COUNTING EIGENVALUES FOR AUTOMORPHISMS
OF RIEMANN SURFACES

JOHN LAWRENCE\(^1\) AND FRANK ZORZITTO\(^2\)

Abstract. Let \(n\) be a prime, \(A, B, C\) disjoint sets, \(f\colon \mathbb{Z}^n \to A \cup B \cup C\) be such that \(f(x) \in A\) iff \(f(-x) \in C\) and \(f(x + y) \in C\) whenever \(f(x), f(y) \in A\). Then the cardinality of \(f^{-1}[B]\) tends to infinity with \(n\). Using this, certain eigenvalues for automorphisms of the Riemann surfaces defined by the equation \(y^n = x^{m_1}(x - 1)^{m_2}(x - z)^{m_3}\) are counted.

1. The geometric setting. For every complex number \(z \neq 0, 1\) the equation

\[
y^n = x^{m_1}(x - 1)^{m_2}(x - z)^{m_3},
\]

where \(n\) is a prime number, \(m_1, m_2, m_3\) are positive integers less than \(n\), \(\frac{m_1 + m_2 + m_3}{nf}\) and \(x, y\) are complex variables, defines a Riemann surface \(R(z)\) of genus \(n - 1\). Such Riemann surfaces \(R(z)\) and their connection to the hypergeometric differential equation

\[
z(z - 1) \frac{d^2w}{dz^2} + ((\alpha + \beta + 1)z - \gamma) \frac{dw}{dz} + \alpha \beta w = 0
\]

have been studied in [1] by A. Kuribayashi.

The vector space \(V(z)\) of differentials of the first kind on \(R(z)\) has dimension equal to the genus \(n - 1\). In [1] it is proved that the differentials of the form

\[
\omega = x^{k_1}(x - 1)^{k_2}(x - z)^{k_3}y^{-l}dx,
\]

where \(l, k_1, k_2, k_3\) are integers satisfying the conditions

\[
(a) \ 0 < l < n, 0 < k_1, k_2, k_3 < n,
(b) m_i l < k_in + n, i = 1, 2, 3,
(c) (m_1 + m_2 + m_3)l > (k_1 + k_2 + k_3)n + n,
\]

span \(V(z)\).

Any automorphism \(\sigma\) on \(R(z)\) induces a linear transformation \(S\) on \(V(z)\) according to \(S\colon fdg \mapsto (f \circ \sigma)d(g \circ \sigma)\) for every differential, \(\omega = fdg\), of the first kind on \(R(z)\). In particular, for \(\xi\) a primitive \(n\)th root of unity, the automorphism \(\sigma\), that maps every \((x, y)\) on \(R(z)\) to \((x, \xi y)\), generates all...
automorphisms which leave $x$ fixed. The differentials $\omega$ given by (3) are eigenvectors for the linear operator $S$ on $V(z)$ induced by the automorphism $\sigma: (x, y) \mapsto (x, zy)$. In fact $\omega$ goes to $\xi^{n-l} \omega$. The operator $S$ is diagonalizable by simply taking a base for $V(z)$ from the differentials given by (3) and (4). For a given integer $l = 1, \ldots, n-1$, the number $\xi^{n-l}$ is an eigenvalue of $S$ whenever there exist integers $k_1, k_2, k_3$ satisfying the inequalities (4). Indeed, in that case the differential $\omega = x^{k_1}(x-1)^{k_2}(x-z)^{k_3} dx$ is an eigenvector of $S$.

The question posed by Kuribayashi, which we wish to discuss is: "For how many $l$'s between 0 and $n$ are both $\xi^{n-l}$ and $\xi^l$ eigenvalues of $S$?"

**Theorem 1.** Let all notations be as above. The number of integers $l = 1, \ldots, n-1$ for which both $\xi^l$ and $\xi^{n-l}$ are eigenvalues of $S$, always exceeds 0 and tends to infinity as $n$ tends to infinity.

2. A counting problem. To prove Theorem 1 the following estimate will be used.

For any positive integer $n$ let $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ be the group of integers modulo $n$. Let $A, B, C$ be three-disjoint sets, and let $f: \mathbb{Z}_n \to A \cup B \cup C$ be a function satisfying:

(a) $f(1) \in A$,
(b) $f(x) \in A$ if and only if $f(-x) \in C$,
(c) $f(x), f(y) \in A$ implies $f(x+y) \not\in C$.

Under these conditions $f$ must map into $B$ quite often.

**Theorem 2.** If $N$ is the cardinality of $f^{-1}[B]$, then $N(4N + 3) \geq n$. Furthermore, if $n$ is a prime, then merely conditions (5),(a),(b),(c) will ensure this inequality.

**Proof.** Let $F: Z \to A \cup B \cup C$ be given by $F(x) = f(x)$, for any $x \in Z$. Any set $I = \{k+1, k+2, \ldots, k+r\}$ of consecutive integers such that $F[I] \subseteq A \cup B$ will be called a chain of length $r$ through $A \cup B$. Let $r$ be the largest integer for which there exists a chain $I = \{k+1, k+2, \ldots, k+r\}$ of length $r$ through $A \cup B$. Obviously, from condition (5),(a),(b) and the nature of $F$, $r < n$.

We shall prove $r \leq 4N + 1$. The interval $(2k + r/2, 2k + 3r/2 + 1]$ contains more that $r$ integers. By the maximality of $r$ there is an integer $m$ in this interval such that $F(m) \in C$. For an integer $m \in (2k + r/2, 2k + 3r/2 + 1]$ the number of pairs of integers $(i,j)$, such that $i,j = 1, \ldots, r$ and $2k + i + j = m$, is not less than $(r - 1)/2$. Thus there are at least $(r - 1)/2$ pairs $(i,j)$ such that $k + i, k + j \in I$ and $F(k + i + k + j) = F(m) \in C$. Condition (5),(c) then implies that for each such pair $(i,j)$, either $F(k + i) \in B$ or $F(k + j) \in B$. A given integer $h = 1, \ldots, r$ can appear at most twice as a component in the pairs $(i,j)$ such that $2k + i + j = m$. Thus there are not less than $(r - 1)/4$ integers $h = 1, \ldots, r$ such that $F(k + h) \in B$. That is, $(r - 1)/4 \leq N$, or $r \leq 4N + 1$. 

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
If \( J = \{k + 1, \ldots , k + s\} \) is now any chain through \( A \) (instead of \( A \cup B \)) of length \( s \), then \( J + J = \{2k + 2, \ldots , 2k + 2s\} \) is a chain of length \( 2s - 1 \) through \( A \cup B \), because of condition (5),(c). Hence \( 2s - 1 < 4N + 1 \), or \( s < 2N + 1 \).

Let \( J_1, J_2, \ldots , J_t \) be the successive chains through \( A \), that are included in the interval \([0, n - 1]\). Their union has cardinality equal to that of \( f^{-1}[A] \). By (5),(c) this cardinality equals that of \( f^{-1}[C] \), which then must be \((n - N)/2\). The bound of \( 2N + 1 \) on the length of each \( J_i \) then implies that \( t(2N + 1) > (n - N)/2 \).

If \( l \) is the last element of any chain through \( A \), then \( F(l + 1) \in B \), due to (5),(c) and the fact that \( F(l), F(1) \in A \). Thus in each gap between the chains \( J_1, \ldots , J_t \) there is an integer \( x \) such that \( F(x) \in B \). These \( x \)'s are distinct modulo \( n \). Also note \( F(0) \in B \), from (5),(b). Therefore, \( t < N \). From the earlier inequality we deduce \( N(2N + 1) > (n - N)/2 \), which reduces to \( N(4N + 3) > n \).

The case where \( n \) is prime but (5),(a) is not assumed reduces as follows to the case where (5),(a) is assumed. If \( f(\bar{x}) \in B \) for all \( \bar{x} \in \mathbb{Z}_n \), then \( N(4N + 3) > n \) trivially. So we can suppose in light of (5),(b) that \( f(\bar{i}) \in A \) for some nonzero \( \bar{i} \in \mathbb{Z}_n \). Let \( f': \mathbb{Z}_n \to A \cup B \cup C \) be defined by \( f'(\bar{x}) = f(\bar{i} \bar{x}) \). The function \( f' \) still enjoys properties (5),(b),(c), plus \( f'(0) \in A \). Also \( f'^{-1}[B] = \bar{i}f'^{-1}[B] \). Since the nonzero elements of \( \mathbb{Z}_n \) form a group, \( f^{-1}[B] \) has the same cardinality \( N \), as \( f^{-1}[B] \). It follows that, because \( f' \) satisfies (5),(a),(b),(c), \( N(4N + 3) > n \).

3. Application. We return to the situation and notations of Theorem 1. For any integer \( x \) and each of the \( m_1, m_2, m_3 \) let \( m_1x \) denote the integer in \( \{1, 2, \ldots , n\} \) that is congruent to \( m_1x \) modulo \( n \). Let \( F(x) = m_1x + m_2x + m_3x \), where addition is the usual addition (not modulo \( n \)) of integers.

The function \( F \) has the following properties.

\[
\begin{align*}
(a) \quad 3 &< F(x) < 3n, \\
(b) \quad n &\nmid F(x) \text{ if and only if } n \nmid x, \\
(c) \quad F(x) = F(y) &\text{ if and only if } n|x - y, \\
(d) \quad F(x) < n &\text{ if and only if } F(n - x) > 2n, \\
(e) \quad F(x), F(y) < n &\text{ implies } F(x + y) < 2n.
\end{align*}
\]

**Proposition 3.** For \( l = 1, \ldots , n - 1 \) the number \( \xi^{n-l} \) is an eigenvalue of \( S \) if and only if \( F(l) > n \).

**Proof.** That \( \xi^{n-l} \) is an eigenvalue of \( S \) is tantamount to the existence of a solution \( k_1, k_2, k_3 \) to (4).

Suppose \( F(l) > n \). For each \( i = 1, 2, 3 \), let \( k_i \) be the number of times \( n \) divides \( m_i l \). Clearly \( 0 < k_i < n \), and the division formula

\[
m_i l = k_i n + m_i l, \quad 0 < m_i l < n,
\]

yields a solution of (4),(a),(b). Adding equations (7) over \( i = 1, 2, 3 \) provides
\[(\sum m_i)^l = (\sum k_i)n + \sum \bar{m}_i^l = (\sum k_i)n + F(l) > (\sum k_i)n + n,\]

thereby solving (4),(c) as well.

Conversely, suppose inequalities (4) are solved by some \(k_1, k_2, k_3\). Since (4),(c) will remain satisfied for any lesser \(k_i\)'s, it can be assumed that for each \(i = 1, 2, 3\), \(k_i\) is also the least integer satisfying (4),(a),(b). Thus each \(k_i\) is precisely the number of times \(n\) divides \(m_i^l\); and (7) holds for each \(k_i\). Adding up the equations (7) over \(i = 1, 2, 3\), and use of (4),(c) then leads to \(F(l) > n\).

**Corollary 4.** For any \(l = 1, \ldots, n - 1\) either \(\xi^l\) or \(\xi^{n-l}\) must be an eigenvalue of \(S\). Both \(\xi^l\) and \(\xi^{n-l}\) are eigenvalues of \(S\) if and only if \(n < F(l) < 2n\).

This follows easily from (6),(d).

**Proof of Theorem 1.** By Corollary 4 it is enough to prove that the number, \(M\), of \(l\)'s in \(\{1, \ldots, n - 1\}\), for which \(n < F(l) < 2n\), tends to infinity as \(n\) tends to infinity. We shall prove

\[(M + 1)(4(M + 1) + 3) > n.\]

Let \(A = \{0, 1, \ldots, n - 1\}\), \(B = \{n, n + 1, \ldots, 2n - 1\}\), \(C = \{2n, \ldots, 2n - 1\}\). The function \(f: Z_n \to A \cup B \cup C\) given by \(f(\bar{x}) = F(x)\) when \(x \neq 0\) and \(f(\bar{0}) = n\) is well defined because of (6),(c). For \(l = 1, \ldots, n - 1\), \(n < F(l) < 2n\) exactly when \(f(\bar{1}) \in B\). On noting that \(f(\bar{0}) \in B\), we see that \(M + 1\) equals the cardinality of \(f^{-1}[B]\). Also properties (5),(b),(c) follow for \(f\) from properties (6),(d),(e) for \(F\), and \(n\) is prime. Theorem 2 then implies that \((M + 1)(4(M + 1) + 3) > n\).

The statement in Theorem 1, that there always exists an \(l\) in \(\{1, \ldots, n - 1\}\) making \(\xi^{n-l}\) and \(\xi^l\) eigenvalues of the operator \(S\), follows from (8) for \(n > 11\). In that case \(M\) must be at least 1. As for the primes 2, 3, 5, 7 it is easy to check that the statement is still valid.

A conjecture for a sharper inequality to replace (8) is \(3M > n\).

**References**


Department of Pure Mathematics, University of Waterloo, Waterloo, Ontario, Canada