ON THE DISCRIMINANTS OF TRUNCATED LOGARITHMIC POLYNOMIALS

John Cullinan
Department of Mathematics, Bard College, Annandale-On-Hudson, New York
cullinan@bard.edu

Rylan Gajek-Leonard
Department of Mathematics, Union College, Schenectady, New York
gajekler@union.edu

Received: 12/30/24, Revised: 3/2/25, Accepted: 4/6/25, Published: 4/25/25

Abstract

We provide evidence for a conjecture of Yamamura that the truncated logarithmic polynomials

$$F_n(x) = 1 + x + \frac{x^2}{2} + \cdots + \frac{x^n}{n}$$

have Galois group S_n for all $n \geq 1$.

1. Introduction

A pioneering result of Schur [11] asserts that the truncated exponential polynomials,

$$1 + x + \frac{x^2}{2!} + \cdots + \frac{x^n}{n!},$$

are irreducible over $\mathbf{Q}$ with Galois group A_n (if $4 \mid n$) or S_n (otherwise). What can be said about the Galois groups of rational polynomials arising from series truncations of other interesting functions?

Motivated by Schur's work, in [12] the authors consider the irreducibility and Galois properties of the polynomials

$$F_n(x) = 1 + x + \frac{x^2}{2} + \cdots + \frac{x^n}{n}.$$

These polynomials arise as the truncated Maclaurin polynomials of the functions $F(x) = 1 - \log(1 - x)$. A main result of [12] is that $\mathrm{Gal}_{\mathbf{Q}}(F_n) \simeq S_n$ for any $n \geq 12$ with $n \not\equiv 1 \bmod 4$ and for any *prime* value of $n \equiv 1 \bmod 4$ (cf. [12, Theorem 3.1]).

DOI: 10.5281/zenodo.15283716

This work, together with numerical computations at small values of n, prompted Yamamura [13] to conjecture the following.

Conjecture 1 (Yamamura)**.** For all $n \geq 1$, we have $\mathrm{Gal}_{\mathbf{Q}}(F_n) \simeq S_n$.

In this article, we offer:

- (Theorem 3) A proof of Yamamura's conjecture for infinitely many *composite* integers $n \equiv 1 \bmod 4$, thereby extending the results of [12].
- (Proposition 1) A short proof – different from that of [12] – of Yamamura's conjecture in the case $n \not\equiv 1 \bmod 4$.
- (Sections 2 and 5) Commentary on why one might expect a full proof in the case $n \not\equiv 1 \bmod 4$ to be difficult.

By a Newton polygon argument in [12], the F_n are irreducible over $\mathbf{Q}$ with $\mathrm{Gal}_{\mathbf{Q}}(F_n) \supseteq A_n$ for all $n \geq 1$. Thus, Yamamura's conjecture amounts to proving that the discriminant of F_n is not a rational square once $n > 1$. Let us now set some notation.

The discriminant of a univariate polynomial $P(x)$ of degree n and leading coefficient a_n is given by

$$\mathrm{disc}(P) = (-1)^{\binom{n}{2}} a_n^{-1} \,\mathrm{Res}(P, P'). \tag{1}$$

Computing the derivative

$$F_n'(x) = 1 + x + x^2 + \cdots + x^{n-1},$$

whose roots are the nontrivial n-th roots of unity, the discriminant we seek is therefore

$$\mathrm{disc}(F_n) = (-1)^{\binom{n}{2}} n \prod_{\{\theta : F_n'(\theta) = 0\}} F_n(\theta). \tag{2}$$

Let $L_n = \mathrm{lcm}\{1, 2, \ldots, n\}$. Then

$$F_n(x) = \frac{\widetilde{F}_n(x)}{L_n},$$

where $\widetilde{F}_n(x)$ is a polynomial with integer coefficients. The relations

$$\theta^n = 1 \qquad \text{and} \qquad 1 + \theta + \theta^2 + \cdots + \theta^{n-1} = 0$$

hold when θ is an n-th root of unity, which allow us to simplify $\widetilde{F}_n(\theta)$; we have

$$\widetilde{F}_n(\theta) = \sum_{k=0}^{n-2} a_k \theta^k \qquad \text{where} \qquad a_k = \begin{cases} L_n + \frac{L_n}{n} - \frac{L_n}{n-1} & \text{if } k = 0 \\ \frac{L_n}{k} - \frac{L_n}{n-1} & \text{if } k > 0. \end{cases} \tag{3}$$

Replacing $F_n(\theta)$ with $\widetilde{F}_n(\theta)/L_n$ in Equation (2) yields the following expression for the discriminant of $F_n(x)$:

$$\operatorname{disc}(F_n) = (-1)^{\binom{n}{2}} \frac{n}{L_n^{n-1}} \prod_{\{\theta : F_n'(\theta)=0\}} \widetilde{F}_n(\theta). \tag{4}$$

Note that the product

$$\mathcal{P}_n := \prod_{\{\theta : F_n'(\theta)=0\}} \widetilde{F}_n(\theta) \tag{5}$$

is an integer. As we will see below, the main difficulty in proving Yamamura's conjecture is understanding the prime factorization of $\mathcal{P}_n$. We pause for an illustrative example.

Example 1. Let $n = 9$. Then we compute

$$\operatorname{disc}(F_9) = \frac{9}{L_9^8} \prod_{\{\theta : F_9'(\theta)=0\}} \widetilde{F}_9(\theta) = \left(\frac{3}{2^{12}3^85^47^4}\right)^2 \mathcal{P}_9,$$

hence $\operatorname{disc}(F_9)$ is a rational square if and only if $\mathcal{P}_9$ is. In this case, we compute

$$\mathcal{P}_9 = 1531 \cdot 3137311 \cdot 113564970051005791,$$

and these prime factors do not appear to be predictable *a priori*.

The above example illustrates the main difficulty in proving $\operatorname{disc}(F_n) \notin \mathbf{Q}^{\times 2}$ when n is a square: the factor $\mathcal{P}_n$ is typically not divisible by primes dividing n, so we cannot use "small" primes to our advantage. And, additionally, the prime divisors of $\mathcal{P}_n$ may be quite difficult or impossible to characterize.

In [12] the authors show that if $n \equiv 0, 2, 3 \pmod 4$, then $\operatorname{disc}(F_n) \notin \mathbf{Q}^{\times 2}$. They then prove that if $n \equiv 1 \pmod 4$ and n is prime, then $\operatorname{disc}(F_n) \notin \mathbf{Q}^{\times 2}$. In some cases we give independent, streamlined proofs of these discriminant results, as well as some mild generalizations, as follows.

Theorem 1. *If $n \equiv 0, 2, 3 \pmod 4$, or if $n \equiv 1 \pmod 4$ and is the odd power of a prime, then $\operatorname{disc}(F_n) \notin \mathbf{Q}^{\times 2}$.*

Regarding the prime divisors of $\mathcal{P}_n$, we can say the following as a generalization of Example 1.

Theorem 2. *If $n = p^{2e}$ for an odd prime p and a positive integer e, then $\mathcal{P}_n$ is coprime to p.*

However, the main contribution of this paper is to give substantially new infinite families of integers $n \equiv 1 \pmod 4$ for which $\operatorname{disc}(F_n)$ is not a rational square.

Theorem 3. *Let m be a positive integer. For all but finitely many primes q, if $mq \equiv 1 \pmod 4$ then $\mathrm{disc}(F_{mq}) \notin \mathbf{Q}^{\times 2}$.*

Remark 1. For each integer m one can explicitly compute the finite set of primes for which the above theorem does not apply. It is then a matter of computation to check that $\mathrm{disc}(F_n) \notin \mathbf{Q}^{\times 2}$ for each of these exceptional primes. We give examples to demonstrate this in the final section of this article.

Before proving our results, we briefly survey the calculation of discriminants for number-theoretic purposes.

2. Commentary on Discriminants, Resultants, and Arithmetic

The systematic study of the algebraic properties of families of orthogonal polynomials appears to originate in two papers of Holt [6, 7], in which he studies the irreducibility of certain Legendre polynomials. Holt's methods were generalized significantly by Ille and Schur [11], leading to extensive studies of the irreducibility and Galois theory of many families of hypergeometric polynomials (e.g., Jacobi, Laguerre, Chebyshev, Hermite). Assuming irreducibility, there are Newton Polygon methods that will allow one to prove that the Galois group contains A_n. Deciding whether or not the Galois group is all of S_n is then a matter of determining when the discriminant is a rational square.

The applications of orthogonal polynomials to arithmetic go beyond computational Galois theory. In particular, if $\mathrm{ss}_p(t) \in \mathbf{F}_p[t]$ denotes the supersingular polynomial (whose roots are the supersingular j-invariants of elliptic curves over $\mathbf{F}_p$), then $\mathrm{ss}_p(t)$ is the reduction modulo p of a certain Jacobi polynomial. For more background and for other interesting lifts of $\mathrm{ss}_p(t)$ to $\mathbf{Q}$, see [8, 10]. A conjecture of Mahburg and Ono [9] states that the "Jacobi lifts" are irreducible with maximal Galois group, and in [5] we gave evidence for this conjecture using many of the techniques originally described by Schur.

In the case of the classical families of orthogonal polynomials, the discriminants tend to have nice expressions. A prototypical example is the case of the truncated exponential polynomials

$$e_n(x) = \sum_{j=0}^{n} \frac{x^j}{j!},$$

whose discriminants are given by $\mathrm{disc}(e_n) = (-1)^{\binom{n}{2}} (n!)^n$. This formula is a key feature of Coleman's proof that $\mathrm{Gal}_{\mathbf{Q}}(e_n)$ always contains A_n and equals S_n if and only if $4 \nmid n$ [2]. We note that if

$$L_n^{(\alpha)}(x) = \sum_{i=0}^{n} (-1)^i \binom{n+\alpha}{n-i} \frac{x^i}{i!}$$

denotes the nth Generalized Laguerre Polynomial (GLP), then $e_n(x) = L_n^{(-1-n)}(x)$.

Ultimately, the reason that certain hypergeometric polynomials (including all of the ones mentioned above) have such tidy discriminant formulas is that they satisfy a Sturm-Liouville differential equation, relating the derivative of a member of the family to another member, and that the polynomials solve certain recurrence relations; for example, in the case of the GLP we have

$$\frac{\mathrm{d}}{\mathrm{d}x} L_n^{(\alpha)}(x) = -L_{n-1}^{(\alpha+1)}(x).$$

The recurrence relations, together with the differential equations, typically allow for explicit discriminant formulas, via Equation (1), which are amenable to arithmetic study.

This is not the case with the truncated logarithmic polynomials $F_n(x)$ – the derivative of $F_n(x)$ does not belong to the same family (as in the case of the classical orthogonal polynomials). However, the roots of $F_n'(x)$ are the nontrivial n-th roots of unity, hence are independently equipped with a good deal of algebraic and arithmetic symmetry. Thus, from the point of view of discriminants, our family $\{F_n(x)\}$ is more amenable to computation than a "random" family of polynomials, but is harder to work with than a family of classical orthogonal polynomials. This manifests itself in Equation (4) where we understand some of the prime factorization quite well (viz., n/L_n^{n-1}) and the rest ($\mathcal{P}_n$) not at all.

3. Preliminary Results

Combining Equations (4) and (5), we can write

$$\operatorname{disc}(F_n) = (-1)^{\binom{n}{2}} \frac{n\mathcal{P}_n}{L_n^{n-1}}. \tag{6}$$

By Equation (5), $\mathcal{P}_n$ is an integer since it is the resultant of integral polynomials. We start with a lemma showing that $\mathcal{P}_n$ is positive.

Lemma 1. *Let $\mathcal{P}_n$ be defined as in Equation (5). Then $\mathcal{P}_n$ is positive.*

Proof. Let $n > 1$. If n is odd, the roots of $F_n'(x) = 1 + x + x^2 + \cdots + x^{n-1}$ come in complex-conjugate pairs. If n is even, then -1 is the unique real root of $F_n'(x)$, while the remaining roots come in complex-conjugate pairs. For each pair of complex-conjugate roots $(\theta, \overline{\theta})$, we have

$$F_n(\theta)F_n(\overline{\theta}) = F_n(\theta)\overline{F_n(\theta)} = \|F_n(\theta)\|^2 > 0,$$

taking advantage of the fact that the polynomial $F_n(x)$ has real coefficients. One also verifies directly that $F_n(-1) > 0$. Therefore, whether n is even or odd, we have

$$\mathcal{P}_n = \prod_{\{\theta:\ F_n'(\theta)=0\}} \widetilde{F}_n(\theta) = L_n^{1-n} \prod_{\{\theta:\ F_n'(\theta)=0\}} F_n(\theta) > 0,$$

as claimed. □

We now give a concise proof that $\operatorname{disc}(F_n) \notin \mathbf{Q}^{\times 2}$ when $n \not\equiv 1 \pmod 4$.

Proposition 1. *If $n \equiv 0, 2,$ or $3 \pmod 4$, then $\operatorname{disc}(F_n) \notin \mathbf{Q}^{\times 2}$.*

Proof. Applying Lemma 1 to Equation (6) shows that if $n \equiv 2, 3 \pmod 4$, then $\operatorname{disc}(F_n) < 0$ and hence is not a rational square. If $n \equiv 0 \pmod 4$, we first compute $\operatorname{disc}(F_4) = 725/432 \notin \mathbf{Q}^{\times 2}$. If $n \geq 8$, then there exists a prime number in the interval $(n/2, n-2)$. Fix such a prime ℓ and observe that $v_\ell(n) = 0$ and that $v_\ell(L_n) = 1$. Thus, $v_\ell\left(n/L_n^{n-1}\right)$ is odd. For a nontrivial n-th root of unity θ, consider $\widetilde{F}_n(\theta)$. Reducing Equation (3) modulo ℓ, we have $\widetilde{F}_n(\theta) \equiv (L_n/\ell)\,\theta^\ell \pmod \ell$, whence $\mathcal{P}_n$ is coprime to ℓ:

$$\begin{aligned}
\mathcal{P}_n &= \prod_{\{\theta:F_n'(\theta)=0\}} \widetilde{F}_n(\theta) \\
&\equiv \prod_{\{\theta:F_n'(\theta)=0\}} \frac{L_n}{\ell}\theta^\ell \pmod \ell \\
&\equiv \left(\frac{L_n}{\ell}\right)^{n-1} \cdot (-1) \pmod \ell \\
&\not\equiv 0 \pmod \ell.
\end{aligned}$$

Thus, $v_\ell(\operatorname{disc}(F_n))$ is odd and so $\operatorname{disc}(F_n) \notin \mathbf{Q}^{\times 2}$. □

This brings us to the case $n \equiv 1 \pmod 4$, which is the most mysterious. We start by generalizing [12, Thm. 3.1] to when n is a prime power.

Theorem 4. *Let $p \equiv 1 \pmod 4$, e a positive integer, and $n = p^e$. Then $\mathcal{P}_n$ is coprime to p.*

Proof. We start by reducing the factors $\widetilde{F}_n(\theta)$ of $\mathcal{P}_n$ modulo p:

$$\begin{aligned}
a_0 &= L_n + \frac{L_n}{n} - \frac{L_n}{n-1} \equiv \frac{L_n}{n} \pmod p \not\equiv 0 \pmod p, \text{ and} \\
a_k &= \frac{L_n}{k} - \frac{L_n}{n-1} \equiv 0 \pmod p
\end{aligned}$$

for all $k = 1, \dots n-2$, due to the fact that $0 \leq v_p(k) \leq e-1$ for all such k. Therefore

$$\mathcal{P}_n = \prod_{\{\theta : F_n'(\theta)=0\}} \widetilde{F}_n(\theta) \equiv \prod_{\{\theta : F_n'(\theta)=0\}} \frac{L_n}{n} \equiv \left(\frac{L_n}{n}\right)^{n-1} \not\equiv 0 \pmod{p},$$

as claimed. □

Corollary 1. *Let $p \equiv 1 \pmod 4$, e a positive integer, and $n = p^e$. If e is odd, then $\operatorname{disc}(F_n) \notin \mathbf{Q}^{\times 2}$. If e is even, then $\operatorname{disc}(F_n) \notin \mathbf{Q}^{\times 2}$ if and only if $\mathcal{P}_n \notin \mathbf{Q}^{\times 2}$.*

Proof. Note that whether e is even or odd, we have

$$v_p\left(\operatorname{disc}(F_n)\right) = v_p(n) - (n-1)v_p(L_n) + v_p(\mathcal{P}_n) = e - e(n-1) + 0,$$

by Theorem 4. If e is odd, then $v_p\left(\operatorname{disc}(F_n)\right)$ is odd (because $n \equiv 1 \pmod 4$) and hence $\operatorname{disc}(F_n) \notin \mathbf{Q}^{\times 2}$. If e is even, then n/L_n^{n-1} is a rational square, hence $\operatorname{disc}(F_n)$ is a rational square if and only if $\mathcal{P}_n$ is. □

By Example 1, we cannot expect to make much general progress on the case when $n \equiv 1 \pmod 4$ when n is a square, due to the unpredictable prime factorization of $\mathcal{P}_n$. For the rest of the paper, we assume $n \equiv 1 \pmod 4$ is not a square.

4. The Case $n = mq$

Fix a positive integer m, let ω be a primitive mth root of unity, and define

$$X(m) := \prod_{k=1}^{m-1} \left(\frac{1}{m} + \omega^k + \frac{1}{2}\omega^{2k} + \cdots + \frac{1}{(m-1)}\omega^{(m-1)k}\right)$$
$$Y(m) := 1 + \frac{1}{2} + \cdots + \frac{1}{m}.$$

Observe that both $X(m)$ and $Y(m)$ are rational numbers. Consider the set

$$\mathrm{E}_m = \{\text{primes } \ell \mid v_\ell(X(m)) > 0,\, v_\ell(Y(m)) > 0, \text{ and } m\ell \equiv 1 \pmod 4\},$$

consisting of all prime divisors of $X(m)$ and $Y(m)$ whose product with m is congruent to 1 (mod 4).

Remark 2. While E_m can be computed explicitly for fixed m, we expect that saying anything in general about this set could be difficult. Even without considering $X(m)$, the set E_m relies on understanding p-adic properties of the sequence $Y(m)$ of harmonic numbers, which is known to be a hard problem (see [1]).

Theorem 5. *For all primes q such that $q \notin \mathrm{E}_m$, if $q > m$ and $n := mq \equiv 1 \pmod 4$, we have $\operatorname{disc}(F_n) \notin \mathbf{Q}^{\times 2}$.*

Proof. Recall that

$$\operatorname{disc}(F_{mq}) = \frac{mq}{L_{mq}^{mq-1}}\mathcal{P}_{mq}. \tag{7}$$

Since $mq \equiv 1 \pmod 4$, we have that $v_q\left(\frac{mq}{L_{mq}^{mq-1}}\right)$ is odd. Thus, if $v_q(\mathcal{P}_{mq})$ is even, then $\operatorname{disc}(F_{mq}) \notin \mathbf{Q}^{\times 2}$. We now compute $\mathcal{P}_{mq} \pmod q$.

Let $\theta_k = \exp(2\pi i/mq)^k$ and $\omega = \exp(2\pi i/m)$. Then

$$\mathcal{P}_{mq} = \prod_{k=1}^{mq-1}\left(\sum_{j=0}^{mq-2} a_j\theta_k^j\right).$$

Reducing each coefficient modulo q gives us

$$\begin{aligned}
\mathcal{P}_{mq} &\equiv \prod_{k=1}^{mq-1}\left(a_0 + a_q\theta_k^q + a_{2q}\theta_k^{2q} + \cdots + a_{(m-1)q}\theta_k^{(m-1)q}\right) \pmod q \\
&\equiv \prod_{k=1}^{mq-1}\left(a_0 + a_q\omega^k + a_{2q}\omega^{2k} + \cdots + a_{(m-1)q}\omega^{k(m-1)}\right) \pmod q \\
&\equiv \prod_{k=1}^{mq-1}\left(\frac{L_{mq}}{mq} + \frac{L_{mq}}{q}\omega^k + \frac{L_{mq}}{2q}\omega^{2k} + \cdots + \frac{L_{mq}}{(m-1)q}\omega^{k(m-1)}\right) \pmod q \\
&\equiv \underbrace{\left(\frac{L_{mq}}{q}\right)^{mq-1}}_{\not\equiv 0 \pmod q}\prod_{k=1}^{mq-1}\left(\frac{1}{m} + \frac{\omega^k}{1} + \frac{\omega^{2k}}{2} + \cdots + \frac{\omega^{k(m-1)}}{(m-1)}\right) \pmod q.
\end{aligned}$$

As k ranges over $1, \ldots, mq-1$, the product in the last congruence above can be rewritten as

$$\begin{aligned}
\prod_{k=1}^{mq-1}\left(\frac{1}{m} + \frac{\omega^k}{1} + \frac{\omega^{2k}}{2} + \cdots + \frac{\omega^{k(m-1)}}{(m-1)}\right) &= (X(m)Y(m))^{q-1}\,X(m) \\
&= X(m)^qY(m)^{q-1}.
\end{aligned}$$

Thus,

$$\mathcal{P}_{mq} \equiv \left(\frac{L_{mq}}{q}\right)^{mq-1} X(m)^qY(m)^{q-1} \pmod q,$$

which is coprime to q by the hypothesis that $X(m)$ and $Y(m)$ are both coprime to q. Thus, $v_q(\mathcal{P}_{mq}) = 0$ and so $\operatorname{disc}(F_{mq}) \notin \mathbf{Q}^{\times 2}$. □

5. Examples and Conclusions

We conclude the paper with several examples and observations. We start by setting $m = p$, a prime number, in Theorem 5. If we fix p, then as long as both $X(p)$

and $Y(p)$ are coprime to $q > p$, we can conclude that $\mathrm{disc}(F_{pq}) \notin \mathbf{Q}^{\times 2}$. For the remaining values of $q \in \mathrm{E}_p$, we can check by hand as long as it is computationally feasible. The following result is a sample implementation of our methods. We note that other examples with $n = pq$ are similarly easy to generate.

Proposition 2. *For any prime q, if $n = 3q$, $5q$, or $7q$, then* $\mathrm{disc}(F_n) \notin \mathbf{Q}^{\times 2}$.

Proof. If $n \equiv 2, 3 \pmod 4$, we are done by Proposition 1. We have seen in Example 1 that $\mathrm{disc}(F_9) \notin \mathbf{Q}^{\times 2}$. By using the `issquare` command in `PariGP` we check that neither $\mathrm{disc}(F_{25})$ nor $\mathrm{disc}(F_{49})$ is a rational square.

It therefore suffices to consider $n = 3q$, $5q$, or $7q$ in the case $n \equiv 1 \pmod 4$ and $q > 3, 5, 7$, respectively. By Theorem 5, we are reduced to checking finitely many cases. In Table 1 we compute, for each value of p, the rational numbers $X(p)$ and $Y(p)$ and determine the set E_p.

p	$X(p)$	$Y(p)$	E_p
3	$13/36$	$11/6$	$\{11\}$
5	$(11 \cdot 101 \cdot 3001)/(2^8 3^4 5^4)$	$137/(2^2 \cdot 3 \cdot 5)$	$\{101, 137, 3001\}$
7	$1170728665999621/(2^{12} 3^6 5^6 7^6)$	$(3 \cdot 11^2)/(2^2 \cdot 5 \cdot 7)$	$\{11\}$

Table 1: $X(p)$, $Y(p)$, and E_p for $p \in \{3, 5, 7\}$.

In each case we find an auxiliary prime ℓ for which $\mathrm{disc}(F_n)$ is not a square modulo ℓ:

$$\begin{aligned} \mathrm{disc}(F_{33}) &\equiv 14 \pmod{37} \\ \mathrm{disc}(F_{505}) &\equiv 200 \pmod{509} \\ \mathrm{disc}(F_{685}) &\equiv 443 \pmod{709} \\ \mathrm{disc}(F_{15005}) &\equiv 13652 \pmod{15017} \\ \mathrm{disc}(F_{77}) &\equiv 39 \pmod{79}; \end{aligned}$$

none of these are squares. □

We close with several observations which suggest that a different approach than that discussed in this paper may be necessary in order to prove Yamamura's conjecture in general. In particular, the condition that $n = mq$ with $q > m$ is a strong hypothesis that we cannot remove. What cases are left to prove? Among all $n \equiv 1 \pmod 4$, either

- n is an odd square, or

- n has at least two distinct prime divisors, and at least one prime divisor at which n has odd valuation.

In the second case, Theorem 5 handles values of the form

$$n = q_1^{e_1} q_2^{e_2} \cdots q_{r-1}^{e_r - 1} q_r,$$

for prime numbers $q_1 < q_2 < \cdots < q_r$. With regard to generalizing the proof of Theorem 5, we present the following data as evidence that a different approach is needed.

1. The condition $q > m$ in Theorem 5 allows us to compute $\widetilde{F}_{mq}(\theta) \pmod q$ easily – the only a_k which are not divisible by q are the a_{jq} for $j = 1, \ldots, m-1$. If $q < m$, then we would need to include additional multiples of q less than m.

   For example, consider $n = 21 = 3 \cdot 7$. By Proposition 2, we know that $\operatorname{disc}(F_{21}) \notin \mathbf{Q}^{\times 2}$ by working modulo 7. However, if we were to localize at the prime 3 instead, we first directly compute in `PariGP` that $v_3(\operatorname{disc}(F_{21})) = -34$, and then separately compute using (7) that

   $$v_3\left(\operatorname{disc}(F_{21})\right) = v_3(21) - 20v_3(L_{21}) + v_3(\mathcal{P}_{21}) = 1 - 40 + v_3(\mathcal{P}_{21}),$$

   whence $v_3(\mathcal{P}_{21}) = 5$. Therefore, it is not the case that if $v_p(n)$ is odd then $v_p\left(\operatorname{disc}(F_n)\right)$ is odd as well.

   To finish this example, we note that the prime factorization of $\mathcal{P}_{21}$ is

   $$\begin{aligned}\mathcal{P}_{21} = {} & 3^5 \cdot 31 \cdot 41^2 \cdot 335642497 \cdot 1236257387 \cdot 11513876767 \\ & \times 1381773062083 \cdot 3484835094151 \cdot 22041977186540318184049849 07 \\ & \times 900498913761021263552721322658562631017320322187479058732367538134039202916 81\end{aligned}$$

   This computation was carried out on `PariGP` in 38.5 minutes on a personal laptop.

2. Setting $m = 8$ in Theorem 5 implies $n \equiv 0 \pmod 4$, hence $m = 9$ is the smallest composite value of m for which we can have $n \equiv 1 \pmod 4$. In that case we compute

   $$\begin{aligned}X(9) &= \frac{37 \cdot 229 \cdot 367 \cdot 98481394090065580021}{2^{24}3^{16}5^87^8} \\ Y(9) &= \frac{7129}{2^3 \cdot 3^2 \cdot 5 \cdot 7}.\end{aligned}$$

   Thus, if $q \notin \{37, 229, 7129, 98481394090065580021\}$, we can immediately conclude that $\operatorname{disc}(F_{9q}) \notin \mathbf{Q}^{\times 2}$ (note that $367 \equiv 3 \pmod 4$). However, for the

remaining values of q we run into some of the computational limits of this question.

Let $q = 37$. One can verify in `PariGP` that $v_{37}(\mathcal{P}_{333}) = 37$, which agrees with

$$\mathcal{P}_{mq} \equiv \left(\frac{L_{mq}}{q}\right)^{mq-1} X(m)^q Y(m)^{q-1} \pmod{q}$$

from the proof of Theorem 5. Therefore, none of the primes < 333 can be used to immediately deduce whether or not $\mathrm{disc}(F_{333})$ is a rational square. The next prime larger than 333 is 337 and we check that $\mathrm{disc}(F_{333}) \equiv 157 \pmod{337}$, which is not a square; this computation took 16.2 seconds on a personal computer. However, a similar analysis is computationally infeasible for the remaining values of q.

3. It is not necessarily the case that if $p > n$, then $v_p(\mathrm{disc}(F_n))$ is odd (which would automatically imply $\mathrm{disc}(F_n) \notin \mathbf{Q}^{\times 2}$). For example, we have

$$v_{4019}(\mathrm{disc}(F_{15})) = v_{4019}(\mathcal{P}_{15}) = 2.$$

4. We checked all odd square values of n from 1 to 1000 and in none of those cases do we find that $\mathrm{disc}(F_n)$ is a rational square.

Acknowledgment. We would like to thank the referee for their comments which improved the exposition and clarity of the paper.

References

[1] D.W. Boyd, A p-adic study of the partial sums of the harmonic series, *Exp. Math.* **3** (1994), 287-302.

[2] R. Coleman, On the Galois groups of exponential Taylor polynomials, *Enseign. Math.* **33**, (1987), 183-189.

[3] J. Cullinan and F. Hajir, Ramification in iterated towers for rational functions, *Manuscripta Math.* **137** (2012), 273-286.

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

[5] J. Cullinan and R. Gajek-Leonard, On the Newton polygons of Kaneko-Zagier lifts of supersingular polynomials, *Res. Number Theory* **2** (2016), 1-16.

[6] J.B. Holt, On the irreducibility of Legendre's polynomials, *Proc. Lond. Math. Soc.* **12** (1913), 126-132.

[7] J.B. Holt, The irreducibility of Legendre's polynomials, *Proc. Lond. Math. Soc.* **11** (1913), 351-356.

[8] M. Kaneko and D. Zagier, Supersingular j-invariants, hypergeometric series, and Atkin's orthogonal polynomials, in *Computational Perspectives on Number Theory*, Amer. Math. Soc., Providence, RI, 1998, 97-126.

[9] K. Mahlburg and K. Ono, Arithmetic of certain hypergeometric modular forms, *Acta Arith.* **113** (2004), 39-55.

[10] P. Morton, Explicit identities for invariants of elliptic curves, *J. Number Theory* **120** (2006), 234-271.

[11] I. Schur, *Gessammelte Abhandlungen*, Vol. 3, Springer, 1973.

[12] M.K. Shokri, J. Shaffaf, and R. Taleb, Galois groups of Taylor polynomials of some elementary functions, *Int. J. Number Theory* **15** (2019), 1127-1141.

[13] K. Yamamura, MathSciNet review of [12].