# ALGEBRAIC PROPERTIES OF KANEKO-ZAGIER LIFTS OF SUPERSINGULAR POLYNOMIALS

JOHN CULLINAN, FARSHID HAJIR

Abstract. The supersingular polynomial $\mathfrak{S}_\ell(x) \in \mathbf{F}_\ell[x]$ has many well-studied lifts to $\mathbf{Q}[x]$. Among these is one introduced by Kaneko and Zagier, which, when interpreted as a specialized Jacobi polynomial, is seen to coincide with a lift discovered by Brillhart and Morton a few years later. The algebraic properties of this family of lifts of $\mathfrak{S}_\ell(x)$ are not well-understood. We focus on a conjecture of Mahlburg and Ono regarding the maximality of their Galois groups (when shorn of their trivial linear factors), and also establish their irreducibility in some previously unknown cases.

## 1. Introduction

1.1. **Background and Notation.** Consider a positive integer $\ell \geq 5$ coprime to 6. Let $n, e$ be the quotient and remainder, respectively, of $\ell/12$, i.e. $\ell = 12n + e$ with $e \in \{1, 5, 7, 11\}$ and $n \geq 0$. We also write $k = \ell - 1 = 12n + r$ where $r = e - 1$ belongs to $\{0, 4, 6, 10\}$. We note that $k$ is even and not congruent to 2 mod 3. There is a unique pair $(\lambda, \mu) \in \{\pm 1\} \times \{\pm 1\}$ such that $e - 6 = 2\lambda + 3\mu$. Similarly, there is a unique pair $(\delta, \epsilon) \in \{0, 1\} \times \{0, 1\}$ such that $r = 4\delta + 6\epsilon$. They are related by $(\lambda, \mu) = (2\delta - 1, 2\epsilon - 1)$. We use this notation throughout without further comment.

If $\ell$ is a prime number, we can define the *supersingular polynomial* $\mathfrak{S}_\ell \in \overline{\mathbf{F}}_\ell[j]$ in a single variable, $j$, by

$$\mathfrak{S}_\ell(j) = \prod_{j'} (j - j')$$

where $j'$ runs over all the $j$-invariants of supersingular elliptic curves in $\overline{\mathbf{F}}_\ell$. We recall some well-known facts about $\mathfrak{S}_\ell(j)$: it lies in $\mathbf{F}_\ell[j]$, has degree $n + \delta + \epsilon$, and is divisible by $j^\delta (j - 1728)^\epsilon$. There is therefore a well-defined polynomial $\mathfrak{s}_\ell \in \mathbf{F}_\ell[j]$ of degree $n$ satisfying

$$\mathfrak{S}_\ell(j) = j^\delta (j - 1728)^\epsilon \mathfrak{s}_\ell(j).$$

In their beautiful and influential paper [9], Kaneko and Zagier describe a number of natural lifts of $\mathfrak{s}_\ell$ from $\mathbf{F}_\ell$ to $\mathbf{Q}$ coming from the theory of elliptic modular forms. These include lifts due to Hasse-Deuring, Deligne, and Atkin as well as one due to Kaneko and Zagier, denoted $\widetilde{F}_k(j)$. In [9] the authors focus on the connection to modular forms, hence the emphasis on $k = 12n + r$ as the index of the polynomial, as opposed to $\ell = k + 1$, or the degree of the polynomial, namely $n = (k - r)/12$. We recall that the space $M_k$ of weight $k$ holomorphic modular forms on $\mathrm{PSL}_2(\mathbf{Z})$ has dimension $n + 1$.

1.2. **The Kaneko-Zagier polynomial.** To define the Kaneko-Zagier polynomial, let $j(z), \Delta(z), E_m(z)$ denote the classical $j$-function, discriminant form, and normalized weight $m$ Eisentein series, respectively. Every element $f(z)$ of $M_k$ has an expression of the form

$$f(z) = \Delta(z)^n E_4(z)^\delta E_6(z)^\epsilon \widetilde{f}((j(z)),$$

for a unique polynomial $\widetilde{f}(j)$ of degree at most $n$, the coefficient of $j^n$ in $\widetilde{f}(j)$ being equal to the constant coefficient in the Fourier expansion of $f$. In [9], the authors give four different choices of $f(z)$ for which $\widetilde{f}(j)$ is a lift of $\mathfrak{s}_\ell(j)$. The easiest to describe is $f = E_{\ell-1}$, the normalized weight $\ell - 1$ Eisenstein series. Another

2010 *Mathematics Subject Classification.* 11R32, 11R09, 33C45.

*Key words and phrases.* Kaneko-Zagier polynomials, Galois group, Hardy-Littlewood conjectures.

choice due to Kaneko-Zagier, which will be our focus here, is for a certain modular form $F_k$ we now describe. Let $\theta_k$ be the differential operator on $M_k$ defined by

$$\theta_k f(z) = q\frac{d}{dq}f(z) - \frac{k}{12}E_2(z)f(z),$$

where, as usual, $q = e^{2\pi iz}$ and $E_2 = \Delta'/\Delta$. There is a unique normalized form $F_k(z) \in M_k$ satisfying

$$\theta_{k+2}\theta_k F_k(z) - \frac{k(k+2)}{144}E_4(z)F_k(z) = 0.$$

As we will see shortly, the corresponding Kaneko-Zagier polynomial $\widetilde{F}_k(j)$ lies in $\mathbf{Q}[j]$ and has degree $n$. It is shown in [9] that, when $\ell$ is prime, $\widetilde{F}_{\ell-1}(j)$ and $\widetilde{E}_{\ell-1}(j)$ have $\ell$-integral coefficients and satisfy

$$\widetilde{E}_{\ell-1}(j) \equiv \widetilde{F}_{\ell-1}(j) \equiv \mathfrak{s}_\ell(j) \mod \ell.$$

As we will see in §2, the second congruence was independently derived by Brillhart and Morton [1].

1.3. **Algebraic Properties.** The study of algebraic properties of $\widetilde{F}_k(j)$ was initiated by Mahlburg and Ono in [10], in which they put forward the following conjecture (in analogy with a similar expectation for the lift $\widetilde{E}_{\ell-1}(j)$ of $\mathfrak{s}_\ell(j)$).

**Conjecture 1.4** (Mahlburg-Ono)**.** *With notation as in the opening paragraph, for each $\ell \geq 5$ coprime to 6, the Kaneko-Zagier polynomial $\widetilde{F}_{\ell-1}(j)$ is irreducible and has Galois group $S_n$ over $\mathbf{Q}$.*

Mahlburg and Ono give several infinite families of integers $k$ for which $\widetilde{F}_k$ is irreducible and they also check for most of those particular families that the discriminant is not a square. We extend their results here in several directions. The main results of this paper can be summarized as follows.

**Theorem 1.5.** *For $\ell \geq 5$ coprime to 6, the discriminant of $\widetilde{F}_{\ell-1}(x)$ is not a square in $\mathbf{Q}$.*

**Theorem 1.6.** *Suppose $\widetilde{F}_{\ell-1}(x)$ is irreducible over $\mathbf{Q}$. If $\ell$ can be expressed as $\ell = p + 6q$ where $p$ and $q$ are primes and $n/2 < q < n-2$, then the Galois group of $\widetilde{F}_{\ell-1}(x)$ is $S_n$.*

**Remark 1.7.** As we will explain later, according to standard conjectures in analytic number theory about the distribution of primes, every large enough integer $\ell$ coprime to 6 is expected to have one (and indeed many) expressions as $p+6q$ with the $q$ in the specified range. Thus, Theorem 1.6 reduces the Mahlburg-Ono conjecture to expected properties of prime distributions. Though the latter are far out of reach at present, Theorem 1.6 does nevertheless provide a highly effective and speedy numerical criterion for checking the Mahlburg-Ono conjecture for any given $\ell$: namely, starting with the smallest prime exceeding $n/2$ and going up, we look for a prime $q$ such that $\ell - 6q$ is also prime. Any such pair, together with a verification of the irreducibility of $\widetilde{F}_{\ell-1}(x)$, constitutes a "certificate" that this polynomial has Galois group $S_n$. This method allows us to verify the "Galois part" of the Mahlburg-Ono conjecture for $\ell$ up to a billion.

**Theorem 1.8.** *For $\ell \leq 10^9$ coprime to 6, if $\widetilde{F}_{\ell-1}(x)$ is irreducible, then its Galois group is $S_n$.*

While our focus is mostly on the Galois group in this paper, we do have the following result on irreducibility of Kaneko-Zagier polynomials, which is a complement to Theorem 1.1 in Mahlburg-Ono [10].

**Theorem 1.9.** *If $\ell$ is of one the forms $6\cdot 4^\nu+1, 6\cdot 4^\nu-5, 3\cdot 4^\nu+5,$ or $3\cdot 4^\nu-1$, then $\widetilde{F}_{\ell-1}(x)$ is irreducible over $\mathbf{Q}$.*

## 2. The Kaneko-Zagier Polynomial as a Specialized Jacobi Polynomial

2.1. **Relation to the Brillhart-Morton polynomial.** Our starting point is an explicit expression for $\widetilde{F}_k(j)$ as a hypergeometric polynomial given by Kaneko and Zagier. To describe this explicit form, recall that the ${}_2F_1$ Gauss hypergeometric function is defined by

$${}_2F_1\left[\begin{matrix} a & b \\ & c \end{matrix}; x\right] \overset{\text{def}}{=} \sum_{\nu=0}^{\infty} \frac{(a)_\nu (b)_\nu}{(c)_\nu}\frac{x^\nu}{\nu!},$$

where $(\cdot)_\nu$ is the Pochhammer symbol, given by $(a)_\nu = a(a-1)(a-2)\dots(a-\nu+1)$. Kaneko and Zagier [9] show (in their Theorem 5.ii applied with the involution $\sigma$ that swaps 0 and $\infty$) that

$$\widetilde{F}_k(j) = 1728^n \binom{n+\lambda/3}{n} \times {}_2F_1\left[\begin{matrix}-n & n+e/6\\ & 1+\lambda/3\end{matrix}; \frac{j}{1728}\right], \tag{1}$$

where we recall the notation is as in the opening paragraph of the introduction. As was pointed out by Kaneko and Zagier, see the last paragraph of §8 in [9], the expression (1) essentially identifies $\widetilde{F}_k(x)$ as a Jacobi Polynomial. To make this explicit, we recall that the *Jacobi Polynomial* with characteristics $(\alpha, \beta)$ can be defined as the following hypergeometric polynomial:

$$P_n^{(\alpha,\beta)}(x) = \frac{(\alpha+1)_n}{n!}\,{}_2F_1\left[\begin{matrix}-n & 1+\alpha+\beta+n\\ & 1+\alpha\end{matrix}; \frac{1-x}{2}\right], \tag{2}$$

see [13]. With the choice $(\alpha, \beta) = (\lambda/3, \mu/2)$, we find $1 + \alpha + \beta = e/6$ and setting $x = 1 - j/864$ in (2), (1) simplifies to become

$$\widetilde{F}_k(j) = 1728^n P_n^{(\lambda/3,\mu/2)}\left(1 - \frac{j}{864}\right). \tag{3}$$

We should point out that the right hand side of (3) is precisely the polynomial denoted $J_\ell(j)$ in [1]; thus, the Brillhart-Morton polynomial $J_\ell$ actually coincides with the Kaneko-Zagier polynomial $\widetilde{F}_{\ell-1}$. Brillhart and Morton (see [1, Theorem 3]) give an independent proof that $J_\ell(j)$ is a lift of $\mathfrak{s}_\ell(j)$.

2.2. **Shifted Jacobi Polynomials.** For convenience we switch from the variable $j$ to the more conventional $x$ for our polynomials. The expression (2) for $P_n^{(\alpha,\beta)}(x)$ shows that when expanded in powers of $(1-x)$, the coefficients of this polynomial are explicit and highly factored. It is remarkable that the same is true for its coefficients in powers of $x$. Indeed, if we define

$$J_n^{(\alpha,\beta)}(x) \stackrel{\text{def}}{=} P_n^{(\alpha,\beta)}(2x+1),$$

we have the nice expansion, [13]

$$J_n^{(\alpha,\beta)}(x) = \sum_{j=0}^{n} \binom{n+\alpha}{n-j}\binom{n+\alpha+\beta+j}{j} x^j.$$

This same shift was useful (for Jacobi polynomials with characteristics $(\alpha, \beta) = (\pm 1/2, 0)$) for studying the algebraic properties of Legendre polynomials in [4].

**Definition 2.3.** For any integer $\ell \geq 5$ coprime to 6, if we write $\ell = 12n + 3\mu + 2\lambda + 6$ where $n \geq 0$ and $\lambda, \mu \in \{\pm 1\}$, we define

$$\mathfrak{K}_\ell(x) = K_n^{(\lambda,\mu)}(x) \stackrel{\text{def}}{=} 3^n n! J_n^{(\lambda/3,\mu/2)}(2x) = \sum_{j=0}^{n} \binom{n}{j} \left[\prod_{k=j+1}^{n}(\lambda + 3k) \prod_{k=1}^{j}(6n + 3\mu + 2\lambda + 6k)\right] x^j.$$

We can now state the expression of $\widetilde{F}_k(x)$ in terms of the polynomial we have just introduced.

**Lemma 2.4.** *For any integer $\ell \geq 5$ coprime to 6, if we write $\ell = 12n+3\mu+2\lambda+6$ where $n \geq 0$, $\lambda, \mu \in \{\pm 1\}$, we have*

$$\widetilde{F}_{\ell-1}(x) = \frac{576^n}{n!}\mathfrak{K}_\ell\left(\frac{-x}{2 \times 1728}\right).$$

*In particular, $\mathfrak{K}_\ell(x)$ and the Kaneko-Zagier polynomial $\widetilde{F}_{\ell-1}(x)$ share the same irreducibility and Galois properties.*

*Proof.* The formula follows immediately from (3) and the definitions of $P_n^{(\alpha\beta)}(x)$, $J_n^{(\alpha,\beta)}(x)$ and $\mathfrak{K}_\ell(x)$. □

In light of Lemma 2.4, the factorization and Galois properties of the Kaneko-Zagier polynomial $\widetilde{F}_{\ell-1}(x)$ exactly mirror those of the polynomial $\mathfrak{K}_\ell(x)$, and from now on we will work with $\mathfrak{K}_\ell(x)$ instead. The rationale for introducing $\mathfrak{K}_\ell(x)$ is that it has been scaled to have coefficients in $\mathbf{Z}$, making it a bit easier to compute its Newton Polygons at well-chosen primes. The shape of those Newton Polygons can then be used to prove algebraic facts about $\mathfrak{K}_\ell(x)$.

The layout of the paper is as follows. First, we give a criterion for an arbitrary specialization of the Jacobi polynomial $P_n^{(\alpha,\beta)}(x)$ to have a non-square discriminant and then show that this criterion applies to $K_n^{(\lambda,\mu)}(x)$ for all $n, \lambda, \mu$. We then move on to an investigation of the Newton Polygons of the $\mathfrak{K}_\ell(x)$ at large primes. The idea is that if we have a decomposition $\ell = 12n + e = p + 6q$, where $p$ is a prime and $1 \le q \le n$, then the $p$-adic Newton polygon of $\mathfrak{K}_\ell(x)$ will have a slope $1/q$ segment. The Galois group of this polynomial will then have a $q$-cycle; if $q > n/2$, a theorem of Jordan will then imply that the Galois group contains $A_n$, hence is $S_n$ by our result on the discriminant. Finally, we conclude with some new cases of irreducibility of the $\mathfrak{K}_\ell(x)$ in the final section.

## 3. Discriminant Formulæ

In this section we prove a general result on the discriminants of Jacobi polynomials and then employ similar techniques as in [5] to show that for all $n$ and all choices of $\lambda$ and $\mu$, the discriminant of $K_n^{(\lambda,\mu)}(x)$ is not a rational square. Fix $\alpha, \beta \in \mathbf{Q}$ and recall

$$P_n^{(\alpha,\beta)}(x) = \sum_{j=0}^{n} \binom{n+\alpha}{n-j} \binom{n+\alpha+\beta+j}{j} \left(\frac{x-1}{2}\right)^j,$$

which was our motivation for defining $J_n^{(\alpha,\beta)}(x) \stackrel{\text{def}}{=} P_n^{(\alpha,\beta)}(2x+1)$. It is well-known [13, thm. 6.71] that the discriminant of the Jacobi polynomial is given by

$$\operatorname{disc} P_n^{(\alpha,\beta)}(x) = 2^{-n(n-1)} \prod_{k=1}^{n} k^{k-2n+2}(k+\alpha)^{k-1}(k+\beta)^{k-1}(k+n+\alpha+\beta)^{n-k}. \tag{4}$$

Moreover, the discriminant of a general polynomial of degree $n$ satisfies the transformation laws:

$$\operatorname{disc}(\nu f(\kappa x + \gamma)) = \left(\nu^2 \kappa^n\right)^{n-1} \operatorname{disc}(f(x)). \tag{5}$$

For parameters $u, v, t, w$ with $u$ and $v$ non-zero, we define the following polynomial in $\mathbf{Z}[x]$:

$$\mathscr{J}_n(u,v,t,w;x) \stackrel{\text{def}}{=} n!u^n J_n^{(t/u,w/v)}(vx) = \sum_{j=0}^{n} \binom{n}{j} \prod_{k=j+1}^{n} (t+uk) \prod_{k=1}^{j} (tv+uw+(k+n)uv) x^j.$$

Note that for $\ell = 12n + 2\lambda + 3\mu + 6$, with $\lambda, \mu \in \{\pm 1\}$, we have $\mathfrak{K}_\ell(x) = \mathscr{J}_n(3,2,\lambda,\mu;x)$.

**Proposition 3.1.** *The discriminant of $\mathscr{J}_n(u,v,t,w;x)$ is given by the following formula:*

$$\operatorname{disc} \mathscr{J}_n(u,v,t,w;x) = u^{n(n-1)} \prod_{k=1}^{n} k^k (uk+t)^{k-1}(vk+w)^{k-1}(uv(n+k)+vt+uw)^{n-k}.$$

*Proof.* Since we already have a formula for the discriminant of $P_n$, we apply (5) a few times in order to relate the discriminant of $\mathscr{J}_n$ to that of $P_n$, as follows:

$$\begin{aligned}
\operatorname{disc} \mathscr{J}_n(u,v,t,w;x) &= \operatorname{disc} n!u^n J_n^{(t/u,w/v)}(vx) \\
&= \left((n!u^n)^2 v^n\right)^{n-1} \operatorname{disc} J_n^{(t/u,w/v)}(x) \\
&= \left((n!u^n)^2 v^n\right)^{n-1} \operatorname{disc} P_n^{(t/u,w/v)}(2x+1) \\
&= \left((n!u^n)^2 v^n\right)^{n-1} \operatorname{disc} P_n^{(t/u,w/v)}(2x) \\
&= \left((n!u^n)^2 v^n\right)^{n-1} 2^{n(n-1)} \operatorname{disc} P_n^{(t/u,w/v)}(x).
\end{aligned}$$

When we apply (4) to the last equation, several simplifications occur and we have:

$$\begin{aligned}
\operatorname{disc} \mathscr{J}_n(u,v,t,w;x) &= \left((n!u^n)^2 v^n\right)^{n-1} \prod_{k=1}^{n} k^{k-2n+2}(k+t/u)^{k-1}(k+w/v)^{k-1}(n+k+t/u+w/v)^{n-k} \\
&= u^{n(n-1)} \prod_{k=1}^{n} k^k (uk+t)^{k-1}(vk+w)^{k-1}(uv(n+k)+vt+uw)^{n-k},
\end{aligned}$$

as claimed. ☐

**Proposition 3.2.** *Let $u, v, t, w \in \mathbf{Z}$. Suppose $u, v \geq 2$, $\gcd(uv, tv + uw) = 1$, and $uv + vt + uw$ is odd. Then there exists $N \in \mathbf{Z}$ such that for all $n \geq N$, $\operatorname{disc} \mathscr{J}_n(u, v, t, w; x)$ is not a square in $\mathbf{Q}^\times$.*

*Proof.* Let us explain the strategy of the proof. From the formula of the preceding Proposition, we separate out two factors of $\operatorname{disc} \mathscr{J}_n(u, v, t, w; x) = AB$ as follows:

$$A = u^{n(n-1)} \prod_{k=1}^{n} k^k [(uk + t)(vk + w)]^{k-1}, \qquad B = \prod_{k=1}^{n} (uv(n + k) + vt + uw)^{n-k}.$$

If we can show that there exists an integer $k_0 \in [1, n]$ such that

(1) $p = uv(n + k_0) + uw + vt$ is prime, and
(2) $n - k_0$ is odd, and
(3) $p$ does not divide $A$,

then it will follow that $\operatorname{disc} \mathscr{J}_n$ is not a rational square, since the $p$-valuation of $\operatorname{disc} \mathscr{J}_n(u, v, t, w; x)$ would then clearly be odd.

To ease the notation, let $x = uv(n + 1) + vt + uw$, and $y = uv(2n) + vt + uw$. One checks easily that to satisfy conditions (1) and (2) above is to find a prime $p$ in $[x, y]$ in the congruence class $uv + vt + uw \bmod 2uv$.

The main result of [12] can be adapted to show that if $k, m$ are coprime integers, and $0 < \delta < 1$ is a real number, the interval $[x, (1 + \delta)x]$ contains a prime $p \equiv m \mod k$ once $x$ surpasses a bound depending only on $k, m$ and $\delta$. It's easy to see that for any fixed $\delta \in \mathbf{R}$ with $0 < \delta < 1$, there exists $N_0$ such that $[x, y] \subseteq [x, (1 + \delta)x]$ for all $n \geq N_0$. Indeed, the latter inclusion is equivalent to the inequality $\delta x \leq (n - 1)uv$, since the interval $[x, y]$ has length $(n - 1)uv$, so to be completely explicit, we can take $N_0 = (1 - \delta)^{-1}(2 + t/u + w/v) - t/u - w/v$. Restricting to $n \geq N_0$, we now want to show that $[x, (1 + \delta)x]$ contains a prime in the congruence class $uv + vt + uw \bmod 2uv$.

By [12], there exists $x_0$ so that for all $x \geq x_0$, $[x, (1 + \delta)x]$ contains a prime in every admissible congruence class modulo $2uv$. Let

$$N = \max\left\{ \frac{x_0 - tv - uw}{uv}, \frac{|t| - vt - uw}{u}, \frac{|w| - vt - uw}{v}, N_0 \right\}.$$

By construction, for $n \geq N$ the interval $[uv(n + 1) + vt + uw, 2n + vt + uw]$ is guaranteed to contain a prime $p$ of the form $uv(n + k_0) + tv + uw$ with $n - k_0$ odd, so that $\operatorname{ord}_p(B) = n - k_0$ is odd. On the other hand, the fact that $n \geq N \geq \max((|t| - vt - uw)/u, (|w| - vt - uw)/v)$ ensures that $p > \max(nu + |t|, nv + |w|)$, hence $\operatorname{ord}_p(A) = 0$. Thus, we have found a prime $p$ for which

$$\operatorname{ord}_p \operatorname{disc} \mathscr{J}_n(u, v, t, w; x) = n - k_0,$$

is odd, and hence $\operatorname{disc} \mathscr{J}_n$ is not a rational square. ☐

**Remark 3.3.** In order for an integer of the form $uv(n + k) + vt + uw$ to be prime, it is necessary that $\gcd(uv, tv + uw) = 1$, and it is easy to find examples of irreducible $\mathscr{J}_n$ with square discriminant when $\gcd(uv, tv + uw) \neq 1$, *e.g.* $\mathscr{J}_3(2, 2, 71, 7; x)$.

We illustrate all of this as it pertains to the $\mathfrak{K}_\ell(x)$.

**Corollary 3.4.** *For $\ell = 12n + 2\lambda + 3\mu + 6$, where $\lambda, \mu \in \{\pm 1\}$ and $n \geq 1$, the discriminant of $\mathfrak{K}_\ell(x)$ satisfies*

$$\operatorname{disc} \mathfrak{K}_\ell(x) = \operatorname{disc} K_n^{(\lambda,\mu)}(x) = 3^{n^2 - n} \prod_{k=1}^{n} k^k (3k + \lambda)^{k-1} (2k + \mu)^{k-1} (6k + 6n + 2\lambda + 3\mu)^{n-k},$$

*and it is not a square in $\mathbf{Q}^\times$.*

*Proof.* Applying Proposition 3.1, we immediately obtain the discriminant formula, which was also derived (up to change in notation) by Mahlburg and Ono in [10]. The claim that this discriminant is not a square for large enough $n$ follows immediately from Proposition 3.2, because the parameters $u = 3$, $v = 2$, $t = \lambda$, $w = \mu$ satisfy its two conditions, namely $\gcd(uv, tv + uw) = \gcd(6, 2\lambda + 3\mu) = \gcd(6, e - 6) = 1$ and $uv + tv + uw = e$ is co-prime to 6 by assumption and in particular is odd. Since we want to verify this for all $n$ and not just $n$ large enough, we need an explicit value for the bound $N$ in the proof of Proposition 3.2. In the notation of that proof, we choose $\delta = 0.9$ so that we can take $N_0 = 27$. It's then easy to see that Proposition 3.2 applies with bound $N = x_0/6$ as long as $x_0$ is large enough to guaranteed that for all $x > x_0$, the interval $[x, 1.9x]$ contains a prime in every admissible congruence class modulo 12. We now explain why we can take $x_0 = 480$.

In [5] it was shown that if $x \geq 10^{10}$ then the interval $[x, 1.048x)$ contains a prime in every congruence class modulo 12, hence the same is true for intervals of the form $[x, 1.9x]$. For $x \leq 10^{10}$ we apply a similar argument to the one in [5], though with a slightly different parameter (in the notation of that paper, $\epsilon = 0.3$). Using that argument, it follows that the interval $[x, 1.9x]$ contains a prime in every congruence class modulo 12 once

$$x > \left(\frac{2.072(1+\sqrt{1.9})\cdot 4}{0.9}\right)^2 \simeq 479.7.$$

For small values of $n$, it is easily checked in Pari that disc $K_n^{\lambda,\mu}(x)$ is not a square in $\mathbf{Q}$ for all four choices of signs $\lambda, \mu$, completing the proof. □

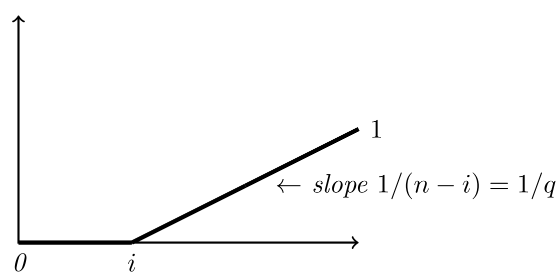
**Corollary 3.5.** *If $\mathfrak{K}_\ell(x)$ is irreducible over $\mathbf{Q}$, then its Galois group is not contained in $A_n$.*

**Remark 3.6.** In [10] it was already shown (in the slightly different notation explained in the introduction) that for many values of $\ell$ the discriminant of $\mathfrak{K}_\ell(x)$ is not a square. Corollary 3.4 establishes this for all values of $\ell$.

## 4. Newton Polygons at Large Primes

In [10], Mahlburg and Ono identified several special families of integers $k$ for which $\widetilde{F}_k(x)$ is an Eisenstein polynomial at some prime $p$. Another way of saying that a polynomial $f$ of degree $n$ is Eisenstein at $p$ is that its $p$-adic Newton polygon $\mathrm{NP}_p(f)$ is pure of slope $\pm 1/n$. In this section, we (mostly) set aside the question of irreducibility and, for the purposes of showing the Galois group is large, look for primes $p$ at which the Newton polygon of $\mathfrak{K}_\ell(x)$ is not quite pure, but close to it. It turns out such primes are in plentiful supply, as we now demonstrate.

**Proposition 4.1.** *Suppose the positive integer $\ell$ is coprime to 6 and write $\ell = 12n + e$ with $n \geq 0$ and $e = 2\lambda + 3\mu + 6 \in \{1, 5, 7, 11\}$ with $\lambda, \mu \in \{\pm 1\}$. For every prime $p \in [\ell - 6n, \ell - 6]$, satisfying $p \equiv e \bmod 6$, let $q = (\ell - p)/6$. Note that $q$ is an integer in the interval $[1, n]$. Then, the $p$-adic Newton polygon of $\mathfrak{K}_\ell(x)$ consists of a slope 0 segment of length $n - q$ and a slope $1/q$ segment of length $q$. In other words, if $p = 6n + 6i + e$ is prime with $0 \leq i \leq n - 1$, so that $i = n - q$, then the $p$-adic Newton polygon of $\mathfrak{K}_\ell(x)$ has the following shape:*




*Proof.* The proof follows easily from the explicit form of the coefficients, namely $\mathfrak{K}_\ell(x) = \sum_{j=0}^n a_j x^j$ with

$$a_j = \binom{n}{j} \underbrace{\prod_{k=j+1}^{n} (3k+\lambda)}_{A_j} \underbrace{\prod_{k=1}^{j} (6n + 6k + e - 6)}_{B_j},$$

where we remind the reader that we write $e = 6 + 2\lambda + 3\mu$. Let $p$ be a prime in $[\ell - 6n, \ell - 6]$ satisfying $p \equiv e \bmod 6$. There is a unique $i$ in $[0, n-1]$ such that $p = 6n + 6i + e - 6$, and we have $n - i = (\ell - p)/6 = q$.

Since $p \geq 6n+e-6 \geq 6n-5$, $\mathrm{ord}_p \binom{n}{j} = \mathrm{ord}_p A_j = 0$ for all $j$. Moreover, $2p > 12n+e-6$, hence

$$\mathrm{ord}_p(a_j) = \mathrm{ord}_p(B_j) = \begin{cases} 0 & \text{if } 0 \leq j \leq i \\ 1 & \text{if } i+1 \leq j \leq n. \end{cases}$$

Hence, the $p$-adic Newton polygon of $\mathfrak{K}_\ell(x)$ is as claimed. ☐

We note that since $\ell - 6n \approx \ell/2$, primes $p$ to which the previous proposition applies (namely the prime congruent to $e \mod 6$ in $[\ell-6n, \ell]$) are in plentiful supply. Indeed, by Dirichlet's theorem, their number is asymptotic to $\frac{\ell}{4\log \ell}$. Since the Newton polygon of a product of polynomials is the Minkowski sum [6, §8.3] of the Newton polygon of the factors, Proposition 4.1 places restrictions on the degrees of possible factors of $\mathfrak{K}_\ell(x)$.

**Corollary 4.2.** *We have:*

1. *Let $\ell = 12n+e$ with $e \in \{1,5,7,11\}$ and let $p \equiv e \mod 6$ be a prime in $[\ell-6n, \ell-6]$; put $q = (\ell-p)/6$. If $g(x) \in \mathbf{Q}[x]$ is a degree $d \geq n/2$ divisor of $\mathfrak{K}_\ell(x)$, then $\deg g(x) \geq q$.*
2. *If $p \geq 13$ is a prime and $e$ is the remainder of $p \div 12$, then $\mathfrak{K}_{2p-e}(x)$ is irreducible.*

*Proof.* In light of Dumas' Lemma (see, for example [3, Corollary 2.7]), the first claim is immediate from the Proposition. For the second claim, let us write $p = 6n+e$ and set $\ell = 2p-e = 12n+e$. Since $p = \ell - 6n$, we can either apply part (1) of the Corollary to show that $\mathfrak{K}_\ell(x)$ is irreducible or use Proposition 4.1 itself to show directly that $\mathfrak{K}_\ell(x)$ is Eisenstein at $p$, hence irreducible. ☐

**Remark 4.3.** Part (2) of Corollary 4.2 simply reaffirms some cases of Theorem 1.1 in Mahlburg-Ono [10], namely those referring to cases 1,4,7, and 14 in their theorem.

For the application to the Galois group, we recall the following facts.

**Theorem 4.4.** *Let $f(x) \in \mathbf{Z}[x]$ be an irreducible polynomial of degree $n$ and $p$ a prime. Let $G$ be the Galois group over $\mathbf{Q}$ of $f(x)$. Suppose the $p$-adic Newton polygon of $f(x)$ has a segment of slope $r/s$ written in reduced form, i.e. $r, s$ are co-prime integers. Then*

1. *$s$ divides $|G|$.*
2. *If $s$ is a prime in the range $n/2 < s < n-2$, then $G = A_n$ in the case $\mathrm{disc}(f)$ is a square and $G = S_n$ otherwise.*

*Proof.* The first result is a basic fact about Newton polygons: briefly, since the $p$-adic valuation of a root $\alpha$ of $f$ is $r/s$, $s$ divides a ramification index in $\mathbf{Q}(\alpha)/\mathbf{Q}$ and hence it divides $|G|$; for more details, see e.g. [7]. The second result is Jordan's criterion [14]: a transitive subgroup of $S_n$ containing a cycle of prime length $s$ with $n/2 < s < n-2$ contains $A_n$. ☐

We can now state the main theorem of this section.

**Theorem 4.5.** *Suppose $\ell = 12n+e$ with $e \in \{1,5,7,11\}$. Assume $\mathfrak{K}_\ell(x)$ is irreducible over $\mathbf{Q}$ and let $G$ be its Galois group. Then,*

1. *For every prime $p \in [6n+e, 12n+e]$ satisfying $p \equiv e \pmod 6$, $q = (\ell-p)/6$ divides $|G|$.*
2. *If $\ell = p+6q$ and $p, q$ are primes satisfying either of the equivalent conditions (i) $q \in (n/2, n-2)$ or (ii) $p \in (6n+12+e, 9n+e)$, then $G = S_n$.*

*Proof.* We simply apply Theorem 4.4 to Proposition 4.1 and Corollary 3.4 ☐

**Remark 4.6.** Theorem 4.5 gives an effective criterion for checking the Galois part of the Mahlburg-Ono conjecture for any given $\ell$. After checking irreducibility of $\mathfrak{K}_\ell(x)$, a much shorter computation to find a suitable prime pair $(p,q)$ satisfying condition (2) of the theorem would run over the primes $q > n/2$, testing each time whether $p = \ell - 6q$ is prime. Assuming such a prime pair $(p,q)$ is found with $q < n-2$, it is in essence a certificate that $G = S_n$. We used GP-Pari [11] to carry out this procedure for finding such prime pairs for all $\ell$ coprime to 6 in the range $(551, 10^9)$. We did not check irreducibility of the polynomials in this entire range but for the smaller range $1 \leq \ell \leq 10^5$, we checked the irreducibility of $\mathfrak{K}_\ell(x)$ in Magma [2]. For those $\ell \leq 551$ coprime to 6 which do not admit a decomposition $\ell = p+6q$ with $q \in (n/2, n-2)$, we verified that $G = S_n$ in MAGMA. Thus, we have fully checked the Mahlburg-Ono conjecture for all $\ell$ coprime to 6 in the range $[1, 10^5]$.

We now explain why, in addition to being a numerical criterion for checking the Mahlburg-Ono conjecture, Theorem 4.5 provides heuristic evidence for it as well. In their celebrated series of papers on the *Partitio Numerorum*, Hardy and Littlewood present conjectures for the distribution of primes in a number of arithmetic contexts. For example, fixing positive integers $a$ and $b$, they estimate the asymptotics of the number of ways of expressing a large integer $\ell$ as $ap+bq$ with $p, q$ prime. Let us write $\mathscr{N}(\ell)$ for the number of prime pairs $(p, q)$ such that $\ell = p + 6q$. For simplicity, we focus on the case where $\ell$ is prime but this is just to simplify the formula a little. Conjecture C from [8] predicts that for large primes $\ell$,

$$\mathscr{N}(\ell) \sim \frac{2C_2}{3}\frac{\ell-1}{\ell-2}\frac{\ell}{(\log \ell)^2}, \qquad \text{where } C_2 := \prod_{\text{primes } r\geq 3}\left(1-\frac{1}{(r-1)^2}\right) \approx 0.6601618\ldots.$$

Now, let us write $\mathscr{N}_*(\ell)$ for the number of prime pairs $(p, q)$ such that $\ell = p + 6q$ with $q$ restricted to $(n/2, n-2)$, where as usual $n = \lfloor \ell/12 \rfloor$. In the computation of $\mathscr{N}(\ell)$, $q$ is allowed to roam inside the interval $[1, 2n]$, but $(n/2, n-2)$ covers just a quarter of that interval as $n \to \infty$, so it is reasonable to expect that $\mathscr{N}_*(\ell) \sim^? \frac{1}{4}\mathscr{N}(\ell)$.

| $\ell$ | $\mathscr{N}(\ell)$ | $\mathscr{N}_*(\ell)$ | $\mathscr{N}_*(\ell)/\mathscr{N}(\ell)$ | $\mathscr{N}(\ell)/\mathscr{H}(\ell)$ |
|---:|---:|---:|---:|---:|
| 101 | 5 | 1 | 0.200 | 0.421 |
| 1009 | 19 | 6 | 0.315 | 0.489 |
| 10007 | 86 | 21 | 0.244 | 0.603 |
| 100003 | 492 | 107 | 0.217 | 0.674 |
| 1000003 | 3157 | 734 | 0.232 | 0.730 |
| 10000019 | 22128 | 5381 | 0.243 | 0.765 |
| 100000007 | 162251 | 39182 | 0.241 | 0.799 |
| 1000000007 | 1249125 | 302624 | 0.242 | 0.820 |
| 10000000019 | 9909630 | 2411952 | 0.243 | 0.837 |
| 100000000003 | 80503641 | 19650597 | 0.244 | 0.852 |
| 1000000000039 | 666827226 | 163133972 | 0.244 | 0.864 |

TABLE 1. Representative Data For $\mathscr{N}(\ell)$ and $\mathscr{N}_*(\ell)$

In addition to finding just one prime pair $(p, q)$ for each $\ell$ coprime to 6 up to $10^9$, we also computed $\mathscr{N}(\ell)$ and $\mathscr{N}_*(\ell)$ for many large prime numbers $\ell$ as a numerical study of the roubustness of the Hardy-Littlewood asymptotics in this limited range, with a particular interest on the hypothesis that $\mathscr{N}_*(\ell)/\mathscr{N}(\ell) \sim 1/4$, which our data tend to support. In the table above, we give some representative results, only for primes just exceeding powers of 10. The last column lists the computed values of $\mathscr{N}(\ell)/\mathscr{H}(\ell)$ where

$$\mathscr{H}(\ell) := \frac{2C_2}{3}\frac{\ell-1}{\ell-2}\frac{\ell}{(\log \ell)^2}.$$

Note that while $\mathscr{N}(\ell)/\mathscr{H}(\ell)$ is quite a bit smaller than 1, it does exhibit a generally upward movement, so the Hardy-Littlewood Conjecture's prediction that it tends towards 1 as $\ell$ becomes larger seems reasonable. The expectation that $\mathscr{N}_*(\ell) \sim \mathscr{N}(\ell)/4$ is more strongly reflected in the data we collected.

## 5. New Cases of Irreducibility

For this section we set $n = 2^\nu$ with $\nu > 0$ and give a purity result for the 2-adic Newton polygon for certain choices of $\lambda, \mu$ and $\nu$. In particular, this will imply that $K_n^{(\lambda,\mu)}(x)$ is irreducible for these choices.

**Theorem 5.1.** *Let $n = 2^\nu$. If $\nu$ is odd and $\lambda = -1$, or if $\nu$ is even and $\lambda = 1$, then $\mathrm{NP}_2(K_n^{(\lambda,\mu)}(x))$ is pure of slope $(n-1)/n$. In particular, under these conditions the polynomial $K_n^{(\lambda,\mu)}(x)$ is irreducible over $\mathbf{Q}$.*

*Proof.* The final conclusion follows from the fact that the Newton polygon is pure with denominator $n$, since the Newton polygon of a product is the Minkowski sum of the Newton polygons of the factors. Write $K_n^{(\lambda,\mu)}(x) = \sum_{j=0}^{n} a_j x^j$. We break the proof into three parts; first we show that $\mathrm{ord}_2(a_n) = 0$, then $\mathrm{ord}_2(a_0) = n-1$, and then finally that $\mathrm{ord}_2 a_j > (n-j)(n-1)/n$ when $0 < j < n$, thereby showing that the 2-adic valuations of the middle coefficients lie above the line defined by the two endpoints.

**Step 1:** $\operatorname{ord}_2 a_n = 0$**.** It is clear for all choices of $\lambda$ and $\mu$ that $a_n$ is odd:

$$a_n = 3^n 2^n n! \binom{2n + \lambda/3 + \mu/2}{n} = (12n + 2\lambda + 3\mu)(12n - 6 + 2\lambda + 3\mu) \cdots (6n + 6 + 2\lambda + 3\mu).$$

**Step 2:** $\operatorname{ord}_2 a_0 = n - 1$**.** We only give details for the case of odd $\nu$ and $\lambda = -1$; the case of even $\nu$ is similar. The proof is by induction on $\nu$ with $\nu = 1$ being clear. Let $\nu = 2m + 1$. Then

$$\begin{aligned}
\operatorname{ord}_2(a_0) &= \operatorname{ord}_2 \prod_{j=0}^{2^{2m+1}-1} (2 + 3j) \\
&= \operatorname{ord}_2 \prod_{j=0}^{2^{2m}-1} (2 + 6j) && \text{(omitting the odd terms)} \\
&= 2^{2m} + \operatorname{ord}_2 \prod_{j=0}^{2^{2m}-1} (1 + 3j) \\
&= 2^{2m} + \operatorname{ord}_2 \prod_{j=0}^{2^{2m}-2} (4 + 3j) && \text{(reindexing)} \\
&= 2^{2m} + \operatorname{ord}_2 \prod_{j=0}^{2^{2m-1}-1} (4 + 6j) && \text{(omitting the odd terms)} \\
&= 2^{2m} + 2^{2m-1} + \operatorname{ord}_2 \prod_{j=0}^{2^{2m-1}-1} (2 + 3j) \\
&= 2^{2m} + 2^{2m-1} + 2^{2m-1} - 1 && \text{(by induction)} \\
&= n - 1.
\end{aligned}$$

**Step 3:** $\operatorname{ord}_2 a_j > (n - j)(n - 1)/n$**.** Again, we give details in the case of odd $\nu$ and $\lambda = -1$. Recall that $0 < j < n$ so that the binomial coefficient will now contribute to the valuation:

$$\begin{aligned}
\operatorname{ord}_2(a_j) &= \operatorname{ord}_2 \left( \binom{n}{j} \prod_{k=j+1}^{n} (3k - 1) \underbrace{\prod_{k=1}^{j} (6n + 6k + 4 + 3\mu)}_{\text{odd}} \right) \\
&= \operatorname{ord}_2 \binom{n}{j} + \operatorname{ord}_2(a_0) - \operatorname{ord}_2 \left( \prod_{k=0}^{j-1} (2 + 3k) \right),
\end{aligned}$$

where the latter equality follows from writing $a_j = a_0 / \prod_{k=0}^{j-1}(2+3k)$. Moreover, since $n = 2^\nu$, the 2-valuation of $\binom{n}{j}$ is simply $\nu - \operatorname{ord}_2(j)$. Combining this with $\operatorname{ord}_2 a_0 = n - 1$ gives us

$$\operatorname{ord}_2(a_j) = n - 1 + \nu - \operatorname{ord}_2(j) - \underbrace{\operatorname{ord}_2 \prod_{k=0}^{j-1} (2 + 3k)}_{\stackrel{\text{def}}{=} \Delta_j}.$$

**Step 3** of the proof will then follow by showing $\nu - \operatorname{ord}_2(j) - \operatorname{ord}_2(\Delta_j) > j/n - j$, *i.e.* that

$$j/n + \operatorname{ord}_2(\Delta_j) + \operatorname{ord}_2(j) < \nu + j.$$

Write $j$ in base-2 as $j = 2^{m_0} + \cdots + 2^{m_\ell}$ with $0 \le m_0 < m_1 < \cdots < m_\ell < \nu$. Then

$$\begin{aligned} j/n + \mathrm{ord}_2(j) + \mathrm{ord}_2(\Delta_j) &< 1 + \mathrm{ord}_2(j) + \mathrm{ord}_2(\Delta_j) \\ &= 1 + m_0 + \mathrm{ord}_2(\Delta_j) \\ &< 1 + m_0 + 2^{m_\ell} \qquad \text{since } \mathrm{ord}_2(\Delta_{2^u}) = \begin{cases} 2^u & u \text{ even} \\ 2^u - 1 & u \text{ odd} \end{cases} \\ &\qquad\qquad \text{and } \mathrm{ord}_2(\Delta_j) \text{ is non-decreasing in } j \\ &< 1 + m_0 + j \\ &\le \nu + j. \end{aligned}$$

This completes the proof of Theorem 5.1 and of Theorem 1.9. □

**Remark 5.2.** We have strong computational evidence for further purity results of this type for the $p$-adic Newton Polygons when $n$ is a power of and odd prime $p$. We explore this and more in a forthcoming paper.

## References


[1] J. Brillhart, P. Morton, Class numbers of quadratic fields, Hasse invariants of elliptic curves, and the supersingular polynomial, J. Number Theory **106** (2004) 79-111.

[2] W. Bosma, J. Cannon, C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput., **24** (1997), 235–265

[3] M. Bush, F. Hajir. An irreducibility lemma. J. Ramanujan Math. Soc. **23** (2008), no. 1, 33-41.

[4] J. Cullinan, F. Hajir. On the Galois groups of Legendre polynomials. Indag. Math. (N.S.) **25** (2014), no. 3, 534 – 552.

[5] J. Cullinan, F. Hajir. Primes of prescribed congruence class in short intervals. INTEGERS **12** (2012) #A56.

[6] G. Dumas. Sur quelques cas d'irréductibilité des polynomes à coefficients rationnels. J. de Math. Pures et Appl. **2** (1906), 191 – 258.

[7] F. Hajir, On the Galois group of generalized Laguerre Polynomials. J. Théor. Nombres Bordeaux **17**, (2005) no. 2, 517–525.

[8] G.H. Hardy and J.E. Littlewood, Some problems of *Partitio Numerorum* III: On the expression of a number as a sum of primes, Acta Math. **44** (1923), 1-70.

[9] M. Kaneko, D. Zagier. Supersingular j-invariants, hypergeometric series, and Atkin's orthogonal polynomials. Computational perspectives on number theory (Chicago, IL, 1995), 97–126, AMS/IP Stud. Adv. Math., **7**, Amer. Math. Soc., Providence, RI, 1998.

[10] K. Mahlburg, K. Ono. Arithmetic of certain hypergeometric modular forms. Acta Arith. **113** (2004), no. 1, 39–55.

[11] PARI/GP, version `2.5.0`, Bordeaux, 2011, `http://pari.math.u-bordeaux.fr/`.

[12] O. Ramaré, R. Rumely. Primes in arithmetic progressions. Math. Comp. **65** (1996), no. 213, 397-425.

[13] G. Szegö, Orthogonal Polynomials, 4th ed. Providence, RI: Amer. Math. Soc., 1975.

[14] H. Wielandt, Finite permuation groups, Academic Press, New York, 1964.



Department of Mathematics, Bard College, Annandale-On-Hudson, NY 12504
*E-mail address*: `cullinan@bard.edu`

Department of Mathematics and Statistics, University of Massachusetts, Amherst, MA 01002
*E-mail address*: `hajir@math.umass.edu`