GENERALIZATION OF ATKIN’S ORTHOGONAL POLYNOMIALS AND SUPERSINGULAR ELLIPTIC CURVES

YING-YING TRAN

(Communicated by Matthew A. Papanikolas)

Abstract. In a 1998 paper, Kaneko and Zagier explain unpublished work of Atkin which exhibits an infinite sequence of polynomials with the property that when suitable polynomials are reduced mod $p$ for a prime $p$, one gets the locus of supersingular elliptic curves. Here we generalize this phenomenon by considering the continued fraction expansions of modular and quasimodular forms.

1. Introduction and statement of results

An elliptic curve $E$ over a field $K$ of characteristic $p > 0$ is called supersingular if the group $E(K)$ has no $p$-torsion, where $K$ is the algebraic closure of $K$. This condition depends only on the $j$-invariant of $E$ and there are only finitely many supersingular $j$-invariants in $\mathbb{F}_p$. We are interested in the polynomial

$$S_p(j) := \prod_{\substack{E/F_p, \ E \text{ supersingular}}} (j - j(E)) \in \mathbb{F}_p[j].$$

The first few supersingular polynomials are:

$$S_5(j) = j,$$
$$S_7(j) = j + 1,$$
$$S_{11}(j) = j(j + 10),$$
$$\vdots$$
$$S_{37}(j) = (j + 29)(j^2 + 31j + 31).$$

Atkin defines a sequence of monic polynomials $A_n(j) \in \mathbb{Q}[j]$, with $\deg A_n(j) = n$, as the orthogonal polynomials with respect to a special scalar product and shows that if $n_p$ is the degree of $S_p$, then $S_p(j) \equiv A_{n_p}(j)$ mod $p$. The first few Atkin
polynomials are:
\[ A_0(j) = 1, \]
\[ A_1(j) = j - 720, \]
\[ A_2(j) = j^2 - 1640j + 269280, \]
\[ A_3(j) = j^3 - \frac{12576}{5}j^2 + 1526958j - 107765865, \]
\[ A_4(j) = j^4 - 384j^3 + 3528552j^2 - 1133263680j + 44184000960. \]

Atkin’s observation is illustrated by the following examples:
\[ A_2(j) \equiv j^2 + 13j + 12 = (j + 1)(j + 12) \pmod{19}, \]
\[ A_3(j) \equiv j^3 + j^2 + 11j = j(j + 4)(j + 20) \pmod{23}, \]
\[ A_3(j) \equiv j^3 + 2j^2 + 21j = j(j + 4)(j + 27) \pmod{29}. \]

Kaneko and Zagier [2] interpret this result using the theory of continued fractions
and convergents for power series, applying this theory to a particular quasimodular
form
\[ \Phi := \frac{E_2E_4}{E_6j}, \]
where \( E_k \) is the weight \( k \) Eisenstein series and \( j \) is the usual modular invariant,
recalled in Section 2. Kaneko and Zagier then show that the Atkin polynomials are
the denominators of the convergents of \( \Phi \), and thus \( S_p \) is the denominator of the
\( n_p \)th convergent of \( \Phi \).

Here we generalize Kaneko and Zagier’s results. Rather than consider \( \Phi = \frac{E_2E_4}{E_6j} \),
we will consider more general modular and quasimodular forms. To present
cleaner results, instead of searching for \( S_p \), we will consider \( S^*_p \), where \( S^*_p \) is the
supersingular locus away from 0 and 1728.

Table 1

<table>
<thead>
<tr>
<th>( E_{p-1} )</th>
<th>( E_{p+1} )</th>
<th>( j - 1728 )</th>
<th>( j )</th>
<th>( n^*(a, b, c, d, p) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( a \leq 0 )</td>
<td>( e &lt; 0 )</td>
<td>( a + c \leq (a+e)e )</td>
<td>( 2a + b + 3d \leq 3 + (2a+e)\delta )</td>
<td>( 1 - cm )</td>
</tr>
<tr>
<td>( a + c &gt; (a+e)e )</td>
<td>( 2a + b + 3d \geq 3 + (2a+e)\delta )</td>
<td>( \frac{2}{3}(1-\delta)a + \frac{b}{3} + d - (m + \frac{d}{3})c )</td>
<td></td>
<td></td>
</tr>
<tr>
<td>( a \geq 0 )</td>
<td>( e &gt; 0 )</td>
<td>( a + c \geq (a+e)e )</td>
<td>( 2a + b + 3d \geq 3 + (2a+e)\delta )</td>
<td>( em )</td>
</tr>
<tr>
<td>( a + c &lt; (a+e)e )</td>
<td>( 2a + b + 3d &gt; 3 + (2a+e)\delta )</td>
<td>( em - \frac{2}{3}(1-\delta)a - \frac{b}{3} - d + \frac{2\delta}{3} )</td>
<td></td>
<td></td>
</tr>
<tr>
<td>( a &lt; 0 )</td>
<td>( a + c \geq (a+e)e )</td>
<td>( 2a + b + 3d \geq 3 + (2a+e)\delta )</td>
<td>( 1 - a(m + \delta + \varepsilon - 1) )</td>
<td></td>
</tr>
<tr>
<td>( a + c &lt; (a+e)e )</td>
<td>( 2a + b + 3d \geq 3 + (2a+e)\delta )</td>
<td>( 1 - (a + b + c + \varepsilon) )</td>
<td></td>
<td></td>
</tr>
<tr>
<td>( a + c \geq (a+e)e )</td>
<td>( 2a + b + 3d \geq 3 + (2a+e)\delta )</td>
<td>( 1 + m(m + \delta + \varepsilon - 1) )</td>
<td></td>
<td></td>
</tr>
<tr>
<td>( a + c &lt; (a+e)e )</td>
<td>( 2a + b + 3d \geq 3 + (2a+e)\delta )</td>
<td>( 1 + \frac{d}{3} )</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
Theorem 1. If \( \Phi = E_2^a E_4^b E_6^c \Delta^d \), then let \( w(\Phi) := 2a + 4b + 6c + 12d \). Let \( p \geq 5 \) be a prime such that \( p - 1 \) divides \( w(\Phi) \), and define \( e := a + \frac{w(\Phi)}{p-1} \). If \( e \neq 0 \), then for some integer \( n^*(a,b,c,d,p) \) defined in Table 1, \((S_p^*)^e \) (resp. \((S_p^*)^{-e} \)) divides the denominator (resp. numerator) of the \((n^*(a,b,c,d,p))\)th convergent of \( \Phi j^{d-1} \) if \( e > 0 \) (resp. if \( e < 0 \)).

In the rows with \( \Phi \), our proof does not give a convergent, for reasons discussed in the proof.

Remark. When \( w(\Phi) = 0 \), \( p - 1 \) divides \( w(\Phi) \) for every prime \( p \), with \( e = a \). Thus, if \( w(\Phi) = 0 \), then for every prime \( p \), \( S_p \) divides the numerator or denominator of some convergent. Kaneko and Zagier’s \( \Phi := \frac{E_2 E_4}{E_{12}} \) falls in this particular category.

2. Preliminaries

2.1. Modular forms. For \( k \) even and positive, let \( B_k \) be the \( k \)th Bernoulli number, and let \( E_k(\tau) \) be the \( k \)th Eisenstein series

\[
E_k(\tau) = 1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \left( \sum_{d|n} d^{k-1} \right) q^n \quad (q = e^{2\pi i \tau}).
\]

\( E_k \) is a modular form of weight \( k \) for \( k \geq 4 \) and for \( k = 2 \) is “nearly modular” or quasimodular:

\[
E_2(\frac{a\tau + b}{c\tau + d}) = (c\tau + d)^2 E_2(\tau) + \frac{6}{\pi i} c (c\tau + d) \quad \left( \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \right),
\]

where \( \Gamma = \text{PSL}(2,\mathbb{Z}) \). In addition, let

\[
\Delta(\tau) := \frac{E_4(\tau)^3 - E_6(\tau)^2}{1728} = q \prod_{n=1}^{\infty} (1 - q^n)^{24} \in M_{12}
\]

and

\[
j(\tau) := \frac{E_4(\tau)^3}{\Delta(\tau)},
\]

where \( M_k \) is the space of modular forms of weight \( k \) on \( \Gamma \) for even \( k > 2 \). It is easy to see that

\[
j(\tau) - 1728 = \frac{E_6(\tau)^2}{\Delta(\tau)}.
\]

For any even integer \( k > 2 \), we can express \( k \) uniquely in the form

\[
k = 12m + 4\delta + 6\varepsilon \quad \text{with} \quad m \in \mathbb{Z}_{\geq 0}, \quad \delta \in \{0,1,2\}, \quad \varepsilon \in \{0,1\}.
\]

In fact, if \( k + 1 = p \) is a prime, then \( m, \delta, \) and \( \varepsilon \) are given explicitly by

\[
m = \left\lfloor \frac{p}{12} \right\rfloor, \quad \delta = \begin{cases} 0 & \text{if } p \equiv 1 \mod 3, \\ 1 & \text{if } p \equiv 2 \mod 3, \end{cases} \quad \varepsilon = \begin{cases} 0 & \text{if } p \equiv 1 \mod 4, \\ 1 & \text{if } p \equiv 3 \mod 4. \end{cases}
\]

Then \( \dim M_k = m + 1 \) and any modular form in \( M_k \) can be written uniquely as

\[
f(\tau) = \Delta(\tau)^m E_4(\tau)^\delta E_6(\tau)^\varepsilon \tilde{f}(j(\tau))
\]

for some polynomial \( \tilde{f} \) of degree \( \leq m \) in \( j(\tau) \), the coefficient of \( j^m \) in \( \tilde{f} \) being equal to the constant term of the Fourier expansion of \( f \). In particular, for primes \( p \geq 5 \) with \( \delta \) and \( \varepsilon \) as defined in equation (4),

\[
S_p(j) \equiv j^\delta (j - 1728)^\varepsilon \tilde{E}_{p-1} \mod p,
\]
a result apparently first noticed by Deligne (cf. [4]). We will concentrate our interest on the supersingular locus away from 0 and 1728; i.e. \( S_p^*(j) = \tilde{E}_{p-1} \).

2.2. Orthogonal polynomials, continued fractions, and convergents. Let \( V \) be the vector space of single-variable polynomials over \( \mathbb{R} \) and \(( , )\) a scalar product on \( V \) of the form \((f, g) = \phi(fg)\), where \( \phi(f) = \int_a^b f(X)v(X)dX \) for some real numbers \( a < b \) and some positive function \( v \) on \((a, b)\). Applying the Gram-Schmidt process to \( \{X^n\}_{n \geq 0} \) (which is a basis of \( V \)), we obtain a unique basis of orthogonal monic polynomials \( P_n \) by the recursion

\[
P_n(X) = X^n - \sum_{m=0}^{n-1} \frac{(X^n, P_m)}{(P_m, P_m)} P_m(X),
\]

as long as \((P_n, P_n) \neq 0\) for all \( n \), which is true, since \((f, f) > 0\) for all \( f \neq 0 \). Let \( g_n = (X^n, 1) = \phi(X^n) \). Then \( P_n(X) \) satisfy the recursion

\[
(7) \quad P_0 = 0, \quad P_1 = g_0, \quad P_{n+1} = (x - a_n)P_n - b_n P_{n-1},
\]

for some constants \( a_n, b_n \in \mathbb{R} \), where \( b_n = \frac{(P_n, P_n)}{(P_{n-1}, P_{n-1})} \neq 0 \). Further, define the polynomials \( Q_n(X) \) recursively as

\[
(8) \quad Q_0 = 1, \quad Q_1 = x - g_1/g_0, \quad Q_{n+1} = (x - a_n)Q_n - b_n Q_{n-1}.
\]

Then

\[
(9) \quad \frac{P_n(X)}{Q_n(X)} = \Phi(X) + O(X^{-2n-1}) \in \mathbb{R}[[X^{-1}]],
\]

where \( \Phi(X) := \sum_{n=0}^{\infty} g_n X^{-n-1} \in \mathbb{R}[[X^{-1}]] \). Define \( \lambda_n \in \mathbb{R} \) \((n \geq 1)\) by the continued fraction expansion

\[
g_0 + g_1 x + g_2 x^2 + \cdots = \frac{g_0}{1 - \frac{\lambda_1 x}{1 - \frac{\lambda_2 x}{1 - \cdots}}}. \in \mathbb{R}[[x]].
\]

Then \( \lambda_n \neq 0 \) and \( a_n = \lambda_2 + \lambda_2 + \lambda_2, b_n = \lambda_2 \lambda_2 \) for \( n \geq 1 \).

It is not hard to see that if \( b_n \neq 0 \), then \( \gcd(P_n, Q_n) = 1 \), which implies that if \( A(X) \) and \( B(X) \) are polynomials such that

\[
A(X) \quad B(X) = \Phi(X) + O(X^{-2n-1})
\]

and \( \deg B \leq \deg Q_n \), then \( B \) is a constant multiple of \( Q_n \). Therefore, \( P_n/Q_n \) is the best possible approximation for the degree of the denominator (cf. [1], [2]).

3. Proof of the main theorem

We will first prove a technical proposition about quasimodular forms. Throughout \( p \geq 5 \) is prime. Recall that the degree of a rational function \( P(x) = f(x)/g(x) \), where \( f \) and \( g \) are polynomials, is

\[
\deg P = \deg f - \deg g.
\]
3.1. A technical proposition.

**Proposition 2.** Given $\Phi = E_2^a E_4^b E_6^c \Delta^d$, let $w(\Phi)$ and $e$ be as in Theorem 1. If $p - 1$ divides $w(\Phi)$, then $\Phi$ is a rational function in $j$ modulo $p$ of degree $-d$. In fact,

$$\Phi \equiv j^{\frac{1}{2}}(2a-2a\delta+b-e\delta)(j-1728)^{\frac{1}{2}}(a-ae+c-e\epsilon)\tilde{E}_{p-1}^{a} \tilde{E}_{p+1}^{a} \mod p,$$

where $\delta$ and $\epsilon$ are those corresponding to $k = p - 1$ as defined in (4).

**Proof.** If $p \geq 5$ is a prime, then we know that $E_{p-1} \equiv 1 \mod p$ and $E_{p+1} \equiv 2 \mod p$. Thus we have

$$\Phi = E_2^a E_4^b E_6^c \Delta^d \equiv E_{p+1}^{a} E_4^b E_6^c \Delta^d \tilde{E}_{p-1}^{a} \mod p,$$

where $e = a + \frac{w(\Phi)}{p-1}$. Then $\Phi$ has weight 0, which implies that $\Phi$ is a rational function in $j$ modulo $p$.

Define $m$, $\delta$, and $\epsilon$ as the numbers defined by (4) with $k = p - 1$. Then the corresponding numbers for $k = p + 1$ are $m + \delta + \epsilon - 1$, $2(1 - \delta)$, and $1 - \epsilon$ respectively. Equation (5) for $E_{p-1}$ and $E_{p+1}$ then becomes

$$E_{p-1} = \Delta^m E_4^a E_6^b \tilde{E}_{p-1}, \quad E_{p+1} = \Delta^{m+\delta+\epsilon-1} E_4^{b+1} E_6^{-\epsilon} \tilde{E}_{p+1},$$

so

$$\Phi \equiv \Delta^{a+\delta+\epsilon-\epsilon} E_4^b E_6^c \tilde{E}_{p-1} \mod p.$$

$\Phi$ is a rational function in $j$, and $\tilde{E}_{p+1}$ and $S_p$ are polynomials in $j$, so

$$F := \Delta^{a+\delta+\epsilon-\epsilon} E_4^b E_6^c \tilde{E}_{p+1}$$

is a rational function in $j$ and a weight 0 modular form. Because $F$ is weight 0, then

$$4(2a-2a\delta+b-e\delta)+6(a-ae+c-e\epsilon) = 12(a-an_p-d+em),$$

which implies that 3 divides $2a-2a\delta+b-e\delta$ and 2 divides $a-ae+c-e\epsilon$. Therefore,

$$F = j^{\frac{1}{2}}(2a-2a\delta+b-e\delta)(j-1728)^{\frac{1}{2}}(a-ae+c-e\epsilon)$$

and

$$\Phi \equiv j^{\frac{1}{2}}(2a-2a\delta+b-e\delta)(j-1728)^{\frac{1}{2}}(a-ae+c-e\epsilon) \tilde{E}_{p-1}^{a} \tilde{E}_{p+1}^{a} \mod p.$$

Furthermore, $\tilde{E}_{p-1}$ and $\tilde{E}_{p+1}$ have degree $m$ and $m+\delta+\epsilon-1 = n_p-1$ respectively, so $\Phi$ has degree $-d$. \qed

3.2. Proof of the main theorem.** Drawing together the results from convergents, some identities of modular forms, and the previous proposition, we are ready to prove Theorem 1.

**Proof.** From Proposition 2 we know that $\Phi$ is a rational function in $j$ of degree $-d$. Thus, let us consider $\Phi_j^{d-1}$ which has degree $-1$ in $j$. From (10),

$$\Phi_j^{d-1} = j^{\frac{1}{2}}(2a-2a\delta+3d-e\delta-3)(j-1728)^{\frac{1}{2}}(a-ae+c-e\epsilon) \tilde{E}_{p-1}^{a} \tilde{E}_{p+1}^{a} \mod p.$$

Because $\Phi_j^{d-1}$ is a rational function, it can be expressed as the quotient of two polynomials. Furthermore, induction easily shows that every convergent has degree $-1$, as does $\Phi_j^{d-1}$. Then $\Phi_j^{d-1}$ is a perfect, and hence a best possible, approximation to itself, so $\Phi_j^{d-1}$ must equal its convergents once the degree of the denominator of the convergent agrees with that of the denominator of $\Phi_j^{d-1}$.\[\]
Thus, if we can prove that the appropriate power of $S_p^*$ divides the numerator (or denominator) of $\Phi j^{d-1}$, then indeed the appropriate power of $S_p^*$ must also divide the numerator (or denominator) of the $n^*$th convergent of $\Phi j^{d-1}$, where $n^*$ is the degree of the denominator of $\Phi j^{d-1}$. More specifically, $S_p^* = \tilde{E}_{p-1}$, so we need only to seek appearances of $\tilde{E}_{p-1}$.

We break this down into cases, corresponding to the signs of the exponents. If $e < 0$, then $\tilde{E}_{p-1}$ (and hence $S_p^*$) is in the numerator. If everything else is in the denominator, i.e. $2a - 2a\delta + b + 3d - e\delta - 3 \leq 0$, $a - ae + c - e\varepsilon \leq 0$, and $a \leq 0$, then the degree of the numerator is $-em$ and $n^* = 1 - em$. If only the exponents of $j$ and $\tilde{E}_{p-1}$ are positive, then the degree of the numerator is $-em + \frac{1}{3}(2a - 2a\delta + b + 3d - e\delta - 3)$ and $n^* = 1 - em + \frac{1}{3}(2a - 2a\delta + b + 3d - e\delta - 3)$.

If the exponents of $\tilde{E}_{p-1}$, $j$, and $j - 1728$ are positive but the exponent of $\tilde{E}_{p+1}$ is zero or negative, then it is easier to compute the degree of the denominator. The degree of $\tilde{E}_{p+1}$ is $m + \delta + \varepsilon - 1$, which gives the degree of the denominator to be $-a(m + \delta + \varepsilon - 1)$, and hence $n^* = -a(m + \delta + \varepsilon - 1)$. The rest of the cases follow in similar fashion.

If $e > 0$, then $\tilde{E}_{p-1}$, and hence $S_p^*$, is in the denominator, and as before, we can compute the degree of the denominator or numerator to find the desired $n^*$.

Now all that remains is to address those cases indicated in the table with $\mathbf{x}$. In those cases, all the exponents are of the same sign (and nonzero), meaning that the numerator or the denominator is 1. Recall that $\Phi j^{d-1}$ is of degree $-1$. Immediately, we can rule out the case of the denominator being 1. If the numerator is 1, then the denominator must be of degree 1, but the exponents are nonzero, which forces the denominator to be of degree at least 3. Thus, we reach a contradiction, which indicates that those cases cannot be attained.

\[\square\]

4. Examples

In this section, we will consider various quasimodular forms $\Phi j^{d-1}$ and appropriate primes $p$ to cover some of the cases in Theorem 1.

**Example.** Let $\Phi = \frac{E_2E_4^3\Delta^4 j^2}{E_6}$ and $p = 37$. Then

$$\Phi \equiv \frac{j^4 \tilde{E}_{38}}{(j - 1728)E_{36}^2} \mod 37,$$

and the denominator of the seventh convergent is congruent to

$$(j^2 + 31j + 31)^2(j + 29)^2(j + 11) = (S_{37}^*)^2(j + 11) = S_{37}^2(j + 11).$$

**Example.** Let $\Phi = E_2^2E_4E_6^2\Delta$ and $p = 17$. Then

$$\Phi \equiv \frac{(j - 1728)^2\tilde{E}_{18}}{j\tilde{E}_{16}^4} \mod 17,$$

and the denominator of the fifth convergent is congruent to

$$j(j + 9)^4 = (S_{17}^*)^4 j = S_{17}(j + 9)^3.$$

**Example.** Let $\Phi = \frac{\Delta^8 j^7}{E_2^2E_4^8E_6^2}$ and $p = 43$. Then

$$\Phi \equiv \frac{j(j - 1728)\tilde{E}_{42}^4}{\tilde{E}_{42}^2} \mod 43,$$
and the numerator of the fifteenth convergent is congruent to
\[(j + 2)^4(j^2 + 19j + 16)^4j(j + 35) = (S_{43}^*)^4j(j + 35) = S_{43}(j + 2)^3(j^2 + 19j + 16)^3j.\]

**Example.** Let \( \Phi = \frac{E_4^2 E_6 \Delta}{E_2^2} \) and \( p = 23 \). Then
\[\Phi \equiv \frac{j(j - 1728)\tilde{E}_{22}}{E_{24}^2} \mod 23,\]
and the numerator of the fourth convergent is congruent to
\[j(j + 20)(j + 4) = S_{23}^* j(j + 20) = S_{23}.\]

**References**


Department of Mathematics, Malott Hall, Cornell University, Ithaca, New York 14853-4201

E-mail address: yytran@math.cornell.edu