critical point. Thus it makes extensive use of a (p -adic) metric and has a dynamical flavor. Our proof uses an estimate for the degrees of the curves $C_{1,n}$ and $C_{2,m}$, followed by a resultant calculation, so is much more algebraic in nature. We mention in particular the interesting explicit formula (Lemma 8) for the resultant

$$\text{Res}(x^{p^n} - x - A, x^{p^m} - x - B) \in \mathbb{F}_p[A, B].$$

This formula is used to show (Theorem 11) that a certain resultant has maximal degree by showing that it has maximal degree when reduced modulo 3.

Thurston's theorem deals also with the case that the critical points are preperiodic, i.e., have finite orbits. Using an algebraic trick, we are able to give an algebraic proof of this result for cubic polynomials in the case that the critical points have tail length at most 1. We give the exact statement and proof in Section 3. It would be quite interesting to extend this result to allow arbitrary preperiodic behavior.

2. PROOF OF THURSTON RIGIDITY FOR CUBIC POLYNOMIALS

In this section we give the proof of Theorem 1. Making a change of variables, we may assume that our cubic polynomials have the form

$$f_{x,y}(z) = z^3 - 3x^2z + y$$

with marked critical points $\pm x$. For the given integers $n, m \geq 1$, we let

$$(1) \quad F^{(n)}(x, y) = f_{x,y}^n(x) - x \quad \text{and} \quad G^{(m)}(x, y) = f_{x,y}^m(-x) + x.$$

Then the solutions to

$$(2) \quad F^{(n)}(x, y) = G^{(m)}(x, y) = 0$$

are exactly the pairs (α, β) with the property that the critical points of $f_{\alpha,\beta}(z)$ have periods n and m , respectively.

Let $(\alpha, \beta) \in \mathbb{C}$ be a solution to (2). The curves $F^{(n)} = 0$ and $G^{(m)} = 0$ intersect transversally at (α, β) if and only if the Jacobian determinant does not vanish, i.e.,

$$\det \begin{pmatrix} F_x^{(n)}(\alpha, \beta) & G_x^{(m)}(\alpha, \beta) \\ F_y^{(n)}(\alpha, \beta) & G_y^{(m)}(\alpha, \beta) \end{pmatrix} \neq 0.$$

In general, the Jacobian determinant is the polynomial

$$(3) \quad J(x, y) = \det \begin{pmatrix} F_x^{(n)}(x, y) & G_x^{(m)}(x, y) \\ F_y^{(n)}(x, y) & G_y^{(m)}(x, y) \end{pmatrix} \in \mathbb{Z}[x, y].$$

Then the curves $F^{(n)} = 0$ and $G^{(m)} = 0$ intersect transversally at all of their intersection points if and only if the ideal

$$(F^{(n)}(x, y), G^{(m)}(x, y), J(x, y)) \subset \mathbb{C}[x, y]$$

is the unit ideal.

We will prove that $(F^{(n)}, G^{(m)}, J) = (1)$ by proving the following two assertions.

- All solutions (α, β) to $F^{(n)} = G^{(m)} = 0$ are 3-adically integral.
- $J(x, y) \equiv 1 \pmod{3}$.

Remark 2. Our proof of Theorem 1, *mutatis mutandis*, can be used to show the following more general result. Let $p \geq 3$ be prime and let

$$f_{x,y}(z) = z^p - px^{p-1}z - y.$$

The critical points of $f_{x,y}$ are the points ζx , where $\zeta \in \mu_{p-1}$. Let ζ_1 and ζ_2 be distinct $(p - 1)^{\text{st}}$ roots of unity. Fix integers $n, m \geq 1$. Then the curves

$$f_{x,y}^n(\zeta_1 x) = \zeta_1 x \quad \text{and} \quad f_{x,y}^m(\zeta_2 x) = \zeta_2 x$$

intersect transversally.

We begin with a lemma that describes the iterates of $f_{x,y}(z)$ evaluated at $z = x$.

Lemma 3. *Let*

$$f_{x,y}(z) = z^3 - 3x^2z + y.$$

Then

$$(4) \quad f_{x,y}^n(z) = f_{-x,y}^n(z).$$

The iterates of $f_{x,y}$ evaluated at x have the following properties:

- (a) *As a polynomial in x ,*

$$(5) \quad f_{x,y}^n(x) = \sum_{k=0}^{3^n} a_k(y)x^{3^n-k} \in \mathbb{Z}[y][x]$$

with

$$(6) \quad \deg a_k(y) \leq 4 \left\lfloor \frac{k}{3} \right\rfloor - k,$$

$$(7) \quad a_0(y) = (-2)^{3^{n-1}} \equiv 1 \pmod{3},$$

$$(8) \quad a_{3^n}(y) = y^{3^{n-1}} + (\text{lower order terms}).$$

(By convention, a polynomial with negative degree is the zero polynomial.)

(b) Reducing modulo 3, we have

$$f_{x,y}^n(x) \equiv x^{3^n} + y + y^3 + y^9 + \dots + y^{3^{n-1}} \pmod{3}.$$

(c) For $n, m \geq 1$, define

$$F^{(n)}(x, y) = f_{x,y}^n(x) - x \quad \text{and} \quad G^{(m)}(x, y) = f_{x,y}^m(-x) + x.$$

Then $F^{(n)}(x, y) \in \mathbb{Z}[x, y]$ and $G^{(m)}(x, y) \in \mathbb{Z}[x, y]$. Further

$$G^{(m)}(x, y) = F^{(m)}(-x, y)$$

and

$$F^{(n)}(x, y) \equiv x^{3^n} - x + y + y^3 + y^9 + \dots + y^{3^{n-1}} \pmod{3},$$

$$G^{(m)}(x, y) \equiv -x^{3^m} + x + y + y^3 + y^9 + \dots + y^{3^{m-1}} \pmod{3}.$$

Remark 4. The upper bound on the right-hand side of (6) has the form

k	0	1	2	3	4	5	6	7	8	9	10	11	12	...
$4\lfloor k/3 \rfloor - k$	0	-1	-2	1	0	-1	2	1	0	3	2	1	4	...

Experimentally, it seems that the polynomials $a_k(y)$ appearing in the expansion (5) satisfy

$$\deg a_k(y) = 4\lfloor k/3 \rfloor - k \quad \text{for all } k \text{ except } k = 3^n - 1,$$

and $a_{3^n-1}(y) = 0$. It would probably not be hard to prove this by induction.

Proof. It is clear that we can write $f_{x,y}^n(x)$ in the form (5) for some polynomials $a_k(y) \in \mathbb{Z}[y]$, so it remains to prove that these polynomials satisfy (6), (7) and (8). We begin with the proof of (6), which is by induction on n . To indicate the dependence on n , we write $a_k^{(n)}(y)$. For $n = 1$ we have

$$f_{x,y}^1(x) = z^3 - 3x^2z + y \Big|_{z \rightarrow x} = -2x^3 + y,$$

so

$$a_0^{(1)}(y) = -2, \quad a_1^{(1)}(y) = a_2^{(1)}(y) = 0, \quad a_3^{(1)}(y) = y.$$

Next we assume that (6) is true for n and we compute

$$\begin{aligned} f_{xy}^{n+1}(x) &= f_{xy}(f_{xy}^n(x)) \\ &= f_{xy}^n(x)^3 - 3x^2 f_{xy}^n(x) + y \\ (9) \quad &= \left(\sum_{k=0}^{3^n} a_k^{(n)}(y)x^{3^n-k} \right)^3 - 3x^2 \left(\sum_{k=0}^{3^n} a_k^{(n)}(y)x^{3^n-k} \right) + y. \end{aligned}$$

We consider first the cubed expression in (9). If it is multiplied out, we obtain a sum of terms of the form

$$a_i^{(n)}(y)x^{3^n-i} a_j^{(n)}(y)x^{3^n-j} a_k^{(n)}(y)x^{3^n-k} = a_i^{(n)}(y)a_j^{(n)}(y)a_k^{(n)}(y)x^{3^{n+1}-i-j-k}$$

with $0 \leq i, j, k \leq 3^n$. Applying (6) to $a_i^{(n)}(y)$, $a_j^{(n)}(y)$, and $a_k^{(n)}(y)$, we find that

$$\begin{aligned} \deg(a_i^{(n)}(y)a_j^{(n)}(y)a_k^{(n)}(y)) &\leq 4 \left\lfloor \frac{i}{3} \right\rfloor - i + 4 \left\lfloor \frac{j}{3} \right\rfloor - j + 4 \left\lfloor \frac{k}{3} \right\rfloor - k \\ &\leq 4 \left\lfloor \frac{i+j+k}{3} \right\rfloor - i - j - k, \end{aligned}$$

where the last line follows from the elementary inequality (see Section 4)

$$(10) \quad [t_1] + [t_2] + [t_3] \leq [t_1 + t_2 + t_3] \quad \text{for all } t_1, t_2, t_3 \in \mathbb{R}.$$

Thus terms coming from the cubed expression in (9) satisfy (6) for $n + 1$. Since it is easy to see that the other terms in (9) satisfy (6) for $n + 1$, this completes the proof by induction that (6) holds for all $n \geq 1$.

In order to prove (7), we observe that if we assign weight 1 to both x and z and weight 0 to y , then the terms of weight 3^n in $f_{xy}^n(z)$ are precisely the ones that come from repeatedly cubing the degree 3 expression $z^3 - 3x^2z$, i.e.,

$$f_{xy}^n(z) = (z^3 - 3x^2z)^{3^{n-1}} + (\text{lower weight terms}).$$

Hence

$$\begin{aligned} a_0^{(n)}(y) &= \text{coefficient of } x^{3^n} \text{ in } f_{xy}^n(x) \\ &= \text{coefficient of } x^{3^n} \text{ in } (-2x^3)^{3^{n-1}} \\ &= (-2)^{3^{n-1}}. \end{aligned}$$

The proof of (8) is a trivial induction on n . More precisely, if we let y have weight 1 and x and z have weight 0, then

$$\begin{aligned} f_{x,y}^{n+1}(x) &= f_{x,y}^n(x)^3 - 3x^2f_{x,y}^n(x) + y \\ &= (y^{3^{n-1}} + (\text{lower weight terms}))^3 \\ &\quad - 3x^2(y^{3^{n-1}} + (\text{lower weight terms})) + y \\ &= y^{3^n} + (\text{lower weight terms}). \end{aligned}$$

This completes the proof of (a).

For (b) we are working modulo 3, so

$$f_{x,y}(z) \equiv z^3 + y \pmod{3}.$$

An easy induction gives the desired result:

$$\begin{aligned} f_{x,y}^{n+1}(x) &\equiv f(f_{x,y}^n(x)) \pmod{3} \\ &\equiv f_{x,y}^n(x)^3 + y \pmod{3} \\ &\equiv (x^{3^n} + y + y^3 + y^9 + \dots + y^{3^{n-1}})^3 + y \pmod{3} \\ &\equiv x^{3^{n+1}} + y^3 + y^9 + y^{27} + \dots + y^{3^n} + y \pmod{3}. \end{aligned}$$

To prove the first part of (c), we evaluate (4) at $z = -x$ to obtain $f_{x,y}^n(-x) = f_{-x,y}^n(-x)$. Substituting this into the definition of $G^{(n)}(x, y)$ yields

$$G^{(n)}(x, y) = f_{x,y}^n(-x) + x = f_{-x,y}^n(-x) + x = F^{(n)}(-x, y).$$

Finally, the values of $F^{(n)}$ and $G^{(n)}$ modulo 3 follow from the value of $f_{x,y}^n(x)$ modulo 3 computed in (b). \square

An immediate consequence of Lemma 3 is the mod 3 value of the Jacobian.

Proposition 5. *The Jacobian determinant $J(x, y) \in \mathbb{Z}[x, y]$ defined by (3) satisfies*

$$J(x, y) \equiv 1 \pmod{3}.$$

Proof. Differentiating the formulas for $F^{(n)}(x, y)$ and $G^{(m)}(x, y)$ in Lemma 3(c) and reducing modulo 3 yields

$$J(x, y) = \det \begin{pmatrix} F_x^{(n)}(x, y) & G_x^{(m)}(x, y) \\ F_y^{(n)}(x, y) & G_y^{(m)}(x, y) \end{pmatrix} \equiv \det \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix} \equiv 1 \pmod{3}.$$

□

Before tackling the 3-integrality of the common roots of $F^{(n)}(x, y)$ and $G^{(m)}(x, y)$, we prove two elementary lemmas. With an eye towards generalizations, we work over \mathbb{F}_p .

Lemma 6. *Let p be a prime, let $m, n \geq 1$ be integers, let $d = \gcd(m, n)$, and let τ denote the p -power Frobenius map. Then*

$$(11) \quad \prod_{u \in \mathbb{F}_{p^n}} \prod_{v \in \mathbb{F}_{p^m}} (T - u - v) = \frac{\tau^d \circ (\tau^n - 1) \circ (\tau^m - 1)}{\tau^d - 1}(T) \in \mathbb{F}_p[T].$$

Remark 7. The meaning of the right-hand side of (11) is as follows. The rational expression $\frac{\tau^d \circ (\tau^n - 1) \circ (\tau^m - 1)}{\tau^d - 1}$ is actually a polynomial in τ , since d divides m . In other words, it is an element of $\mathbb{Z}[\tau]$. We then use the natural action of $\mathbb{Z}[\tau]$ on $\mathbb{F}_p[T]$ defined by

$$\left(\sum a_i \tau^i \right) (f(T)) = \sum a_i f(T)^{p^i}.$$

Proof. We first observe that if $u_1, u_2 \in \mathbb{F}_{p^n}$ and $v_1, v_2 \in \mathbb{F}_{p^m}$ satisfy

$$u_1 + v_1 = u_2 + v_2,$$

then

$$u_1 - u_2 = v_1 - v_2 \in \mathbb{F}_{p^n} \cap \mathbb{F}_{p^m} = \mathbb{F}_{p^d}.$$

Hence

$$\prod_{u \in \mathbb{F}_{p^n}} \prod_{v \in \mathbb{F}_{p^m}} (T - u - v) = \left(\prod_{w \in (\mathbb{F}_{p^n} + \mathbb{F}_{p^m}) / \mathbb{F}_{p^d}} (T - w) \right)^{p^d}.$$

Let

$$\varphi(T) = \prod_{w \in (\mathbb{F}_{p^n} + \mathbb{F}_{p^m}) / \mathbb{F}_{p^d}} (T - w) \quad \text{and} \quad \psi(T) = \frac{(\tau^n - 1) \circ (\tau^m - 1)}{\tau^d - 1}(T).$$

Our earlier observation shows that $\varphi(T)$ has distinct roots and it is monic of degree p^{n+m-d} .

We next observe that for any $u \in \mathbb{F}_{p^n}$ and $v \in \mathbb{F}_{p^m}$, we have

$$\begin{aligned} \psi(u + v) &= \frac{(\tau^n - 1) \circ (\tau^m - 1)}{\tau^d - 1}(u + v) \\ &= \left(\frac{\tau^m - 1}{\tau^d - 1} \right) \circ (\tau^n - 1)(u) + \left(\frac{\tau^n - 1}{\tau^d - 1} \right) \circ (\tau^m - 1)(v) \\ &= 0, \end{aligned}$$

since $\tau^n(u) = u$ and $\tau^m(v) = v$. Thus $\psi(T)$ vanishes at each of the roots of $\varphi(T)$, and $\varphi(T)$ has simple roots, so $\varphi(T) \mid \psi(T)$. But $\psi(T)$ is monic and has the same

degree p^{n+m-d} as $\varphi(T)$. Hence $\psi(T) = \varphi(T)$, and therefore

$$\begin{aligned} \prod_{u \in \mathbb{F}_{p^n}} \prod_{v \in \mathbb{F}_{p^m}} (T - u - v) &= \varphi(T)^{p^d} = \psi(T)^{p^d} = \tau^d(\psi(T)) \\ &= \frac{\tau^d \circ (\tau^n - 1) \circ (\tau^m - 1)}{\tau^d - 1}(T). \end{aligned}$$

This completes the proof of Lemma 6. □

Lemma 8. *Let p be a prime, let $m, n \geq 1$ be integers, let $d = \gcd(m, n)$, and let τ denote the p -power Frobenius map. Then working in $\mathbb{F}_p[A, B]$, we have*

$$\text{Res}(x^{p^n} - x - A, x^{p^m} - x - B) = \frac{\tau^d \circ (\tau^m - 1)}{\tau^d - 1}(A) - \frac{\tau^d \circ (\tau^n - 1)}{\tau^d - 1}(B).$$

Remark 9. Lemma 8 uses Frobenius to give a compact expression for the resultant, but we can also write it out explicitly as

$$\text{Res}(x^{p^n} - x - A, x^{p^m} - x - B) = \sum_{i=1}^{m/d} A^{p^{id}} - \sum_{i=1}^{n/d} B^{p^{id}}.$$

Proof. Let $\alpha, \beta \in \overline{\mathbb{F}_p(A, B)}$ be roots, respectively, of

$$x^{p^n} - x - A \quad \text{and} \quad x^{p^m} - x - B.$$

The extensions $\overline{\mathbb{F}_p}(\alpha)/\overline{\mathbb{F}_p}(A)$ and $\overline{\mathbb{F}_p}(\beta)/\overline{\mathbb{F}_p}(B)$ are Artin–Schreier extensions. The conjugates of α over $\overline{\mathbb{F}_p}(A)$ are

$$\{\alpha + u : u \in \mathbb{F}_{p^n}\},$$

and similarly for β , so we have factorizations

$$x^{p^n} - x - A = \prod_{u \in \mathbb{F}_{p^n}} (x - \alpha - u) \quad \text{and} \quad x^{p^m} - x - B = \prod_{v \in \mathbb{F}_{p^m}} (x - \beta - v).$$

We now compute

$$\begin{aligned} &\text{Res}(x^{p^n} - x - A, x^{p^m} - x - B) \\ &= \prod_{u \in \mathbb{F}_{p^n}} \prod_{v \in \mathbb{F}_{p^m}} (\alpha + u - \beta - v) && \text{see [7, 2.13(b)],} \\ &= \prod_{u \in \mathbb{F}_{p^n}} \prod_{v \in \mathbb{F}_{p^m}} ((\alpha - \beta) - u - v) \\ &= \frac{\tau^d \circ (\tau^n - 1) \circ (\tau^m - 1)}{\tau^d - 1}(\alpha - \beta) && \text{from Lemma 6,} \\ &= \frac{\tau^d \circ (\tau^m - 1)}{\tau^d - 1}(A) - \frac{\tau^d \circ (\tau^n - 1)}{\tau^d - 1}(B) && \text{since } (\tau^n - 1)(\alpha) = A \\ & && \text{and } (\tau^m - 1)(\beta) = B. \end{aligned}$$

This completes the proof of Lemma 8. □

Remark 10. We observe that for $m = n$, Lemma 8 can be proven directly from the Sylvester matrix. To ease notation, let $N = p^n$. Then the Sylvester matrix for the

to obtain

$$\begin{aligned} \deg\left(\prod_{i=1}^{M+N} S_{i,\sigma(i)}\right) &\leq \sum_{i=1}^M \left(\frac{\sigma(i)-i}{3} - 4\left\{\frac{\sigma(i)-i}{3}\right\}\right) \\ &\quad + \sum_{i=1}^N \left(\frac{\sigma(i+M)-i}{3} - 4\left\{\frac{\sigma(i+M)-i}{3}\right\}\right) \\ &= \frac{1}{3}\left(\sum_{j=1}^{M+N} j - \sum_{i=1}^M i - \sum_{i=1}^N i\right) \\ &\quad - 4\sum_{i=1}^M \left\{\frac{\sigma(i)-i}{3}\right\} - 4\sum_{i=1}^N \left\{\frac{\sigma(i+M)-i}{3}\right\} \\ &= \frac{MN}{3} - 4\sum_{i=1}^M \left\{\frac{\sigma(i)-i}{3}\right\} - 4\sum_{i=1}^N \left\{\frac{\sigma(i+M)-i}{3}\right\} \\ &\leq \frac{MN}{3} = 3^{m+n-1}. \end{aligned}$$

Since the determinant of the Sylvester matrix is a sum of terms of this form, we have proven that

$$\deg(\det S) \leq 3^{m+n-1}.$$

We are next going to evaluate $\det S$ modulo 3. To ease notation, we let

$$Y_n = y + y^3 + y^9 + \dots + y^{3^{n-1}} \quad \text{and} \quad Y_m = y + y^3 + y^9 + \dots + y^{3^{m-1}}.$$

Then Lemma 3(c) says that

$$\begin{aligned} F^{(n)}(x, y) &\equiv x^N - x + Y_n \pmod{3}, \\ G^{(m)}(x, y) &\equiv -x^M + x + Y_m \pmod{3}. \end{aligned}$$

Working modulo 3, this allows us to compute

$$\begin{aligned} \text{Res}_x(F^{(n)}(x, y), G^{(m)}(x, y)) &\equiv \text{Res}_x(x^N - x + Y_n, -x^M + x + Y_m) \pmod{3} \\ &\equiv -\text{Res}_x(x^N - x + Y_n, x^M - x - Y_m) \pmod{3}. \end{aligned}$$

We apply Lemma 8 with $A = -Y_n$ and $B = Y_m$. Letting $d = \gcd(m, n)$ and τ denote 3-power Frobenius, this gives

$$\begin{aligned} \det(S) &= \text{Res}_x(F^{(n)}(x, y), G^{(m)}(x, y)) \\ &\equiv -\frac{\tau^d \circ (\tau^m - 1)}{\tau^d - 1}(-Y_n) + \frac{\tau^d \circ (\tau^n - 1)}{\tau^d - 1}(Y_m) \pmod{3} \\ &\equiv \tau^m(Y_n) + \tau^{m-d}(Y_n) + \dots + \tau^d(Y_n) \\ &\quad + \tau^n(Y_m) + \tau^{n-d}(Y_m) + \dots + \tau^d(Y_m) \pmod{3} \\ &\equiv Y_n^{3^m} + Y_m^{3^n} + (\text{lower order terms}) \pmod{3} \\ &\equiv 2y^{3^{m+n-1}} + (\text{lower order terms}) \pmod{3}. \end{aligned}$$

We have now proven that

$$\deg(\det S) \leq 3^{m+n-1} \quad \text{and} \quad \det S \equiv 2y^{3^{m+n-1}} + (\text{l.o.t.}) \pmod{3}.$$

It follows that $\det S$ has degree exactly equal to 3^{m+n-1} and that its leading coefficient is relatively prime to 3, which completes the proof of Proposition 11. \square

We now have all of the tools needed to prove Theorem 1.

Proof of Theorem 1. Let (α, β) be a solution to

$$F^{(n)}(x, y) = G^{(m)}(x, y) = 0.$$

To ease notation, let

$$R^{(n,m)}(y) = \text{Res}_x(F^{(n)}(x, y), G^{(m)}(x, y)).$$

A standard property of the resultant of two polynomials says that it is in the ideal generated by those polynomials [7, 2.13(c)]. Thus there are polynomials $U(x, y), V(x, y) \in \mathbb{Z}[x, y]$ such that

$$U(x, y)F^{(n)}(x, y) + V(x, y)G^{(m)}(x, y) = R^{(n,m)}(y).$$

Substituting $(x, y) = (\alpha, \beta)$, we find that $R^{(n,m)}(\beta) = 0$. Proposition 11 says that $R^{(n,m)}(y) \in \mathbb{Z}[y]$ has leading coefficient prime to 3, which proves that β is 3-adically integral. We next use Lemma 3(a) to write

$$F^{(n)}(x, y) = f_{x,y}^n(x) - x = (-2)^{3^{n-1}} x^{3^n} + \sum_{k=1}^{3^n} a_k(y) x^{3^n-k} - x.$$

Substituting $y = \beta$ we see that α is a root of the polynomial $F^{(n)}(x, \beta)$ whose coefficients are 3-adically integral and whose leading coefficient is a 3-adic unit. Hence α is also 3-adically integral.

Now consider the value $J(\alpha, \beta)$ of the Jacobian determinant (3). Proposition 5 says that there is a polynomial $K(x, y) \in \mathbb{Z}[x, y]$ satisfying

$$J(x, y) = 1 + 3K(x, y).$$

We know that α and β are 3-adically integral, so the same is true of $J(\alpha, \beta)$ and $K(\alpha, \beta)$. Taking norms down to \mathbb{Q} , we find that

$$\mathbf{N}_{\mathbb{Q}(\alpha,\beta)/\mathbb{Q}} J(\alpha, \beta) = \mathbf{N}_{\mathbb{Q}(\alpha,\beta)/\mathbb{Q}} (1 + 3K(\alpha, \beta)) \equiv 1 \pmod{3}.$$

In particular, $J(\alpha, \beta) \neq 0$. It follows that the ideal

$$(F^{(n)}(x, y), G^{(m)}(x, y), J(x, y)) \subset \mathbb{C}[x, y]$$

is the unit ideal, since if it were not, then $F^{(n)}$, $G^{(m)}$, and J would have a common root. This completes the proof that the curves $F^{(n)}(x, y) = 0$ and $G^{(m)}(x, y) = 0$ intersect transversally. \square

3. PREPERIODIC CRITICAL POINTS — A MODEST BEGINNING

Generalizing the notation from Theorem 1, for $i, j \geq 1$ we let

$$C_{1,n,i} = \left\{ (f, c_1, c_2) \in \mathcal{P}_3^{\text{crit}} : \begin{array}{l} f^{i+n}(c_1) = f^i(c_1) \text{ and} \\ f^{i-1+n}(c_1) \neq f^{i-1}(c_1) \end{array} \right\},$$

$$C_{2,m,j} = \left\{ (f, c_1, c_2) \in \mathcal{P}_3^{\text{crit}} : \begin{array}{l} f^{j+m}(c_2) = f^j(c_2) \text{ and} \\ f^{j-1+m}(c_2) \neq f^{j-1}(c_2) \end{array} \right\}.$$

In words, $(f, c_1, c_2) \in C_{1,n,i}$ if c_1 is purely preperiodic with tail length i and cycle length dividing n , and similarly for $C_{2,m,j}$. For convenience, we let $C_{1,n,0} = C_{1,n}$ and $C_{2,m,0} = C_{2,m}$.

Thurston’s theorem implies that $C_{1,n,i}$ and $C_{2,m,j}$ intersect transversally. We sketch a 3-adic proof of a very special case. The key to the proof is the following elementary identity.

Lemma 12. *We have*

$$(13) \quad f_{x,y}^{n+1}(x) - f_{x,y}(x) = (f_{x,y}^n(x) - x)^2 (f_{x,y}^n(x) + 2x).$$

In particular, we have

$$F^{(n,1)}(x, y) = \frac{f_{x,y}^{n+1}(x) - f_{x,y}(x)}{(f_{x,y}^n(x) - x)^2} \in \mathbb{Z}[x, y],$$

and $F^{(n,1)}(x, y)$ satisfies

$$\begin{aligned} F^{(n,1)}(x, y) &\equiv F^{(n)}(x, y) \pmod{3}, \\ F_x^{(n,1)}(x, y) &\equiv 1 \pmod{3}, \\ F_y^{(n,1)}(x, y) &\equiv -1 \pmod{3}. \end{aligned}$$

Proof. The polynomial $f_{x,y}(z)$ has a critical point at $z = x$, so the difference $f_{x,y}(z) - f_{x,y}(x)$ should be divisible by $(z - x)^2$. Explicitly, we find that

$$f_{x,y}(z) - f_{x,y}(x) = (z - x)^2(z + 2x).$$

Substituting $z = f_{x,y}^n(x)$ gives (13). Then the function we have called $F^{(n,1)}(x, y)$ is given by

$$F^{(n,1)}(x, y) = f_{x,y}^n(x) + 2x.$$

Reducing modulo 3 gives

$$F^{(n,1)}(x, y) = f_{x,y}^n(x) + 2x \equiv f_{x,y}^n(x) - x = F^{(n)}(x, y) \pmod{3}.$$

The formulas for the partial derivatives of $F^{(n,1)}(x, y) \pmod{3}$ then follow by differentiating the formula for $F^{(n)}(x, y)$ given in Lemma 3(c). □

Theorem 13. (a) $C_{1,n,1}$ and $C_{2,m,0}$ intersect transversally.

(b) $C_{1,n,1}$ and $C_{2,m,1}$ intersect transversally.

Proof. As usual, let

$$f_{x,y}(z) = z^3 - 3x^2z + y$$

be a cubic polynomial normalized to have critical points $\pm x$. Then the points $(f_{x,y}, x, -x)$ in $C_{1,n,1}$ are the points satisfying

$$f_{x,y}^{n+1}(x) = f_{x,y}(x) \quad \text{and} \quad f_{x,y}^n(x) \neq x.$$

From Lemma 12, these points satisfy

$$F^{(n,1)}(x, y) = f_{x,y}^n(x) + 2x = 0,$$

so the locus $F^{(n,1)}(x, y) = 0$ contains the curve $C_{1,n,1}$. We will show that the curves

$$F^{(n,1)}(x, y) = 0 \quad \text{and} \quad G^{(m)}(x, y) = 0$$

intersect transversally.

The first part of the proof is to show that the intersection points are 3-adically integral. This can be proven using the resultant methods, *mutatis mutandis*, of this paper. It is also proven in a more general setting by Epstein [3]. We then

compute the Jacobian using the congruences for the derivatives $F_x^{(n,1)}(x, y)$ and $F_y^{(n,1)}(x, y)$ given in Lemma 12 and differentiating the formula for $G^{(m)}(x, y)$ given in Lemma 3(c). Thus

$$\begin{aligned} J(x, y) &= \det \begin{pmatrix} F_x^{(n,1)}(x, y) & G_x^{(m)}(x, y) \\ F_y^{(n,1)}(x, y) & G_y^{(m)}(x, y) \end{pmatrix} \pmod{3} \\ &\equiv \det \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix} \equiv 1 \pmod{3}. \end{aligned}$$

The proof for $C_{1,n,1}$ and $C_{2,m,1}$ is almost identical, since replacing x by $-x$ in Lemma 12 gives

$$G_x^{(m,1)}(x, y) \equiv 1 \pmod{3} \quad \text{and} \quad G_y^{(m,1)}(x, y) \equiv 1 \pmod{3}.$$

□

4. PROOF OF (10)

For the convenience of the reader, we prove the elementary inequality (10) used in the proof of Lemma 3. For $t \in \mathbb{R}$, write $t = [t] + \{t\}$, where $0 \leq \{t\} < 1$ is the fractional part of t . Then (10) is equivalent to the inequality

$$\{t_1 + t_2 + t_3\} \leq \{t_1\} + \{t_2\} + \{t_3\}.$$

This inequality is invariant under $t_i \rightarrow t_i + k$ for any $k \in \mathbb{Z}$, so without loss of generality, we may assume that $0 \leq t_i < 1$ for all $1 \leq i \leq 3$. Then the desired inequality is

$$\{t_1 + t_2 + t_3\} \leq t_1 + t_2 + t_3,$$

which is trivially true. (There is nothing special about a sum of three terms. The same proof shows that $\sum [t_i] \leq [\sum t_i]$.)

ACKNOWLEDGEMENTS

The author would like to thank Adam Epstein for suggesting generalizing Gleason's 2-adic proof to prove other cases of Thurston's theorem, Adam Epstein and Bjorn Poonen for ongoing discussions of related matters, and the referee for some helpful suggestions. He would also like to thank Xander Faber for organizing and the CRM for funding the May 2010 workshop "Moduli Spaces and the Arithmetic of Dynamical Systems" at the Bellairs Research Institute in Barbados, where these discussions began.

REFERENCES

- [1] A. Douady and J. H. Hubbard. Exploring the Mandelbrot set. The Orsay notes. www.math.cornell.edu/~hubbard/OrsayEnglish.pdf.
- [2] A. Douady and J. H. Hubbard. A proof of Thurston's topological characterization of rational functions. *Acta Math.*, 171(2):263–297, 1993. MR1251582 (94j:58143)
- [3] A. Epstein. Integrality and rigidity for postcritically finite polynomials, *Bull. London Math. Soc.*, 2011, doi:10.1112/blms/bdr059.
- [4] G. Levin. Multipliers of periodic orbits in spaces of rational maps. *Ergodic Theory and Dynamical Systems*, 31(01): 197–243, 2011. MR2755929
- [5] C. T. McMullen and D. P. Sullivan. Quasiconformal homeomorphisms and dynamics. III. The Teichmüller space of a holomorphic dynamical system. *Adv. Math.*, 135(2):351–395, 1998. MR1620850 (99e:58145)

- [6] J. Milnor. Cubic polynomial maps with periodic critical orbit. I. *Complex Dynamics*. A K Peters, Wellesley, MA, 2009: 333–411. MR2508263
- [7] J. H. Silverman. *The Arithmetic of Dynamical Systems*, volume 241 of Graduate Texts in Mathematics. Springer, New York, 2007. MR2316407 (2008c:11002)

DEPARTMENT OF MATHEMATICS, BOX 1917, BROWN UNIVERSITY, PROVIDENCE, RHODE ISLAND
02912

E-mail address: `jhs@math.brown.edu`