ACTA ARITHMETICA
169.1 (2015)

Prime rational functions

by

Omar Kihel and Jesse Larone (St. Catharines)

1. Introduction. Let $f(x)$ be a non-constant polynomial. Ayad's paper [1] and Beardon's paper [2] deal with the possibility of expressing $f(x)$ as the composition of two polynomials $g(x)$ and $h(x)$ with degrees at least 2. In this case $f(x)$ is said to be *composite*, otherwise it is said to be *prime*. We extend this concept to rational functions as follows. Let $\mathbb{C}[x]$ be the ring of complex polynomials and let $\mathbb{C}(x)$ be its field of fractions. When we refer to the complex rational function $f(x)$, we mean the unique ratio $f_1(x)/f_2(x)$ of complex polynomials $f_1(x)$ and $f_2(x)$ where $f_2(x)$ is monic and no linear factor divides both $f_1(x)$ and $f_2(x)$. We then define the *degree* of $f(x)$ by

$$\deg f(x) = \max\{\deg f_1(x), \deg f_2(x)\}.$$

Let $f(x)$ be a non-constant complex rational function. We call $f(x)$ *composite* if there exist complex rational functions $g(x)$ and $h(x)$, both with degrees at least 2, such that $f(x) = g(h(x))$. Otherwise, we call $f(x)$ *prime*. In Section 2, we motivate these definitions of prime and composite rational functions, and we make use of the set of units under function composition to provide conditions on the multiplicities of the zeros and poles of a rational function $f(x)$ which are sufficient to conclude that $f(x)$ is prime.

Beardon [2] proved that if a polynomial $f(x)$ of degree n has more than $n/2$ critical values, then $f(x)$ is prime. Ayad [1] defined the multiplicity of a critical value and proved that if a polynomial $f(x)$ of degree n has more than d simple critical values where d is the greatest proper divisor of n, then $f(x)$ is prime. Ayad also provided examples of prime polynomials by considering the valencies of their critical points. In Section 3, we define the resultant of two rational functions. Motivated by Ayad's results in [1], we present conditions on the critical values of a rational function $f(x)$ under which $f(x)$ is prime and use these results to provide examples of prime rational functions.

2010 *Mathematics Subject Classification*: Primary 11C08; Secondary 12E05, 26C15.
Key words and phrases: prime polynomials, prime rational functions, critical values, critical points, resultant.

2. Units and composite rational functions. Let $f(x)$ be a complex rational function. Then $f(x)$ can be expressed as the ratio of two complex polynomials such that no linear factor divides both of the polynomials in its numerator and its denominator, and we say that $f(x)$ is in its *most reduced form.* Since such a reduced form is useful when trying to determine the degree of a rational function, we provide an expression for the reduced form of a composition of two rational functions. The validity of the lemma is easily verified.

LEMMA 2.1. *Let $g(x)$ and $h(x)$ be rational functions in their most reduced forms with*

$$g(x) = \frac{b\prod_{i=1}^{m_1}(x-\alpha_i)}{\prod_{j=1}^{m_2}(x-\beta_j)} \quad \text{and} \quad h(x) = \frac{h_1(x)}{h_2(x)}.$$

Then the expression for $g(h(x))$ given by

$$g(h(x)) = \frac{bh_2(x)^{\deg g - m_1}\prod_{i=1}^{m_1}(h_1(x)-\alpha_i h_2(x))}{h_2(x)^{\deg g - m_2}\prod_{j=1}^{m_2}(h_1(x)-\beta_j h_2(x))}$$

is in its most reduced form.

We prove a proposition which will be essential for the rest of this paper.

PROPOSITION 2.2. *Let K be a field and let $f(x) = f_1(x)/f_2(x)$ be a rational function over K in its most reduced form. Then*

$$\deg f = [K(x) : K(f)].$$

Proof. We have $K(f) \subset K(x) = K(f, x)$ where x is a primitive element of $K(x)$ over $K(f)$. Then x is a root of the polynomial

$$F(y) = f_1(y) - f \cdot f_2(y) \in K(f)[y]$$

and $\deg F = \max\{\deg f_1, \deg f_2\}$. Since F is a linear polynomial in f, any factorization of F in $K[f, y]$ must be of the form

$$F(y) = u(y)(v_1(y) + f \cdot v_2(y))$$

where $u(y), v_1(y), v_2(y) \in K[f, y]$. If $u(y)$ has degree at least 1, this contradicts the assumption that $f(x)$ is a rational function in its most reduced form since $u(y)$ must divide both $f_1(y)$ and $f_2(y)$. Therefore F is irreducible in $K[f, y]$ and also in $K(f)[y]$. Then $[K(x) : K(f)] = \deg F = \max\{\deg f_1, \deg f_2\} = \deg f$. ∎

PROPOSITION 2.3. *Let K be a field and let $f(x) = g(h(x))$ where $f(x)$, $g(x)$, and $h(x)$ are rational functions over K. Then*

$$\deg f = \deg g \cdot \deg h.$$

Proof. We have $K(f) \subset K(h) \subset K(x)$ with $[K(x) : K(f)] = \deg f$, $[K(x) : K(h)] = \deg h$, $[K(h) : K(f)] = \deg g$. The desired result follows. ∎

COROLLARY 2.4. *Let $f(x)$ be a complex rational function of degree p where p is a prime number. Then $f(x)$ is prime.*

We recall that a rational function $\mu(x)$ is a *unit under function composition* if there exists another rational function $\mu^{-1}(x)$ such that $\mu(\mu^{-1}(x)) = \mu^{-1}(\mu(x)) = x$. Then $\deg \mu(x) \cdot \deg \mu^{-1}(x) = \deg x = 1$, and it follows that both $\mu(x)$ and $\mu^{-1}(x)$ must have degree 1. We claim that the complex rational functions of degree 1 form the group of units under function composition, which is the motivation for the requirement that the composition factors of a composite function have degree at least 2. One can verify that the function $\mu(x) = \frac{ax+b}{cx+d}$ has degree 1 if and only if $ad - bc \neq 0$, and in this case it has an inverse given by $\mu^{-1}(x) = \frac{dx-b}{-cx+a}$. When we refer to a *unit* $\mu(x)$, we mean that $\mu(x)$ is a unit under function composition.

This group of units will be very useful in the study of whether a function is prime, due to the following result.

LEMMA 2.5. *Let f be a complex rational function and let μ be a unit. If either $f \circ \mu$ or $\mu \circ f$ is composite, then f is composite. Conversely, if f is composite, then both $f \circ \mu$ and $\mu \circ f$ are composite.*

Proof. If $\mu \circ f$ is composite, then $\mu \circ f = g \circ h$ for some complex rational functions g and h with degrees at least 2, so that $f = (\mu^{-1} \circ g) \circ h$ is composite. Similarly, if $f \circ \mu$ is composite, then $f \circ \mu = g \circ h$ for complex rational functions g and h with degrees at least 2, so that $f = g \circ (h \circ \mu^{-1})$ is composite.

Conversely, if f is composite, then $f = g \circ h$ for complex rational functions g and h with degrees at least 2, so that $\mu \circ f = (\mu \circ g) \circ h$ and $f \circ \mu = g \circ (h \circ \mu)$ are both composite. ∎

The following two lemmas will be frequently used. The first provides a particular pair of composition factors for composite rational functions, and the second relates the numerator and denominator degrees of a composite rational function with those of its composition factors.

LEMMA 2.6. *Let $f(x)$ be a complex composite rational function. There exist complex rational functions $g(x)$ and $h(x)$ of degrees at least 2 such that $f(x) = g(h(x))$ where the numerator degree of $h(x)$ is larger than its denominator degree.*

Proof. Since $f(x)$ is composite, there exist complex rational functions $G(x)$ and $H(x)$ of degrees at least 2 such that $f(x) = G(H(x))$. We let $\mu(x)$ be a complex rational function of degree 1. We consider the expression $\mu(H(x))$ explicitly, and we will choose $\mu(x)$ so that $\mu(H(x))$ has larger numerator degree than denominator degree. Let $H(x) = H_1(x)/H_2(x)$ and consider two cases.

(i) If $\deg H_1 > \deg H_2$, we let $\mu(x) = x$.
(ii) If $\deg H_1 \le \deg H_2$, we write $H_1(x) = aH_2(x) + r(x)$ where $a \in \mathbb{C}$ and $\deg r < \deg H_2$. Then $H(x) = a + r(x)/H_2(x)$ and we let $\mu(x) = 1/(x-a)$.

In both cases, $\mu(H(x))$ has numerator degree greater than its denominator degree. Since $\mu(x)$ has degree 1, there exists $\mu^{-1}(x)$ such that $\mu^{-1}(\mu(x)) = x$. We define $g(x) = G(\mu^{-1}(x))$ and $h(x) = \mu(H(x))$. Then

$$f = G \circ H = G \circ \mu^{-1} \circ \mu \circ H = (G \circ \mu^{-1}) \circ (\mu \circ H) = g \circ h$$

is a decomposition of f such that $f(x) = g(h(x))$ where the numerator degree of $h(x)$ is larger than its denominator degree. ∎

Lemma 2.7. *Let $f(x)$ be a composite complex rational function with $f(x) = g(h(x))$. Let n_1, m_1, and k_1 be the numerator degrees of $f(x)$, $g(x)$, and $h(x)$ respectively and let n_2, m_2, and k_2 be the denominator degrees of $f(x)$, $g(x)$, and $h(x)$ respectively. If $k_1 > k_2$, then*

$$n_1 - n_2 = (m_1 - m_2)(k_1 - k_2).$$

Proof. Let $h(x) = h_1(x)/h_2(x)$ and let

$$g(x) = \frac{b\prod_{i=1}^{m_1}(x-\alpha_i)}{\prod_{j=1}^{m_2}(x-\beta_j)}$$

have degree m. Then

$$f(x) = \frac{f_1(x)}{f_2(x)} = \frac{bh_2(x)^{m-m_1}\prod_{i=1}^{m_1}(h_1(x)-\alpha_i h_2(x))}{h_2(x)^{m-m_2}\prod_{j=1}^{m_2}(h_1(x)-\beta_j h_2(x))}.$$

Since $k_1 > k_2$ by assumption, the numerator and denominator degrees of $f(x)$ satisfy $n_1 + (m-m_2)k_2 + m_2k_1 = n_2 + (m-m_1)k_2 + m_1k_1$. It follows that $n_1 - n_2 = (m_1 - m_2)(k_1 - k_2)$ as desired. ∎

The following property extends the relationship between the degree of a polynomial and that of its derivative to the case of a rational function.

Lemma 2.8. *Let $f(x)$ be a complex rational function with numerator degree n_1 and denominator degree n_2, and let $f'(x)$ have numerator degree n_1' and denominator degree n_2'. If $n_1 - n_2 \neq 0$, then $n_1' - n_2' = n_1 - n_2 - 1$.*

Proof. Let

$$f(x) = \frac{ax^{n_1} + f_1(x)}{x^{n_2} + f_2(x)}$$

where $a \neq 0$, $\deg f_1(x) < n_1$, and $\deg f_2(x) < n_2$. Then the reduced form of $f'(x)$ can be obtained by simplifying the expression

$$\frac{(an_1x^{n_1-1} + f_1'(x))(x^{n_2} + f_2(x)) - (ax^{n_1} + f_1(x))(n_2x^{n_2-1} + f_2'(x))}{(x^{n_2} + f_2(x))^2}.$$

We first expand the numerator and denominator to write it in the form

$$\frac{a(n_1 - n_2)x^{n_1+n_2-1} + g_1(x)}{x^{2n_2} + g_2(x)}$$

where $\deg g_1(x) < n_1 + n_2 - 1$ and $\deg g_2 < 2n_2$. The numerator and denominator degrees of $f'(x)$ then satisfy $n_1' + 2n_2 = n_2' + n_1 + n_2 - 1$, and it follows that $n_1' - n_2' = n_1 - n_2 - 1$. ∎

THEOREM 2.9. *Let $f(x)$ be a complex rational function with numerator degree n_1 and denominator degree n_2. Let d be the greatest proper divisor of $n = \deg f$. If $|n_1 - n_2| > 0$ is divisible by a prime number $p > d$, then $f(x)$ is prime. If $|n_1 - n_2| > 0$ is divisible by a prime number $p = d$ and $f(x) = g(h(x))$ is composite, then either $g(x)$ or $h(x)$ is a polynomial.*

Proof. Suppose that $f(x)$ is composite. There exist complex rational functions $g(x)$ and $h(x)$ of degrees $m, k \geq 2$ respectively such that $f(x) = g(h(x))$ and $h(x)$ has larger numerator degree than denominator degree. Let m_1 and k_1 be the numerator degrees of $g(x)$ and $h(x)$ respectively, and let m_2 and k_2 be the denominator degrees of $g(x)$ and $h(x)$ respectively. Assume without loss of generality that $n_1 > n_2$. Then $n_1 - n_2 = (m_1 - m_2)(k_1 - k_2)$, and it follows that $m_1 > m_2$.

To prove the first claim, we assume that $p > d$. Since $p \mid (n_1 - n_2)$ where $n_1 - n_2 = (m - m_2)(k - k_2)$, we have either $p \mid (m - m_2)$ or $p \mid (k - k_2)$. Then either $p \leq m - m_2 \leq m \leq d < p$ or $p \leq k - k_2 \leq k \leq d < p$, both cases yielding a contradiction. Therefore $f(x)$ is prime.

To prove the second claim, we assume that $p = d$. Since $p \mid (n_1 - n_2)$, we have either $p \mid (m - m_2)$ or $p \mid (k - k_2)$. Then either $d = p \leq m - m_2 \leq d - m_2$ so that $m_2 = 0$ and $g(x)$ is a polynomial, or $d = p \leq k - k_2 \leq d - k_2$ so that $k_2 = 0$ and $h(x)$ is a polynomial. ∎

COROLLARY 2.10. *Let $f(x)$ be a complex rational function of degree n and let d be the greatest proper divisor of n. If $f(x)$ has a zero or a pole whose multiplicity is divisible by a prime number $p > d$, then $f(x)$ is prime.*

Proof. Let $f(x)$ have numerator degree n_1, denominator degree n_2, and let

$$f(x) = \frac{c\prod_{i=1}^{m_1}(x - \alpha_i)^{a_i}}{\prod_{j=1}^{m_2}(x - \beta_j)^{b_j}}.$$

We first consider when $f(x)$ has a zero whose multiplicity is divisible by a prime number $p > d$, and we assume without loss of generality that this zero is α_1 which has multiplicity a_1. We define the unit $\mu(x) = (\alpha_1 x + 1)/x$ where $\alpha_1 \cdot 0 - 1 \cdot 1 = -1 \neq 0$. Then

$$f(\mu(x)) = \frac{cx^{n-n_1}\prod_{i=1}^{m_1}((\alpha_1 x+1)-\alpha_i x)^{a_i}}{x^{n-n_2}\prod_{j=1}^{m_2}((\alpha_1 x+1)-\beta_j x)^{b_j}} = \frac{cx^{n-n_1}\prod_{i=2}^{m_1}((\alpha_1-\alpha_i)x+1)^{a_i}}{x^{n-n_2}\prod_{j=1}^{m_2}((\alpha_1-\beta_j)x+1)^{b_j}}$$

has numerator degree N_1 and denominator degree N_2 satisfying

$$N_1 + (n-n_2) + n_2 = N_2 + (n-n_1) + (n_1 - a_1).$$

Then $N_2 - N_1 = a_1$ is divisible by $p > d$, so that $f(\mu(x))$ satisfies the conditions of Theorem 2.9 and is prime. Therefore $f(x)$ is also prime.

If $f(x)$ has a pole with multiplicity divisible by $p > d$, we consider the unit $\nu(x) = 1/x$. Then $\nu(f(x))$ will have a zero with multiplicity divisible by $p > d$, so that $\nu(f(x))$ and $f(x)$ are prime. ∎

The remainder of this section is primarily dedicated to providing examples of prime rational functions. We compose these prime rational functions with units to obtain examples of prime polynomials.

Theorem 2.11. *Let $f(x)$ be a complex rational function with numerator degree n_1 and denominator degree n_2, where n_1 and n_2 are relatively prime integers such that $n_1 > n_2$. If the denominator of $f(x)$ is of the form $(x-\gamma)^{n_2}$ for some $\gamma \in \mathbb{C}$, then $f(x)$ is prime.*

Proof. Suppose for contradiction that $f(x)$ is composite. There exist complex rational functions $g(x)$ and $h(x)$ such that $f(x) = g(h(x))$, where $g(x)$ is prime and $h(x) = h_1(x)/h_2(x)$ satisfies $\deg h_1(x) > \deg h_2(x)$. We assume without loss of generality that $h_2(x)$ is monic. Let $k_1 = \deg h_1$ and $k_2 = \deg h_2$, and let

$$g(x) = \frac{c\prod_{i=1}^{m_1}(x-\alpha_i)}{\prod_{j=1}^{m_2}(x-\beta_j)}.$$

Since $n_1 > n_2$ and $k_1 > k_2$, it follows from Lemma 2.7 that $m_1 > m_2$. Then $f(x)$ is given by the expression

$$f(x) = \frac{c\prod_{i=1}^{m_1}(h_1(x)-\alpha_i h_2(x))}{h_2(x)^{m_1-m_2}\prod_{j=1}^{m_2}(h_1(x)-\beta_j h_2(x))}.$$

Since the denominator of $f(x)$ is $(x-\gamma)^{n_2}$, there exists a non-zero constant c' such that

$$(x-\gamma)^{n_2} = c' h_2(x)^{m_1-m_2}\prod_{j=1}^{m_2}(h_1(x)-\beta_j h_2(x)).$$

Consequently, the linear factor $x-\gamma$ must divide either $h_2(x)^{m_1-m_2}$ or $c'\prod_{j=1}^{m_2}(h_1(x)-\beta_j h_2(x))$, but this factor cannot divide both as this implies that $x-\gamma$ will also divide $h_1(x)$ where $h(x)$ has no linear factor dividing both its numerator and its denominator. Thus we obtain two cases:

$(x-\gamma)^{n_2} = h_2(x)^{m_1-m_2}$ and $c' \prod_{j=1}^{m_2}(h_1(x) - \beta_j h_2(x))$ is a non-zero constant, or $(x-\gamma)^{n_2} = c' \prod_{j=1}^{m_2}(h_1(x) - \beta_j h_2(x))$ and $h_2(x)^{m_1-m_2}$ is a non-zero constant.

(i) If $h_2(x)^{m_1-m_2}$ is constant, then $h_2(x)$ is constant since $m_1 > m_2$, and $h(x)$ is a polynomial. Then $f(x) = g(h(x))$ has numerator degree $n_1 = m_1 k_1$ and denominator degree $n_2 = m_2 k_1$, contradicting n_1 and n_2 being relatively prime.

(ii) If $c' \prod_{j=1}^{m_2}(h_1(x) - \beta_j h_2(x))$ is constant, then $m_2 = 0$ or $h_1(x) - \beta_j h_2(x) = c_j \in \mathbb{C}^*$ for $j = 1, \ldots, m_2$. We reject $m_2 = 0$, as this would imply that $f(x)$ has numerator degree $n_1 = m_1 k_1$ and denominator degree $n_2 = m_1 k_2$, contradicting n_1 and n_2 being relatively prime. We now consider the remaining possibility by choosing any two values β_{j_1} and β_{j_2} where $1 \le j_1, j_2 \le m_2$. We solve the expressions $h_1(x) - \beta_{j_1} h_2(x) = c_{j_1}$ and $h_1(x) - \beta_{j_2} h_2(x) = c_{j_2}$ for $h_1(x)$ to obtain

$$c_{j_1} + \beta_{j_1} h_2(x) = c_{j_2} + \beta_{j_2} h_2(x).$$

It follows that $c_{j_1} - c_{j_2} = (\beta_{j_2} - \beta_{j_1}) h_2(x)$. Since $h_2(x)$ is not constant, we have $c_{j_1} = c_{j_2}$ and $\beta_{j_1} = \beta_{j_2}$ for every pair j_1 and j_2. We set $\beta_j = \beta$ and $c_j = c$ for all $j = 1, \ldots, m_2$. Now $h_1(x) = c + \beta h_2(x)$, and we let

$$\nu(x) = c + \beta x, \quad \mu(x) = \frac{\nu(x)}{x}, \quad \text{and} \quad G(x) = \frac{G_1(x)}{G_2(x)} = g(\mu(x))$$

so that $h_1(x) = \nu(h_2(x))$ and $f(x) = G(h_2(x))$. We note that $\mu(x)$ is a unit since $\beta \cdot 0 - c \cdot 1 = -c \neq 0$.

If $k_2 > 1$, then $f(x)$ has numerator degree $n_1 = \deg G_1 \cdot k_2$ and denominator degree $n_2 = \deg G_2 \cdot k_2$, contradicting n_1 and n_2 being relatively prime integers. If $k_2 = 1$, then $h_2(x)$ is a unit. Since $g(x)$ is prime, it follows that $G(x)$ and $f(x)$ are prime.

All possible cases have been considered, and we conclude that $f(x)$ is prime. ∎

COROLLARY 2.12. *Let $f(x) = (x-\alpha_1)^{e_1}(x-\alpha_2)^{e_2}$ be a complex polynomial such that $e_1, e_2 \ge 1$ and $\alpha_1 \neq \alpha_2$. Then $f(x)$ is prime if and only if e_1 and e_2 are relatively prime.*

Proof. Suppose that e_1 and e_1 are not relatively prime. There exists an integer $b \ge 2$ such that $e_1 = a_1 b$ and $e_2 = a_2 b$ for some positive integers a_1 and a_2. We can then write $g(x) = x^b$ and $h(x) = (x-\alpha_1)^{a_1}(x-\alpha_2)^{a_2}$, where both $g(x)$ and $h(x)$ have degrees at least 2. Then $f(x) = g(h(x))$ is composite.

Conversely, suppose that e_1 and e_2 are relatively prime. Then e_2 and $e_1 + e_2$ are relatively prime as well. We define the units $\nu(x) = 1/x$ and $\mu(x) = (\alpha_1 x + 1)/x$ where $\alpha_1 \cdot 0 - 1 \cdot 1 = -1 \neq 0$. The function

$$\nu(f(\mu(x))) = \nu\left(\frac{((\alpha_1 x+1)-\alpha_1 x)^{e_1}((\alpha_1 x+1)-\alpha_2 x)^{e_2}}{x^{e_1+e_2}}\right)$$
$$= \frac{x^{e_1+e_2}}{((\alpha_1-\alpha_2)x+1)^{e_2}}$$

is prime by Theorem 2.11 since e_2 and e_1+e_2 are relatively prime. Therefore $f(x)$ is prime. ■

THEOREM 2.13. *Let $f(x) = (x-\alpha_1)^{e_1}(x-\alpha_2)^{e_2}(x-\alpha_3)^{e_3}$ be a complex polynomial of degree n such that α_1, α_2 and α_3 are distinct complex numbers and $e_1, e_2, e_3 \geq 1$. If e_1, e_2, and e_3 are pairwise relatively prime integers all relatively prime to n, then $f(x)$ is prime.*

Proof. Suppose for contradiction that $f(x)$ is composite. Then there exist rational functions $g(x)$ and $h(x)$ with degrees at least 2 such that $f(x) = g(h(x))$, where

$$g(x) = \frac{c\prod_{i=1}^{m_1}(x-\alpha_i)}{\prod_{j=1}^{m_2}(x-\gamma_j)}$$

and $h(x) = h_1(x)/h_2(x)$ satisfies $k_1 = \deg h_1 > \deg h_2 = k_2$. We consider the polynomial $f(x)$ as a rational function whose denominator is the constant polynomial 1. Since $n > 0$ and $k_1 > k_2$, it follows that $m_1 > m_2$. Then $f(x)$ is given by the expression

$$f(x) = \frac{c\prod_{i=1}^{m_1}(h_1(x)-\alpha_i h_2(x))}{h_2(x)^{m_1-m_2}\prod_{j=1}^{m_2}(h_1(x)-\gamma_j h_2(x))}.$$

Since the denominator of $f(x)$ is the constant 1, there exists a non-zero constant c' such that

$$1 = c' h_2(x)^{m_1-m_2}\prod_{j=1}^{m_2}(h_1(x)-\gamma_j h_2(x)).$$

It follows that $h_2(x)$ is a non-zero constant. Thus $h(x)$ is a polynomial. Since $h(x)$ is not a constant polynomial, we must have $m_2 = 0$. Therefore $g(x)$ is also a polynomial.

We now assume without loss of generality that $f(x)$ is the composition of the polynomials $g(x)$ and $h(x)$ where $h(x)$ is monic, and we write $g(x)$ in the form

$$g(x) = a\prod_{i=1}^{m}(x-\beta_i)^{b_i}$$

where $\beta_1, \ldots, \beta_m$ are all of the roots of $g(x)$. Then

$$f(x) = a\prod_{i=1}^{m}(h(x)-\beta_i)^{b_i}.$$

Since $f(x)$ and $h(x)$ are monic, we obtain $a = 1$. Since $h(x)-\beta_i$ and $h(x)-\beta_j$ do not have any roots in common when $i \neq j$, it follows that $1 \leq m \leq 3$.

If $m = 1$, then $f(x) = (h(x) - \beta_1)^{b_1}$, and hence we obtain $h(x) - \beta_1 = (x-\alpha_1)^{r_1}(x-\alpha_2)^{r_2}(x-\alpha_3)^{r_3}$ for some integers r_1, r_2, and r_3. Then $e_1 = r_1 b_1$, $e_2 = r_2 b_1$, and $e_3 = r_3 b_1$ so that b_1 divides the pairwise relatively prime integers e_1, e_2, and e_3. Thus $b_1 = 1$ and $\deg g = 1$, yielding a contradiction.

If $m = 2$, then $f(x) = (h(x)-\beta_1)^{b_1}(h(x)-\beta_2)^{b_2}$. We assume without loss of generality that $h(x)-\beta_1 = (x-\alpha_1)^{r_1}$ and $h(x)-\beta_2 = (x-\alpha_2)^{r_2}(x-\alpha_3)^{r_3}$ for some integers r_1, r_2, and r_3. Then $r_1 = \deg h = r_2 + r_3$, $e_1 = r_1 b_1$, $e_2 = r_2 b_2$, and $e_3 = r_3 b_2$ so that b_2 divides the relatively prime integers e_2 and e_3. Thus $b_2 = 1$ and $r_1 = r_2 + r_3 = e_2 + e_3$. It follows that $r_1 = \deg h > 1$ divides both e_1 and $n = e_1 + e_2 + e_3$, yielding a contradiction.

If $m = 3$, then $f(x) = (h(x)-\beta_1)^{b_1}(h(x)-\beta_2)^{b_2}(h(x)-\beta_3)^{b_3}$. We assume without loss of generality that $h(x)-\beta_1 = (x-\alpha_1)^{r_1}$, $h(x)-\beta_2 = (x-\alpha_2)^{r_2}$, and $h(x) - \beta_3 = (x - \alpha_3)^{r_3}$ where $r_1 = r_2 = r_3 = \deg h$. Then $e_1 = r_1 b_1$, $e_2 = r_2 b_2$, and $e_3 = r_3 b_3$, so that $\deg h > 1$ divides the pairwise relatively prime integers e_1, e_2, and e_3, yielding a contradiction.

All of the possible values of m have been rejected. Therefore $f(x)$ is prime. ∎

Theorem 2.14. *Let $f(x)$ be a complex rational function with numerator degree n_1 and denominator degree n_2. Let d be the greatest proper divisor of $n = \deg f$. If $n_2 - n_1 > d$ and $n_2 - n_1$ is relatively prime to n_1 as well as to the multiplicities of all zeros of $f(x)$, then $f(x)$ is prime.*

Proof. Suppose for a contradiction that $f(x)$ is composite. There exist complex rational functions $g(x)$ and $h(x)$ such that $f(x) = g(h(x))$. Let

$$f(x) = \frac{a\prod_{i=1}^{N}(x-a_i)^{e_i}}{f_2(x)}, \qquad g(x) = \frac{b\prod_{i=1}^{m_1}(x-\alpha_i)}{\prod_{j=1}^{m_2}(x-\beta_j)}, \qquad h(x) = \frac{h_1(x)}{h_2(x)}$$

where $k_1 = \deg h_1 > \deg h_2 = k_2$. Since $n_2 - n_1 > d > 0$, we conclude from Lemma 2.7 that $n_2 - n_1 = (m_2 - m_1)(k_1 - k_2)$ so that $m_2 > m_1$, and we obtain

$$\frac{a\prod_{i=1}^{N}(x-a_i)^{e_i}}{f_2(x)} = \frac{bh_2(x)^{m_2-m_1}\prod_{i=1}^{m_1}(h_1(x)-\alpha_i h_2(x))}{\prod_{j=1}^{m_2}(h_1(x)-\beta_j h_2(x))}.$$

If $m_2 - m_1 = 1$, then $n_2 - n_1 = k_1 - k_2 \le k_1 \le d$ yields a contradiction to $n_2 - n_1 > d$, so we have $m_2 - m_1 \ge 2$. Since n_1 and $n_2 - n_1$ are relatively prime, so are n_1 and n_2. It follows that $h_2(x)$ cannot be constant, since if $h(x)$ is a polynomial, its degree must divide both n_1 and n_2. Then $h_2(x)$ has degree at least 1 and $h_2(x)^{m_2-m_1}$ divides $a\prod_{i=1}^{N}(x-a_i)^{e_i}$, where $m_2 - m_1$ must then divide e_i for some $i = 1, \ldots, N$. The integer $m_2 - m_1$ also divides $n_2 - n_1$, which contradicts $n_2 - n_1$ being relatively prime to the multiplicities of all of the zeros of $f(x)$. Therefore $f(x)$ is prime. ∎

The following example shows that the condition of $n_2 - n_1$ being relatively prime to the multiplicities of all of the zeros of $f(x)$ is necessary.

EXAMPLE 2.15. Let
$$f(x) = \frac{(x-3)^4(x^3 - 3x^2 + 2x + 2)}{(x-1)^{15}}.$$
The zeros of $x^3 - 3x^2 + 2x + 2$ all have multiplicity 1, so $n_2 - n_1 = 8$ is relatively prime to all of these multiplicities as well as to $n_1 = 7$. The condition $n_2 - n_1 > d = 5$ is also satisfied. The integer $n_2 - n_1 = 8$ is not relatively prime to 4, and this is sufficient for the above theorem to fail, for $f(x) = g(h(x))$ where $g(x) = (x-1)/x^5$ and $h(x) = (x-1)^3/(x-3)$.

COROLLARY 2.16. *Let $f(x)$ be a complex polynomial of degree n with at least two distinct roots and let d be the greatest proper divisor of n. If there exists a root of $f(x)$ with multiplicity $e > d$ such that e is relatively prime to n as well as to the multiplicities of all other roots of $f(x)$, then $f(x)$ is prime.*

Proof. Let
$$f(x) = a \prod_{i=1}^{N} (x - \alpha_i)^{e_i}$$
where $N \geq 2$, and assume without loss of generality that α_1 is the root with multiplicity $e_1 > d$ which is relatively prime to n and to all other multiplicities. Define the unit $\mu(x) = (\alpha_1 x + 1)/x$ where $\alpha_1 \cdot 0 - 1 \cdot 1 = -1 \neq 0$. Then the function
$$f(\mu(x)) = \frac{a \prod_{i=1}^{N}((\alpha_1 x + 1) - \alpha_i x)^{e_i}}{x^n} = \frac{a \prod_{i=2}^{N}((\alpha_1 - \alpha_i)x + 1))^{e_i}}{x^n}$$
has numerator degree $n_1 = n - e_1$ and denominator degree $n_2 = n$. Since e_1 and n are relatively prime, so are n_1 and n_2. Then $n_2 - n_1 = e_1 > d$ and $n_2 - n_1$ is relatively prime to n_1 as well as to e_i for all $i = 2, \ldots, N$. Then $f(\mu(x))$ satisfies the conditions of Theorem 2.14 and is prime. Therefore $f(x)$ is also prime. ∎

3. Critical values of composite rational functions. Let $f(x)$ be a non-constant complex rational function. Let $x_0 \in \mathbb{C}$ lie in the domain of the function $f(x)$. The smallest integer $i \geq 1$ such that $f^{(i)}(x_0) \neq 0$ is called the *valency* of $f(x)$ at x_0 and is denoted by $v_f(x_0)$. If $v_f(x_0) \geq 2$, then x_0 is called a *critical point* of $f(x)$. A number $t_0 \in \mathbb{C}$ is a *critical value* of $f(x)$ if there exists a critical point x_0 of $f(x)$ such that $f(x_0) = t_0$.

THEOREM 3.1. *Let $f(x)$ be a complex rational function of degree n and let d be the greatest proper divisor of n. Suppose that $f(x)$ has a critical* *point $x_0 \in \mathbb{C}$ such that its valency $v_f(x_0)$ is divisible by a prime number $p > d$. Then $f(x)$ is prime.*

Proof. Let $v_f(x_0) = e$ be the valency of some critical point x_0 of $f(x)$ such that e is divisible by a prime number $p > d$. It follows that $f^{(i)}(x_0) = 0$ for all $i = 1, \ldots, e-1$ and $f^{(e)}(x_0) \neq 0$. Then $f'(x)$ has a zero of order $e-1$ at x_0, so there exists a rational function $q(x)$ such that $f'(x) = (x-x_0)^{e-1}q(x)$ where $q(x_0) \neq 0$. Then there exists a rational function $y(x)$ such that $f(x) - f(x_0) = (x-x_0)^e y(x)$ where $y(x_0) \neq 0$. We define the unit $\mu(x) = x - f(x_0)$. Then x_0 is a zero of $\mu(f(x)) = (x-x_0)^e y(x)$ with multiplicity e divisible by the prime number $p > d$. Thus $\mu(f(x))$ is prime by Corollary 2.10, and $f(x)$ is prime as well. ∎

A useful tool in the study of a polynomial's critical values is the discriminant, which can be described through the resultant of two polynomials. Let R be an integral domain and let K be its field of fractions. Let $u(x) = a_n x^n + \cdots + a_1 x + a_0$ and $v(x) = b_m x^m + \cdots + b_1 x + b_0$ be polynomials over R. Let $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_m$ be all of the roots of $u(x)$ and $v(x)$ respectively in an algebraic closure of K. The *resultant* of $u(x)$ and $v(x)$ is given by

$$\mathrm{Res}_x(u(x), v(x)) = a_n^m b_m^n \prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i - \beta_j).$$

We then define the *discriminant* of the polynomial $u(x)$ by

$$D(u(x)) = \frac{(-1)^{n(n-1)/2}}{a_n}\,\mathrm{Res}_x(u(x), u'(x)).$$

We extend this concept to rational functions as follows. Let K be a field, and let $u(x) = u_1(x)/u_2(x)$ and $v(x) = v_1(x)/v_2(x)$ be rational functions over K in their most reduced forms, where we assume without loss of generality that $u_2(x)$ and $v_2(x)$ are monic. We then define the *resultant* of $u(x)$ and $v(x)$ by

$$\mathrm{Res}_x(u(x), v(x)) = \mathrm{Res}_x(u_1(x), v_1(x)).$$

From this definition, we may obtain information regarding the critical values of rational functions similar to what can be obtained for polynomials from the standard definition of the resultant. We require the following properties, which are analogous to those for the resultant of two polynomials found in [1]. The proof is omitted.

(1) Let $u(x)$ and $v(x)$ be rational functions as described above. Let $u_1(x) = a_n x^n + \cdots + a_1 x + a_0$ and $v_1(x) = b_m x^m + \cdots + b_1 x + b_0$ be polynomials with roots $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_m$ respectively in an algebraic closure of K. Then

$$\mathrm{Res}_x(v(x), u(x)) = (-1)^{nm}\,\mathrm{Res}_x(u(x), v(x)).$$

(2) Under the same hypotheses as in (1),

$$\operatorname{Res}_x(u(x), v(x)) = a_n^m \prod_{i=1}^{n} v_1(\alpha_i).$$

(3) $u(x)$ and $v(x)$ have a zero in common if and only if

$$\operatorname{Res}_x(u(x), v(x)) = 0.$$

(4) For an additional rational function $w(x) = w_1(x)/w_2(x)$ over K,

$$\operatorname{Res}_x(u(x), v(x)w(x)) = \operatorname{Res}_x(u_1(x), p(x)) \operatorname{Res}_x(u_1(x), q(x)),$$

where $p(x)$ is the quotient obtained from dividing $v_1(x)$ by the monic greatest common divisor of $v_1(x)$ and $w_2(x)$, and $q(x)$ is the quotient obtained from dividing $w_1(x)$ by the monic greatest common divisor of $w_1(x)$ and $v_2(x)$.

Let $f(x)$ be a complex rational function and let $f'(x)$ be the derivative of $f(x)$. We write $f(x) = f_1(x)/f_2(x)$ and $f'(x) = \varphi_1(x)/\varphi_2(x)$, where we assume without loss of generality that $\varphi_2(x)$ is monic. This expression for $f'(x)$ is the most reduced expression of

$$F(x) = \frac{f_1'(x)f_2(x) - f_1(x)f_2'(x)}{f_2(x)^2},$$

and it follows that $\varphi_2(x)$ divides $f_2(x)^2$. Since the reduced expression for $f'(x)$ is obtained by simplifying linear factors from the numerator and denominator of $F(x)$, where $f_1(x)$ and $f_2(x)$ share no common linear factors, the only such linear factors which can be simplified must divide both $f_2(x)$ and $f_2'(x)$. We conclude that $f_2(x)$ divides $\varphi_2(x)$. Thus $f(x)$ and $f'(x)$ have the same domain.

Let $\beta_1, \ldots, \beta_m$ be all of the zeros of $f'(x)$. Then β_i is in the domain of $f'(x)$, and also in the domain of $f(x)$, for $i = 1, \ldots, m$. Let t be a variable, let b be the leading coefficient of $\varphi_1(x)$, and let $n = \deg f(x)$. Consider the function $R(t) = \operatorname{Res}_x(f(x) - t, f'(x))$. Using the properties of the resultant, we have

$$\begin{aligned} R(t) &= \operatorname{Res}_x\left(\frac{f_1(x) - tf_2(x)}{f_2(x)}, \frac{\varphi_1(x)}{\varphi_2(x)}\right) = \operatorname{Res}_x\Big(f_1(x) - tf_2(x), b\prod_{i=1}^{m}(x - \beta_i)\Big) \\ &= (-1)^{nm} b^n \prod_{i=1}^{m}(f_1(\beta_i) - tf_2(\beta_i)) = (-1)^{nm} b^n \prod_{i=1}^{m} f_2(\beta_i) \prod_{i=1}^{m}(f(\beta_i) - t). \end{aligned}$$

We remark that since β_i is a zero of $f'(x)$, it is a critical point of $f(x)$ and $f(\beta_i)$ is a critical value of $f(x)$ for $i = 1, \ldots, m$. It immediately follows that $R(t_0) = 0$ if and only if t_0 is a critical value of $f(x)$. Similarly to the definition of the multiplicity of a critical value of a polynomial found in [1], we define the *multiplicity* of the critical value t_0 as the multiplicity of t_0 as a root of $R(t)$, and we call a critical value with multiplicity equal to one a *simple* critical value.

LEMMA 3.2. *Let $f(x)$ be a composite complex rational function of degree n and let d be the greatest proper divisor of n. Let $f(x) = g(h(x))$ where $h(x) = h_1(x)/h_2(x)$ satisfies $k = \deg h_1(x) > \deg h_2(x)$, and let n_1 and n_2 be the numerator and denominator degrees of $f(x)$ respectively. Let $R(t)$ be the resultant of $f(x) - t$ and $f'(x)$. Then there exists $c \in \mathbb{C}^*$, a non-negative integer ℓ, and a polynomial $p(x)$ dividing the numerator of $h'(x)$ such that*

$$R(t) = ct^{\ell}\big(\mathrm{Res}_x(g(x) - t, g'(x))\big)^k \,\mathrm{Res}_x(f(x) - t, p(x)),$$

where $\ell > 0$ if n_1 and n_2 are relatively prime integers satisfying $n_2 - n_1 > d$.

Proof. We will write $u(t) \sim v(t)$ to denote that the functions $u(t)$ and $v(t)$ are equal up to multiplication by a constant. Let

$$g'(x) = \frac{b\prod_{i=1}^{m_1}(x-\alpha_i)}{\prod_{j=1}^{m_2}(x-\beta_j)}, \qquad h'(x) = \frac{h_1'(x)h_2(x) - h_1(x)h_2'(x)}{h_2(x)^2} = \frac{q_1(x)}{h_2(x)q_2(x)}$$

where $q_1(x)$ and $q_2(x)$ share no common factor, and let $m = \deg g'(x)$. Then

$$f'(x) = \frac{bh_2(x)^{m-m_1}q_1(x)\prod_{i=1}^{m_1}(h_1(x) - \alpha_i h_2(x))}{h_2(x)^{m-m_2+1}q_2(x)\prod_{j=1}^{m_2}(h_1(x) - \beta_j h_2(x))}.$$

The only linear factors which can be simplified in this expression for $f'(x)$ are shared factors between $h_2(x)^{m-m_1}$ and $h_2(x)^{m-m_2+1}q_2(x)$ or shared factors between $q_1(x)$ and $\prod_{j=1}^{m_2}(h_1(x) - \beta_j h_2(x))$. We let $H(x)$ be the quotient obtained from dividing $h_2(x)^{m-m_1}$ by the monic greatest common divisor of $h_2(x)^{m-m_1}$ and $h_2(x)^{m-m_2+1}q_2(x)$, and we let $p(x)$ be the quotient obtained from dividing $q_1(x)$ by the monic greatest common divisor of $q_1(x)$ and $\prod_{j=1}^{m_2}(h_1(x) - \beta_j h_2(x))$. Letting $R(t)$ be the resultant of $f(x) - t$ and $f'(x)$, we then have

$$R(t) = \mathrm{Res}_x\Big(f_1(x) - tf_2(x), bH(x)p(x)\prod_{i=1}^{m_1}(h_1(x) - \alpha_i h_2(x))\Big).$$

We consider the above expression as a product of three factors.

The first factor is

$$R_1 = \mathrm{Res}_x\Big(f_1(x) - tf_2(x), \prod_{i=1}^{m_1}(h_1(x) - \alpha_i h_2(x))\Big).$$

For each $i = 1, \ldots, m_1$, the equation $h_1(x) - \alpha_i h_2(x) = 0$ has k solutions $s_{i,1}, \ldots, s_{i,k}$. For any index r, the solution $s_{i,r}$ satisfies $h_1(s_{i,r}) - \alpha_i h_2(s_{i,r}) = 0$, so that $h(s_{i,r}) = \alpha_i$. Since α_i is a zero of $g'(x)$ for $i = 1, \ldots, m_1$, each of these zeros must also be in the domain of $g(x)$ and $g(\alpha_i) = g(h(s_{i,r})) = f(s_{i,r})$ for $i = 1, \ldots, m_1$ and $r = 1, \ldots, k$. We then have

$$\begin{aligned} R_1 &\sim \prod_{i=1}^{m_1}\prod_{r=1}^{k}(f_1(s_{i,r}) - tf_2(s_{i,r})) \sim \prod_{i=1}^{m_1}\prod_{r=1}^{k}(f(s_{i,r}) - t) \\ &\sim \prod_{i=1}^{m_1}\prod_{r=1}^{k}(g(\alpha_i) - t) \sim \Big(\prod_{i=1}^{m_1}(g(\alpha_i) - t)\Big)^k \sim \big(\mathrm{Res}_x(g(x) - t, g'(x))\big)^k. \end{aligned}$$

The second factor is

$$R_2 = \mathrm{Res}_x(f_1(x) - tf_2(x), H(x)).$$

If $m_1 \geq m_2$, then $H(x)$ is constant and this factor is constant. If $m_2 > m_1$, $H(x)$ will not be constant if $h_2(x)$ is not constant and $m_2 - m_1 > 2$. In this case, we let $\ell = \deg H$ and let $s_1, \ldots, s_\ell$ be all of the roots of $H(x)$. Since $H(x)$ divides $h_2(x)^{m_2 - m_1}$, every such root s of $H(x)$ satisfies $h_2(s) = 0$, and so $|h(s)|$ is infinite. Since $m_2 > m_1$, the function $f(x) = g(h(x))$ has a value of zero at $x = s_r$ for $r = 1, \ldots, \ell$. Then we have

$$R_2 \sim \prod_{r=1}^{\ell}(f_1(s_r) - tf_2(s_r)) \sim \prod_{r=1}^{\ell}(f(s_r) - t) \sim (-t)^\ell.$$

In particular, if $n_2 - n_1 > d$ where n_1 and n_2 are relatively prime integers, from Lemma 2.7 we have $d < n_2 - n_1 = (\deg g_2 - \deg g_1)(\deg h_1 - \deg h_2) \leq (\deg g_2 - \deg g_1)d$, so that $\deg g_2 - \deg g_1 > 1$. From Lemma 2.8, we then have $m_2 - m_1 = -(\deg g_1 - \deg g_2 - 1) = \deg g_2 - \deg g_1 + 1 > 2$. The polynomial $h_2(x)$ cannot be constant, as this would imply that $k = \deg h_1$ would divide both n_1 and n_2, yielding a contradiction. It follows that $H(x)$ will not be constant in this case, and by our definition of the function $H(x)$ we have

$$\begin{aligned} \ell = \deg H &\geq (m_2 - m_1 - 1)k_2 - \deg q_2 \\ &\geq (m_2 - m_1 - 2)k_2 = (\deg g_2 - \deg g_1 - 1)k_2. \end{aligned}$$

The final factor is

$$R_3 = \mathrm{Res}_x(f(x) - t, b \cdot p(x)),$$

and we conclude that for some non-zero complex number c we have

$$R(t) = ct^\ell\big(\mathrm{Res}_x(g(x) - t, g'(x))\big)^k\,\mathrm{Res}_x(f(x) - t, p(x))$$

where ℓ is a non-negative integer such that $\ell > 0$ when n_1 and n_2 are relatively prime integers satisfying $n_2 - n_1 > d$. ∎

COROLLARY 3.3. *Let $f(x)$ be a composite complex rational function of degree n which has a right composition factor of degree k. Let $R(t)$ be the resultant of $f(x) - t$ and $f'(x)$. Then there exists a non-negative integer ℓ and polynomials $A(t)$ and $B(t)$ such that $R(t) = t^\ell[A(t)]^k B(t)$ and $\deg B(t) \leq 2k - 1$. Moreover, if d is the greatest proper divisor of n, if n_1 and n_2 are the numerator and denominator degrees of $f(x)$ respectively, and if n_1 and n_2 are relatively prime integers such that $n_2 - n_1 > d$, then $\ell > 0$.*

Proof. Recall that we write $u(t) \sim v(t)$ to denote that the functions $u(t)$ and $v(t)$ are equal up to multiplication by a constant. Since $f(x)$ is composite with a right composition factor of degree k, there exist complex rational functions $g(x)$ and $h(x) = h_1(x)/h_2(x)$ such that $f(x) = g(h(x))$ and $k = \deg h_1(x) > \deg h_2(x)$. Then there exists $c \in \mathbb{C}^*$, a non-negative integer ℓ, and a polynomial $p(x)$ which divides the numerator of $h'(x)$, such that

$$R(t) = ct^\ell \big(\mathrm{Res}_x(g(x) - t, g'(x))\big)^k \,\mathrm{Res}_x(f(x) - t, p(x)),$$

and where $\ell > 0$ if n_1 and n_2 are relatively prime integers satisfying $n_2 - n_1 > d$.

Setting $A(t) = \mathrm{Res}_x(g(x) - t, g'(x))$ and $B(t) = c\,\mathrm{Res}_x(f(x) - t, p(x))$ yields the desired expression for $R(t)$, so it only remains to show that $\deg B(t) \le 2k - 1$. We let $p(x) = b\prod_{i=1}^r (x - \alpha_i)$. Since $p(x)$ divides the numerator of $h'(x)$, it follows that $p(x)$ must divide the numerator of

$$\frac{h_1'(x)h_2(x) - h_1(x)h_2'(x)}{h_2(x)^2},$$

so that $r \le \deg h_1(x) + \deg h_2(x) - 1 \le 2k - 1$. Writing $B(t)$ explicitly, we obtain

$$B(t) = c\,\mathrm{Res}_x\bigg(\frac{f_1(x) - tf_2(x)}{f_2(x)}, p(x)\bigg) \sim \mathrm{Res}_x\Big(f_1(x) - tf_2(x), \prod_{i=1}^r (x - \alpha_i)\Big)$$
$$\sim \prod_{i=1}^r (f_1(\alpha_i) - tf_2(\alpha_i))$$

so that $\deg B(t) \le r \le 2k - 1$. ∎

The following two results show that the polynomial $R(t)$ obtained by taking the resultant of a complex rational function $f(x) - t$ and its derivative can be useful in determining whether $f(x)$ is prime. The first result concerns the non-zero critical values of $f(x)$, and its proof follows a similar method to [1, proof of Theorem 1]. The second result concerns only the critical value zero.

THEOREM 3.4. *Let $f(x)$ be a complex rational function of degree n and let d be the greatest proper divisor of n. Suppose that $f(x)$ has at least $2d$ non-zero simple critical values. Then $f(x)$ is prime.*

Proof. Suppose for contradiction that $f(x)$ is composite. There exist complex rational functions $g(x)$ and $h(x)$ of degrees $m, k \ge 2$ respectively such that $f(x) = g(h(x))$. We let $R(t)$ be the resultant of $f(x) - t$ and $f'(x)$, and we write $R(t) = t^\ell [A(t)]^k B(t)$ where ℓ is a non-negative integer and $\deg B(t) \le 2k - 1$. Let δ be the number of non-zero simple critical values of $f(x)$. Since these critical values must be roots of the polynomial $B(t)$, we obtain

$$2k - 1 \geq \deg B(t) \geq \delta \geq 2d \geq 2k,$$

which is a contradiction. Therefore $f(x)$ is prime. ∎

THEOREM 3.5. *Let $f(x)$ be a complex rational function of degree n, let d be the greatest proper divisor of n, and let n_1 and n_2 be the numerator and denominator degrees of $f(x)$ respectively. If n_1 and n_2 are relatively prime integers such that $n_2 - n_1 > d$, and if zero is a critical value of $f(x)$ with multiplicity $e < (n_2 - n_1 - d)/d$, then $f(x)$ is prime. In particular, if zero is not a critical value of $f(x)$, then $f(x)$ is prime.*

Proof. Suppose for contradiction that $f(x)$ is composite. There exist complex rational functions $g(x)$ and $h(x)$ such that $f(x) = g(h(x))$ and that $h(x)$ has larger numerator degree than denominator degree. Let m_1 and k_1 be the numerator degrees of $g(x)$ and $h(x)$ respectively, and let m_2 and k_2 be the denominator degrees of $g(x)$ and $h(x)$ respectively. Since we assume that $k_1 > k_2$ and $n_2 > n_1$, we have $n_2 - n_1 = (m_2 - m_1)(k_1 - k_2)$. It follows that $m_2 > m_1$ and

$$m_2 - m_1 - 1 = \frac{n_2 - n_1}{k_1 - k_2} - 1 \geq \frac{n_2 - n_1}{k_1} - 1 \geq \frac{n_2 - n_1}{d} - 1 = \frac{n_2 - n_1 - d}{d}.$$

Since n_1 and n_2 are relatively prime, we know that $h(x)$ cannot be a polynomial as this would imply $\deg h$ divides both n_1 and n_2. Then $k_2 \geq 1$ and we obtain $(m_2 - m_1 - 1)k_2 \geq m_2 - m_1 - 1 \geq (n_2 - n_1 - d)/d$. We now let $R(t)$ be the resultant of $f(x) - t$ and $f'(x)$, and we write $R(t) = t^{\ell}[A(t)]^{k_1} B(t)$. From the arguments presented in the proof of Lemma 3.2, we have $\ell \geq (m_2 - m_1 - 1)k_2$. It follows that zero is a critical value of $f(x)$ of multiplicity at least $(m_2 - m_1 - 1)k_2$; but by assumption the multiplicity e of this critical value satisfies $e < (n_2 - n_1 - d)/d \leq (m_2 - m_1 - 1)k_2$, yielding a contradiction. ∎

The following result provides some examples of prime functions.

PROPOSITION 3.6. *Let $f(x) = (x^n + a)/(x^m + b)$ where $a, b \in \mathbb{C}$ are not both zero, let d be the greatest proper divisor of* $\deg f$, *and let n and m be relatively prime positive integers such that $|n - m| > d$. Then $f(x)$ is prime.*

Proof. We assume without loss of generality that $n \leq m$, and we consider two cases.

Assume first that $a \neq 0$. Suppose for contradiction that $f(x)$ is composite. Since m and n are relatively prime integers, it follows that $n \neq m$ thus $n < m$. Then zero must be a critical value of $f(x)$ by Lemma 3.2. We show that no critical point of $f(x)$ yields zero as a critical value.

If $b \neq 0$, then

$$f'(x) = \frac{x^{n-1}((n - m)x^m + (-am)x^{m-n} + (bn))}{(x^m + b)^2}.$$

Let $\xi_1, \ldots, \xi_{m+n-1}$ be all of the zeros of $f'(x)$. Then $\xi_1, \ldots, \xi_{m+n-1}$ are the critical points of $f(x)$, and for each $i = 1, \ldots, m+n-1$ we have either $\xi_i^{n-1} = 0$ or $(n-m)\xi_i^m + (-am)\xi_i^{m-n} + (bn) = 0$. A critical point ξ with $\xi^{n-1} = 0$ satisfies $\xi = 0$ and $f(\xi) = a/b \neq 0$. For the second case we assume towards a contradiction that a critical point ξ satisfies $(n-m)\xi^m + (-am)\xi^{m-n} + (bn) = 0$. From $f(\xi) = 0$ we have $\xi^n + a = 0$, so that $\xi^n = -a \neq 0$ and $(n-m)\xi^m + (m)\xi^{m-n}\xi^n + (bn) = n(\xi^m + b) = 0$. Then $\xi^m + b = 0$ yields a contradiction, since $f(x)$ has no linear factor dividing both its numerator and its denominator.

If $b = 0$, then

$$f'(x) = \frac{(n-m)x^n + (-am)}{x^{m+1}}.$$

Let $\xi_1, \ldots, \xi_n$ be all of the zeros of $f'(x)$. Then $\xi_1, \ldots, \xi_n$ are the critical points of $f(x)$, and for each $j = 1, \ldots, n$ we have $\xi_j^n = -am/(m-n)$. If $f(\xi_j) = 0$, then $-a = -am/(m-n)$ yields $m - n = m$, contradicting $n > 0$.

Therefore zero cannot be a critical value of the function $f(x)$, and we conclude that $f(x)$ is prime.

Assume now that $a = 0$. Then by assumption we have $b \neq 0$, and $f(x) = x^n/(x^m + b)$ is prime if and only if $F(x) = (x^m + b)/x^n$ is prime. Since m and n are relatively prime integers such that $m > n$, we conclude by Theorem 2.11 that $F(x)$ is prime. Therefore $f(x)$ is prime. ■

We conclude this section by providing some examples which show that, in general, knowing whether the numerator and denominator polynomials of a rational function $f(x)$ are prime or composite is not sufficient to conclude whether $f(x)$ itself is prime or composite.

Example 3.7. Let

$$f(x) = \frac{f_1(x)}{f_2(x)} = \frac{4x^3 + 6x^2 + 4x + 1}{x^4 - 2x^3 - x^2}.$$

Then $f_1(x)$ is prime, $f_2(x)$ is prime by [1, Theorem 1] since all of its critical values are simple, and $f(x)$ is composite since it is the composition of $g(x) = -\frac{x^2-1}{x-2}$ and $h(x) = \frac{x^2+2x+1}{x^2}$.

Example 3.8. Let

$$f(x) = \frac{f_1(x)}{f_2(x)} = \frac{x^5 + 1}{x^3}.$$

Then $f_1(x)$ and $f_2(x)$ are both prime, and $f(x)$ is prime.

Example 3.9. Let

$$f(x) = \frac{f_1(x)}{f_2(x)} = \frac{x^2 + 1}{x^4}.$$

Then $f_1(x)$ is prime, $f_2(x)$ is composite, and $f(x)$ is composite.

Example 3.10. Let

$$f(x) = \frac{f_1(x)}{f_2(x)} = \frac{x^5+1}{x^4}.$$

Then $f_1(x)$ is prime, $f_2(x)$ is composite, and $f(x)$ is prime.

Example 3.11. Let

$$f(x) = \frac{f_1(x)}{f_2(x)} = \frac{x^9+1}{x^6}.$$

Then $f_1(x)$, $f_2(x)$, and $f(x)$ are all composite.

Example 3.12. Let

$$f(x) = \frac{f_1(x)}{f_2(x)} = \frac{x^9+1}{x^4}.$$

Then $f_1(x)$ and $f_2(x)$ are composite, and $f(x)$ is prime by Theorem 2.11.

4. Concluding remark. It would be of interest to find other results similar to Proposition 2.3 and Lemma 2.7. In particular, another mapping $\psi : \mathbb{C}(x) \to \mathbb{Z}$ for which $\psi(g \circ h) = \psi(g) \cdot \psi(h)$ is satisfied for rational functions g and h could potentially provide many more examples of prime functions.

Acknowledgements. The authors express their gratitude to the anonymous referee for constructive suggestions which improved the quality of the paper. They also thank Prof. Mohamed Ayad for many helpful discussions during the preparation of this paper.

The first author was supported in part by NSERC.

References

[1] M. Ayad, *Critical points, critical values of a prime polynomial*, Complex Variables Elliptic Equations 51 (2006), 143–160.

[2] A. F. Beardon, *Composition factors of polynomials*, Complex Variables Theory Appl. 43 (2001), 225–239.

Omar Kihel, Jesse Larone
Department of Mathematics
Brock University
St. Catharines, Ontario L2S 3A1, Canada
E-mail: okihel@brocku.ca
jl08yo@brocku.ca

Received on 5.6.2014
and in revised form on 11.2.2015 (7830)