PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 141, Number 4, April 2013, Pages 1135–1141
S 0002-9939(2012)11433-9
Article electronically published on August 20, 2012

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 In a 1998 paper, Kaneko and Zagier explain unpublished work of Atkin which exhibits an infinite sequence of polynomials with the property that when suitable polynomials are reduced mod p for a prime p, one gets the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 $E(\overline{K})$ has no p-torsion, where $\overline{K}$ 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 $\overline{\mathbb{F}}_p$. We are interested in the polynomial

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

The first few supersingular polynomials are:

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

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

Received by the editors July 22, 2010 and, in revised form, August 9, 2011.
2010 *Mathematics Subject Classification.* Primary 14H52, 11F33.

polynomials are:

$$\begin{aligned} A_0(j) &= 1, \\ A_1(j) &= j - 720, \\ A_2(j) &= j^2 - 1640j + 269280, \\ A_3(j) &= j^3 - \frac{12576}{5}j^2 + 1526958j - 107765856, \\ A_4(j) &= j^4 - 3384j^3 + 3528552j^2 - 1133263680j + 44184000960. \end{aligned} \tag{2}$$

Atkin's observation is illustrated by the following examples:

$$\begin{aligned} A_2(j) &\equiv j^2 + 13j + 12 = (j+1)(j+12) \mod 19, \\ A_3(j) &\equiv j^3 + j^2 + 11j = j(j+4)(j+20) \mod 23, \\ A_3(j) &\equiv j^3 + 2j^2 + 21j = j(j+4)(j+27) \mod 29. \end{aligned}$$

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

$$\Phi := \frac{E_2 E_4}{E_6 j},$$

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 Φ, and thus S_p is the denominator of the n_pth convergent of Φ.

Here we generalize Kaneko and Zagier's results. Rather than consider $\Phi = \frac{E_2 E_4}{E_6 j}$, 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

$\tilde{E}_{p-1}$	$\tilde{E}_{p+1}$	$j - 1728$	j	$n^*(a,b,c,d,p)$
$e < 0$	$a \le 0$	$a + c \le (a+e)\varepsilon$	$2a+b+3d \le 3 + (2a+e)\delta$	$1 - em$
			$2a+b+3d > 3 + (2a+e)\delta$	$\frac{2}{3}(1-\delta)a + \frac{b}{3} + d - (m + \frac{\delta}{3})e$
		$a + c > (a+e)\varepsilon$	$2a+b+3d \le 3 + (2a+e)\delta$	$1 - em + \frac{a}{2} + \frac{c}{2} - \frac{\varepsilon}{2}(a+e)$
			$2a+b+3d > 3 + (2a+e)\delta$	$-a(m + \delta + \varepsilon - 1)$
	$a > 0$	$a + c \le (a+e)\varepsilon$	$2a+b+3d \le 3 + (2a+e)\delta$	$1 - em + a(m + \delta + \varepsilon - 1)$
			$2a+b+3d > 3 + (2a+e)\delta$	$-\frac{a}{2} - \frac{c}{2} + \frac{\varepsilon}{2}(a+e)$
		$a + c > (a+e)\varepsilon$	$2a+b+3d \le 3 + (2a+e)\delta$	$-\frac{2}{3}(1-\delta)a - \frac{b}{3} - d + \frac{\delta e}{3} + 1$
			$2a+b+3d > 3 + (2a+e)\delta$	✠
$e > 0$	$a \ge 0$	$a + c \ge (a+e)\varepsilon$	$2a+b+3d \ge 3 + (2a+e)\delta$	em
			$2a+b+3d < 3 + (2a+e)\delta$	$em - \frac{2}{3}(1-\delta)a - \frac{b}{3} - d + \frac{\delta e}{3} + 1$
		$a + c < (a+e)\varepsilon$	$2a+b+3d \ge 3 + (2a+e)\delta$	$\frac{a}{2}(\varepsilon - 1) - \frac{c}{2} + (m + \frac{\varepsilon}{2})e$
			$2a+b+3d < 3 + (2a+e)\delta$	$1 + a(m + \delta + \varepsilon - 1)$
	$a < 0$	$a + c \ge (a+e)\varepsilon$	$2a+b+3d \ge 3 + (2a+e)\delta$	$em - a(m + \delta + \varepsilon - 1)$
			$2a+b+3d < 3 + (2a+e)\delta$	$1 + \frac{a}{2}(1-\varepsilon) + \frac{c}{2} - \frac{\varepsilon e}{2}$
		$a + c < (a+e)\varepsilon$	$2a+b+3d \ge 3 + (2a+e)\delta$	$\frac{2}{3}(1-\delta)a + \frac{b}{3} + d - \frac{e\delta}{3}$
			$2a+b+3d < 3 + (2a+e)\delta$	✠

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 Φj^{d-1} if $e > 0$ (resp. if $e < 0$).*

In the rows with ✠, 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 $\Phi := \frac{E_2 E_4}{E_6 j}$ falls in this particular category.

2. Preliminaries

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

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

E_k is a modular form of weight k for $k \geq 4$ and for $k = 2$ is "nearly modular" or quasimodular:

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

where $\Gamma = PSL(2, \mathbb{Z})$. 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 Γ 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

$$k = 12m + 4\delta + 6\varepsilon \qquad \text{with} \quad m \in \mathbb{Z}_{\geq 0}, \quad \delta \in \{0, 1, 2\}, \quad \varepsilon \in \{0, 1\}. \tag{3}$$

In fact, if $k + 1 = p$ is a prime, then m, δ, and ε are given explicitly by

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

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

$$f(\tau) = \Delta(\tau)^m E_4(\tau)^\delta E_6(\tau)^\varepsilon \tilde{f}(j(\tau)) \tag{5}$$

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 δ and ε as defined in equation (4),

$$S_p(j) \equiv j^\delta (j - 1728)^\varepsilon \tilde{E}_{p-1} \mod p, \tag{6}$$

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

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

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

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

Then

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

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

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

Then $\lambda_n \neq 0$ and $a_n = \lambda_{2n} + \lambda_{2n+1}$, $b_n = \lambda_{2n-1}\lambda_{2n}$ 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

$$\frac{A(X)}{B(X)} = \Phi(X) + O(X^{-2n-1})$$

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* Φ *is a rational function in* j *modulo* p *of degree* $-d$. *In fact,*

$$\Phi \equiv j^{\frac{1}{3}(2a-2a\delta+b-e\delta)}(j-1728)^{\frac{1}{2}(a-a\varepsilon+c-e\varepsilon)}\tilde{E}_{p-1}^{-e}\tilde{E}_{p+1}^{a} \mod p, \tag{10}$$

where δ *and* ε *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 $E_{p+1} \equiv E_2 \mod p$. Thus we have

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

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

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

$$E_{p-1} = \Delta^m E_4^\delta E_6^\varepsilon \tilde{E}_{p-1}, \qquad E_{p+1} = \Delta^{m+\delta+\varepsilon-1} E_4^{2-2\delta} E_6^{1-\varepsilon} \tilde{E}_{p+1},$$

so

$$\Phi \equiv \Delta^{am+a\delta+a\varepsilon-a+d-em} E_4^{2a-2a\delta+b-e\delta} E_6^{a-a\varepsilon+c-e\varepsilon} \tilde{E}_{p+1}^a \tilde{E}_{p-1}^{-e} \mod p.$$

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

$$F := \Delta^{am+a\delta+a\varepsilon-a+d-em} E_4^{2a-2a\delta+b-e\delta} E_6^{a-a\varepsilon+c-e\varepsilon}$$

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

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

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

$$F = j^{\frac{1}{3}(2a-2a\delta+b-e\delta)}(j-1728)^{\frac{1}{2}(a-a\varepsilon+c-e\varepsilon)}$$

and

$$\Phi \equiv j^{\frac{1}{3}(2a-2a\delta+b-e\delta)}(j-1728)^{\frac{1}{2}(a-a\varepsilon+c-e\varepsilon)}\tilde{E}_{p-1}^{-e}\tilde{E}_{p+1}^{a} \mod p.$$

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

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 Φ is a rational function in j of degree $-d$. Thus, let us consider Φj^{d-1} which has degree -1 in j. From (10),

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

Because Φj^{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 Φj^{d-1}. Then Φj^{d-1} is a perfect, and hence a best possible, approximation to itself, so Φj^{d-1} must equal its convergents once the degree of the denominator of the convergent agrees with that of the denominator of Φj^{d-1}.

Thus, if we can prove that the appropriate power of S_p^* divides the numerator (or denominator) of Φj^{d-1}, then indeed the appropriate power of S_p^* must also divide the numerator (or denominator) of the n^*th convergent of Φj^{d-1}, where n^* is the degree of the denominator of Φj^{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. $2a - 2a\delta + b + 3d - e\delta - 3 \leq 0$, $a - a\varepsilon + c - e\varepsilon \leq 0$, 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 ✠. In those cases, all the exponents are of the same sign (and nonzero), meaning that the numerator or the denominator is 1. Recall that Φj^{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. □

4. Examples

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

Example. Let $\Phi = \frac{E_2 E_4^4 \Delta^3 j^2}{E_6^3}$ and $p = 37$. Then

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

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 $\Phi = E_2^2 E_4 E_6^2 \Delta$ and $p = 17$. Then

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

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 $\Phi = \frac{\Delta^8 j^7}{E_2^5 E_4^8 E_6^2}$ and $p = 43$. Then

$$\Phi \equiv \frac{j(j - 1728)\tilde{E}_{42}^4}{\tilde{E}_{44}^5} \mod 43,$$

and the numerator of the fifteenth convergent is congruent to

$$(j+2)^4(j^2+19j+16)^4 j(j+35) = (S_{43}^*)^4 j(j+35) = S_{43}(j+2)^3(j^2+19j+16)^3 j.$$

Example. Let $\Phi = \frac{E_4^2 E_6 \Delta}{E_2^2}$ and $p = 23$. Then

$$\Phi \equiv \frac{j(j-1728)\tilde{E}_{22}}{\tilde{E}_{24}^2} \mod 23,$$

and the numerator of the fourth convergent is congruent to

$$j(j+20)(j+4) = S_{23}^* j(j+20) = S_{23}.$$

References

[1] G. E. Andrews, R. Askey, and R. Roy, *Special functions*, Cambridge University Press, Cambridge, 1999. MR1688958 (2000g:33001)

[2] M. Kaneko and D. Zagier, *Supersingular j-invariants, hypergeometric series, and Atkin's orthogonal polynomials*, Computational perspectives on number theory (Chicago, IL, 1995), AMS/IP **7** (1998), pages 97-126. MR1486833 (99b:11064)

[3] K. Ono, *The web of modularity: Arithmetic of the coefficients of modular forms and q-series*, Conference Board of the Mathematical Sciences, Regional Conference Series, **102**, AMS, Providence, 2004. MR2020489 (2005c:11053)

[4] J-P. Serre, *Congruences et formes modulaires (d'après H.P.F. Swinnerton-Dyer)*, Sém. Bourbaki **416** (1971/72), 319–338. MR0466020 (57:5904a)

[5] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1986. MR817210 (87g:11070)

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

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