Cullinan and Gajek-Leonard *Res. Number Theory* (2016) 2:8
DOI 10.1007/s40993-016-0064-5

Research in Number Theory

RESEARCH Open Access

On the Newton polygons of Kaneko-Zagier lifts of supersingular polynomials

John Cullinan* and Rylan Gajek-Leonard

*Correspondence:
cullinan@bard.edu
Department of Mathematics,
Bard College,
Annandale-On-Hudson,
NY 12504, USA

Abstract

Let p be a prime number. The *supersingular polynomial* $\mathfrak{S}_p(x)$ in characteristic p is the polynomial over $\mathbf{F}_p$ whose roots in $\overline{\mathbf{F}_p}$ are the supersingular j-invariants of elliptic curves over $\mathbf{F}_p$. In this paper we study the Newton polygons of certain rational lifts of $\mathfrak{S}_p(x)$ connected to the theory of Jacobi polynomials. As a corollary to our results on the Newton polygons, we obtain new cases of irreducibility for these supersingular lifts, providing more evidence for the general irreducibility conjecture of Mahlburg and Ono.

Keywords: Kaneko-Zagier polynomials, Supersingular, Newton polygons

Mathematics Subject Classification: 11R32, 11R09, 33C45

1 Background

Let $p > 3$ be a prime number and let E be an elliptic curve defined over the finite field $\mathbf{F}_p$. Recall that E is *supersingluar* if the p^n-torsion $E[p^n]$ of E is trivial for all n (there are many equivalent characterizations of supersingularity, see [8, V.4] for more details and examples). For a fixed prime p, there are finitely many supersingular j-invariants in characteristic p, which prompts the following definition. The *supersingular polynomial*

$$\mathfrak{S}_p(x) = \prod_{j'}(x - j') \in \overline{\mathbf{F}_p}[x]$$

is defined to be the polynomial over $\overline{\mathbf{F}_p}$ whose roots j' are the supersingular j-invariants in characteristic p; it is known [5] that $\mathfrak{S}_p(x)$ is in fact defined over $\mathbf{F}_p$. The purpose of this paper is to study a particular lift to $\mathbf{Q}$ of $\mathfrak{S}_p(x)$; namely, a family of polynomials, indexed by p, with rational coefficients whose reduction mod p coincides with $\mathfrak{S}_p(x)$. The family that we shall study was first introduced by Kaneko and Zagier in [5] and subsequently studied by Brillhart and Morton [2], Mahlburg and Ono [6], and many others. In [5], the authors describe several different natural lifts of $\mathfrak{S}_p(x)$; the family we study in this paper is in fact a family of Jacobi polynomials.

We follow [4] in our choice of notation for the remainder of the paper. Write $p = 12n+e$ with $e \in \{1, 5, 7, 11\}$ and $n \geq 0$ and set $k = p - 1$. Let $\lambda, \mu \in \{\pm 1\}$ be such that $e - 6 = 2\lambda + 3\mu$ and $\epsilon, \delta \in \{0, 1\}$ such that $e - 1 = 4\delta + 6\epsilon$. It is known that $\mathfrak{S}_p(x)$ has degree $n + \delta + \epsilon$ and has the factorization

$$\mathfrak{S}_p(x) = x^{\delta}(x - 1728)^{\epsilon}\mathfrak{s}_p(x),$$

Springer Open

where $\mathfrak{s}_p(x)$ is a degree-n polynomial defined over $\mathbf{F}_p$. Kaneko and Zagier originally introduced a family of polynomials they denote $\widetilde{F}_k(x) \in \mathbf{Q}[x]$ such that $\widetilde{F}_k(x) \equiv \mathfrak{s}_p(x) \pmod{p}$; in [5] the emphasis is on the connection to modular forms where the index k is a natural choice since the dimension of the space of weight k holomorphic modular forms on $\mathrm{PSL}_2(\mathbf{Z})$ has dimension $n+1$. Mahlburg and Ono in [6] conjecture that the $\widetilde{F}_k$ are irreducible over $\mathbf{Q}$ with full Galois group and in [4] the authors gave new evidence for both the irreducibility and the Galois group conjectures. The main tool used in [4] was the Newton polygon and the purpose of this paper is to work out the Newton polygons in more generality. As a corollary, we will obtain new cases of irreducibility of these supersingular lifts.

Continuing with our notational conventions, we recall that the classical degree-n Jacobi polynomial $P_n^{(\alpha,\beta)}(x)$ can be expressed in terms of the hypergeometric function

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

It can be shown (see [4, Section 2] for a complete derivation) that

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

which connects the original notation of [5] with our own. In [4, Lemma 2.4] it was shown that the polynomial

$$M_n^{(\lambda,\mu)}(x) \stackrel{\text{def}}{=} \sum_{j=0}^{n}\binom{n}{j}\left[\prod_{k=j+1}^{n}(\lambda+3k)\prod_{k=1}^{j}(6n+3\mu+2\lambda+6k)\right]x^j$$

with integral coefficients has the same irreducibility and Galois properties as the $\widetilde{F}_k(x)$ (the proof involves judicious linear shifts of the variable and clearing denominators). In this paper we change notation slightly to aid in the computation of the Newton polygon. Namely, we focus on the monic version of the $M_n^{(\lambda,\mu)}(x)$ and denote them by $S_n^{(\lambda,\mu)}(x)$:

$$S_n^{(\lambda,\mu)}(x) \stackrel{\text{def}}{=} \sum_{j=0}^{n}\binom{n}{j}\prod_{k=j+1}^{n}\frac{6k+2\lambda}{6n+2\lambda+3\mu+6k}\,x^j \stackrel{\text{def}}{=} \sum_{j=0}^{n}A_j x^j.$$

With all of this notation in place we can now state the main results of the paper.

Theorem 1 *Let $p>3$ be a prime and let r be a positive integer. Let $n=(p^r-\lambda)/3$, where*

$$\lambda = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 3, \\ (-1)^r & \text{if } p \equiv -1 \pmod 3. \end{cases}$$

Define

$$V_k = \begin{cases} (p^k-1)/3 & \text{if } p \equiv 1 \pmod 3, \\ (p^{2k}-1)/3 & \text{if } p \equiv -1 \pmod 3 \text{ and } r \text{ is even}, \\ (p^{2k+1}+1)/3 & \text{if } p \equiv -1 \pmod 3 \text{ and } r \text{ is odd}. \end{cases}$$

Then:

(1) *If $p \equiv 1 \pmod 3$, then the vertices of $\mathrm{NP}_p(S_n^{(1,\mu)}(x))$ are*

$$(V_0, r), (V_1, r-1), (V_1, r-2), \ldots, (V_r, 0).$$

In particular, $\mathrm{NP}_p(S_n^{(1,\mu)}(x))$ consists of r segments of lengths $\frac{p-1}{3}, \frac{p^2-p}{3}, \ldots, \frac{p^r-p^{r-1}}{3}$ with respective slopes

$$\frac{-3}{p-1}, \frac{-3}{p^2-p}, \ldots, \frac{-3}{p^r-p^{r-1}}.$$

(2) *If* $p \equiv -1 \pmod 3$, $p > 5$, *and* r *is even, then the vertices of* $\mathrm{NP}_p(S_n^{(1,\mu)}(x))$ *are*

$$(V_0, r/2), (V_1, r/2-1), (V_2, r/2-2), \ldots, (V_{r/2}, 0).$$

In particular, $\mathrm{NP}_p(S_n^{(1,\mu)}(x))$ *consists of* $r/2$ *segments of lengths* $\frac{p^2-1}{3}, \frac{p^4-p^2}{3}, \ldots, \frac{p^r-p^{r-2}}{3}$ *with respective slopes*

$$\frac{-3}{p^2-1}, \frac{-3}{p^4-p^2}, \ldots, \frac{-3}{p^r-p^{r-2}}.$$

(3) If $p \equiv -1 \pmod 3$, $p > 5$, *and* r *is odd, then the vertices of* $\mathrm{NP}_p(S_n^{(-1,\mu)}(x))$ *are*

$$(0, (r+1)/2), (V_0, (r+1)/2-1), (V_1, (r+1)/2-2), \ldots, (V_{(r-1)/2}, 0).$$

In particular, $\mathrm{NP}_p(S_n^{(-1,\mu)}(x))$ *consists of* $(r+1)/2$ *segments of lengths* $\frac{p+1}{3}, \frac{p^3-p}{3}, \ldots, \frac{p^r-p^{r-2}}{3}$ *with respective slopes*

$$\frac{-3}{p+1}, \frac{-3}{p^3-p}, \frac{-3}{p^5-p^3}, \ldots, \frac{-3}{p^r-p^{r-2}}.$$

While these statements do not immediately give irreducibility, we point out that there are certain special cases that do. The following corollary gives new Eisenstein results that extend some of the cases of [6, Theorem 1.1].

Corollary 1 *With all notation as above, set* $r = 1$ *in Parts (1) and (3) of Theorem 1 and* $r = 2$ *in Part (2). Then for* $\lambda, \mu \in \{\pm 1\}$ *we have*

(1) *If* $p \equiv \lambda \pmod 3$, *then* $S_{(p-\lambda)/3}^{(\lambda,\mu)}(x)$ *is Eisenstein at* p.
(2) *If* $p \equiv -1 \pmod 3$, *then* $S_{(p^2-1)/3}^{(1,\mu)}(x)$ *is Eisenstein at* p.

The proof of Theorem 1 involves an analysis of the p-valuations of the coefficients of the $S_n^{(\lambda,\mu)}(x)$. Because of the form of the coefficients, the computations are notationally intricate. Therefore, in the next section we give a non-technical sketch of the proof that clearly outlines each step. We then prove Theorem 1 in Sect. 3 and give further remarks in Sect. 4. The final section of the paper is devoted to computational evidence for further Eisenstein properties of the $S_n^{(\lambda,\mu)}(x)$ at small primes. We conclude by proving a new case of irreducibility when n is a power of 7 that complements a similar result in [6, Theorem 1.1].

2 Notation and outline of the proofs

In this section we continue to outline our main result on the Newton Polygons of certain $S_n^{(\lambda,\mu)}(x)$. Let $p > 3$ be a prime, $r > 0$ a positive integer, $\lambda, \mu \in \{\pm 1\}$ with the relationship between p, λ, n, and r that

$$n = \frac{p^r - \lambda}{3} \in \mathbf{Z}.$$

In other words, if $p \equiv 1 \pmod 3$ then $\lambda = 1$, while if $p \equiv -1 \pmod 3$ then $\lambda = -1$ for odd r and $\lambda = 1$ for even r. We will apply all of this notation to the polynomials

$$S_n^{(\lambda,\mu)}(x) = \sum_{j=0}^{n} \binom{n}{j} \prod_{k=j+1}^{n} \frac{6k+2\lambda}{6n+2\lambda+3\mu+6k} x^j = \sum_{j=0}^{n} A_j x^j.$$

We set the additional notation

$$c(n,\lambda,\mu,k) \stackrel{\text{def}}{=} \frac{6k+2\lambda}{6n+2\lambda+3\mu+6k}$$

so that $A_j = \binom{n}{j}\prod_{k=j+1}^{n} c(n,\lambda,\mu,k)$. Before outlining the theorems (Fig. 1), we give a picture in the figure below of the Newton polygons at p of the $S_n^{(\lambda,\mu)}(x)$ when $n=(p^r-1)/3$ and $\lambda=1$:

We will break the proof of Theorem 1 into several lemmas and, due to the intricate notation, we will first give an informal sketch of the proofs. We focus on part (1) of Theorem 1 since the ideas behind the other two are similar.

The goal of Sect. 3 is to show that the vertices of the Newton polygon have coordinates $\left(\frac{p^s-1}{3}, r-s\right)$ for $s=0,\ldots,r$. To do this, we start in Lemma 1 by showing the binomial coefficients $\binom{\frac{p^r-1}{3}}{\frac{p^s-1}{3}}$ are not divisible by p. This allows us to simplify the polynomials $S_n^{(\lambda,\mu)}(x)$ by twisting out the binomial coefficients. This technique was used by Schur in [7] to compute the Newton polygons of a wider class of polynomials than the truncated exponentials; see [3] for an account of this. Lemma 2 and Corollary 2 establish the identity $\operatorname{ord}_p A_j = r-s$ when $j=\frac{p^s-1}{3}$. To finish the proof of the Newton polygon, it remains to show that the intermediate coefficients all have p-valuation greater than or equal to $r-s$; we prove this in Lemma 3. We now proceed to the proofs.

3 Main results

To see that the Newton polygons of the $S_n^{(\lambda,\mu)}(x)$ are as claimed, we begin by proving part (1) of Theorem 1. In preparation for the theorem, we set $\lambda=1$, and let $p\equiv 1 \pmod 3$. Recall that $S_n^{(1,\mu)}(x)=\sum_{j=0}^{n} A_j x^j$ with

$$A_j = \binom{n}{j}\prod_{k=j+1}^{n} c(n,1,\mu,k).$$

In what follows, Lemmas 1 and 2 and Corollary 2 establish the vertices of the Newton polygon. Lemma 3 then shows that the p-valuations of the intermediate (non-break) coefficients are strictly larger than those of the breaks. Together, these three lemmas prove part (1) of Theorem 1.

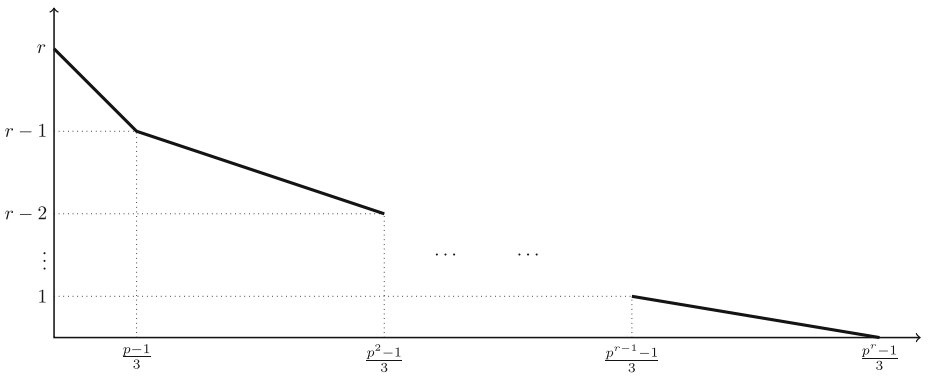

Fig. 1 p-Adic Newton polygon of $S^{(1,1)}_{(p^r-1)/3}(x)$

Lemma 1 *Let p be a prime congruent to 1 modulo 3. Let $r, s \in \mathbf{Z}_{\geq 0}$ with $r \geq s$. Then the binomial coefficient $\binom{\frac{p^r-1}{3}}{\frac{p^s-1}{3}}$ is coprime to p.*

Proof Recall that if $N_0 + N_1 p + \cdots N_k p^k$ is the base-p expansion of the positive integer N, then

$$\operatorname{ord}_p N! = \frac{N - (\sum_{i=0}^{k} N_i)}{p-1}.$$

By writing p^r as the telescoping sum

$$\begin{aligned} p^r &= p + p^2 - p + p^3 - p^2 + \cdots + p^r - p^{r-1} \\ &= p + (p-1)p^2 + (p-1)p^3 + \cdots + (p-1)p^{r-1}, \end{aligned}$$

it follows that the base-p expansion of $(p^r - 1)/3$ is given by

$$\frac{p^r - 1}{3} = \sum_{k=0}^{r-1} \frac{(p-1)}{3} p^k.$$

Therefore

$$\begin{aligned} \operatorname{ord}_p \binom{\frac{p^r-1}{3}}{\frac{p^s-1}{3}} &= \operatorname{ord}_p \left(\frac{p^r-1}{3}\right)! - \operatorname{ord}_p \left(\frac{p^s-1}{3}\right)! - \operatorname{ord}_p \left(\frac{p^r-p^s}{3}\right)! \\ &= \frac{p^r - 1 - r(p-1)}{3(p-1)} - \frac{p^s - 1 - s(p-1)}{3(p-1)} \\ &\quad - \frac{p^r - p^s - r(p-1) + s(p-1)}{3(p-1)} = 0, \end{aligned}$$

as claimed. □

Lemma 2 *With all notation as above,* $\operatorname{ord}_p A_0 = r$.

Proof Write $A_0 = \prod_{k=1}^{n} \frac{6k+2}{6n+2+3\mu+6k}$ so that

$$\operatorname{ord}_p A_0 = \sum_{k=1}^{n} \operatorname{ord}_p(6k+2) - \sum_{k=1}^{n} \operatorname{ord}_p(6n+2+3\mu+6k). \tag{2}$$

Recall we set $n = (p^r - 1)/3$. We first count the number of k such that $6k + 2$ has p-valuation equal to ℓ. Since p is odd, we divide by 2 and count the p-valuations of $3k + 1$. We set some notation. Let $\mathsf{N} = \{1, \ldots, n\}$ and $X_\ell \stackrel{\text{def}}{=} \{k \in \mathsf{N} \mid \operatorname{ord}_p(3k+1) = \ell\}$. Then the X_ℓ partition N:

$$\mathsf{N} = \coprod_{\ell=0}^{r} X_\ell.$$

One can check (in fact, one can give an explicit formula for the $k \in X_\ell$) that the size of X_ℓ is given by

$$\#X_\ell = \begin{cases} 1 & \text{if } \ell = r, \\ \frac{p-1}{3} \cdot p^{r-\ell-1} & \text{if } 0 < \ell < r, \\ \frac{p-1}{3} \cdot p^{r-1} - 1 & \text{if } \ell = 0. \end{cases}$$

Similarly, define $Y_\ell \stackrel{\text{def}}{=} \{k \in \mathsf{N} \mid \operatorname{ord}_p(6n+2+3\mu+6k) = \ell\}$. In this case, $Y_r = \emptyset$ and it is easy to check that

$$\#Y_\ell = \begin{cases} \frac{p-1}{3} \cdot p^{r-\ell-1} & \text{if } 0 < \ell < r, \\ \frac{p-1}{3} \cdot p^{r-1} & \text{if } \ell = 0. \end{cases}$$

Altogether, the k that belong to X_0 or Y_0 do not contribute to the p-valuation of A_0. For each ℓ with $0 < \ell < r$, it is the case that $\#X_\ell = \#Y_\ell$. Consequently, all the terms in the sum (2) cancel except for the contribution from X_r, which consists of the single element $k = (p^r - 1)/3$. It follows that $\operatorname{ord}_p A_0 = r$, as claimed. □

Corollary 2 *Let $s \in \{0, 1, 2, \ldots, r\}$. Then $\operatorname{ord}_p(A_{\frac{p^s-1}{3}}) = r - s$.*

Proof Observe that

$$A_j = \binom{n}{j} \prod_{k=j+1}^{n} c(n, 1, \mu, k) = \binom{n}{j} \frac{\prod_{k=1}^{n} c(n, 1, \mu, k)}{\prod_{k=1}^{j} c(n, 1, \mu, k)}.$$

Set $n = (p^r - 1)/3$, $j = (p^s - 1)/3$, and apply Lemma 1 to the binomial coefficient. Then

$$\begin{aligned} \operatorname{ord}_p(A_{\frac{p^s-1}{3}}) &= \operatorname{ord}_p \prod_{k=1}^{(p^r-1)/3} c(n, 1, \mu, k) - \operatorname{ord}_p \prod_{k=1}^{(p^s-1)/3} c(n, 1, \mu, k) \\ &= r - \operatorname{ord}_p \prod_{k=1}^{(p^s-1)/3} c(n, 1, \mu, k), \end{aligned}$$

by Lemma 2. However, if one replaces "r" by "s" in the expression for n, then the same argument in Lemma 2 applies *mutatis mutandis* to the product $\operatorname{ord}_p \prod_{k=1}^{(p^s-1)/3} c(n, 1, \mu, k)$, whence

$$\operatorname{ord}_p \prod_{k=1}^{(p^s-1)/3} c(n, 1, \mu, k) = s$$

so that $\operatorname{ord}_p(A_{\frac{p^s-1}{3}}) = r - s$. □

Lemma 3 *Let $s \in [0, r] \cap \mathbf{Z}$ and let j be an index with $\frac{p^s-1}{3} < j < \frac{p^{s+1}-1}{3}$. Then $\operatorname{ord}_p A_j \geq r - s$.*

Proof Recall that $A_j = \binom{n}{j} \prod_{k=j+1}^{n} c(n, 1, \mu, k)$ so that we may write

$$\begin{aligned} \operatorname{ord}_p A_j &= \operatorname{ord}_p \binom{n}{j} + \operatorname{ord}_p \frac{\prod_{k=1}^{n} c(n, 1, \mu, k)}{\prod_{k=1}^{(p^s-1)/3} c(n, 1, \mu, k) \cdot \prod_{k=(p^s-1)/3+1}^{j} c(n, 1, \mu, k)} \\ &= \operatorname{ord}_p \binom{n}{j} + r - s - \operatorname{ord}_p \prod_{k=(p^s-1)/3+1}^{j} c(n, 1, \mu, k). \end{aligned}$$

Since $\operatorname{ord}_p \binom{n}{j} \geq 0$, it will suffice to prove $\operatorname{ord}_p \prod_{k=(p^s-1)/3+1}^{j} c(n, 1, \mu, k) \leq 0$. Continuing with the dévissage, write

$$c(n, 1, \mu, k) = \frac{6k+2}{6n+2+3\mu+6k} \stackrel{\text{def}}{=} \frac{N(k)}{D(k)},$$

so that

$$\operatorname{ord}_p \prod_{k=(p^s-1)/3+1}^{j} c(n,1,\mu,k) = \sum_{k=(p^s-1)/3+1}^{j} \operatorname{ord}_p N(k) - \sum_{k=(p^s-1)/3+1}^{j} \operatorname{ord}_p D(k).$$

We will treat each sum separately.

For the numerators, we have

$$\begin{aligned}\sum_{k=(p^s-1)/3+1}^{j} \operatorname{ord}_p N(k) &= \sum_{k=(p^s-1)/3+1}^{j} \operatorname{ord}_p (6k+2) \\ &= \sum_{k=(p^s-1)/3+1}^{j} \operatorname{ord}_p (3k+1) \\ &= \sum_{m=1}^{j-(p^s-1)/3} \operatorname{ord}_p (p^s+3m).\end{aligned}$$

Moreover, since for m in the stated range it is never the case that $\operatorname{ord}_p (p^s+3m) > s$, it follows that

$$\operatorname{ord}_p (p^s+3m) = \operatorname{ord}_p(3m) = \operatorname{ord}_p(m),$$

whence

$$\sum_{m=1}^{j-(p^s-1)/3} \operatorname{ord}_p (p^s+3m) = \sum_{m=1}^{j-(p^s-1)/3} \operatorname{ord}_p(m) = \operatorname{ord}_p \left(j - \frac{p^s-1}{3}\right)!$$

We can rewrite the denominators similarly:

$$\begin{aligned}\sum_{k=(p^s-1)/3+1}^{j} \operatorname{ord}_p D(k) &= \sum_{k=(p^s-1)/3+1}^{j} \operatorname{ord}_p 6\left(\frac{p^r-1}{3}\right) + 2 + 3\mu + 6k \\ &= \sum_{m=1}^{j-(p^s-1)/3} \operatorname{ord}_p (2p^r + 2p^s + 6m - 2 + 3\mu).\end{aligned}$$

Again, because of the range of m, it is never the case that $\operatorname{ord}_p (2p^s + 6m - 2 + 3\mu) = r$, hence

$$\operatorname{ord}_p (2p^r + 2p^s + 6m - 2 + 3\mu) = \operatorname{ord}_p (2p^s + 6m - 2 + 3\mu).$$

However, for the denominators there is a unique index m in the range $1 \le m < \frac{p^{s+1}-1}{3}$ such that

$$\operatorname{ord}_p (2p^s + 6m - 2 + 3\mu) = s+1;$$

namely

$$m = \frac{p^{s+1} - (3\mu - 2)}{6},$$

so that $6m + 3\mu - 2 = p^{s+1}$. Altogether, this shows we can compute the p-valuation of the denominator of A_j by means of the formula

$$\sum_{m=1}^{j-(p^s-1)/3} \operatorname{ord}_p\left(2p^r + 2p^s + 6m - 2 + 3\mu\right)$$
$$= \begin{cases} \sum_{m=1}^{j-(p^s-1)/3} \operatorname{ord}_p\left(6m + 3\mu - 2\right) & \text{if } j < \frac{p^{s+1}-(3\mu-2)}{6} \\ \sum_{m=1}^{j-(p^s-1)/3} \operatorname{ord}_p\left(6m + 3\mu - 2\right) - 1 & \text{if } j \geq \frac{p^{s+1}-(3\mu-2)}{6}. \end{cases}$$

To finish the proof, recall that we need to show $\operatorname{ord}_p(D(k)) \geq \operatorname{ord}_p(N(k))$. But [1, Prop. 2.2] establishes the integrality of the product

$$\frac{k^n}{n!}\prod_{m=1}^{n-1}(1+km).$$

This is applicable to our setup by setting $n = j - (p^s - 1)/3$ and $k = 6$; it shows that $6^n N(k)/D(k)$ is integral. While the quotient $N(k)/D(k)$ itself may not be integral, since $p > 3$ it is certainly p-integral, which is sufficient to prove the Lemma. □

To recap, this sequence of Lemmas establishes the Newton polygon of $S_n^{(1,\mu)}(x)$ when $n = (p^r - 1)/3$ and $p \equiv 1 \pmod 3$. For parts (2) and (3) of Theorem 1, the ideas and proofs are nearly identical, so we give brief sketches of the arguments rather than detailed proofs. Both parts (2) and (3) can be proved via a similar sequence of Lemmas:

Step 1. It is easy to check that Lemma 1 holds for the polynomials in parts (2) and (3) of Theorem 1 as well. That is, using the notation of Theorem 1

$$\operatorname{ord}_p\binom{n}{V_k} = 0,$$

where for parts (2) and (3) of Theorem 1 we have

$$\text{Part (2)}: \; p \equiv -1 \pmod 3,\; r \text{ even},\; n = \frac{p^r-1}{3},\; V_k = \frac{p^{2k}-1}{3}$$
$$\text{Part (3)}: \; p \equiv -1 \pmod 3,\; r \text{ odd},\; n = \frac{p^r+1}{3},\; V_k = \frac{p^{2k+1}+1}{3}.$$

In other words, the binomial coefficients do not contribute to the vertices of the Newton polygons.

Step 2. To extend Lemma 2 to the polynomials of Parts (2) and (3) of Theorem 1, we need to show that

$$\text{Part (2): } \operatorname{ord}_p A_0 = r/2,$$
$$\text{Part (3): } \operatorname{ord}_p A_0 = (r+1)/2.$$

Each of these can be obtained in a similar way to the strategy of Lemma 2. For each case, we consider two partitions the set $\mathbb{N}$: one partition is into the k for which the p-valuation of the numerator equals ℓ and the other is into the k for which the p-valuation of the denominator equals ℓ. It then remains to count the elements of the subsets and subtract. For completeness we give the partitions along with the sizes for each of Parts (2) and (3) of Theorem 1; recall that X_ℓ denotes the number of k for which $6k + 2\lambda$ has p-valuation ℓ and Y_ℓ denotes the number of k for which $6n + 2\lambda + 3\mu + 6k$ has p-valuation ℓ:

Part (2):	$\#X_\ell = \begin{cases} 1 & \text{if } \ell = r \\ \frac{p^{r-\ell}-p^{r-\ell-1}+(-1)^\ell}{3} & \text{if } 0 < \ell < r \\ \frac{p^r-p^{r-1}}{3} & \text{if } \ell = 0 \end{cases}$
	$\#Y_\ell = \#X_\ell + (-1)^{\ell-1}$ for $0 \le \ell \le r$
Part (3):	$\#X_\ell = \begin{cases} 1 & \text{if } \ell = r \\ \frac{p^{r-\ell}-p^{r-\ell-1}-(-1)^\ell}{3} & \text{if } 0 \le \ell < r \end{cases}$
	$\#Y_\ell = \#X_\ell + (-1)^\ell$ for $0 \le \ell \le r$

We then compute $\operatorname{ord}_p A_0$ as the weighted sum of the $\#X_\ell$ and $\#Y_\ell$:

$$\begin{aligned}
\text{Part (2): } \operatorname{ord}_p A_0 &= r \cdot 1 + \sum_{\ell=1}^{r-1} \ell \cdot \frac{p^{r-\ell} - p^{r-\ell-1} + (-1)^\ell}{3} \\
&\quad - \sum_{\ell=1}^{r-1} \ell \cdot \left(\frac{p^{r-\ell} - p^{r-\ell-1} + (-1)^\ell}{3} + (-1)^{\ell-1} \right) \\
&= r - \sum_{\ell=1}^{r-1} \ell(-1)^{\ell-1} = r/2; \\
\text{Part (3): } \operatorname{ord}_p A_0 &= r \cdot 1 + \sum_{\ell=1}^{r-1} \ell \cdot \frac{p^{r-\ell} - p^{r-\ell-1} - (-1)^\ell}{3} \\
&\quad - \sum_{\ell=1}^{r-1} \ell \cdot \left(\frac{p^{r-\ell} - p^{r-\ell-1} - (-1)^\ell}{3} + (-1)^\ell \right) \\
&= r - \sum_{\ell=1}^{r-1} \ell(-1)^\ell = (r+1)/2.
\end{aligned}$$

Step 3. Observe that $\operatorname{ord}_p A_{V_k}$ is the difference of $\operatorname{ord}_p A_0$ when $n = (p^r - \lambda)/3$ and $\operatorname{ord}_p A_0$ when $n = (p^s - \lambda)/3$. By Lemma 2, this establishes the vertices of the Newton polygon.

Step 4. It remains to show that the p-valuations of the intermediate coefficients between the V_k lie above the breaks. As in Lemma 3, it will suffice to prove that

$$\begin{aligned}
&\text{Part (2): } \operatorname{ord}_p \prod_{k=(p^{2s}-1)/3+1}^{j} c(n, 1, \mu, k) \le 0 \\
&\text{Part (3): } \operatorname{ord}_p \prod_{k=(p^{2s+1}+1)/3+1}^{j} c(n, -1, \mu, k) \le 0.
\end{aligned}$$

Continuing with the same approach, define $N(k)$ and $D(k)$ to be the numerator and denominator of $c(n, \lambda, \mu, k)$, respectively. A similar argument shows that

$$\begin{aligned}
&\text{Part (2): } \operatorname{ord}_p \prod_{k=(p^{2s}-1)/3+1}^{j} N(k) = \sum_{m=1}^{j-(p^{2s}-1)/3} (p^{2s}+3m) = \operatorname{ord}_p \left(j - \frac{p^{2s}-1}{3} \right)! \\
&\text{Part (3): } \operatorname{ord}_p \prod_{k=(p^{2s+1}+1)/3+1}^{j} N(k) = \sum_{m=1}^{j-(p^{2s+1}+1)/3} (p^{2s+1}+3m) = \operatorname{ord}_p \left(j - \frac{p^{2s+1}+1}{3} \right)!
\end{aligned}$$

For the denominators, it suffices to use the quantities

$$\text{Part (2):} \quad \sum_{m=1}^{j-(p^{2s}-1)/3} (6m + 3\mu - 2),$$

$$\text{Part (3):} \quad \sum_{m=1}^{j-(p^{2s+1}+1)/3} (6m + 3\mu + 2).$$

Exactly as in Lemma 3, we can use [1, Prop. 2.2] to show that the p-valuation of the denominators of the $c(n, -1, \mu, k)$ are at least as large as that of the numerators and hence that the respective p-valuations are ≤ 0.

Steps 1–4 establish the remaining cases (2) and (3) of Theorem 1. As a corollary to case (2) by setting $r = 2$, we obtain the following result which extends the first case of [6, Theorem 1.1].

Corollary 3 *Let p be a prime number congruent to -1 modulo 3 and let $n = (p^2 - 1)/3$. Then for $\mu \in \{\pm 1\}$, the polynomial $S_n^{(1,\mu)}(x)$ is Eisenstein at p.*

4 Further remarks

Theorem 1 exploits the product structure of the *numerators* of the $c(n, \lambda, \mu, k)$. The same analysis can be performed for the denominators as well. In that case, we obtain the following complementary results to Theorem 1.

Theorem 2 *Let $p > 3$ be a prime and let r be a positive integer. Let $\lambda, \mu \in \{\pm 1\}$ and set $n = (p^r - 6 - 2\lambda - 3\mu)/6 \in \mathbf{Z}$. Define*

$$W_k = \begin{cases} (p^r - p^{r-k})/6 & \text{if } p \equiv 1 \pmod 3 \\ (p^r - p^{r-2k})/6 & \text{if } p \equiv -1 \pmod 3 \end{cases}$$

and let

$$\lambda = \begin{cases} -1 & \text{if } p \equiv 1 \pmod 3, \text{ or if } p \equiv -1 \pmod 3 \text{ and } r \text{ is even,} \\ 1 & \text{if } p \equiv -1 \pmod 3 \text{ and } r \text{ is odd.} \end{cases}$$

Then:

(1) *If $p \equiv 1 \pmod 3$ then the vertices of $\mathrm{NP}_p\big(S_n^{(-1,\mu)}(x)\big)$ are*

$$\big(W_0, -r\big), \big(W_1, -(r-1)\big), \big(W_2, -(r-2)\big), \ldots, \big(W_{r-1}, -1\big), \\ \big(W_{r-1} + (p - 4 - 3\mu)/6, 0\big),$$

In particular, $\mathrm{NP}_p(S_n^{(-1,\mu)}(x))$ consists of r segments of lengths $\frac{p^r - p^{r-1}}{6}, \frac{p^{r-1} - p^{r-2}}{6}, \ldots \frac{p^2 - p}{6}, \frac{p-4-3\mu}{6}$, with respective slopes

$$\frac{6}{p^r - p^{r-1}}, \frac{6}{p^{r-1} - p^{r-2}}, \ldots, \frac{6}{p^2 - p}, \frac{6}{p - 4 - 3\mu}.$$

(2) *If $p \equiv -1 \pmod 3$, $p > 5$, and r is even, then the vertices of $\mathrm{NP}_p\big(S_n^{(-1,\mu)}(x)\big)$ are*

$$\big(W_0, -r/2\big), \big(W_1, -(r/2-1)\big), \big(W_2, -(r/2-2)\big), \ldots, \big(W_{r/2-1}, -1\big), \\ \big(W_{r/2-1} + (p^2 - 4 - 3\mu)/6, 0\big).$$

In particular, $\mathrm{NP}_p(S_n^{(-1,\mu)}(x))$ *consists of* $r/2$ *segments of lengths* $\frac{p^r-p^{r-2}}{6}, \frac{p^{r-2}-p^{r-4}}{6}, \ldots, \frac{p^4-p^2}{6}, \frac{p^2-4-3\mu}{6}$ *with respective slopes*

$$\frac{6}{p^r-p^{r-2}}, \frac{6}{p^{r-2}-p^{r-4}}, \ldots, \frac{6}{p^4-p^2}, \frac{6}{p^2-4-3\mu}.$$

(3) *If* $p \equiv -1 \pmod 3$, $p > 11$, *and* r *is odd, then the vertices of* $\mathrm{NP}_p\big(S_n^{(1,\mu)}(x)\big)$ *are*

$$\big(W_0, -(r+1)/2\big), \big(W_1, -(r+1)/2+1\big), \big(W_2, -(r+1)/2+2\big), \ldots,$$
$$\big(W_{(r+1)/2-1}, -1\big), \big(W_{(r+1)/2-1} + (p-8-3\mu)/6, 0\big).$$

In particular, $\mathrm{NP}_p(S_n^{(1,\mu)}(x))$ *consists of* $(r+1)/2$ *segments of lengths* $\frac{p^r-p^{r-2}}{6}, \frac{p^{r-2}-p^{r-4}}{6}, \ldots, \frac{p^3-p}{6}, \frac{p-8-3\mu}{6}$ *with respective slopes*

$$\frac{6}{p^r-p^{r-2}}, \frac{6}{p^{r-2}-p^{r-4}}, \ldots, \frac{6}{p^3-p}, \frac{6}{p-8-3\mu}.$$

Pictorially, the shape of a typical Newton polygon of this type is as follows (Fig. 2).

While the following are not new, we do immediately recover some of the Eisenstein results of [6, Theorem 1.1] as special cases.

Corollary 4 *With all notation as above, we have*

(1) *Let* $p \equiv 1 \pmod 3$, $p > 3$, *and let* $n = \frac{p-4-3\mu}{6}$. *Then* $S_n^{(-1,\mu)}(x)$ *is Eisenstein at* p.
(2) *Let* $p \equiv -1 \pmod 3$, $p > 5$, *and let* $n = \frac{p^2-4-3\mu}{6}$. *Then* $S_n^{(-1,\mu)}(x)$ *is Eisenstein at* p.
(3) *Let* $p \equiv -1 \pmod 3$, $p > 11$, *and let* $n = \frac{p-8-3\mu}{6}$. *Then* $S_n^{(1,\mu)}(x)$ *is Eisenstein at* p.

5 Small primes and irreducibility conjectures

So far we have focused on the p-adic Newton polygons of the $S_n^{(\lambda,\mu)}(x)$ when $n = (p^r-\lambda)/3$. In this section we focus on the primes $p = 3, 5, 7$, and 11 and give computational evidence for new Eisenstein results when the degree n is a power of p. Proofs of these conjectures are likely to be established by techniques other than the ones we have presented in the

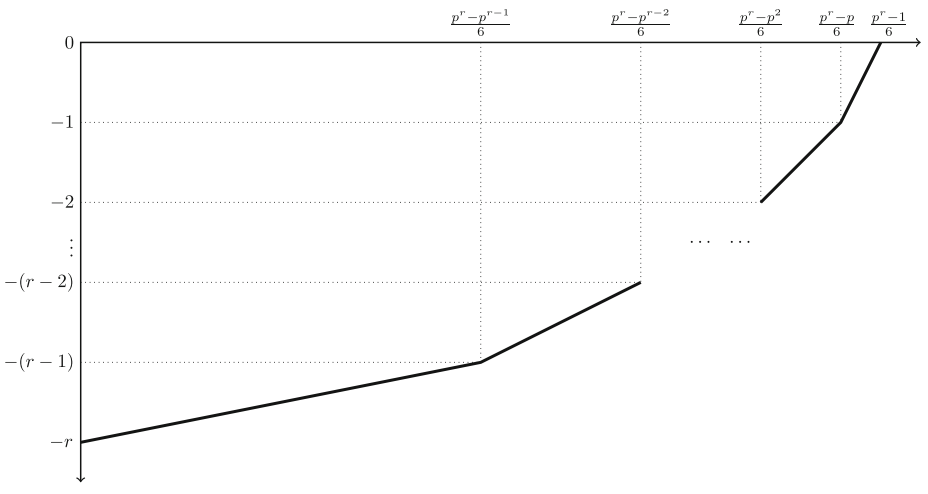

Fig. 2 p-Adic Newton polygon of $S_{(p^r-1)/6)}^{(-1,-1)}(x)$ when $p \equiv 1 \pmod 3$

previous sections, since our conjectures are based on *translates* of the polynomials and will require the p-adic valuation of special values of the polynomials.

In [4], Hajir and the first author showed that certain polynomials of the form $S_{2^m}^{(\lambda,\mu)}(x)$ are Eisenstein at $p = 2$; specifically, using the notation of [4] we know

Theorem 3 (Theorem 5.1 of [4]) *Let $n = 2^\nu$. If ν is odd and $\lambda = -1$, or if ν 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* $\mathbf{Q}$.

It is then a simple matter to translate from the $K_n^{(\lambda,\mu)}(x)$ notation to the $S_n^{(\lambda,\mu)}(x)$ notation of this paper. In [6, Theorem 1.1], Mahlburg and Ono proved that the $S_{7^\alpha}^{(-1,1)}(x)$ are Eisenstein at $p = 7$ for all $\alpha \geq 1$ and proved similar Eisenstein results for $p = 5$ and $p = 11$ as well. However, the prime $p = 3$ appears not to be covered by any results in the literature. In the following conjecture, we expand upon the Eisenstein results of [6] and propose new Eisenstein properties at the prime $p = 3$.

Conjecture 1 *With all notation as above, the polynomials $S_n^{(\lambda,\mu)}(x)$ have the following Eisenstein properties.*

(1) $S_{5^{2\alpha}}^{(-1,-1)}(x+3)$ *is Eisenstein at* 5 *for all* $n \geq 1$;
(2) $S_{5^{2\alpha+1}}^{(1,1)}(x+3)$ *is Eisenstein at* 5 *for all* $n \geq 1$;
(3) $S_{11^{2\alpha+1}}^{(1,\mu)}(x+1)$ *is Eisenstein at 11 for all* $n \geq 0$;
(4) $S_{3^\alpha}^{(\lambda,\mu)}(x-1)$ *is Eisenstein at 3 for all* $\lambda, \mu \in \{\pm 1\}$ *and for all* $n \geq 1$.

In terms of numerical evidence for the conjecture, we have verified the following cases of Conjecture 1 in Pari/gp:

Polynomial	p	Cases verified
$S_{3^\alpha}^{(\lambda,\mu)}(x-1)$	3	$1 \leq \alpha \leq 8$
$S_{5^{2\alpha}}^{(-1,-1)}(x+3)$	5	$\alpha = 1, 2$
$S_{5^{2\alpha+1}}^{(1,1)}(x+3)$	5	$\alpha = 1, 2$
$S_{11^{2\alpha+1}}^{(1,\mu)}(x+1)$	11	$\alpha = 0, 1$

Finally, we will prove an Eisenstein result similar to one of the many in [6, Theorem 1.1] in the case where the degree is a power of 7. Namely, Mahburg and Ono prove that their polynomials are Eisenstein at $p = 7$ when "$r = 6$" (in their notation) and the degree is a power of 7. We will now work out the complementary "$r = 0$" case (so set $\mu = 1$).

Theorem 4 *The polynomials $S_{7^\alpha}^{(-1,1)}(x)$ are Eisenstein at $p = 7$.*

Before proving Theorem 4 we establish some notation. Recall that we write $S_n^{(\lambda,\mu)}(x) = \sum_{j=0}^{n} A_j x^j$ where

$$A_j = \binom{n}{j} \prod_{k=j+1}^{n} c(n,\lambda,\mu,k) = \binom{n}{j} \prod_{k=j+1}^{n} \frac{6k+2\lambda}{6n+2\lambda+3\mu+6k}.$$

The constant coefficient of $S_{7^\alpha}^{(-1,1)}(x)$ is given by

$$A_0 = \prod_{k=1}^{7^\alpha} \frac{6k-2}{6\cdot 7^\alpha + 6k - 5},$$

and observe that the numerator $6k-2$ and denominator $6\cdot 7^\alpha + 6k - 5$ of the k-th term in the product cannot simultaneously be divisible by 7. This prompts the following definitions:

$$X_N(s) \stackrel{\text{def}}{=} \{k \in [1, 7^\alpha] \cap \mathbf{Z} \mid \text{ord}_7(6k-2) = \alpha - s, \}$$
$$X_D(s) \stackrel{\text{def}}{=} \{k \in [1, 7^\alpha] \cap \mathbf{Z} \mid \text{ord}_7(6\cdot 7^\alpha + 6k - 5) = \alpha - s\}.$$

The proof of Theorem 4 will follow once we show that the 7-adic Newton polygon has the shape given in Fig. 3.

Lemma 4 *For $s \in \mathbf{Z}$, the sizes of $X_N(s)$ and $X_D(s)$ are given by the following formulas*

(1) $\#X_N(s) = \#X_D(s) = 6\cdot 7^{s-1}$ *for* $s = 1, \ldots, \alpha$;
(2) $\#X_N(0) = 1$ *and* $\#X_D(0) = 0$;
(3) $\#X_N(1) = 0$ *and* $\#X_D(-1) = 1$;
(4) $\#X_N(s) = \#X_D(s) = 0$ *if* $s < -1$ *or if* $s > \alpha$.

Proof Because of the range $1 \le k \le 7^\alpha$ it is clear that $X_N(s) = X_D(s) = \emptyset$ if $s < -1$ or if $s > \alpha$. Similarly, it is easy to show that $X_N(0) = \{\frac{2\cdot 7^\alpha + 1}{3}\}$, $X_D(-1) = \{\frac{7^\alpha + 5}{6}\}$, and that $X_N(-1) = X_D(0) = \emptyset$. It therefore remains to see that $\#X_n(s) = \#X_D(s) = 6\cdot 7^{s-1}$ for $s = 1, \ldots, \alpha$. But for k in the range $1 \le k \le 7^\alpha$, one can easily verify that $k \in X_N(s)$ if and only if $6k - 2 = m7^{\alpha - s}$ with $\gcd(m, 7) = 1$, where

$$m = 4 + 6t,\ t \in \{0, \ldots, 7^s - 1\} \setminus \{4 + \ell\cdot 7\}_{\ell=1}^{7^{s-1}-1}.$$

Similarly, $k \in X_D(s)$ if and only if k is of the form

$$k = 6\cdot 7^\alpha + 1 + 6t, \text{ where } t \in \{0, \ldots, 7^s - 1\} \setminus \{1 + 7\ell\}_{\ell=1}^{7^{s-1}}.$$

Both sets $X_N(s)$ and $X_D(s)$ have size $6\cdot 7^{s-1}$, as claimed. □

Corollary 5 *Write* $S_{7^\alpha}^{(-1,1)}(x) = \sum_{j=0}^{7^\alpha} A_j x^j$. *Then* $\text{ord}_7 A_0 = -1$.

Proof Since $A_0 = \prod_{k=1}^{7^\alpha} \frac{6k-2}{6\cdot 7^\alpha + 6k - 5}$ we can compute $\text{ord}_7 A_0$ by the sizes of the sets $X_N(s)$ and $X_D(s)$ for $s = -1, \ldots, \alpha$. By Lemma 4 the number of terms with positive valuation

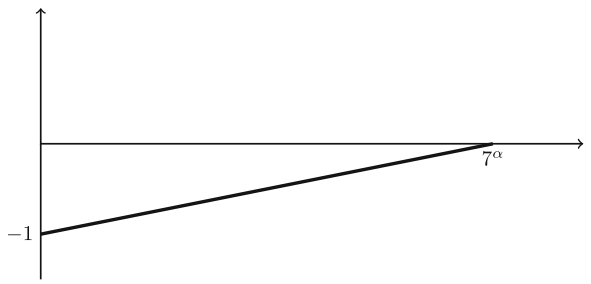

Fig. 3 7-Adic Newton polygon of $S_{7^\alpha}^{(-1,1)}(x)$

$\alpha - s$ equals the number with negative valuation $\alpha - s$ for $s = 1, \ldots, \alpha$. There is then a single value of k for which $\frac{6k-2}{6\cdot 7^\alpha + 6k - 5}$ contributes a positive valuation of α and a single value of k for which it contributes a negative valuation of $r + 1$ (parts (2) and (3) of the Lemma). Altogether, the 7-valuation of A_0 equals -1, as claimed. □

Since the entire family $S_n^{(\lambda,\mu)}(x)$ is monic, it follows that $\mathrm{ord}_7 A_n = 0$. Therefore, in order to show that the 7-adic Newton polygon of $S_{7^\alpha}^{(-1,1)}(x)$ is as claimed, it suffices to show that $\mathrm{ord}_7 A_j \geq 0$ for $j = 1, \ldots, 7^\alpha - 1$. We will obtain this as a corollary to the following sequence of Lemmas.

Lemma 5 *Let* $A_j = \prod_{k=1}^{j} \frac{6k-2}{6\cdot 7^\alpha + 6k - 5}$. *Then*

$$\mathrm{ord}_7 A_j = \begin{cases} \mathrm{ord}_7 \prod_{k=1}^{j} \frac{6k-2}{6k-5} & \text{if } 1 \leq j < \frac{7^\alpha + 5}{6} \\ \mathrm{ord}_7 \prod_{k=1}^{j} \frac{6k-2}{6k-5} - 1 & \text{if } j \geq \frac{7^\alpha + 5}{6}. \end{cases}$$

Proof This is a simple computation. □

Lemma 5 allows us to shift our focus to the 7-valuation of the product $\prod_{k=1}^{j} \frac{6k-2}{6k-5}$. Continuing, since 7 is odd we can divide the product by 2^j. Reindexing, we get

$$\mathrm{ord}_7 \prod_{k=1}^{j} \frac{6k-2}{6k-5} = \mathrm{ord}_7 \prod_{k=0}^{j-1} \frac{3k+2}{6k+1}.$$

In preparation for the next lemma we introduce some notation. Let q be a prime number, n a positive integer, and let $x \in \mathbf{Z}$ be invertible modulo q^n. Denote by $i_{q^n}(x)$ the unique representative among the integers $1, \ldots, q^n - 1$ of the inverse of x modulo q^n.

Lemma 6 *With all notation as above, we have* $0 \geq \mathrm{ord}_7 \prod_{k=0}^{j-1} \frac{3k+2}{6k+1} \geq -\alpha$.

Proof According to [1, Formula 2.9], we may write the 7-valuations of the numerators in the following explicit forms:

$$\mathrm{ord}_7 \prod_{k=0}^{j-1} (6k+1) = \sum_{n \geq 1} \left\lfloor \frac{j - 1 + i_{7^n}(6)}{7^n}, \right\rfloor$$
$$\mathrm{ord}_7 \prod_{k=0}^{j-1} (3k+2) = \sum_{n \geq 1} \left\lfloor \frac{j - 1 + i_{7^n}(3/2)}{7^n} \right\rfloor.$$

It is easy to show that

$$i_{7^n}(6) = 6 + 5 \cdot 7 + \cdots + 5 \cdot 7^{n-1},$$
$$i_{7^n}(3/2) = 3 + 2 \cdot 7 + \cdots + 2 \cdot 7^{n-1}.$$

If x and y are positive real numbers, then we will employ the elementary observation that

$$\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor \leq \lfloor x \rfloor + \lfloor y \rfloor + 1$$

in the estimate of $\operatorname{ord}_7 \prod_{k=0}^{j-1} \frac{3k+2}{6k+1}$. Write

$$\begin{aligned}\operatorname{ord}_7 \prod_{k=0}^{j-1} \frac{3k+2}{6k+1} &= \sum_{n\geq 1} \left\lfloor \frac{j-1+i_{7^n}(3/2)}{7^n} \right\rfloor - \left\lfloor \frac{j-1+i_{7^n}(6)}{7^n} \right\rfloor \\ &= \sum_{n\geq 1} \left\lfloor \frac{j-1+(3+2\cdot 7+\cdots+2\cdot 7^{n-1})}{7^n} \right\rfloor \\ &\quad - \left\lfloor \frac{j-1+(6+5\cdot 7+\cdots+5\cdot 7^{n-1})}{7^n} \right\rfloor \\ &= \sum_{n\geq 1} \left\lfloor \frac{j-1+(3+2\cdot 7+\cdots+2\cdot 7^{n-1})}{7^n} \right\rfloor \\ &\quad - \left\lfloor \frac{j-1+(3+2\cdot 7+\cdots+2\cdot 7^{n-1})}{7^n} + \frac{3+3\cdot 7+\cdots 3\cdot 7^{n-1}}{7^n} \right\rfloor.\end{aligned}$$

Applying the elementary inequality of the floor function to each summand yields

$$0 = \sum_{n\geq 1} 0 \geq \operatorname{ord}_7 \prod_{k=0}^{j-1} \frac{3k+2}{6k+1} \geq \sum_{n\geq 1} -1.$$

There are at most α nonzero terms in the sum, whence $0 \geq \operatorname{ord}_7 \prod_{k=0}^{j-1} \frac{3k+2}{6k+1} \geq -\alpha$, as claimed. □

Lemma 7 *Let $\alpha, j \geq 1$. Then $0 \geq \operatorname{ord}_7 \prod_{k=1}^{j} \frac{6k-2}{6\cdot 7^\alpha+6k-5} \geq -\alpha - 1$.*

Proof This follows from Lemmas 5 and 6. □

Corollary 6 *With all notation as above, $\operatorname{ord}_7 A_j \geq 0$ for $j = 1, \ldots 7^\alpha - 1$.*

Proof Since $A_j = \binom{7^\alpha}{j} \prod_{k=j+1}^{7^\alpha} \frac{6k-2}{6\cdot 7^\alpha+6k-5} = \binom{7^\alpha}{j} \frac{A_0}{\prod_{k=1}^{j} \frac{6k-2}{6\cdot 7^\alpha+6k-5}}$, we have

$$\begin{aligned}\operatorname{ord}_7 A_j &= \operatorname{ord}_7 \binom{7^\alpha}{j} \frac{A_0}{\prod_{k=1}^{j} \frac{6k-2}{6\cdot 7^\alpha+6k-5}} \\ &= \alpha - \operatorname{ord}_7 j - 1 - \operatorname{ord}_7 \prod_{k=1}^{j} \frac{6k-2}{6\cdot 7^\alpha+6k-5}.\end{aligned}$$

Since $0 \leq \operatorname{ord}_7(j) \leq \alpha - 1$ and using Lemma 7, this gives the desired bound. □

To recap, since $S_{7^\alpha}^{(-1,1)}(x)$ is monic we have $\operatorname{ord}_7 A_n = 0$, while Corollary 5 establishes $\operatorname{ord}_7 A_0 = -1$. Corollary 6 then shows $\operatorname{ord}_7 A_j \geq 0$ for all intermediate j. Therefore $S_{7^\alpha}^{(-1,1)}(x)$ is Eisenstein at 7, hence irreducible over $\mathbf{Q}$.

Authors' contributions
Both authors made substantial contributions to conception of the article as well as all computations, proofs, writing, and final approval of the document. Both authors read and approved the final manuscript.

Acknowledgements
We would like to thank Farshid Hajir for alerting us to reference [1] and Farshid Hajir, Ken Ono, and the anonymous referees for helpful comments.

Competing interests
The authors declare that they have no competing interests.

Received: 21 July 2016 Accepted: 26 October 2016
Published online: 14 December 2016

References

1. Amdeberhan, T., Moll, V., Straub, A.: The p-adic valuation of k-central binomial coefficients. Acta Arith. **140**, 31–42 (2009)
2. Brillhart, J., Morton, P.: Class numbers of quadratic fields, Hasse invariants of elliptic curves, and the supersingular polynomial. J. Number Theory **106**, 79–111 (2004)
3. Coleman, R.: On the Galois groups of exponential Taylor polynomials. Enseign. Math. **33**, 183–189 (1987)
4. Cullinan, J., Hajir, F.: Algebraic properties of Kaneko-Zagier lifts of supersingular polynomials. To appear in Proceedings of the American Mathematical Society
5. Kaneko, M., Zagier, D.: Supersingular j-invariants, hypergeometric series, and Atkin's orthogonal polynomials. Computational perspectives on number theory (Chicago, IL, 1995). AMS/IP Stud. Adv. Math. **7**, 97–126 (1998)
6. Mahlburg, K., Ono, K.: Arithmetic of certain hypergeometric modular forms. Acta Arith. **113**(1), 39–55 (2004)
7. Schur, I.: Einige Sätze über Primzahlen mit Anwendungen auf Irreduzibilitätsfragen I (1929) Gessammelte Abhandlungen, Band III, vol. 64, pp. 140–151. Springer, Berlin (1973)
8. Silverman, J.H.: The arithmetic of elliptic curves. Graduate texts in mathematics, vol. 106. Springer, Berlin (2009)