

# SYSTEMS OF ORTHOGONAL POLYNOMIALS ARISING FROM THE MODULAR $j$ -FUNCTION

STEPHANIE BASHA, JAYCE GETZ, HARRIS NOVER, AND EMMA SMITH

ABSTRACT. Let  $\mathfrak{S}_p(x) \in \mathbb{F}_p[x]$  be the polynomial whose zeros are the  $j$ -invariants of supersingular elliptic curves over  $\overline{\mathbb{F}}_p$ . Generalizing a construction of Atkin described in a recent paper by Kaneko and Zagier [5], we define an inner product  $\langle \cdot, \cdot \rangle_\psi$  on  $\mathbb{R}[x]$  for every  $\psi(x) \in \mathbb{Q}[x]$ . Suppose a system of orthogonal polynomials  $\{P_{n,\psi}(x)\}_{n=0}^\infty$  with respect to  $\langle \cdot, \cdot \rangle_\psi$  exists. We prove that if  $n$  is sufficiently large and  $\psi(x)P_{n,\psi}(x)$  is  $p$ -integral, then  $\mathfrak{S}_p(x) \mid \psi(x)P_{n,\psi}(x)$  over  $\mathbb{F}_p[x]$ . Further, we obtain an interpretation of these orthogonal polynomials as a  $p$ -adic limit of polynomials associated to  $p$ -adic modular forms.

## 1. INTRODUCTION AND STATEMENT OF RESULTS

Let  $j(z)$  denote the usual modular function of weight zero

$$j(z) := q^{-1} + 744 + \dots$$

Here and throughout this paper,  $q = e^{2\pi iz}$ . Given  $\psi(x) \in \mathbb{R}[x]$ , we define a symmetric bilinear form on  $\mathbb{R}[x]$  by letting, for  $f(x), g(x) \in \mathbb{R}[x]$ ,

$$(1.1) \quad \langle f, g \rangle_\psi = \frac{6}{\pi} \int_{\pi/3}^{\pi/2} f(j(e^{i\theta}))g(j(e^{i\theta}))\psi(j(e^{i\theta}))d\theta.$$

For  $\psi = 1$ , Kaneko and Zagier investigate this bilinear form, which is due to Atkin, in great detail [5]. Here we generalize some of their results for most  $\psi \in \mathbb{Q}[x]$ . We begin by making the following definition:

**Definition.** A polynomial  $\psi(x) \in \mathbb{R}[x]$  is **good** if there exists a set of monic orthogonal polynomials  $\{P_{i,\psi}\}_{i=0}^\infty$  with respect to  $\langle \cdot, \cdot \rangle_\psi$ . That is, the degree of  $P_{i,\psi}$  is  $i$ , and

$$\langle P_{n,\psi}, P_{m,\psi} \rangle_\psi = h_{m,n} \delta_{m,n},$$

where  $h_{m,n} \in \mathbb{R}$  and  $\delta_{m,n}$  is the Kronecker delta-function.

*Remark.* For  $\psi$  to be good it is sufficient that  $\langle \cdot, \cdot \rangle_\psi$  be a definite bilinear form. Since  $j(e^{i\theta})$  maps  $[\pi/3, \pi/2]$  to  $[0, 1728]$  bijectively, any  $\psi$  with no zeros of odd order in the interval  $(0, 1728)$  will induce a definite bilinear form  $\langle \cdot, \cdot \rangle_\psi$ . This observation immediately implies that the vast majority of  $\psi$  are good; more precisely, if we fix all but the constant term of a prospective  $\psi \in \mathbb{Z}[x]$ , there is only a finite number of constant terms for which  $\psi$  could possibly be bad.

---

*Date:* November 10, 2004.

The authors would like to thank the following organizations for their generous support of the 2003 Research Experience for Undergraduates that led to this paper: the National Science Foundation, the University of Wisconsin at Madison, the David and Lucile Packard Foundation, the Alfred P. Sloan Foundation, and the John S. Guggenheim Foundation.

Let  $p \geq 5$  be prime and let  $E/\overline{\mathbb{F}}_p$  be an elliptic curve. Then  $E$  is called *supersingular* if  $E(\overline{\mathbb{F}}_p)$  has no  $p$ -torsion. The  $j$ -invariant of such an  $E$  is called a *supersingular  $j$ -invariant* over  $\overline{\mathbb{F}}_p$ . We fix the notation

$$(1.2) \quad \Omega_p := \{j_i : j_i \text{ is a supersingular } j\text{-invariant over } \overline{\mathbb{F}}_p\}$$

and

$$(1.3) \quad g_p := |\Omega_p|.$$

We define the supersingular locus  $\mathfrak{S}_p(x)$  as

$$(1.4) \quad \mathfrak{S}_p(x) = \prod_{j_i \in \Omega_p} (x - j_i) \in \mathbb{F}_p[x].$$

The fact that  $g_p$  is finite and that  $\mathfrak{S}_p(x) \in \mathbb{F}_p[x]$  is well-known (see, for example, [5], [7]).

In order to relate a polynomial in  $\mathbb{Q}[x]$  to  $\mathfrak{S}_p(x)$  we require the notion of  $p$ -integrality. We will define  $p$ -integrality using the  $p$ -adic norm. Fix a prime  $p$ . Any nonzero  $t \in \mathbb{Q}$  may be written uniquely as  $t = \frac{a}{b}p^r$  where  $a, b, r \in \mathbb{Z}$ ,  $b > 0$ , and  $\gcd(p, ab) = \gcd(a, b) = 1$ . We then define the  $p$ -adic norm for  $v \in \mathbb{Q}$  as

$$(1.5) \quad |v|_p := \begin{cases} p^{-r} & \text{if } v \neq 0 \\ 0 & \text{if } v = 0 \end{cases}$$

A rational number  $t$  is said to be  $p$ -integral if  $|t|_p \leq 1$ . A polynomial  $f(x) \in \mathbb{Q}[x]$  is  $p$ -integral if all of its coefficients are  $p$ -integral; in this case, the reduction modulo  $p$  is well-defined. With this in mind, we make the following definition.

**Definition.** Let  $\psi(x) \in \mathbb{Q}[x]$  be good and write

$$P_{n,\psi}(x) = \sum_{i=0}^n a_i x^i \quad \text{and} \quad \psi(x) = \sum_{i=0}^m b_i x^i.$$

If  $p$  is a prime, then we define the following powers of  $p$

$$(1.6) \quad \begin{aligned} \alpha_{n,\psi}(p) &= \max(\{|a_i|_p : 0 \leq i \leq n\}), \\ \beta_\psi(p) &= \max(\{|b_i|_p : 0 \leq i \leq m\}). \end{aligned}$$

Note that  $\alpha_{n,\psi}(p)P_{n,\psi}(x)$  and  $\beta_\psi(p)\psi(x)$  are both  $p$ -integral.

We may now state our main theorem.

**Theorem 1.** Fix a prime  $p \geq 5$  and suppose  $\psi(x) \in \mathbb{Q}[x]$  is good. Let

$$d_{\psi,p} := \deg(\gcd(\mathfrak{S}_p(x), \beta_\psi(p)\psi(x)))$$

over  $\mathbb{F}_p[x]$ . If  $n \geq g_p - d_{\psi,p}$  then

$$\mathfrak{S}_p(x) \mid \beta_\psi(p)\psi(x)\alpha_{n,\psi}(p)P_{n,\psi}(x)$$

in  $\mathbb{F}_p[x]$ .

*Remark.* This theorem, in the  $\psi(x) = 1$  case, recovers a theorem of Atkin described in a recent paper by M. Kaneko and D. Zagier [5]. Our method offers a new proof of this result.

Given Theorem 1, it is natural to consider the  $p$ -adic properties of these systems of orthogonal polynomials. Before we state our result in this direction, we require some basic facts from the theory of modular forms.

For an even integer  $k \geq 2$ , define  $M_k$  to be the finite dimensional vector space of holomorphic modular forms of weight  $k$  under the action of the full modular group  $\mathrm{SL}_2(\mathbb{Z})$ . We fix the notation

$$\sigma_{k-1}(n) := \sum_{d|n} d^{k-1}$$

and denote by  $B_k$  the  $k$ th Bernoulli number. Then the Fourier expansion of the classical Eisenstein series  $E_k(z)$  is

$$E_k(z) := 1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n.$$

For  $k \geq 4$  we have  $E_k(z) \in M_k$ . Although  $E_2(z)$  is not a modular form, it will play an important role later. In addition, we recall the  $\Delta$ -function,

$$\Delta(z) := \frac{E_4(z)^3 - E_6(z)^2}{1728},$$

the unique normalized cusp form of weight 12.

*Remark.* In terms of  $\Delta(z)$  and  $E_4(z)$ , we have

$$j(z) = \frac{E_4(z)^3}{\Delta(z)}.$$

Using these modular forms, we define the notion of a divisor polynomial of a modular form. If  $k \geq 4$  is even, then define  $\tilde{E}_k(z)$  by

$$(1.7) \quad \tilde{E}_k(z) := \begin{cases} 1 & \text{if } k \equiv 0 \pmod{12}, \\ E_4(z)^2 E_6(z) & \text{if } k \equiv 2 \pmod{12}, \\ E_4(z) & \text{if } k \equiv 4 \pmod{12}, \\ E_6(z) & \text{if } k \equiv 6 \pmod{12}, \\ E_4(z)^2 & \text{if } k \equiv 8 \pmod{12}, \\ E_4(z) E_6(z) & \text{if } k \equiv 10 \pmod{12}. \end{cases}$$

Further, define  $m(k)$  by

$$m(k) := \begin{cases} \lfloor k/12 \rfloor & \text{if } k \not\equiv 2 \pmod{12}, \\ \lfloor k/12 \rfloor - 1 & \text{if } k \equiv 2 \pmod{12}. \end{cases}$$

With this notation, if  $f(z) \in M_k$  and  $\tilde{F}(f, x)$  is the unique rational function in  $x$  for which

$$(1.8) \quad f(z) = \Delta(z)^{m(k)} \tilde{E}_k(z) \tilde{F}(f, j(z)),$$

then  $\tilde{F}(f, x)$  is a polynomial, which we will refer to as the *divisor polynomial* for  $f$ . From (1.7) and (1.8), the polynomial  $\tilde{F}(f, x)$  will have zeros precisely at the  $j$ -invariant of the zeros of  $f(z)$ , with possible exceptions at  $j(e^{2\pi i/3}) = 0$  and  $j(i) = 1728$ , depending on the weight of  $f(z)$  modulo 12. For a discussion of divisor polynomials, see [1].

Additionally, we require the machinery of continued fraction expansions (which are of interest in their own right). In particular, in Section 4 we examine the continued fraction

expansion of  $\psi(j(z))\frac{E_2(z)E_4(z)}{E_6(z)}$ . Though it may seem most natural to write this as a continued fraction in terms of  $q$ , it will be useful to regard it formally in terms of

$$\left(\frac{1}{j}\right) = q - 744q^2 + \dots \in \mathbb{Z}[[q]].$$

That is, we write

$$\psi(j(z))\frac{E_2(z)E_4(z)}{E_6(z)} = \frac{\psi(j)}{1 - \frac{\lambda(1)\left(\frac{1}{j}\right)}{1 - \frac{\lambda(2)\left(\frac{1}{j}\right)}{1 - \frac{\lambda(3)\left(\frac{1}{j}\right)}{\ddots}}}}.$$

The  $n$ th partial convergent of this expansion is

$$(1.9) \quad \frac{\psi(j)}{1 - \frac{\lambda(1)\left(\frac{1}{j}\right)}{1 - \frac{\lambda(2)\left(\frac{1}{j}\right)}{1 - \frac{\lambda(3)\left(\frac{1}{j}\right)}{\ddots}}}}.$$

We show in Section 4 that (1.9) is equal to  $\frac{Q_{n,\psi}(j)}{P_{n,\psi}(j)}$  for certain  $Q_{n,\psi}(x) \in \mathbb{Q}[x]$  (see 4.2) and  $P_{n,\psi}(x)$  as above.

These partial convergents are essentially the  $p$ -adic limit of the divisor polynomials of a specific family of  $p$ -adic modular forms. The order of the error term depends only on  $n$ . More precisely, we have the following result.

**Theorem 2.** *Let  $\psi(x) \in \mathbb{Q}[x]$  be good,  $p \geq 5$  be prime, and  $r$  be a positive integer. With  $\alpha_{n,\psi}(p)$  and  $\beta_\psi(p)$  defined as in (1.6) and  $\frac{Q_{n,\psi}(x)}{P_{n,\psi}(x)}$  as above, we have*

$$\beta_\psi(p)\psi(j)\frac{\tilde{F}(E_4E_{\phi(p^r)+2}, j)}{\tilde{F}(E_6(E_{p-1})^{p^r-1}, j)} \equiv \frac{\beta_\psi(p)Q_{n,\psi}(j)}{\alpha_{n,\psi}(p)P_{n,\psi}(j)} + \mathcal{O}\left(\left(\frac{1}{j}\right)^{2n}\right) \pmod{p^r},$$

where  $\phi$  is Euler's  $\phi$ -function.

In the next section, we prove some useful general properties of the bilinear form defined by (1.1). In Section 3 we prove Theorem 1, and in Section 4, we discuss continued fraction expansions in preparation for the proof of Theorem 2 in Section 5. We conclude in Section 6 with an efficient method of computing the  $P_{n,\psi}(x)$ 's and apply this method to illustrate some of our results.

## 2. PRELIMINARY OBSERVATIONS ON THE BILINEAR FORM

Fix  $\psi(x) \in \mathbb{Q}[x]$  and let  $f(x), g(x) \in \mathbb{Q}[x]$  be polynomials. Define rational numbers  $a(m)$  and  $b(n)$  as the coefficients of the formal power series in  $q$ ,

$$(2.1) \quad f(j)g(j)\psi(j)E_2 = \sum_{m \geq m_0} a(m)q^m,$$

and in  $\left(\frac{1}{j}\right)$ ,

$$(2.2) \quad f(j)g(j)\psi(j)\frac{E_2E_4}{E_6} = \sum_{n \geq n_0} b(n)\left(\frac{1}{j}\right)^n.$$

Note that  $a(m)$  and  $b(n)$  depend on  $\psi$ ,  $f$ , and  $g$ . We have the following proposition (see also [5]).

**Proposition 3.** *Let  $f(x), g(x), \psi(x) \in \mathbb{Q}[x]$ . With the notation above, we have*

$$(2.3) \quad \langle f, g \rangle_\psi = a(0),$$

$$(2.4) \quad \langle f, g \rangle_\psi = b(0),$$

$$(2.5) \quad \langle f, g \rangle_\psi = \int_0^{1728} f(x)g(x)\psi(x) \frac{E_4}{2\pi x E_6 j^{-1}(x)} dx.$$

As we will see, Proposition 3 simplifies the explicit computation of orthogonal polynomials with respect to  $\langle, \rangle_\psi$ . In addition, it allows us to use the arithmetic of the coefficients of modular forms to deduce properties of these polynomials. Before we begin the proof of the proposition, we recall the theta operator

$$(2.6) \quad \Theta = q \frac{d}{dq} = \frac{1}{2\pi i} \frac{d}{dz},$$

and Ramanujan's classical identities (see [6], exercise III.2.8)

$$(2.7) \quad \Theta(E_4) = (E_4 E_2 - E_6)/3 \quad \text{and} \quad \Theta(E_6) = (E_6 E_2 - E_4^2)/2.$$

*Proof of Proposition 3.* Let

$$\mathfrak{F} := \left\{ z : -\frac{1}{2} \leq \operatorname{Re}(z) \leq 0 \text{ and } |z| \geq 1 \right\} \cup \left\{ z : 0 < \operatorname{Re}(z) < \frac{1}{2} \text{ and } |z| > 1 \right\}$$

be the standard fundamental domain for the action of  $\mathrm{SL}_2(\mathbb{Z})$  on the upper half plane. We cut off  $\mathfrak{F}$  by a horizontal line

$$C_1 := \left\{ iL - t : -\frac{1}{2} \leq t \leq \frac{1}{2} \right\},$$

where  $L$  is a sufficiently large real number. Define the contour with counterclockwise orientation around

$$\mathfrak{F} \cap \{\operatorname{Im}(z) \leq L\},$$

as in the proof of the  $k/12$  valence formula (see, for example, [6] p. 115), where  $C_2$  denotes the arc from  $e^{2\pi i/3}$  to  $i$  and  $C_3$  the arc from  $i$  to  $e^{\pi i/3}$ . We integrate the left hand side of (2.1) along our contour. Breaking the integral into parts, we note that the sum of the integrals along the lines given by  $\operatorname{Re}(z) = \pm \frac{1}{2}$  cancel. In addition, the residue theorem implies that the entire integral is equal to the sum of the residues. This sum is zero because  $E_2$  and  $j$  are holomorphic on the upper half plane. If  $S := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ , then  $SC_2$  traces the same arc as  $C_3$  with opposite orientation. These observations imply

$$(2.8) \quad - \int_{C_1} f(j)g(j)\psi(j)E_2 dz = \int_{C_2} f(j)g(j)\psi(j)E_2 dz + \int_{C_3} f(j)g(j)\psi(j)E_2 dz,$$

$$(2.9) \quad -\frac{1}{2\pi i} \int_{|q|=R} f(j)g(j)\psi(j)E_2 \frac{dq}{q} = \int_{C_2} f(j)g(j)\psi(j)E_2 dz - \int_{SC_2} f(j)g(j)\psi(j)E_2 dz.$$

On the left side of (2.9), we use the residue theorem to evaluate the integral with respect to  $q$  around the circle  $|q| = R$  with negative orientation. On the right we use the transformation

formula for  $E_2$  (cf. [6] p. 113),

$$(2.10) \quad E_2(-1/z)z^{-2} = E_2(z) + \frac{12}{2\pi iz},$$

and the equalities  $dz = \frac{1}{2\pi i} \frac{dq}{q} = izd\theta$  to obtain

$$\begin{aligned} a(0) &= \int_{C_2} f(j)g(j)\psi(j)E_2 dz - \frac{12}{2\pi i} \int_{C_2} f(j)g(j)\psi(j) \frac{dz}{z} - \int_{C_2} f(j)g(j)\psi(j)E_2 dz, \\ a(0) &= \frac{6}{\pi} \int_{\pi/3}^{\pi/2} f(j(e^{i\theta}))g(j(e^{i\theta}))\psi(j(e^{i\theta}))d\theta. \end{aligned}$$

Note that care is required when changing variables in the previous step.

To prove (2.4), we calculate the differential  $d\left(\frac{1}{j}\right)$  using (2.6) and (2.7).

$$\begin{aligned} \frac{d}{dz} \left( \frac{1}{j} \right) &= \frac{d}{dz} \left( \frac{E_4^3 - E_6^2}{1728E_4^3} \right) = -\frac{1}{1728} \left( \frac{2E_6E_6'E_4^3 - 3E_4^2E_4'E_6^2}{E_4^6} \right), \\ &= -\frac{2\pi i}{1728} \left( \frac{\frac{2}{2}E_6(E_6E_2 - E_4^2)E_4^3 - \frac{3}{3}E_4^2(E_4E_2 - E_6)E_6^2}{E_4^6} \right), \\ &= -\frac{2\pi i}{1728} \frac{E_6}{E_4} \left( \frac{-E_4^3 + E_6^2}{E_4^3} \right) = 2\pi i \frac{E_6}{E_4} \left( \frac{\Delta}{E_4^3} \right), \\ &= 2\pi i \frac{E_6}{E_4} \left( \frac{1}{j} \right). \end{aligned}$$

Thus, we have that

$$dz = \frac{j}{2\pi i} \frac{E_4}{E_6} d\left(\frac{1}{j}\right).$$

Substituting this into the left hand side of (2.8) and applying the residue theorem, we have

$$-\int_{C_1} f(j)g(j)\psi(j)E_2 dz = \frac{1}{2\pi i} \int_{\gamma} f(j)g(j)\psi(j)j \frac{E_2E_4}{E_6} d\left(\frac{1}{j}\right) = b(0).$$

Because  $1/j \sim e^{2\pi iz}$  for  $L$  large,  $\gamma$  is a simple curve around zero with a counterclockwise orientation.

To prove (2.5), recall that on the arc from  $e^{i\pi/3}$  to  $i$  in  $\mathfrak{F}$ , the  $j$ -invariant takes real values. To see this, use the invariance of  $j$  under  $S$  and the fact that  $j(z)$  can be written as a  $q$ -series with real coefficients. Since  $j$  is a continuous bijection from  $\mathfrak{F}$  to  $\mathbb{C}$ ,  $j(e^{\pi i/3}) = 0$ , and  $j(i) = 1728$ , it follows that  $j$  maps this arc monotonically onto  $[0, 1728]$ . Substituting  $x = j(e^{i\theta})$  into (1.1) and noting that  $\frac{d}{dz} \left( \frac{1}{j} \right) = -\frac{1}{j^2} \frac{dj}{dz}$  yield the final equivalence.  $\square$

*Remark.* Define a measure

$$w_\psi(x) := \frac{\psi(x)E_4 dx}{2\pi x E_6 j^{-1}(x)}.$$

Then Proposition 3 tells us that  $\langle \cdot, \cdot \rangle_\psi$  is a real-valued bilinear form on the space of polynomials  $\mathbb{R}[x]$  with respect to the measure  $w_\psi(x)$ . Thus, we can apply the classical theory of real-valued orthogonal polynomials to our particular objects of study. In particular, if  $\psi(x) \in \mathbb{Q}[x]$  is good, then all the zeros of  $P_{n,\psi}(x) \in \mathbb{Q}[x]$  lie in the interval  $[0, 1728]$ . Further, if  $m < n$ , the zeros of  $P_{m,\psi}$  interlace the zeros of  $P_{n,\psi}$  in the sense that any zero of  $P_{m,\psi}$  lies between two zeros of  $P_{n,\psi}$ . For a treatment of orthogonal polynomials, see [2].

We will require the following lemma in the next section.

**Lemma 4.** *Suppose  $\psi(x) \in \mathbb{Q}[x]$  is good. Write*

$$x^n = P_{n,\psi} + c_{(n-1),n}P_{n-1,\psi} + \cdots + c_{0,n}(1).$$

Then

$$\langle x^n, P_{m,\psi} \rangle_\psi = c_{m,n} \langle P_{m,\psi}, P_{m,\psi} \rangle_\psi.$$

Furthermore,  $c_{m,n} = 0$  when  $n < m$ .

*Proof.* This follows immediately from the definition of  $\{P_{n,\psi}\}$ . □

### 3. PROOF OF THEOREM 1

Suppose that  $p \geq 5$  is prime. We begin by recalling two results. Let

$$(3.1) \quad F(E_{p-1}, x) := \begin{cases} \tilde{F}(E_{p-1}, x) & \text{if } p \equiv 1 \pmod{12}, \\ x\tilde{F}(E_{p-1}, x) & \text{if } p \equiv 5 \pmod{12}, \\ (x - 1728)\tilde{F}(E_{p-1}, x) & \text{if } p \equiv 7 \pmod{12}, \\ x(x - 1728)\tilde{F}(E_{p-1}, x) & \text{if } p \equiv 11 \pmod{12}. \end{cases}$$

Then we have the following well-known theorem.

**Proposition 5** (Deligne, [5]). *If  $p \geq 5$  is prime, then*

$$\mathfrak{S}_p(x) \equiv F(E_{p-1}, x) \pmod{p}.$$

The second result characterizes the logarithmic derivative of a modular form on  $\mathrm{SL}_2(\mathbb{Z})$  and gives an explicit description of  $\Theta f$ .

**Proposition 6** ([3]). *If  $f \in M_k$  is a holomorphic modular form and  $e_\tau$  is defined by*

$$e_\tau = \begin{cases} \frac{1}{2} & \text{if } \tau = i, \\ \frac{1}{3} & \text{if } \tau = e^{2\pi i/3}, \\ 1 & \text{otherwise,} \end{cases}$$

then we have the following identity:

$$\frac{k}{12}E_2(z) = \frac{\Theta f(z)}{f(z)} + j(z) \frac{E_6(z)}{E_4(z)} \sum_{\tau \in \mathfrak{F}} \frac{e_\tau \mathrm{ord}_\tau(f)}{j(z) - j(\tau)}.$$

*Remark.* This formula is equivalent to the famous denominator formula for the Monster Lie algebra.

For ease of notation, we also define

$$(3.2) \quad \mathbb{K}_{\left(\frac{1}{j}\right)} \left( \sum_{n \geq n_0} b(n) \left(\frac{1}{j}\right)^n \right) := b(0)$$

and

$$(3.3) \quad \mathbb{K}_q \left( \sum_{n \geq m_0} a(n)q^n \right) := a(0)$$

to be the constant terms in the respective expansions.

We are now ready to prove Theorem 1.

*Proof of Theorem 1.* The von Staudt-Clausen Bernoulli number congruences imply the  $q$ -series congruence

$$E_{p-1}(z) \equiv 1 \pmod{p}$$

(see Section 5 for details). In particular, the Fourier coefficients of  $E_{p-1}(z)$  are  $p$ -integral. Since

$$\tilde{F}(E_{p-1}, j) = \frac{E_{p-1}}{\tilde{E}_k \Delta^{m(k)}}$$

and

$$\tilde{E}_k \Delta^{m(k)} \in \mathbb{Z}[[q]],$$

it follows that  $\tilde{F}(E_{p-1}, j)$  is  $p$ -integral when written as a polynomial in  $j$ .

Use the Euclidean algorithm to find  $h(x) \in \mathbb{Q}[x]$  and  $a(i) \in \mathbb{Q}$  such that

$$(3.4) \quad \alpha_{n,\psi}(p)\beta_\psi(p)P_{m,\psi}(x)\psi(x) = h(x)F(E_{p-1}, x) + a(g_p - 1)x^{g_p-1} + \dots + a(0).$$

As the set of  $p$ -integral elements of  $\mathbb{Q}[x]$  forms a ring, the fact that  $F(E_{p-1}, x)$  and  $\alpha_{n,\psi}(p)\beta_\psi(p)P_{m,\psi}(x)\psi(x)$  are  $p$ -integral implies that  $h$  and the  $a(i)$ 's will also be  $p$ -integral.

By Lemma 4, we have  $c_{m,n} \langle P_{m,\psi}, \alpha_{n,\psi}(p)\beta_\psi(p)P_{m,\psi} \rangle_\psi = \langle x^n, \alpha_{n,\psi}(p)\beta_\psi(p)P_{m,\psi} \rangle_\psi$ . By Proposition 3,

$$(3.5) \quad \langle x^n, \alpha_{n,\psi}(p)\beta_\psi(p)P_{m,\psi} \rangle_\psi = \mathbb{K}_{\left(\frac{1}{j}\right)} \left( j^n \alpha_{n,\psi}(p)\beta_\psi(p)P_{m,\psi}(j)\psi(j) \frac{E_2 E_4}{E_6} \right).$$

This constant term is  $p$ -integral because  $\frac{E_2 E_4}{E_6}$  is  $p$ -integral as a  $\left(\frac{1}{j}\right)$ -series.

Applying Proposition 6 with  $f = E_{p-1}$  and  $k = p - 1$ , we derive the relation

$$(3.6) \quad E_2 = \frac{12}{p-1} \left( \frac{\Theta E_{p-1}}{E_{p-1}} + j(z) \frac{E_6}{E_4} \sum_{\tau \in \mathfrak{F}} \frac{e_\tau \text{ord}_\tau(E_{p-1})}{j(z) - j(\tau)} \right).$$

Combining (3.5) with (3.6) and letting

$$(3.7) \quad P^* := \alpha_{n,\psi}(p)\beta_\psi(p)P_{m,\psi}(j)\psi(j)$$

we have

$$\begin{aligned} \frac{p-1}{12} c_{m,n} \langle P_{m,\psi}, P_{m,\psi} \rangle_\psi &= \mathbb{K}_{\left(\frac{1}{j}\right)} \left( j^n P^* \frac{E_4}{E_6} \left[ \frac{\Theta E_{p-1}}{E_{p-1}} + j(z) \frac{E_6}{E_4} \sum_{\tau \in \mathfrak{F}} \frac{e_\tau \text{ord}_\tau(E_{p-1})}{j(z) - j(\tau)} \right] \right), \\ &= \mathbb{K}_{\left(\frac{1}{j}\right)} \left( j^n P^* \left[ \frac{E_4 \Theta E_{p-1}}{E_6 E_{p-1}} + \sum_{\tau \in \mathfrak{F}} \frac{e_\tau \text{ord}_\tau(E_{p-1}) j(z)}{j(z) - j(\tau)} \right] \right). \end{aligned}$$

We expand (3.4) with  $x = j$  and rewrite the above equality as

$$\begin{aligned} \frac{p-1}{12} c_{m,n} \langle P_{m,\psi}, P_{m,\psi} \rangle_\psi - \mathbb{K}_{\left(\frac{1}{j}\right)} \left( j^n P^* \frac{E_4 \Theta E_{p-1}}{E_6 E_{p-1}} + j^n h(j) F(E_{p-1}, j) \sum_{\tau \in \mathfrak{F}} \frac{e_\tau \text{ord}_\tau(E_{p-1}) j(z)}{j(z) - j(\tau)} \right) \\ = \mathbb{K}_{\left(\frac{1}{j}\right)} \left( j^n (a(g_p - 1)j^{g_p-1} + \dots + a(0)) \sum_{\tau \in \mathfrak{F}} \frac{e_\tau \text{ord}_\tau(E_{p-1}) j(z)}{j(z) - j(\tau)} \right). \end{aligned}$$

Rewriting the sums as geometric series, we have

$$\begin{aligned}
 & \frac{p-1}{12} c_{m,n} \langle P_{m,\psi}, P_{m,\psi} \rangle_\psi - \\
 (3.8) \quad & \mathbb{K}_{\left(\frac{1}{j}\right)} \left( j^n P^* \frac{E_4}{E_6} \frac{\Theta E_{p-1}}{E_{p-1}} + j^n h(j) F(E_{p-1}, j) \sum_{k=0}^{\infty} \frac{\sum_{\tau \in \mathfrak{F}} e_{\tau} \text{ord}_{\tau}(E_{p-1}) j(\tau)^k}{j(z)^k} \right) \\
 & = \mathbb{K}_{\left(\frac{1}{j}\right)} \left( j^n (a(g_p - 1) j^{g_p - 1} + \dots + a(0)) \sum_{k=0}^{\infty} \frac{\sum_{\tau \in \mathfrak{F}} e_{\tau} \text{ord}_{\tau}(E_{p-1}) j(\tau)^k}{j(z)^k} \right).
 \end{aligned}$$

Equivalently, we may write this equality as the following system of linear equations:

$$(3.9) \quad \begin{pmatrix} \sum_{\tau \in \mathfrak{F}} e_{\tau} \text{ord}_{\tau}(E_{p-1}) j(\tau)^0 & \cdots & \sum_{\tau \in \mathfrak{F}} e_{\tau} \text{ord}_{\tau}(E_{p-1}) j(\tau)^{g_p - 1} \\ \vdots & \ddots & \vdots \\ \sum_{\tau \in \mathfrak{F}} e_{\tau} \text{ord}_{\tau}(E_{p-1}) j(\tau)^{g_p - 1} & \cdots & \sum_{\tau \in \mathfrak{F}} e_{\tau} \text{ord}_{\tau}(E_{p-1}) j(\tau)^{2g_p - 1} \end{pmatrix} \begin{pmatrix} a(0) \\ \vdots \\ a(g_p - 1) \end{pmatrix} = V,$$

where  $V$  is a vector with  $g_p$  coordinates, each of which is  $p$ -integral.

Reducing the determinant of this matrix modulo  $p$  and applying Proposition 5, we have

$$D := \begin{vmatrix} \sum_{j_i \in \Omega_p} j_i^0 & \cdots & \sum_{j_i \in \Omega_p} j_i^{g_p - 1} \\ \vdots & \ddots & \vdots \\ \sum_{j_i \in \Omega_p} j_i^{g_p - 1} & \cdots & \sum_{j_i \in \Omega_p} j_i^{2g_p - 1} \end{vmatrix}.$$

We use multilinearity in the rows to simplify this determinant. Let  $S_{g_p}$  be the symmetric group on  $g_p$  elements. Then noting that all matrices with repeated rows have zero determinant, a straightforward calculation gives

$$D = \sum_{\sigma \in S_{g_p}} \begin{vmatrix} j_{\sigma(1)}^0 & \cdots & j_{\sigma(1)}^{g_p - 1} \\ \vdots & \ddots & \vdots \\ j_{\sigma(g_p)}^{g_p - 1} & \cdots & j_{\sigma(g_p)}^{2g_p - 1} \end{vmatrix} = \begin{vmatrix} j_1^0 & \cdots & j_1^{g_p - 1} \\ \vdots & \ddots & \vdots \\ j_p^0 & \cdots & j_p^{g_p - 1} \end{vmatrix}^2.$$

This is the square of a Vandermonde determinant which is nonzero because the  $j_i$  are distinct. Thus, there is a unique vector  $(a_0, \dots, a_{g_p - 1}) \in \mathbb{F}_p^{g_p}$  that is the solution to the reduction of (3.9) modulo  $p$ . To find this unique solution, denote the reduction modulo  $p$  of  $h$  by  $\tilde{h}$  and use the fact that  $\Theta(E_{p-1}(z)) \equiv 0 \pmod{p}$  to reduce (3.8).

$$\begin{aligned}
 0 & = -\mathbb{K}_{\left(\frac{1}{j}\right)} \left( j^n \tilde{h}(j) \mathfrak{S}_p(j) \sum_{\tau \in \mathfrak{S}_p} \frac{1}{j(z) - j(\tau)} \right), \\
 & = \mathbb{K}_{\left(\frac{1}{j}\right)} \left( j^n (a(g_p - 1) j^{g_p - 1} + \dots + a(0)) \sum_{\tau \in \mathfrak{S}_p} \frac{1}{j(z) - j(\tau)} \right).
 \end{aligned}$$

It is clear that  $(a_0, \dots, a_{g_p - 1}) = (0, 0, \dots, 0)$  is a solution to this equation over  $\mathbb{F}_p$ . But then we have

$$\alpha_{n,\psi}(p) \beta_{\psi}(p) P_{m,\psi}(x) \psi(x) \equiv \tilde{h}(x) \mathfrak{S}_p(x) + a(g_p - 1) x^{g_p - 1} + \dots + a(0) \equiv \tilde{h}(x) \mathfrak{S}_p(x) \pmod{p}$$

which immediately implies the theorem.  $\square$

*Remark.* Notice that this proof allows us to weaken the hypotheses regarding the existence of  $\{P_{n,\psi}\}$ . In particular, if  $R(x) \in \mathbb{Q}[x]$  is a monic polynomial of degree  $n \geq g_p - d_{\psi,p}$  and  $\langle x^r, R(x) \rangle_\psi = 0$  for all  $r < n$ , then the same conclusion holds.

*Remark.* With slight modification, the proof of Theorem 1 can be extended to the number field case. In particular, fix  $p \geq 5$ ,  $K$  a number field,  $\mathcal{O}_K$  its ring of integers, and  $\mathfrak{p} \subset \mathcal{O}_K$  a prime ideal above  $p$ . Suppose  $\psi(x) \in \mathcal{O}_K[x]$  is good. Then, under certain conditions,

$$\mathfrak{S}_p(x) \mid \psi(x)P_{n,\psi}(x)$$

over  $(\mathcal{O}_K/\mathfrak{p})[x]$ .

#### 4. CONTINUED FRACTION EXPANSIONS

Orthogonal polynomials are closely related to a certain type of continued fraction expansion (see [2]). Consider the  $\left(\frac{1}{j}\right)$ -expansion of (2.2) with  $f(j) = P_{n,\psi}(j)$ ,

$$(4.1) \quad P_{n,\psi}(j)g(j)\psi(j)\frac{E_2E_4}{E_6} = g(j) \sum_{i \geq n_0} b_\psi(i) \left(\frac{1}{j}\right)^i.$$

The  $q$ -series expansion of  $\frac{E_2E_4}{E_6}$  begins with a constant, while the order of the lowest order term of the  $q$ -series expansion of  $P_{n,\psi}(j)\psi(j)$  is  $-(n+m)$ , where  $m$  is the degree of  $\psi(x)$ . Therefore, as a  $\left(\frac{1}{j}\right)$ -series,  $n_0 = -(n+m)$  in (4.1). Since  $P_{n,\psi}$  is an orthogonal polynomial,  $g(j)b_\psi(i) = 0$  for all  $g(x)$  of degree lower than  $n$ , which in turn implies that  $b_\psi(i) = 0$  for  $0 \leq i \leq n-1$ . Hence, let us define the polynomial

$$(4.2) \quad Q_{n,\psi}(j) = \sum_{i=-(m+n)}^{-1} b_\psi(i) \left(\frac{1}{j}\right)^i.$$

Dividing both sides of (4.1) by  $P_{n,\psi}(j)g(j)$  we obtain

$$(4.3) \quad \psi(j)\frac{E_2E_4}{E_6} = \frac{Q_{n,\psi}(j)}{P_{n,\psi}(j)} + \mathcal{O}\left(\left(\frac{1}{j}\right)^{2n}\right).$$

Let  $y = \frac{1}{j}$ , then (4.3) has a unique continued fraction expansion in terms of  $\lambda(k)$  as

$$(4.4) \quad \psi(j)\frac{E_2E_4}{E_6} = \frac{\psi\left(\frac{1}{y}\right)}{1 - \frac{\lambda(1)y}{1 - \frac{\lambda(2)y}{1 - \frac{\lambda(3)y}{\ddots}}}}$$

with partial convergents given by

$$(4.5) \quad \frac{Q_{n,\psi}(j)}{P_{n,\psi}(j)} = \frac{\psi\left(\frac{1}{y}\right)}{1 - \frac{\lambda(1)y}{1 - \frac{\lambda(2)y}{1 - \frac{\lambda(3)y}{\ddots}}}} = \frac{\psi\left(\frac{1}{y}\right)(1 + C_{1,n})}{1 + D_{1,n}},$$

where

$$C_{m,r} = \sum_{s=m}^{r-1} (-1)^s \sum_{\substack{2 \leq k_1 < \dots < k_s \leq 2r-1 \\ k_{i+1} - k_i \geq 2}} \prod_{i=1}^s \lambda(k_i) y,$$

$$D_{m,r} = \sum_{s=m}^r (-1)^s \sum_{\substack{1 \leq k_1 < \dots < k_s \leq 2r-1 \\ k_{i+1} - k_i \geq 2}} \prod_{i=1}^s \lambda(k_i) y.$$

**Proposition 7.** *Given a continued fraction expansion in  $\lambda(k)$  as in (4.4), the recursion relation for  $P_{n+1,\psi}(j)$  is*

$$(4.6) \quad P_{n+1,\psi}(j) = (j - (\lambda(2n) + \lambda(2n + 1)))P_{n,\psi}(j) - (\lambda(2n)\lambda(2n - 1))P_{n-1,\psi}(j).$$

*Proof.* Recall that  $y = \left(\frac{1}{j}\right)$  and denote  $P_{n,\psi}(j)$  by  $P_{n,\psi}$ . By the partial convergents in (4.5),  $P_{0,\psi} = 1$  and  $P_{1,\psi} = 1 - \lambda(1)y$ . Assume that (4.6) generates the orthogonal polynomials up to  $P_{n,\psi}$ . Let  $\mathcal{P}_{n+1}$  be the next term in the recurrence relation. It is sufficient to show that  $\mathcal{P}_{n+1} = P_{n+1,\psi}$ ; observe that

$$\begin{aligned} \mathcal{P}_{n+1} &= (j - (\lambda(2n) + \lambda(2n + 1)))P_{n,\psi} - (\lambda(2n)\lambda(2n - 1))P_{n-1,\psi} \\ &= j^{n+1} \left\{ (1 - (\lambda(2n) + \lambda(2n + 1))y)D_{1,n} - (\lambda(2n)\lambda(2n - 1))y^2 D_{1,n-1} \right\} \\ &= j^{n+1} D_{1,n+1} + \lambda(2n)\lambda(2n - 1)j^{n-1} D_{1,n-1} - \lambda(2n)\lambda(2n - 1)j^{n-1} D_{1,n-1} \\ &= P_{n+1,\psi}. \end{aligned}$$

We are done by induction. The relation given later as (4.6) matches the relation given in (6.1) for the orthogonal polynomials, and the initial conditions  $P_{-1,\psi} = 0, P_{0,\psi} = 1$  match; hence the orthogonal polynomials generated are identical.  $\square$

When  $\psi(x) = 1$ , Kaneko and Zagier proved the following additional forms of the recurrence relation in [5].

$$P_{n+1,1}(j) = \left( j - 24 \frac{144n^2 - 29}{(2n+1)(2n-1)} \right) P_{n,1}(j) - 36 \left( \frac{(12n-13)(12n-7)(12n-5)(12n+1)}{n(n-1)(2n-1)^2} \right) P_{n-1,1}(j),$$

$$(4.7) \quad P_{n,1}(j) = \sum_{i=1}^n 12^{3i} \left[ \sum_{m=0}^i \binom{-1/12}{i-m} \binom{-5/12}{i-m} \binom{n+12}{m} \binom{n-7/12}{m} \binom{2n-1}{m}^{-1} \right] j^{n-1}.$$

**Proposition 8.** *The orthogonal polynomials  $P_{n,1}$  are  $p$ -integral for all  $n < \frac{p+1}{2}$ .*

*Proof.* This follows from (4.7) since  $\binom{2n-1}{m}^{-1}$  is the only factor contributing an  $n$  to the denominator, so  $n = \frac{p+1}{2}$  is the first time this expression for  $P_{n,1}$  is possibly not  $p$ -integral.  $\square$

## 5. PROOF OF THEOREM 2

We first recall two classical Bernoulli number congruences (see [4], p. 233-238). Let  $D_n$  be the denominator of the  $n$ th Bernoulli number, written in lowest terms. The von Staudt-Clausen congruences state

$$(5.1) \quad D_n = 6 \prod_{(p_i-1)|n} p_i$$

where the  $p_i$ 's are prime. Let  $p \geq 5$  be prime. Now suppose  $m \geq 2$  is even and  $m' \equiv m \pmod{\phi(p^r)}$  where  $\phi$  is the Euler  $\phi$ -function. Then the Kummer congruences state

$$(5.2) \quad \frac{(1 - p^{m'-1})B_{m'}}{m'} \equiv \frac{(1 - p^{m-1})B_m}{m} \pmod{p^r}.$$

Using these congruences, we prove the following lemma.

**Lemma 9.** *For  $r \geq 1$ , the following  $q$ -series congruences hold.*

$$(5.3) \quad (E_{p-1}(z))^{p^{r-1}} \equiv 1 \pmod{p^r}$$

and

$$(5.4) \quad E_{\phi(p^r)+2}(z) \equiv E_2(z) \pmod{p^r}.$$

*Proof.* For (5.3), we have

$$(E_{p-1}(z))^{p^{r-1}} = \left(1 - \frac{2(p-1)}{B_{p-1}} \sum_{n=1}^{\infty} \sigma_{p-1}(n)q^n\right)^{p^{r-1}} = \left(1 - \frac{2(p-1)D_{p-1}}{U_{p-1}} \sum_{n=1}^{\infty} \sigma_{p-1}(n)q^n\right)^{p^{r-1}}$$

where  $U_{p-1}$  is an integer coprime to  $D_{p-1}$ . From (5.1) we have  $p|D_{p-1}$  which implies (5.3) after an application of the binomial theorem.

To prove (5.4), if we let  $m' = 2$ ,  $m = \phi(p^r) + 2$  in (5.2) and note that  $p^{\phi(p^r)+1} \equiv p \pmod{p^r}$  we obtain

$$\frac{B_2}{2} \equiv \frac{B_{\phi(p^r)+2}}{\phi(p^r)+2} \pmod{p^r}.$$

Also by Euler's theorem,

$$\sigma_1(n) \equiv \sigma_{\phi(p^r)+1}(n) \pmod{p^r}.$$

With these two observations we have

$$E_2(z) = 1 - \frac{2(2)}{B_2} \sum_{n=1}^{\infty} \sigma_1(n)q^n \equiv 1 - \frac{2(\phi(p^r)+2)}{B_{\phi(p^r)+2}} \sum_{n=1}^{\infty} \sigma_{\phi(p^r)+1}(n)q^n \pmod{p^r}.$$

□

*Proof of Theorem 2.* From Lemma 9,

$$(5.5) \quad \beta_{\psi}(p)\psi(j) \frac{E_2 E_4}{E_6} \equiv \beta_{\psi}(p)\psi(j) \frac{E_{\phi(p^r)+2} E_4}{(E_{p-1})^{p^{r-1}} E_6} \pmod{p^r}.$$

Note that the definition of  $\beta_{\psi}(p)$  and Lemma 9 imply that the left hand side of (5.5) is  $p$ -integral. The right hand side of (5.5) is a weight zero modular function; hence, it is a rational function in  $j(z)$ . By examining its zeros, we obtain

$$(5.6) \quad \beta_{\psi}(p)\psi(j) \frac{E_4 E_{\phi(p^r)+2}}{E_6 (E_{p-1})^{p^{r-1}}} = \beta_{\psi}(p)\psi(j) \frac{\tilde{F}(E_4 E_{\phi(p^r)+2}, j)}{\tilde{F}(E_6 (E_{p-1})^{p^{r-1}}, j)}.$$

This, together with (4.3), implies that

$$\beta_\psi(p)\psi(j) \frac{\tilde{F}(E_4 E_{\phi(p^r)+2}, j)}{\tilde{F}(E_6 (E_{p-1})^{p^{r-1}}, j)} = \frac{\beta_\psi(p) Q_{n,\psi}(j)}{\alpha_{n,\psi}(p) P_{n,\psi}(j)} + \mathcal{O}\left(\left(\frac{1}{j}\right)^{2n}\right).$$

□

## 6. EXAMPLES

In this section we carry out explicit numerical examples illustrating properties of  $\langle \cdot, \cdot \rangle_\psi$ , Proposition 3 and Theorem 1. Let us first compute  $\langle x, 1 \rangle_\psi$  for  $\psi = x^2 + 5$ . Proposition 3 allows us to forgo the computation of integrals. Using (2.3), we compute that

$$\begin{aligned} \langle x, 1 \rangle_\psi &= \mathbb{K}_q(j(j^2 + 5)E_2) \\ &= \mathbb{K}_q((q^{-1} + 744 + 196884q + 21493760q^2 + \dots) \\ &\quad (q^{-2} + 1488q^{-1} + 947309 + 335950912q + 72474624276q^2 + \dots)(E_2)) \\ &= \mathbb{K}_q((q^{-3} + 2232q^{-2} + 2251265q^{-1} + 1355205960 + \dots) \\ &\quad (1 - 24q - 72q^2 - 96q^3 + \dots)) \\ &= \mathbb{K}_q(q^{-3} + 2208q^{-2} + 2197625q^{-1} + 1301014800 + \dots) \\ &= 1301014800. \end{aligned}$$

This method is simpler than the integral methods, but the number of terms to which each power of  $j$  must be computed in a given polynomial depends upon the degrees of the other polynomials involved. Further, computing powers of  $j$  as a  $q$ -series can be computationally inefficient.

With this in mind, we investigate (2.4). First, we compute that

$$\frac{E_2 E_4}{E_6} = 1 + 720 \left(\frac{1}{j}\right) + 911520 \left(\frac{1}{j}\right)^2 + 1301011200 \left(\frac{1}{j}\right)^3 + \dots$$

Thus

$$\begin{aligned} \langle x, 1 \rangle_\psi &= \mathbb{K}_{\left(\frac{1}{j}\right)}\left(j(j^2 + 5) \frac{E_2 E_4}{E_6}\right) \\ &= \mathbb{K}_{\left(\frac{1}{j}\right)}\left(j(j^2 + 5) \left(1 + 720 \left(\frac{1}{j}\right) + 911520 \left(\frac{1}{j}\right)^2 + 1301011200 \left(\frac{1}{j}\right)^3 + \dots\right)\right) \\ &= \mathbb{K}_{\left(\frac{1}{j}\right)}\left(j^3 + 720j^2 + 911525j + 1301014800 + 1958046588000 \left(\frac{1}{j}\right) + \dots\right) \\ &= 1301014800, \end{aligned}$$

which is, of course, the same result as that obtained from the  $q$ -expansion method. This method benefits from the fact that the  $\left(\frac{1}{j}\right)$ -expansion of  $\frac{E_2 E_4}{E_6}$  only needs to be computed

once. All remaining computations are simple polynomial manipulations where  $j$  can be treated as an indeterminate.

Having found an efficient method for the computation of these bilinear forms, we now describe an efficient method of calculating  $\{P_{n,\psi}\}$  for arbitrary good  $\psi$ . If  $\psi$  is good, then the Gram-Schmidt process will find the orthogonal polynomials. However, we use the simpler three-term recurrence relation

$$(6.1) \quad P_{n+1,\psi} = \left( x - \frac{\langle xP_{n,\psi}, P_{n,\psi} \rangle_\psi}{\langle P_{n,\psi}, P_{n,\psi} \rangle_\psi} \right) P_{n,\psi} - \frac{\langle P_{n,\psi}, P_{n,\psi} \rangle_\psi}{\langle P_{n-1,\psi}, P_{n-1,\psi} \rangle_\psi} P_{n-1,\psi},$$

with

$$P_{0,\psi} = 1 \quad \text{and} \quad P_{1,\psi} = x - \frac{\langle x, 1 \rangle_\psi}{\langle 1, 1 \rangle_\psi}.$$

This relation produces monic orthogonal polynomials, as is easily verified. In particular, note that due to the orthogonality of the  $P_{n,\psi}$ 's and the properties of the bilinear form,

$$\langle xP_{n,\psi}, P_{k,\psi} \rangle_\psi = \langle P_{n,\psi}, P_{k+1,\psi} \rangle_\psi \quad \text{for } k < n.$$

We now consider some examples of  $\{P_{n,\psi}\}$  for various  $\psi$ . For  $\psi = 1$ , the case considered by Kaneko and Zagier in [5], we find that

$$\begin{aligned} P_{0,1} &= 1, \\ P_{1,1} &= x - 720, \\ P_{2,1} &= x^2 - 1640x + 269280, \\ P_{3,1} &= x^3 - \frac{12576}{5}x^2 + 1526958x - 107765856, \\ P_{4,1} &= x^4 - 3384x^3 + 3528552x^2 - 1133263680x + 44184000960, \end{aligned}$$

in agreement with their results.

We pause here to emphasize that, by Theorem 1, a particular polynomial may directly represent as many as four different supersingular loci simultaneously. It will also give information about other supersingular loci by containing them as factors. We illustrate this with our next example.

For  $\psi(x) = x^2 + 5$ , we find that

$$\begin{aligned} P_{0,\psi} &= 1, \\ P_{1,\psi} &= x - \frac{52040592}{36461}, \\ P_{2,\psi} &= x^2 - \frac{4485385228216}{1875639119}x + \frac{2372906709451872}{1875639119}, \\ P_{3,\psi} &= x^3 - \frac{7209571518891215424}{2186844089945375}x^2 \\ &\quad + \frac{7149306835701023004486}{2186844089945375}x - \frac{2002207481689175392607712}{2186844089945375}, \\ P_{4,\psi} &= x^4 - \frac{202095943002576143959552}{48310118130840919867}x^3 + \frac{290727007080443878631657898}{48310118130840919867}x^2 \\ &\quad - \frac{164148366533072105110296588864}{48310118130840919867}x + \frac{28580117310317180831101867891584}{48310118130840919867}. \end{aligned}$$

Factoring  $P_{3,\psi}$  over  $\mathbb{F}_p$  for  $p \in \{23, 29, 31, 37\}$ , we see that

$$\begin{aligned} P_{3,\psi} &\equiv x(x+4)(x+20) \pmod{23}, \\ P_{3,\psi} &\equiv x(x+4)(x+27) \pmod{29}, \\ P_{3,\psi} &\equiv (x+8)(x+27)(x+29) \pmod{31}, \\ P_{3,\psi} &\equiv (x+29)(x^2+31x+31) \pmod{37}. \end{aligned}$$

Further, while  $P_{3,\psi}$  is not 7-integral, we have that

$$7^2 P_{3,\psi} \equiv 5(x+5)(x+1) \pmod{7}.$$

Alternately, using Proposition 5, we may find the supersingular locus for  $p$  by computing  $F(E_{p-1}, x)$ . We thus compute that

$$\begin{aligned} \mathfrak{S}_{23}(x) &= x(x+4)(x+20), \\ \mathfrak{S}_{29}(x) &= x(x+4)(x+27), \\ \mathfrak{S}_{31}(x) &= (x+8)(x+27)(x+29), \\ \mathfrak{S}_{37}(x) &= (x+29)(x^2+31x+31), \\ \mathfrak{S}_7(x) &= x+1, \end{aligned}$$

which agrees with our main result. Thus,  $P_{3,\psi}$  is a lift of four different supersingular loci. It also contains as factors the lifts of the supersingular loci of all the primes from 5 to 19, once the issue of  $p$ -integrality is properly taken into account.

Both of the  $\psi$  above are good, as they have no zeros in the interval  $(0, 1728)$ . What are some examples of bad  $\psi$ ? A particular  $\psi$  is bad if and only if the Gram-Schmidt process fails, which happens exactly when there exists a  $P_{n,\psi}$  such that  $\langle P_{n,\psi}, P_{n,\psi} \rangle_\psi = 0$ . In this case,  $P_{n+1,\psi}$  does not exist. Thus, both  $x - 720$  and  $x^2 - 1266x$  are bad, as in both cases  $\langle 1, 1 \rangle_\psi = 0$ . Also,  $x - 820 + 4\sqrt{25195}$  is bad because, although  $\langle 1, 1 \rangle_\psi = -100 + 4\sqrt{25195}$ ,  $\langle P_{1,\psi}, P_{1,\psi} \rangle_\psi = 0$ . There are two natural questions: first, are there bad rational  $\psi$  such that  $\langle 1, 1 \rangle_\psi$  is non-zero? Second, are there real  $\psi$  which are bad, but for which both  $\langle 1, 1 \rangle_\psi$  and  $\langle P_{1,\psi}, P_{1,\psi} \rangle_\psi$  are non-zero? In fact, we were unable to find  $\psi$  which met either criterion.

#### ACKNOWLEDGEMENTS

The authors sincerely appreciate the opportunity provided by K. Ono and W. McGraw who organized the 2003 Research Experience for Undergraduates (REU) during which this research was conducted. J. Anderson, N. Boston, R. Chatterjee, G. Coogan, J. Lovejoy, J. Rouse, and K. Zuhr also deserve thanks for their lectures and assistance.

#### REFERENCES

- [1] S. Ahlgren, and K. Ono, *Weierstrass points on  $X_0(p)$  and supersingular  $j$ -invariants*, *Mathematische Annalen*, **325** (2003) 355-368.
- [2] G. Andrews, R. Askey, and R. Roy, *Special Functions*, Cambridge University Press, Cambridge, 1999.
- [3] J. Bruinier, W. Kohnen, and K. Ono, *The arithmetic of the values of modular functions and the divisors of modular forms*, *Compositio Math.*, to appear.
- [4] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer Verlag, 1991.
- [5] 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), 97-126.
- [6] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Springer-Verlag, New York, 1993.

- [7] J. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1986.

DEPARTMENT OF MATHEMATICS, SANTA CLARA UNIVERSITY, SANTA CLARA, CA 95053  
*E-mail address:* sbasha@scu.edu

4404 SOUTH AVE. W, MISSOULA, MT 59804  
*E-mail address:* getz@fas.harvard.edu

DEPARTMENT OF MATHEMATICS, CALIFORNIA INSTITUTE OF TECHNOLOGY, PASADENA, CA 91125  
*E-mail address:* nover@its.caltech.edu

5849 SAND RD, BELLINGHAM, WA 98226  
*E-mail address:* emmas@mit.edu