A transformation of rational functions

Elem. Math. 58 (2003) 73 – 83
0013-6018/03/020073-11

Elemente der Mathematik

A transformation of rational functions

George Boros, Michael Joyce and Victor H. Moll

George Boros was born in Norway and lived in Canada for a number of years. He received his Ph.D. from Tulane University in 1997 and is currently on the faculty of Xavier University of Louisiana. His research interests include classical mathematics, combinatorics and number theory.

Michael Joyce graduated Tulane University as a mathematics major in 2000. He is now attending graduate school in the Mathematics Department of Brown University. His mathematical interests are arithmetic geometry and number theory.

Victor H. Moll was born in Santiago, Chile. He studied under Henry McKean at the Courant Institute and joined the Department of Mathematics at Tulane University in the wonderful city of New Orleans. His current mathematical interests lie in the evaluation of definite integrals.

1 Introduction

The problem of evaluating a definite integral exactly is as old as calculus itself. For example Wallis produced the evaluation

$$\int_0^\infty \frac{dx}{(x^2+1)^{m+1}} = \frac{\pi}{2^{2m+1}} \binom{2m}{m}. \tag{1.1}$$

Die Bedeutung elliptischer Integrale, z.B. zur Berechnung des Ellipsenumfangs, dürfte vielen Lesern bekannt sein. Ein solches Integral lässt sich durch iterative Anwendung der Landen-Transformation mit Hilfe des sogenannten arithmetisch-geometrischen Mittels berechnen. Für Integrale von geraden rationalen Funktionen gibt es analoge Transformationen, deren Iteration zur Bestimmung der entsprechenden Integrale führt. In der vorliegenden Note wird nun die Frage untersucht, ob sich Integrale von ungeraden rationalen Funktionen ähnlich behandeln lassen. Dazu wird auf der Menge der rationalen Funktionen eine gewisse Operation eingeführt und deren Fixpunkte studiert. Abschliessend wird diese Operation auf eine spezielle Klasse rationaler Funktionen eingeschränkt und die dazugehörigen Orbits bestimmt, was mit elementaren zahlentheoretischen Erkenntnissen zusammenhängt.

In the study of exact evaluations of definite integrals of rational functions we have observed that *even* ones are easier. The example

$$\int_0^\infty \frac{dx}{(x^4+2ax^2+1)^{m+1}} = \frac{\pi}{2^{m+3/2}(a+1)^{m+1/2}} P_m(a)\,, \tag{1.2}$$

where

$$P_m(a) = 2^{-2m}\sum_{k=0}^{m} 2^k \binom{2m-2k}{m-k}\binom{m+k}{m}(a+1)^k\,, \tag{1.3}$$

is described in [2]. Observe that $P_m(a)$ is a polynomial in a of degree m. Apart from their intrinsic interest, the mathematical questions that arise from the evaluation (1.2) are fascinating. The reader will find in [2] that (1.2) is essentially the coefficient of the Taylor expansion of $h(c) = \sqrt{a+\sqrt{1+c}}$ at $c = 0$. There are many open questions connected to this example. For example, it is not hard to prove that the coefficients $d_l(m)$ of the polynomial $P_m(a)$ can be expressed as

$$d_l(m) = \frac{1}{l!\,m!\,2^{m+l}}\left(\alpha_l(m)\prod_{k=1}^{m}(4k-1) - \beta_l(m)\prod_{k=1}^{m}(4k+1)\right) \tag{1.4}$$

where the functions α_l, β_l are polynomials in m. The linear and quadratic terms are given by

$$d_1(m) = \frac{1}{m!2^{m+1}}\left((2m+1)\prod_{k=1}^{m}(4k-1) - \prod_{k=1}^{m}(4k+1)\right) \tag{1.5}$$

and

$$d_2(m) = \frac{1}{2m!2^{m+2}}\left(2(2m^2+2m+1)\prod_{k=1}^{m}(4k-1) - 2(2m+1)\prod_{k=1}^{m}(4k+1)\right),$$

respectively. We have conjectured that the polynomials α_l and β_l have all their roots on the vertical line $\mathrm{Re}(m) = -1/2$.

In the case of rational functions of degree 6 we have found a surprising connection with the *Landen transformation* $(a,b) \mapsto (a_1,b_1)$, where

$$a_1 = \frac{a+b}{2} \quad \text{and} \quad b_1 = \sqrt{ab}\,. \tag{1.6}$$

It is well-known that (1.6) leaves the elliptic integral

$$G(a,b) = \int_0^{\pi/2} \frac{dt}{\sqrt{a^2\sin^2 t + b^2\cos^2 t}} \tag{1.7}$$

invariant, i.e. $G(a,b) = G(a_1,b_1)$. The transformation (1.6) can be iterated to produce a double sequence (a_n,b_n) such that $0 \le a_n - b_n < 2^{-n}$. It follows that a_n and b_n converge

to a common limit, the so-called *arithmetic-geometric* mean of a and b, denoted by $\mathrm{AGM}(a,b)$. Passing to the limit in $G(a,b) = G(a_n, b_n)$ produces

$$\frac{\pi}{2\,\mathrm{AGM}(a,b)} = \int_0^{\pi/2} \frac{dt}{\sqrt{a^2 \sin^2 t + b^2 \cos^2 t}}\,. \tag{1.8}$$

In this form, the evaluation of the elliptic integral $G(a,b)$ is reduced to an iterative process.

The same type of transformation exists for the integral

$$U_6(a,b;c,d,e) = \int_0^{\infty} \frac{cx^4 + dx^2 + e}{x^6 + ax^4 + bx^2 + 1}\,dx. \tag{1.9}$$

We have shown that if the initial values of the parameters are positive and we define

$$\begin{aligned}
a_{n+1} &= \frac{a_n b_n + 5a_n + 5b_n + 9}{(a_n + b_n + 2)^{4/3}}\,,\\
b_{n+1} &= \frac{a_n + b_n + 6}{(a_n + b_n + 2)^{2/3}}\,,\\
c_{n+1} &= \frac{c_n + d_n + e_n}{(a_n + b_n + 2)^{2/3}}\,,\\
d_{n+1} &= \frac{(b_n + 3)c_n + 2d_n + (a_n + 3)e_n}{a_n + b_n + 2}\,,\\
e_{n+1} &= \frac{c_n + e_n}{(a_n + b_n + 2)^{1/3}}\,,
\end{aligned} \tag{1.10}$$

then U_6 is invariant under this transformation, i.e.

$$U_6(a_n, b_n; c_n, d_n, e_n) = U_6(a_0, b_0; c_0, d_0, e_0)\,. \tag{1.11}$$

Moreover, $(a_n, b_n) \to (3,3)$ and there exists a number L such that $(c_n, d_n, e_n) \to (1,2,1)\,L$. Passing to the limit in (1.11) produces

$$L = \frac{2}{\pi} \int_0^{\infty} \frac{c_0 x^4 + d_0 x^2 + e_0}{x^6 + a_0 x^4 + b_0 x^2 + 1}\,dx\,. \tag{1.12}$$

Thus, as in the elliptic case, the evaluation of the integral is reduced to an iterative process. Transformations similar to (1.10) exist for the integral of any even rational function. The reader can find more general information about these ideas in [4] and [5].

In order to consider the question of the exact integration of a general rational function $R(x)$, we split it into its even and odd parts $R(x) = R_e(x) + R_o(x)$ and integrate to produce

$$\int_0^{\infty} R(x)\,dx = \int_0^{\infty} R_e(x)\,dx + \int_0^{\infty} R_o(x)\,dx\,. \tag{1.13}$$

The integral of the even part can be dealt with by the methods described above, and the integral of the odd part can be transformed to

$$\int_0^\infty R_o(x)\,dx = \frac{1}{2}\int_0^\infty \frac{R_o(\sqrt{t})}{\sqrt{t}}dt \tag{1.14}$$

via $x = \sqrt{t}$. Motivated by this identity we define the map

$$\mathfrak{F}(R)(x) := \frac{R(\sqrt{x}) - R(-\sqrt{x})}{2\sqrt{x}}\,, \tag{1.15}$$

which has the property

$$\int_0^\infty R(x)\,dx = \int_0^\infty R_e(x)\,dx + \frac{1}{2}\int_0^\infty \mathfrak{F}(R)(x)\,dx\,. \tag{1.16}$$

Naturally the definition (1.15) makes sense, even though the integrals in (1.16) may not exist.

In this paper we describe some elementary results of the map $\mathfrak{F}$.

2 The fixed points of $\mathfrak{F}$

The map $\mathfrak{F}$ transforms the rational function $R(x) = P(x)/Q(x)$ into

$$\mathfrak{F}(R)(x) = \frac{P_1(x)}{Q_1(x)}\,, \tag{2.1}$$

with

$$P_1(x) = \frac{1}{2\sqrt{x}}\left(P(\sqrt{x})Q(-\sqrt{x}) - P(-\sqrt{x})Q(\sqrt{x})\right) \tag{2.2}$$

and

$$Q_1(x) = Q(\sqrt{x})Q(-\sqrt{x})\,. \tag{2.3}$$

The reader can easily check that P_1 and Q_1 are polynomials in x. Thus $\mathfrak{F}$ can be considered as a map from the space of rational functions $\mathfrak{R}$ into itself, and the explicit formulas for P_1 and Q_1 show that the degree of R, defined as the maximum of the degrees of P and Q, is not increased by $\mathfrak{F}$, although it is possible for the degree of R to decrease under $\mathfrak{F}$. For example,

$$\mathfrak{F}\left(\frac{x^2+1}{x^3+1}\right) = \frac{x^2+x}{x^3-1} \tag{2.4}$$

and

$$\mathfrak{F}\left(\frac{x}{x^4+1}\right) = \frac{1}{x^2+1}\,. \tag{2.5}$$

A more dramatic reduction occurs if R is an even rational function, in which case $\mathfrak{F}(R)(x) = 0$.

The effect of $\mathfrak{F}$ on the coefficients of the Laurent expansion of R at $x = 0$ leads to a classification of its fixed points. Recall that the Laurent expansion of a rational function has the form

$$R(x) = \sum_{k=-N}^{\infty} a_k x^k \tag{2.6}$$

with $a_{-N} \neq 0$ and $N \in \mathbb{N}$. The function R is said to have a pole of order N if $N > 0$.

Lemma 2.1 *The expansion* (2.6) *yields*

$$\mathfrak{F}(R)(x) = \sum_{k=-\lfloor (N+1)/2 \rfloor}^{\infty} a_{2k+1} x^k \,. \tag{2.7}$$

Proof. The details are elementary and are left to the reader. □

Lemma 2.2 *The order of a pole at* $x = 0$ *for a fixed point of* $\mathfrak{F}$ *is at most* 1.

Proof. By the previous lemma, a fixed point satisfies

$$\sum_{k=-N}^{\infty} a_k x^k = \sum_{k=-\lfloor (N+1)/2 \rfloor}^{\infty} a_{2k+1} x^k \,. \tag{2.8}$$

Consideration of the lowest-order terms then yields $N = 1$. □

The next theorem provides a first description of the fixed points of $\mathfrak{F}$.

Theorem 2.3 *Let* $R(x)$ *be a fixed point of* $\mathfrak{F}$. *Then there are parameters* $\{a_{2t} : t = 0, 1, \ldots\}$ *such that*

$$R(x) = x^{-2} \times \sum_{t=0}^{\infty} a_{2t} f(x^{2t+1}) \,, \tag{2.9}$$

where

$$f(x) = \sum_{j=0}^{\infty} x^{2^j} \,. \tag{2.10}$$

Conversely, any rational function of the form (2.9) *is fixed by* $\mathfrak{F}$.

Proof. The recurrence (2.8) yields $a_k = a_{2k+1}$ for $k \geq 0$. It follows that

$$a_{k_0} = a_{2^j(k_0+1)-1} \,. \tag{2.11}$$

Now any $n \in \mathbb{N}$ can be written uniquely as $n = 2^j(2t+1) - 1$ with $t, j \geq 0$. Thus any fixed point of $\mathfrak{F}$ must be of the form

$$R(x) = \sum_{t=0}^{\infty} \sum_{j=0}^{\infty} a_{2^j(2t+1)-1} x^{2^j(2t+1)-2} = \sum_{t=0}^{\infty} a_{2t} \sum_{j=0}^{\infty} x^{2^j(2t+1)-2} \,.$$

□

Note. The function f above is a classic example of an analytic function with the unit circle as a natural boundary.

We now provide an example that shows that it is possible to choose parameters $\{a_{2t} : t = 0, 1, 2, \ldots\}$ so that R defined by (2.9) is a rational function. It turns out that every fixed point of $\mathfrak{F}$ can be constructed from this example.

Example. Let m be an odd integer and define

$$a_{2j} = \begin{cases} -1 & \text{if } m \text{ divides } 2j+1, \\ 0 & \text{otherwise.} \end{cases}$$

Then

$$R(x) = \frac{1}{x}\sum_{t=0}^{\infty} a_{2t} f(x^{2t+1}) = -\frac{1}{x}\sum_{k=0}^{\infty}\sum_{j=0}^{\infty} x^{2j(2k+1)m}$$

$$= -\frac{1}{x}\sum_{r=0}^{\infty} x^{rm} = \frac{1}{x(x^m-1)}.$$

The reader can check directly that R is fixed by $\mathfrak{F}$.

Note. Let R be a fixed point of $\mathfrak{F}$. Then, for any odd positive integer m, the function

$$B_m(R(x)) = x^{m-1}R(x^m) \tag{2.12}$$

is also fixed by $\mathfrak{F}$. For example, $R(x) = 1/(x-1)$ is fixed by $\mathfrak{F}$, and so

$$B_m(R(x)) = \frac{x^{m-1}}{x^m-1} \tag{2.13}$$

is also fixed by $\mathfrak{F}$. The reader is referred to [3] for a complete classification of fixed points.

3 The dynamics of a specific rational function

The remainder of this paper deals with properties of the specific function

$$R_{j,m}(x) = \frac{x^j}{x^m-1} \quad \text{for } m \text{ odd and } j \in \mathbb{Z} \tag{3.1}$$

under the transformation $\mathfrak{F}$. This example has been chosen for two reasons: first, the special cases $R_{-1,m}$ and $R_{m-1,m}$ have already appeared as fixed points of $\mathfrak{F}$, and second, all the poles of $R_{j,m}$ are on the unit circle and this prevents the growth of the coefficients of the iterates $\mathfrak{F}^{(i)}(R_{j,m})$. Indeed, the possible poles of $\mathfrak{F}(R)$ are among the squares of those of R. Thus the poles of $\mathfrak{F}^{(i)}(x)$ remain of modulus 1.

Lemma 3.1 *The transformation $\mathfrak{F}$ gives*

$$\mathfrak{F}\left(\frac{x^j}{x^m-1}\right) = \frac{x^{\gamma_m(j)}}{x^m-1},$$

where

$$\gamma_m(j) = m\left\lfloor \frac{j}{2} \right\rfloor - \frac{1}{2}(m-1)(j-1) = \begin{cases} (m-1+j)/2 & \text{if } j \text{ is even,} \\ (j-1)/2 & \text{if } j \text{ is odd.} \end{cases} \tag{3.2}$$

Proof. The details are elementary. □

The dynamical properties of the iterates $\mathfrak{F}^{(k)}(R)$ are thus reduced to those of γ_m.

Note. The example $x^j/(x^m+1)$, more natural in view of its integrability, satisfies

$$\mathfrak{F}\left(\frac{x^j}{x^m+1}\right) = \frac{(-1)^j x^{\gamma_m(j)}}{x^m-1}\,,$$

so it leads to the same family of iterates.

We next characterize the fixed points of γ_m.

Lemma 3.2 *The only fixed points of γ_m are $j=-1$ and $j=m-1$. This confirms the fact that the functions*

$$R_{-1,m}(x) = \frac{x^{-1}}{x^m-1} \quad \textit{and} \quad R_{m-1,m}(x) = \frac{x^{m-1}}{x^m-1}$$

are fixed by $\mathfrak{F}$.

Proof. If j is even, the equation $\gamma_m(j)=j$ becomes $mj-(m-1)(j-1)=2j$, and this is satisfied by $j=m-1$, which is even. Similarly, j odd yields $j=-1$. □

The next result establishes the existence of a bounded invariant set for γ_m.

Proposition 3.3 *The iterates $\{\gamma_m^{(n)}(j) : n=0,1,2,\ldots\}$ reach the set*

$$\mathfrak{A}_m := \{0,1,2,\ldots,m-2\} \tag{3.3}$$

in a finite number of steps. Moreover, $\mathfrak{A}_m$ is invariant under the action of γ_m.

Proof. If $j>m-1$ then $\gamma_m(j)<j$. Indeed, the inequality

$$\gamma_m(j) = m\lfloor j/2\rfloor - (m-1)(j-1)/2 < j \tag{3.4}$$

is always valid if j is odd, and for $j=2t$ it becomes

$$mt-(2t-1)(m-1)/2 < 2t\,,$$

which is satisfied by $j>m-1$. The case $j<0$ is similar. Finally, if $0\le j\le m-2$, it follows directly that $0\le\gamma_m(j)\le m-2$. □

The action of $\mathfrak{F}$ on $\mathfrak{A}_m$ yields a partition into orbits $\mathfrak{O}$ of the form

$$\mathfrak{O} = \{j, \gamma_m(j), \gamma_m^{(2)}(j), \ldots, \gamma_m^{(n-1)}(j)\}\,. \tag{3.5}$$

Example. For $m=9$ the set $\mathfrak{A}_9$ consists of two orbits

$$0\mapsto 4\mapsto 6\mapsto 7\mapsto 3\mapsto 1\mapsto 0 \quad\text{and}\quad 2\mapsto 5\mapsto 2\,,$$

and for $m=11$ we have the single orbit

$$0\mapsto 5\mapsto 2\mapsto 6\mapsto 8\mapsto 9\mapsto 4\mapsto 7\mapsto 3\mapsto 1\mapsto 0\,.$$

For special values of m, it is possible to predict the presence of some orbits. The form of the orbits discussed below motivated the results of Section 4.

Lemma 3.4 *Suppose $m = 2^n - 1$ for some $n \in \mathbb{N}$. Then γ_m has at least two orbits of length n.*

Proof. Observe that $\gamma_m^{(j)}(0) = 2^{n-j} - 1$ is always odd, so the orbit of 0 is

$$0 \mapsto 2^{n-1} - 1 \mapsto 2^{n-2} - 1 \mapsto \ldots \mapsto 2^2 - 1 \mapsto 1 \mapsto 0\,.$$

Similarly, the orbit of $j = 2$ is

$$2 \mapsto 2^{n-1} \mapsto 2^{n-1} + 2^{n-2} - 1 \mapsto 2^{n-2} + 2^{n-3} - 1 \mapsto \ldots \mapsto 11 \mapsto 5 \mapsto 2\,,$$

which is also of length n and is disjoint from the orbit of 0. Indeed, the existence of a common term yields $2^{n-k_0} + 2^{n-k_0-1} - 1 = 2^{n-k_1} - 1$, which implies $3 \times 2^{n-k_0-1} = 2^{n-k_1}$, a contradiction. □

4 The inverse function

In this section we show that the dynamics of the function γ_m become clear if we consider the inverse function.

Theorem 4.1 *Let*

$$\delta_m(k) := \begin{cases} 2k+1 & \text{if } 0 \le k \le \frac{m-2}{2}\,, \\ 2k+1-m & \text{if } \frac{m-1}{2} \le k \le m-2\,. \end{cases} \tag{4.1}$$

Then $\delta_m = \gamma_m^{-1}$.

Proof. Both functions map $\mathfrak{A}_m$ into itself, so it suffices to check that $\gamma_m \circ \delta_m = \mathrm{Id}$. If $0 \le k \le (m-3)/2$ then $\delta_m(k) = 2k+1$ is odd, so $\gamma_m(\delta_m(k)) = k$. The calculation for $(m-1)/2 \le k \le m-2$ is similar. □

Now observe that, as sets, the orbits of $k \in \mathfrak{A}_m$ under γ_m and δ_m are the same. In particular, the number of orbits and their sizes are the same.

Theorem 4.2 *Let $k \in \mathfrak{A}_m$. Then its orbit under δ_m is given by*

$$\mathfrak{O}_\delta(k) = \{2^j k + 2^j - 1 \pmod m : j = 0, 1, \ldots\}\,. \tag{4.2}$$

The length of the orbit containing k is

$$L(\mathfrak{O}_\delta(k)) = \mathrm{Ord}(2; m/\gcd(k+1, m)), \tag{4.3}$$

where $\mathrm{Ord}(2;h)$ denotes the multiplicative order of 2 modulo h, that is, the smallest solution of $2^x \equiv 1 \bmod h$.

Proof. The form of the orbit of k is easy to check. Indeed,

$$\delta_m(2^j k + 2^j - 1) = 2(2^j k + 2^j - 1) + 1 = 2^{j+1} k + 2^{j+1} - 1 .$$

Now this orbit closes at the first value of j such that

$$2^j k + 2^j - 1 \equiv k \bmod m .$$

This is equivalent to

$$(2^j - 1)(k + 1) \equiv 0 \bmod m . \tag{4.4}$$

Write $k + 1 = vK$ and $m = vM$ with $v = \gcd(k + 1, m)$. Then (4.4) yields

$$(2^j - 1)K \equiv 0 \bmod M . \tag{4.5}$$

But $\gcd(K, M) = 1$, so

$$2^j \equiv 1 \bmod M . \tag{4.6}$$

□

Corollary 4.3 *The orbit containing* 0 *has length* $\mathrm{Ord}(2; m)$. *It is the largest orbit and the length of any other divides* $\mathrm{Ord}(2; m)$.

Proof. This is clear. □

Theorem 4.4 *Suppose* m *is prime. Then every orbit of* δ_m, *and hence of* γ_m, *has length equal to* $\mathrm{Ord}(2; m)$. *The total number of orbits is* $N(m) = (m - 1)/\mathrm{Ord}(2; m)$.

Proof. The result follows from Theorem 4.2. Every point $k \in \mathfrak{A}_m$ satisfies $\gcd(k + 1, m) = 1$. □

Corollary 4.5 *Suppose* m *is prime. Then* γ_m *has a single orbit if and only if* 2 *is a generator of* $U(m)$, *that is, if* 2 *is a primitive root modulo* m.

Note. The primes $m \leq 100$ for which 2 is a primitive root are

$$\{3, 5, 11, 13, 19, 29, 37, 53, 59, 61, 67, 83\}.$$

Artin [1] conjectured that this occurs for infinitely many primes. See [6] for an update on this conjecture.

Corollary 4.6 *Suppose* $m = p^2$ *with* p *prime. Then the orbits of* γ_m *have lengths* $\mathrm{Ord}(2; p)$ *or* $\mathrm{Ord}(2; p^2) = p \times \mathrm{Ord}(2; p)$.

Proof. Take as initial point $k \in \mathfrak{A}_m$ such that $k + 1 \not\equiv 0 \bmod p$. Then the orbit of k has length $\mathrm{Ord}(2; p^2)$. On the other hand, if $k + 1 = pt$, then the orbit of k has length $\mathrm{Ord}(2; p)$. □

Note. If $m = p^2$ with p prime and if γ_p has N orbits of length $\mathrm{Ord}(2; p)$, then γ_{p^2} has $2N$ orbits, N of them of length $\mathrm{Ord}(2; p)$ and the remaining N of length $\mathrm{Ord}(2; p^2)$. Similar results hold for higher powers.

5 An alternative approach

This section contains an alternative approach to the dynamics of γ_m. Define

$$b_k(j) := \gamma^{(k)}(j) - 2\lfloor \tfrac{1}{2}\gamma^{(k)}(j) \rfloor , \tag{5.1}$$

the parity of $\gamma_m^{(k)}(j)$.

The next result is useful in the study of the arithmetic properties of the map γ_m.

Theorem 5.1 *Suppose γ_m has an orbit of length n with initial point j. Then*

$$(2^n - 1)(j+1) = m \times \sum_{k=0}^{n-1} (1 - b_k(j))\, 2^k . \tag{5.2}$$

Proof. Define $q_k = m(b_k - 1) + 1$. Then $j = 2\lfloor j/2 \rfloor + b_0$ yields $j = 2\gamma_m(j) + q_0$. Iterating this procedure gives

$$j = 2^k \gamma_m^{(k)}(j) + 2^{k-1} q_{k-1} + \cdots + 2q_1 + q_0 .$$

Thus $\gamma_m^{(n)}(j) = j$ yields (5.2). □

Proposition 5.2 *Suppose m is a Sophie Germain prime, that is, a prime of the form $m = 2q + 1$ with q prime. Then there are at most two orbits. In the case of two orbits, both have the same length.*

Proof. Let $n_1, \ldots, n_t$ be the lengths of the orbits. Then we have that $n_1 + \cdots + n_t = 2q$ and also that $\mathrm{Ord}(2; m) > 2$ divides each n_i. Thus $\mathrm{Ord}(2; m) = 2q$ or q. The first case is covered by Corollary 4.5, and in the second case we must have $n_1 = n_2 = q$. □

Note. Both alternatives do occur: $m = 11$ has a single orbit and $m = 23$ has two orbits of length 11 each.

Some of the orbits are restricted by the parity of their elements.

Lemma 5.3 *Let $\mathfrak{O}$ be an orbit that consists of elements of a fixed parity. Then $\mathfrak{O}$ reduces to one of the fixed points of $\mathfrak{F}$.*

Proof. Let $j \in \mathfrak{O}$ and assume j is odd. Then every b_k in (5.2) is 1, so $j = -1$. Similarly, if j is even, then $j = m - 1$. □

Theorem 5.4 *Suppose γ_m has an orbit of length n and $M_n := 2^n - 1$ is a Mersenne prime. Then m is an odd multiple of M_n.*

Proof. The strict inequality

$$\sum_{k=0}^{n-1} (1 - b_k) 2^k < \sum_{k=0}^{n-1} 2^k = M_n$$

follows from $0 \le b_k \le 1$ and Proposition 5.3. Thus (5.2) shows that m must divide M_n. □

Note. The reader is invited to prove this result by using the form of the orbit given in Theorem 4.2.

Acknowledgements. The third author acknowledges the partial support of NSF-DMS 0070567, Project number 540623.

References

[1] Artin, E.: *Collected Papers*, Reading, MA. Addison Wesley, 1965, viii–x.

[2] Boros, G.; Moll, V.: The double square root, Jacobi polynomials and Ramanujan's Master Theorem. *Jour. Comp. Appl. Math.* 130 (2001), 337–344.

[3] Boros, G.; Little, J.; Moll, V.; Mosteig, E.; Stanley, R.: A map on the space of rational functions. In preparation.

[4] Cox, D.: *Gauss and the Arithmetic-Geometric mean*. Notices of the AMS, March 1985, 147–151.

[5] Moll, V.: *The evaluation of integrals: a personal story*. Notices of the AMS, March 2002.

[6] Murty, M. Ram: Artin's Conjecture for primitive roots. *The Mathematical Intelligencer* 10 (1988), 59–67.

[7] Wirsching, G.: *The dynamical system generated by the* $3n + 1$ *function*. Lecture Notes in Mathematics 1681 (1998), Springer-Verlag.

George Boros
Department of Mathematics
Xavier University
New Orleans, LA 70125, USA
e-mail: gboros@xula.edu

Michael Joyce
Department of Mathematics
Brown University
Providence, RI 02912, USA
e-mail: mjoyce@math.brown.edu

Victor H. Moll
Department of Mathematics
Tulane University
New Orleans, LA 70118, USA
e-mail: vhm@math.tulane.edu