

Generalized continued fractions and orbits under the action of Hecke triangle groups

by

ELISE HANSON (Claremont, CA),
ADAM MERBERG (Claremont, CA, and Providence, RI),
CHRISTOPHER TOWSE (Claremont, CA), and
ELENA YUDOVINA (Claremont, CA, and Cambridge, MA)

1. Background. The Hecke triangle groups $G(\lambda)$ are the groups of fractional linear transformations generated by the transformations $S(z) = z + \lambda$ and $T(z) = -1/z$. Hecke [3] showed that these groups are properly discontinuous, and thus useful for studying associated modular forms, only when $\lambda \geq 2$ or $\lambda = \lambda_q = 2 \cos(\pi/q)$ where q is an integer, $q \geq 3$. We will only consider the latter case, $\lambda = \lambda_q$. When confusion will not result, we shall omit the subscript and write simply λ for λ_q .

We define $T(0) = \infty$, $T(\infty) = 0$ and $S(\infty) = \infty$, so that the set $\widehat{\mathbb{Q}}(\lambda_q) := \mathbb{Q}(\lambda_q) \cup \{\infty\}$ is closed under the action of $G(\lambda_q)$. Our interest lies primarily in the orbits of $G(\lambda_q)$ in $\widehat{\mathbb{Q}}(\lambda_q)$.

In the case $q = 3$, we see $\lambda_3 = 2 \cos(\pi/3) = 1$, and under the action of $G(\lambda_3)$ it is well-known that all of $\mathbb{Q} \cup \{\infty\}$ is a single orbit. Furthermore, Leutbecher showed in [4] that $\mathbb{Q}(\lambda_5) \cup \{\infty\}$ consists of only a single orbit. However, no such simple result holds for all q .

We can identify a fractional linear transformation

$$z \mapsto \frac{az + b}{cz + d}$$

with the matrix

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

so that composition of transformations corresponds to matrix multiplication.

2000 *Mathematics Subject Classification*: Primary 11J70; Secondary 11R21, 11A55.
Key words and phrases: continued fractions, Hecke triangle groups.
Research supported by the NSF-REU grant DMS 0453284.

Since a scalar multiple of M corresponds to the same transformation as M itself, we need only look at those transformations with $\det(M) = ad - bc = 1$, and we can identify M with $-M$.

The study of $G(\lambda)$ is thus identified with the study of subgroups of $\text{PSL}_2(\mathbb{R})$ generated by

$$\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

We will sometimes abuse notation and refer to the transformation M .

In [5], Rosen developed the foundations of the generalized continued fractions associated with the Hecke groups. It is clear that for any $a_0, a_1, \dots, a_n \in \mathbb{Z}$ the λ -continued fraction (λcf)

$$(1) \quad a_0\lambda - \frac{1}{a_1\lambda - \frac{1}{a_2\lambda - \dots - \frac{1}{a_n\lambda}}}$$

is equal to the transformation $S^{a_0}TS^{a_1}T \dots TS^{a_n} \in G(\lambda)$ evaluated at 0. The orbit of 0 under $G(\lambda)$, also called the *set of cusps* of $G(\lambda)$, is therefore equivalent to the set that can be expressed in the form (1), that is, the *finite* λ -continued fractions. We abbreviate (1) as $\alpha = [a_0; a_1, \dots, a_n]$, the value of λ being clear from the context.

Extending consideration to infinite continued fractions, two numbers are in the same orbit if they can be expressed as continued fractions which agree beyond a certain point. More precisely, α and β are in the same orbit if α and β can be expressed as $\alpha = [a_0; a_1, a_2, \dots]$ and $\beta = [b_0; b_1, b_2, \dots]$ so that for some non-negative integers l and m , $a_{l+i} = b_{m+i}$ for all $i \in \mathbb{N}$. Furthermore, the λ -continued fractions computed using the nearest integer algorithm of [5] must be among the expansions meeting this condition if α and β are in the same orbit. For this reason, we may assume all λ -continued fractions are computed by this algorithm. (See also [6].)

If we let $\zeta = \zeta_{2q}$ denote the primitive $2q$ th root of unity, $e^{i\pi/q}$, then we have $\lambda = 2 \cos(\pi/q) = \zeta + \zeta^{-1}$. From this we see that $\mathbb{Q}(\lambda)$ is the maximal real subfield of the $2q$ th cyclotomic field. In particular, this means that $[\mathbb{Q}(\lambda) : \mathbb{Q}] = \frac{1}{2}[\mathbb{Q}(\zeta) : \mathbb{Q}] = \frac{1}{2}\phi(2q)$. It is a standard result of the theory of cyclotomic fields that the ring of integers of $\mathbb{Q}(\lambda)$ is simply $\mathbb{Z}[\lambda]$ (see [7]).

Let $h = \lfloor (q - 1)/2 \rfloor$. In [5], Rosen showed that

$$(2) \quad \underbrace{[1; 1, \dots, 1]}_{h \text{ terms}} = \begin{cases} 1, & q \text{ odd,} \\ 2/\lambda, & q \text{ even.} \end{cases}$$

The study of these Hecke triangle groups naturally, therefore, breaks into two cases: q even and q odd.

2. Infinitely many orbits when q is even. The focus of this paper is in understanding the number of distinct orbits in $\widehat{\mathbb{Q}}(\lambda_q)$. In this section we will be interested in the case when q is even.

In [6], the specific cases of $q = 4$ and $q = 6$ were considered. It was shown that every unit in the ring $\mathbb{Z}[\lambda_q]$ had infinite repeating λ_q -continued fraction expansions (for $q = 4, 6$). As the expansions are periodic, it is easy to observe that the orbits are all distinct. Indeed, the units of $\mathbb{Z}[\lambda_q]$ are all of the form $\pm \xi_q^n$, where $\xi_4 = 1 + \sqrt{2}$ and $\xi_6 = 2 + \sqrt{3}$. Writing $\xi_q^n = a_n + b_n \lambda_q$ it was shown that

$$\xi_q^n = 2b_n \lambda + \frac{\varepsilon^n}{2b_n \lambda + \frac{\varepsilon^n}{2b_n \lambda + \dots}}$$

where $\varepsilon = -1$ for $q = 4$ and $\varepsilon = 1$ for $q = 6$.

Furthermore, since the b_n grow monotonically with n , this gives an infinite number of distinct orbits in $\mathbb{Z}[\lambda_q] \subset \widehat{\mathbb{Q}}(\lambda_q)$. As a consequence, one can observe that the (strictly increasing) sequence $\{a_n\}$ of rational integers all have distinct orbits (for $q = 4, 6$).

The following theorem and its corollary vastly improve on these observations.

THEOREM 1. *Let q be even. Then $\mu, \nu \in \mathbb{Z}[\lambda_q^2]$ do not lie in the same orbit under the action of $G(\lambda)$ unless they differ by (multiplication by) a unit of $\mathbb{Z}[\lambda_q^2]$.*

We will use the fact that in the case when q is even, the fields $\mathbb{Q}(\lambda_q)$ and $\mathbb{Q}(\lambda_q^2)$ are distinct and, in fact, $[\mathbb{Q}(\lambda_q) : \mathbb{Q}(\lambda_q^2)] = 2$. This is easy to prove.

LEMMA 2. *A matrix $M \in G(\lambda_q)$ has one of the forms*

$$M_1 = \begin{pmatrix} \alpha & \beta \lambda \\ \gamma \lambda & \delta \end{pmatrix} \quad \text{or} \quad M_2 = \begin{pmatrix} \alpha \lambda & \beta \\ \gamma & \delta \lambda \end{pmatrix},$$

where $\alpha, \beta, \gamma, \delta \in \mathbb{Z}[\lambda^2]$.

Proof. We refer to a matrix of the form M_i as *type i* . Recall that $G(\lambda)$ is generated by S and T , which are of type 2 and type 1, respectively. Applying S to M_1 and M_2 , we get matrices of types 2 and 1, respectively. Applying T , we get types 1 and 2, respectively. ■

Proof of Theorem 1. Let $\mu, \nu \in \mathbb{Z}[\lambda^2]$ and suppose $\mu = M\nu$ with $M \in G(\lambda)$. We assume M is of type 1 (the proof for $M = M_2$ is almost entirely identical). Then

$$\mu = \frac{\alpha \nu + \beta \lambda}{\gamma \lambda \nu + \delta},$$

or

$$\lambda\gamma\mu\nu + \delta\mu = \lambda\beta + \alpha\nu,$$

where all of the coefficients in this equation lie in $\mathbb{Z}[\lambda^2]$. Since $\{1, \lambda\}$ is a vector space basis for $\mathbb{Q}(\lambda)$ over $\mathbb{Q}(\lambda^2)$, we may equate the coefficients of 1 and λ to get

$$(3) \quad \gamma\mu\nu = \beta, \quad \delta\mu = \alpha\nu.$$

Furthermore, the determinant of M must be 1, so

$$(4) \quad \alpha\delta - \beta\gamma\lambda^2 = 1,$$

or, upon multiplying (4) by μ and substituting (3),

$$\alpha^2\nu - \gamma^2\lambda^2\mu^2\nu = (\alpha^2 - \gamma^2\lambda^2\mu^2)\nu = \mu.$$

Since all the numbers here lie in $\mathbb{Z}[\lambda^2]$, we obtain $\nu \mid \mu$. By relabeling ν and μ , the same argument shows that $\mu \mid \nu$ in $\mathbb{Z}[\lambda^2]$. Therefore, μ and ν differ by (multiplication by) a unit in $\mathbb{Z}[\lambda^2]$. ■

COROLLARY 3. *For q even, $\mathbb{Q}(\lambda_q)$ contains infinitely many orbits under the action of $G(\lambda_q)$.*

Proof. We apply Theorem 1 with μ and ν positive rational integers; then $\mu = u\nu$ for some unit u of $\mathbb{Z}[\lambda^2]$. Since $u = \mu/\nu \in \mathbb{Q}$, we must have $u = \pm 1$. Since we took μ and ν to be positive, we have $u = 1$ and $\mu = \nu$. Thus, no two natural numbers are in the same orbit under the action of $G(\lambda_q)$ for any even q . ■

3. A bound on the number of orbits for q odd. In this section we will focus on the case when q is odd. We will develop a lower bound on the number of orbits in $\mathbb{Q}(\lambda)$ under the action of $G(\lambda)$ using ideas seen in [1], [2], and [8]. The main idea is to work modulo 2. We begin with a bit of notation.

Let $O = \mathbb{Z}[\lambda]$ be the ring of integers in $\mathbb{Q}(\lambda)$. We let $\bar{} : O \rightarrow O/2O$ be the natural reduction map and allow it to induce the obvious reductions on $\bar{} : G(\lambda) \rightarrow \overline{G(\lambda)}$.

For any ring R , we define $P^1(R)$, the projective line over R , to consist of (equivalence classes of) the relatively prime pairs of elements of R (so that $rR + sR = R$) with two pairs $\begin{pmatrix} r \\ s \end{pmatrix}$ and $\begin{pmatrix} r' \\ s' \end{pmatrix}$ considered equivalent if $r = ur'$ and $s = us'$ for some unit u in R . The group $\overline{G(\lambda)}$ acts on $P^1(\overline{O})$ by the action given by the usual matrix multiplication. (See Section 2 of [2].)

We consider the size of $P^1(\overline{O})$. Since the projective line contains at least all points of the form $\begin{pmatrix} a \\ 1 \end{pmatrix}$ and $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ for each $a \in \overline{O} = \mathbb{Z}[\lambda]/(2)$, we obtain the following easy bound.

LEMMA 4. *The number of elements in the projective line $P^1(\overline{O})$ is at least $2^{\phi(q)/2} + 1$.*

Of course, the ideal (2) does not have to be prime in O . However, if we know how (2) factors, or indeed, the factorization of *any* ideal \mathfrak{a} in O , we can say much more. The following proposition gives a sense of how one can go about computing the number of elements in $P^1(O/\mathfrak{a})$.

PROPOSITION 5. *Suppose O is a principal ideal domain, and let \mathfrak{a} be a prime of O . Suppose that \mathfrak{a} has norm equal to $\prod_i p_i^{d_i}$ for some primes $p_i \in \mathbb{N}$. Then the number of elements of $P^1(O/\mathfrak{a})$ is at least $\prod(p_i^{d_i} + 1)$.*

Proof. Let us first consider \mathfrak{p} a prime in O of norm p^e for some prime $p \in \mathbb{Z}$ and some $e \in \mathbb{N}$. We show that the number of elements in the projective line $P^1(O/\mathfrak{p}^n O)$ is $p^{ne} + p^{ne-e}$. Indeed, $O/\mathfrak{p}^n O$ is a local ring with maximal ideal \mathfrak{p} . For an element $\begin{pmatrix} r \\ s \end{pmatrix} \in P^1(O/\mathfrak{p}^n O)$, either r or s must be a unit (otherwise, both would lie in \mathfrak{p} , and thus they would not be relatively prime). Therefore, we have p^{ne} elements of the form $\begin{pmatrix} \alpha \\ 1 \end{pmatrix}$ and another p^{ne-e} elements of the form $\begin{pmatrix} 1 \\ \beta \end{pmatrix}$ with β a non-unit; these are pairwise non-equivalent to each other.

Next, we note that for any two relatively prime ideals \mathfrak{m}_1 and \mathfrak{m}_2 , the projective space $P^1(O/\mathfrak{m}_1\mathfrak{m}_2)$ is isomorphic to the product $P^1(O/\mathfrak{m}_1) \times P^1(O/\mathfrak{m}_2)$ by the Chinese Remainder Theorem.

Note that if \mathfrak{p}_1 and \mathfrak{p}_2 happen to be primes with the same norm p^e , the number of elements in $P^1(O/\mathfrak{p}_1\mathfrak{p}_2)$ is $(p^e + 1)^2 > p^{2e} + p^e$, which is the number of elements in $P^1(O/\mathfrak{p}_1^2 O)$. So replacing J distinct primes of the same norm by the J th power of a single prime of that norm reduces the number of elements in the projective line.

Finally, consider a product of a collection of primes having norm p^d . Then the number of elements in the associated projective ring is minimal if the collection consists of one copy of a prime of norm p^d . (Replacing one prime of norm p^d by d primes of norm p^1 clearly increases the number of elements. We want to increase e in the count $p^{ne} + p^{ne-e}$.) The minimum number of elements in the projective ring in this case is when $n = 1$ and $e = d$. We get $p^d + 1$.

In particular, if we have an ideal \mathfrak{a} whose norm is $\prod_i p_i^{d_i}$, the number of elements in $P^1(O/\mathfrak{a}O)$ is at least $\prod_i (p_i^{d_i} + 1)$. ■

LEMMA 6. *Let I be any ideal of O . The map $P^1(O) \rightarrow P^1(O/I)$ induced by the reduction map $O \rightarrow O/I$ is surjective.*

Proof. Let $\begin{pmatrix} \bar{r} \\ \bar{s} \end{pmatrix} \in P^1(O/I)$. We wish to show that there are relatively prime lifts of \bar{r} and \bar{s} to O .

Let r, s be any lifts of \bar{r}, \bar{s} to O , and let X be the (finite) set of prime ideals dividing $(r - s)$. Then $X = X_1 \cup X_2$, where X_1 consists of primes dividing the ideal I and X_2 consists of primes relatively prime to I . By the Chinese Remainder Theorem, we can find ϱ such that $\varrho \equiv r \pmod I$ and

$\varrho \equiv 1 \pmod{\mathfrak{m}}$ for every $\mathfrak{m} \in X_2$. Then $\varrho = r + i$ for some $i \in I$; set $\sigma = s + i$. Since common divisors of ϱ and σ must divide their difference $r - s$, they must lie in X . Since no prime in X_2 can divide ϱ , any common factor of ϱ and σ must lie in X_1 . In other words, they must divide I .

Note that for any prime \mathfrak{p} dividing I , if $\mathfrak{p} \mid (\varrho)$ then $\overline{\mathfrak{p}} \mid (\overline{\varrho}) = (\overline{r})$ in O/I as well. Therefore, if for some $\mathfrak{p} \in X_1$ we have $\mathfrak{p} \mid (\varrho)$ and $\mathfrak{p} \mid (\sigma)$, we would have $\overline{\mathfrak{p}} \mid (\overline{r}) + (\overline{s}) = (\overline{1})$, which is impossible for a prime ideal $\mathfrak{p} \mid I$.

Therefore, ϱ and σ are relatively prime, and $(\frac{\varrho}{\sigma})$ is a lift of $(\frac{\overline{r}}{\overline{s}})$ to $P^1(O)$. ■

We return to the group $\overline{G(\lambda)}$.

LEMMA 7. *For q odd, the group $\overline{G(\lambda)}$ is the dihedral group of order $2q$.*

Proof. See Theorem 3.2 of [1]. ■

It follows that the number of elements of any orbit in $P^1(\overline{O})$ cannot exceed $2q$, the order of the group. In the following proposition we shall look at one particular orbit: the orbit of $\overline{0}$.

PROPOSITION 8. *The size of the orbit of $\overline{0}$ under the action of $\overline{G(\lambda)}$ is at most q .*

Proof. It is clear from Lemma 7 that $\overline{G(\lambda)}$ is generated by \overline{S} and \overline{ST} . The subgroup generated by \overline{ST} has order q . We claim that the orbit of $\overline{0}$ under the action of this subgroup is equal to the entire orbit under the action of $\overline{G(\lambda)}$, and thus has no more than q elements.

For notational convenience, let us write $U = \overline{ST} = \begin{pmatrix} \overline{\lambda} & 1 \\ 1 & 0 \end{pmatrix}$ and let ∞ be the element $(\frac{1}{0}) = U(\overline{0})$ of $P^1(\overline{O})$. We will show that $\overline{S}U^k(\infty) = U^{-k}(\infty)$, which will establish the proposition.

First note that since U is symmetric, so are all powers of U . Furthermore, we can show by induction on k that if we write $U^k = \begin{pmatrix} a & b \\ b & d \end{pmatrix}$, then $a + d = b\overline{\lambda}$. This is true when $k = 1$. We show that this property is preserved by multiplication by U since $U \begin{pmatrix} a & b \\ b & d \end{pmatrix} = \begin{pmatrix} a\overline{\lambda} + b & a \\ a & b \end{pmatrix}$. The desired property comes down to $a\overline{\lambda} + b + b = a\overline{\lambda}$, which is clear modulo 2.

Now, if $U^k = \begin{pmatrix} a & b \\ b & d \end{pmatrix}$, then $U^{-k} = \begin{pmatrix} d & b \\ b & a \end{pmatrix}$. We are therefore trying to show that $a/b + \overline{\lambda} = d/b$, or $a + b\overline{\lambda} = d$. This is equivalent to what we showed in the previous paragraph. ■

THEOREM 9. *For q odd, the number of orbits in $\mathbb{Q}(\lambda)$ under the action of $G(\lambda)$ is at least $(2^{\phi(q)/2} + q + 1)/2q$.*

Proof. The size of an orbit under the action of $\overline{G(\lambda)}$ in $P^1(\overline{O})$ cannot exceed the order of the group, which is at most $2q$. Moreover, by Proposition 8 above, the orbit of 0 has order at most q . Therefore, the number of orbits

in $P^1(\bar{O})$ is at least

$$1 + \frac{\#P^1(\bar{O}) - q}{\#G(\lambda)} \geq \frac{2^{\phi(q)/2} + q + 1}{2q}.$$

Since by Lemma 6 the reduction from O to \bar{O} induces a surjective map from $P^1(O)$ onto $P^1(\bar{O})$, every one of these orbits has a preimage in $P^1(O)$, and clearly the lifts of distinct orbits are themselves distinct orbits.

Note that if $\bar{O} = O/2O$ is not a field, we have strictly more elements in $P^1(\bar{O})$, and therefore strictly more orbits. ■

In Table 1, we list the lower bounds on the number of orbits, t , obtained in Theorem 9.

Table 1. Minimum number of orbits in $\mathbb{Q}(\lambda_q)$ under the action of $G(\lambda_q)$

$q =$	3	5	7	9	11	13	15	17	19
$t \geq$	1	1	2	1	2	3	2	9	14
$q =$	21	23	25	27	29	31	33	35	37
$t \geq$	3	46	21	10	283	530	17	60	3543

REMARK 1. We emphasize that the bounds stated are lower bounds. For $q = 3$ and $q = 5$, the bound of 1 is known to be the actual number of orbits. For $q = 7$, it was conjectured in [6] that there are exactly two orbits, but this claim remains unproven. However, for $q = 9$, the stated bound is 1, but λ -continued fraction computations show that there must be at least five distinct orbits: those of 0, ± 2 , and ± 8 . These all collapse modulo 2, of course.

REMARK 2. Note that for some values of q , the lower bound stated is less than the lower bound given in [2]. Borho and Rosenberger claim, without proof, that the bound that they state follows from their methods. In fact, it appears that their bound is based on the assumption that in the residue field modulo a prime divisor of 2, all of the orbits, with the possible exception of an orbit of two elements, have q elements. In fact, a slight adaptation of their methods (in the proof of their Theorem 5.1) shows that while the orbit of 0 has q elements, all other orbits must have $2q$ elements except for one possible orbit of two elements. We present such an adaptation in the next proposition.

PROPOSITION 10. *Suppose that \bar{O} is a field. Then the orbits in $P^1(\bar{O})$ under the action of $G(\lambda_q)$ have exactly $2q$ elements, with the exception of the orbit of $\bar{0}$ which has q elements and one possible orbit with two elements.*

Proof. Fix an element x of $P^1(\bar{O})$. We know that U has order q , which, we remind the reader, is assumed to be odd throughout this section. Let u and t be the number of elements in the orbit of x under the actions of the cyclic group generated by U and $G(\lambda)$, respectively. Then u must divide q , the order of the subgroup, and t must divide $2q$, the order of the full group.

Thus u must be odd. So either $u = 1$, in which case x is fixed by U , or $u \geq 3$. The u elements of the orbit are fixed by the group element U^u . Thus U^u is a fractional linear transformation which fixes u elements. So if $u \geq 3$, then U^u must be the identity. (Here we are using the assumption that \bar{O} is a field.) This would mean that $q \mid u$, and so u would equal q . We have established that $u = 1$ or $u = q$. In either case, we know that $u \leq t$.

First, let us consider the case $u = 1$. This means that t could only equal 1 or 2, since x is fixed by U . However, if $t = 1$, then x would be fixed by the entire group. In particular, x would be fixed by S . This means that $x = \infty$. But ∞ is not fixed by T . So this is impossible. Therefore, $t = 2$. Note that this case only occurs when x is fixed by U , and U can only fix at most two points. Therefore there is at most one orbit of order 2.

The remaining case is when $u = q$. Here, t can equal either q or $2q$. We consider the action of \bar{S} . The only way t could equal q is if \bar{S} permutes the set $\{x, Ux, \dots, U^{q-1}x\}$. Since \bar{S} has order 2 and this set has an odd number of elements, we see that \bar{S} must fix some U^kx . This means that $U^kx = \infty$, so the orbit of x is the orbit of ∞ (which is the orbit of $\bar{0}$). Any other orbit must have $t = 2q$. ■

From the form of our bound it is clear that the number of orbits as q tends to infinity is unbounded, since $\phi(q)$ grows (approximately) linearly in q . For example, setting $q = 3^n$ we have $\phi(q)/2 = 3^{n-1}$, and the sequence $\frac{2^{3^{n-1}} + 3^n + 1}{2 \cdot 3^n}$ clearly tends to infinity. A stronger result is possible, namely

COROLLARY 11. *For every n , there are only finitely many values of q with no more than n orbits.*

The importance of the proof of Theorem 9 is that it allows us to construct elements whose continued fraction expansion is provably not finite, since the orbits in $P^1(\bar{O})$ are easily computable (\bar{O} is a finite ring). We include two example computations.

EXAMPLE 3. Let $q = 11$. The lower bound we obtain is

$$t \geq \frac{2^5 + 11 + 1}{22} = 2.$$

In this case, the minimal polynomial $x^5 - x^4 - 4x^3 + 3x^2 + 3x - 1$ of λ stays irreducible modulo 2, implying that the ideal (2) remains inert, and $O/2O$ is a field with $2^5 = 32$ elements. The orbit of 0 will consist of 11 elements of $P^1(\bar{O})$ including the single point at infinity. Writing λ for $\bar{\lambda}$ to ease notation, we write the orbit of 0 with the sequence determined by the action of U : $\{0, \infty, \lambda, \lambda^4 + \lambda^3 + 1, \lambda^4 + \lambda^3 + \lambda^2 + \lambda, \lambda^4 + \lambda, 1, \lambda + 1, \lambda^4, \lambda^4 + \lambda^3 + \lambda^2, \lambda^4 + \lambda^3 + \lambda + 1\}$.

The remaining elements of the field form the orbit of length $2q = 22$. Any lifting of them to characteristic 0 is non-cuspidal. So, in particular, we can

state with certainty that the real number λ_{11}^2 , for example, has an infinite λ_{11} -continued fraction expansion. This stands in contrast to λ_{11}^4 , which may or may not have a finite expansion. Numerical computations for λ_{11}^4 yield a continued fraction which does not terminate after 10 000 terms.

EXAMPLE 4. The computation is somewhat more involved in the case when $O/2O$ is not a field, since the elements of the projective line are not all of the form that we counted in Lemma 4. We consider the case $q = 17$, the smallest q for which 2 splits. With strictly more than $2^{\phi(17)/2} + 1 = 257$ elements in the projective ring and strictly more than eight orbits, a full account of all orbits would be excessive. In fact, since 2 splits into two distinct primes of degree 4, the number of elements in the projective ring is $(2^4 + 1)^2 = 289$. Following the proof of Theorem 9, we get a lower bound on the number of orbits of $1 + (289 - 17)/34 = 9$, which agrees with the estimate from the theorem. One can compute the orbit of 0, as in the previous example. The only potentially cuspidal elements in $\mathbb{Q}(\lambda)$ would be congruent to one of the 17 elements of that orbit modulo 2.

4. Fixed points and periodic continued fractions

4.1. *Fixed points and periodic continued fractions.* Let $x \in \mathbb{Q}(\lambda)$ and consider a transformation $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Then x is a fixed point of M if and only if

$$(5) \quad \frac{ax + b}{cx + d} = x.$$

It is easy to see that this relation yields a polynomial equation that is of degree at most two in x . Therefore, when the relation is non-trivial, the equation will have at most two solutions, and M can have at most two fixed points over a field. The relation is trivial only in the case when M is the identity transformation, in which case all points are fixed.

Fixed points of Hecke triangle groups are expressible as periodic continued fractions, i.e. continued fractions of the form in $[a_0; a_1, a_2, \dots]$ for which there exist integers i and k so that $a_j = a_{j+k}$ for all $j \geq i$. Two elements of $\widehat{\mathbb{Q}}(\lambda_q)$ are in the same orbit when they can be expressed as periodic λ -continued fractions with the same periodic part. It can thus be convenient to consider periodic λ -continued fractions as it is easy to tell whether two periodic λ -continued fractions are in the same orbit. However, it is not always easy to find such elements in $\widehat{\mathbb{Q}}(\lambda_q)$, since these are the fixed points of some element M of $G(\lambda)$ which may, as roots of a quadratic polynomial determined by (5), lie in some quadratic extension of $\mathbb{Q}(\lambda)$.

In this section we present some results having to do with periodic λ -continued fractions. We are motivated by the situations present in the cases when $q = 7$ and $q = 9$.

When $q = 7$, there are, conjecturally, just two orbits in $\mathbb{Q}(\lambda_7)$: the cuspidal orbit (i.e. the finite continued fractions) and the orbit of $\lambda^2 - 1 = [\overline{1, -1}]$.

When $q = 9$, we again find that the elements of $\mathbb{Q}(\lambda_9)$ all appear to have λ_9 -continued fraction representations which are either finite or (eventually) periodic. The periodic elements are in the orbits of $2\lambda + 2 = [\overline{3, -4, 1, 1}]$, $8\lambda + 8 = [\overline{12, -1, 3, 1, -2, -18, -1, 40, 3, 1, 1, 1}]$, $-2\lambda - 2$, or $-8\lambda - 8$.

4.2. Period length for $q = 2p^n$ with $p \equiv 3 \pmod{4}$

LEMMA 12. *Let $q \geq 3$ be an integer. If q can be written in the form $q = 2p^n$ for some odd prime p , then the ideals $(\lambda_q^{\phi(q)})$ and (p) of $\mathbb{Z}[\lambda_q]$ are equal.*

The proof of the lemma is left as an exercise in algebraic number theory.

REMARK 5. It can also be shown that λ_q is a unit of $\mathbb{Z}[\lambda_q]$ whenever q is *not* of the form $2p^n$.

THEOREM 13. *Suppose q can be written as $q = 2p^n$ for some prime p congruent to 3 modulo 4. Suppose $x \in \mathbb{Q}(\lambda_q)$ has a periodic continued fraction expansion. Then the length of the period of x is even.*

Proof. Since λ_q is not a unit, we can consider the group $G(\lambda_q)$ modulo λ_q . The reduction is generated by the matrices

$$\overline{S} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \overline{T} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Now let x have a purely periodic continued fraction expansion, that is, let x be a fixed point of $M \in G(\lambda_q)$. Suppose $M \equiv T \pmod{\lambda_q}$. Then $-1/x \equiv x \pmod{\lambda}$. That is, $-1 \equiv x^2 \pmod{\lambda}$.

From Lemma 12, we have $N(\lambda_q) = \pm p$, and from this it follows that $\mathbb{Z}[\lambda]/(\lambda)$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$, and since $p \equiv 3 \pmod{4}$, we know that -1 is not a square modulo λ .

Therefore, $M \equiv S \pmod{\lambda}$. This means that in the decomposition of M into a word in S and T , the number of factors T must be even, and the number of terms in the period of x must be even. Note that if x is eventually periodic (not necessarily purely periodic), the matrix M fixing x is also congruent to S modulo λ , being conjugate to a matrix fixing a purely periodic continued fraction. ■

4.3. Periodic continued fractions for $q = 7$. The following proposition is a step in the direction of proving that, for $q = 7$, there is a single orbit containing periodic continued fractions, and it is the orbit of $\lambda^2 - 1 = [\overline{1, -1}]$.

PROPOSITION 14. *For $q = 7$, if $x \in \mathbb{Q}(\lambda)$ has the continued fraction expansion $x = [\overline{n, -n}]$, then $n = \pm 1$.*

Proof. Suppose $x = \overline{[n, -n]}$. Then unwinding the first part of the continued fraction, we see that $-1/(x - n\lambda) = \overline{[-n, n]} = -x$, so $x^2 - n\lambda x - 1 = 0$. The discriminant of this equation is

$$D = (n\lambda)^2 + 4,$$

which has norm

$$N(D) = n^6 + 24n^4 + 80n^2 + 64.$$

In order for x to be in the field, D must be a square in the field. If D is to be a square in the field, its norm must be a square in \mathbb{Z} , so we can set $n^6 + 24n^4 + 80n^2 + 64 = (n^3 + 12n + \varepsilon)^2$. For $n \geq 32$, we see that $N(D)$ lies strictly between $(n^3 + 12n)^2$ and $(n^3 + 12n + 1)^2$ (in other words, $\varepsilon < 1$), and hence is not a square. Checking numerically, we find that for $1 \leq n < 32$, the only time $N(D)$ is a square is when $n = 1$. ■

5. Open questions and conjectures. We conclude with some remaining questions and directions for further work.

REMARK 6. It is tempting to try to analyze the orbits modulo higher powers of 2. For example, when $q = 7$, it may be possible to conclude that there are only two orbits in characteristic 0 under the action of $G(\lambda)$ by looking 2-adically (the prime 2 remains inert when $q = 7$). Modulo 2 we have the hopeful result of two orbits (one of length 7 and one of length 2); however, to obtain an upper bound on the number of orbits, a lower bound on their order seems necessary. In a ring with zero divisors (such as $O/2^nO$), a lower bound on the size of an orbit is difficult to compute since, in particular, a fractional linear transformation may have many fixed points without being the identity. It will, for example, be the case that the size of $P^1(O/2^nO)$ is even, so S will have to have more than one fixed point.

REMARK 7. For $q > 9$, we believe that there are numbers in $\mathbb{Q}(\lambda)$ whose continued fraction expansion is not periodic. However, the only tools we have so far for showing that the continued fraction expansion of a number does not terminate involve looking modulo (2), and that method will not prove that an element of $\mathbb{Q}(\lambda)$ has a trivial stabilizer. Once again, it may be possible to approach the problem p -adically for some suitably chosen prime p . (It should be noted that Borho [1] demonstrates that no interesting results arise when one considers the continued fractions over a field of characteristic other than 2. However, different results may arise modulo higher powers of a prime.)

REMARK 8. It is unclear whether the estimate we give for the number of orbits is ever accurate when $q > 7$. We know that it is not when $q = 9$, but for higher values of q it is difficult to show that elements belong to distinct orbits.

REMARK 9. Extensive computations of continued fractions of the form $a\lambda^n$ performed using PARI/GP did not find any hyperbolic fixed points in $\mathbb{Q}(\lambda_q)$ for q odd, $11 \leq q \leq 29$. This, however, does not show that any of the elements considered were not hyperbolic fixed points. We thank the referee for pointing out that since “there is always a finite index subgroup without torsion and no elementary Fuchsian group can consist of parabolic elements alone”, there must always exist hyperbolic fixed points.

References

- [1] W. Borho, *Kettenbrüche im Galoisfeld*, Abh. Math. Sem. Univ. Hamburg 39 (1973), 76–82.
- [2] W. Borho und G. Rosenberger, *Eine Bemerkung zur Hecke-Gruppe $G(\lambda)$* , *ibid.*, 83–87.
- [3] E. Hecke, *Lectures on Dirichlet Series, Modular Functions and Quadratic Forms*, Vandenhoeck & Ruprecht, Göttingen, 1983.
- [4] A. Leutbecher, *Über die Heckeschen Gruppen $\mathfrak{G}(\lambda)$* , Abh. Math. Sem. Univ. Hamburg 31 (1967), 199–205.
- [5] D. Rosen, *A class of continued fractions associated with certain properly discontinuous groups*, Duke Math. J. 21 (1954), 549–563.
- [6] D. Rosen and C. Towse, *Continued fraction representations of units associated with certain Hecke groups*, Arch. Math. (Basel) 77 (2001), 294–302.
- [7] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Grad. Texts in Math. 83, Springer, New York, 1997.
- [8] J. Wolfart, *Eine Bemerkung über Heckes Modulgruppen*, Arch. Math. (Basel) 29 (1977), 72–77.

Scripps College
 Claremont, CA 91711, U.S.A.
 E-mail: ehanson@scrippscollege.edu
 ctowse@scrippscollege.edu

Current address of A. Merberg:
 Brown University
 Providence, RI 02912, U.S.A.
 E-mail: adam_merberg@brown.edu

Current address of E. Yudovina:
 Harvard University
 Cambridge, MA 02138, U.S.A.
 E-mail: yudovina@fas.harvard.edu

*Received on 16.7.2007
 and in revised form on 5.6.2008*

(5480)