ON THE GALOIS GROUPS OF LEGENDRE POLYNOMIALS

JOHN CULLINAN, FARSHID HAJIR

Abstract. Ever since Legendre introduced the polynomials that bear his name in 1785, they have played an important role in analysis, physics and number theory, yet their algebraic properties are not well-understood. Stieltjes conjectured in 1890 how they factor over the rational numbers. In this paper, assuming Stieltjes' conjecture, we formulate a conjecture about the Galois groups of Legendre polynomials, to the effect that they are "as large as possible," and give theoretical and computational evidence for it.

1. Introduction

The sequence $(P_m(x))_{m\geq 0}$ of *Legendre polynomials* is an orthogonal family on $[-1,1]$, first introduced by Adrien-Marie Legendre in 1785 [15] as coefficients in a series expansion for the gravitational potential of a point mass. For $m \geq 0$ we can define $P_m(x)$ via the Rodrigues formula

$$P_m(x) := \frac{(-1)^m}{2^m m!}\left(\frac{d}{dx}\right)^m (1-x^2)^m.$$

As a solution $y = P_m(x)$ of the Legendre differential equation

$$\frac{d}{dx}\left[(1-x^2)\frac{dy}{dx}\right] + m(m+1)y = 0,$$

$P_m(x)$ is an eigenfunction of the self-adjoint operator $\frac{d}{dx}(1-x^2)\frac{d}{dx}$ with eigenvalue $-m(m+1)$. It is easy to see that $P_m(-x) = (-1)^m P_m(x)$, prompting us to define the even polynomial of degree $2\lfloor m/2 \rfloor$:

$$L_m(x) = \begin{cases} P_m(x) & \text{if } m \text{ is even;} \\ P_m(x)/x & \text{if } m \text{ is odd.} \end{cases}$$

While their importance in classical physics and analysis dates back to Legendre's paper, the role of Legendre polynomials in number theory became manifest a bit later, for instance as the Hasse invariant

$$W_p(E_\lambda) := (1-\lambda)^m P_m\left(\frac{1+\lambda}{1-\lambda}\right)$$

for the Legendre-form elliptic curve $E_\lambda : y^2 = x(x-1)(x-\lambda)$ over $\mathbf{F}_p$, where $p = 2m+1$ is prime (see [3] and its references). As an indication of the arithmetic depth of this fact, we mention one of its consequences, thanks to the theory of elliptic curves with complex multiplication: say $m = (p-1)/2$ is odd; then the class number of $\mathbf{Q}(\sqrt{-p})$ is one-third the number of linear factors of $P_m(x)$ over $\mathbf{F}_p$ (see Brillhart-Morton [3, Theorem 1(a)]).

The algebraic properties of many similar families of hypergeometric polynomials (Laguerre, Chebyshev, Hermite, Bessel) have been extensively explored using methods pioneered by Schur [21], but results of this nature for Legendre polynomials continue to be fragmentary at best. As regards how Legendre polynomials factor over the rationals, Stieltjes put forward the following

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

Key words and phrases. Legendre polynomials, Galois group, Sophie-Germain primes, Hardy-Littlewood conjectures.

conjecture in an 1890 letter to Hermite [22]: $P_{2n}(x)$ and $P_{2n+1}(x)/x$ are irreducible over $\mathbf{Q}$, i.e $L_m(x)$ is irreducible over $\mathbf{Q}$ for all m. Some cases of Stieltjes' conjecture have been verified by Holt, Ille, Melnikov, Wahab, McCoart [11, 12, 14, 17, 24, 25, 16]; the articles [24] and [16] provide useful summaries. The flavor of these results is that if m or $m/2$ is within a few units of a prime number, then $L_m(x)$ is irreducible over $\mathbf{Q}$ (see for example Corollary 3.4(b), a result of Holt completed by Wahab, which we re-derive). There has been no significant improvement of these results for several decades. From a number-theoretic viewpoint, for primes $p = 2m + 1 \equiv 3 \bmod 4$, the irreducibility of $P_m(x)$ has the intriguing consequence, thanks to the result of Brillhart and Morton quoted above, that the class number of $\mathbf{Q}(\sqrt{-p})$ is "governed" by the number field cut out by a non-zero root of $P_m(x)$, specifically by how the prime p splits in it. We should point out that recent work of Bourgain and Rudnick [2] places Stieltjes' conjecture in a much more general context of expectations for the behavior of eigenfunctions of Laplacians; perhaps a resurgence of interest in the question will ensue.

We assume Stieltjes' conjecture, and turn our attention to the next natural question, namely "What is the Galois group of the degree $2\lfloor m/2 \rfloor$ polynomial $L_m(x)$?" We explore this question here, and conjecture that these Galois groups are as large as possible, namely $S_2 \wr S_n$ where $n = \lfloor m/2 \rfloor$. Our starting point is to note that $L_m(x)$ is an even polynomial, so if we write $m = 2n + \delta$ with $\delta \in \{0, 1\}$, then

$$L_m(x) = P_{2n+\delta}(x)/x^\delta = (-1)^n p_n^{(\delta)}(-x^2),$$

where $p_n^{(0)}(x)$ and $p_n^{(1)}(x)$ are degree n polynomials "underlying" the Legendre polynomials of even and odd degrees, respectively. The choice of $-x^2$ as opposed to x^2 here is for convenience, so that $p_n^{(0)}(x)$ and $p_n^{(1)}(x)$ have non-negative coefficients. The Galois group of $L_{2n+\delta}(x)$ is now seen to be be a subgroup of the wreath product of the group of order 2 with the Galois group of $p_n^{(\delta)}(x)$, and hence an extension of the latter group by an elementary abelian 2-group of rank at most n. We conjecture that $p_n^{(\delta)}(x)$ has full Galois group S_n and that the corresponding elementary abelian 2-component also has maximal rank, namely n; our focus in this paper is on the former aspect, namely the computation of the Galois group of $p_n^{(\delta)}(x)$. We prove some cases of the conjecture and give theoretical as well as computational evidence for it (see Theorems 1.6, 1.7, 1.8, and 1.9). One of our approaches is to exploit *tame* ramification at primes in $(n, 4n)$. In Section 7 we give an alternate approach via primes that are *wildly* ramified in the splitting field of $L_m(x)$.

1.1. **Jacobi Polynomials.** To proceed, we enter into a more detailed description of the polynomials $p_n^{(\delta)}(x)$; in particular, it will be useful to express them as a specialization of Jacobi polynomials, a two-parameter deformation of Legendre polynomials. For this purpose, we will rely on the classic monograph of Szegö [23] as a reference. For $n \geq 0$, the nth degree *Jacobi polynomial* $P_n^{(\alpha,\beta)}(x)$ can be defined by the Rodrigues formula

$$P_n^{(\alpha,\beta)}(x) := \frac{(-1)^n}{2^n n!}(1-x)^{-\alpha}(1+x)^{-\beta}\left(\frac{d}{dx}\right)^n \left[(1-x)^{n+\alpha}(1+x)^{n+\beta}\right].$$

Thus, $P_m(x) = P_m^{(0,0)}(x)$.

Among many explicit expressions for the degree n polynomial $P_n^{(\alpha,\beta)}(x)$, we single out two. First, from [23, 4.3.2], we have

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

The shifted polynomial

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

is also very useful because of the expansion (see [23, 4.21.2]):

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

We begin our investigation by writing $p_n^{(\delta)}(x)$ in terms of the Jacobi Polynomial $P_n^{(\alpha,\beta)}(x)$ with parameters $\alpha = \pm 1/2$, $\beta = 0$. For $n \geq 0$ and $\delta \in \{0,1\}$ we find, using [23, Theorem 4.1], that

$$L_{2n+\delta}(x) = (-1)^n J_n^{(\epsilon/2,0)}(-x^2), \quad \text{where } \epsilon = (-1)^{\delta+1} = 2\delta - 1, \text{ i.e.}$$
$$p_n^{(\delta)}(x) = J_n^{(\delta-1/2,0)}(x).$$

To lighten the notation, we define for $\epsilon \in \{\pm 1\}$

$$J_n^{\epsilon}(x) := J_n^{(\epsilon/2,0)}(x), \qquad \mathscr{J}_n^{\epsilon}(x) := 2^n n! J_n^{\epsilon}(x).$$

The advantage of the polynomial $\mathscr{J}_n^{\epsilon}(x)$ is that it has integer coefficients with a particularly useful factorization as a binomial coefficient times a product of n consecutive odd integers. To describe these coefficients, we introduce the following modified Pochhammer symbol notation:

$$(\!(\alpha)\!)_n := (\alpha+2)(\alpha+4)\cdots(\alpha+2n),$$

and compute

$$\mathscr{J}_n^{\pm}(x) = \sum_{j=0}^{n} \binom{n}{j} (\!(2j \pm 1)\!)_n x^j.$$

We summarize all of this as follows.

Lemma 1.2. *Suppose $m = 2n + \delta$ where $n \geq 0$, $\delta \in \{0,1\}$, and $\epsilon = 2\delta - 1$. Then*

$$(-1)^n\ L_m(x) = J_n^{\epsilon}(-x^2), \qquad (-2)^n n!\ L_m(x) = \mathscr{J}_n^{\epsilon}(-x^2).$$

The preceding lemma essentially reduces the study of many algebraic properties of the Legendre polynomials to the corresponding properties for $\mathscr{J}_n^{\pm}(x)$. The following lemma illustrates this for the question of irreducibility (compare Wahab [24, Cor. 3.4]).

Lemma 1.3. *Suppose $m = 2n + \delta$ where $n \geq 1$, $\delta \in \{0,1\}$, and $\epsilon = 2\delta - 1$. Then $L_m(x)$ is irreducible over $\mathbf{Q}$ if and only if $\mathscr{J}_n^{\epsilon}(x)$ is irreducible over $\mathbf{Q}$.*

Proof. Suppose $\mathscr{J}_n^{\epsilon}(x)$ is irreducible over $\mathbf{Q}$ and let θ be a root of it. We compute

$$\mathbb{N}_{\mathbf{Q}(\theta)/\mathbf{Q}}(-\theta) = \frac{\mathscr{J}_n^{\epsilon}(0)}{(\!(2n+\epsilon)\!)_n} = \frac{(\!(\epsilon)\!)_n}{(\!(2n+\epsilon)\!)_n}.$$

The interval $[2n+2+\epsilon, 4n+\epsilon]$ contains a prime l (Bertrand's Postulate, see Lemma 2.2). The valuation of $\mathbb{N}_{\mathbf{Q}(\theta)/\mathbf{Q}}(-\theta)$ at l is exactly -1, hence $-\theta$ is not a square in $\mathbf{Q}(\theta)$. It follows that $\mathbf{Q}(\sqrt{-\theta})$, which contains the degree n field $\mathbf{Q}(\theta)$, has degree $2n$ over $\mathbf{Q}$. Thus, the degree $2n$ polynomial $\mathscr{J}_n^{\epsilon}(-x^2)$ which has $\sqrt{-\theta}$ as a root, must be the minimal polynomial of this algebraic number, and is therefore irreducible. The other direction is easy and left to the reader. □

1.4. **The main conjecture and results.** From now on, we assume the irreducibility of $\mathscr{J}_n^{\pm}(x)$ and ask what can be said about its Galois group.

Conjecture 1.5. *Suppose $n \geq 1$ is an integer, $\delta \in \{0,1\}$ and $\epsilon = 2\delta - 1$. Suppose the polynomial $\mathscr{J}_n^{\epsilon}(x)$ is irreducible over $\mathbf{Q}$. Then*

(a) The Galois group of $\mathscr{J}_n^{\epsilon}(x)$ over $\mathbf{Q}$ is isomorphic to S_n.

(b) The Galois group of $L_{2n+\delta}(x)$ is isomorphic to the wreath product $S_2 \wr S_n$.

Some corroborating evidence for Conjecture 1.5(a) is provided by the following four theorems.

Theorem 1.6. *Let $n \geq 2$ be an integer and $\epsilon \in \{\pm 1\}$. Then the discriminant of the polynomial $\mathscr{J}_n^{\epsilon}(x)$ is not a square in $\mathbf{Q}^{\times}$. Hence, assuming $\mathscr{J}_n^{\epsilon}(x)$ is irreducible, its Galois group is not contained in A_n.*

Theorem 1.7. *Let $n > 2$ be an integer and $\epsilon \in \{\pm 1\}$. Suppose $\mathscr{J}_n^{\epsilon}(x)$ is irreducible over $\mathbf{Q}$ and that there is a prime number ℓ in the interval $(^{(n+1)}/_2, n-2)$ such that either (a) $2\ell + \epsilon$ is prime; or (b) $2\widehat{\ell} + \epsilon$ is prime, where $\widehat{\ell} = 2n + 1 - \ell$. Then $\mathrm{Gal}(\mathscr{J}_n^{\epsilon}(x)) \simeq S_n$.*

Theorem 1.8. *The Hardy-Littlewood conjecture (*[10, Conj. D]*) implies that Conjecture 1.5(a) holds for all large enough n.*

Theorem 1.9. *Suppose $\delta \in \{0, 1\}$ and $\epsilon = 2\delta - 1$. Then*

(a) For all $n \leq 1\,000\,000\,000$, $\mathrm{Gal}_{\mathbf{Q}}(\mathscr{J}_n^{\epsilon}(x)) \simeq S_n$, assuming this polynomial is irreducible.
(b) For $n \leq 60$ we have $\mathrm{Gal}_{\mathbf{Q}}(L_{2n+\delta}(x)) \simeq S_2 \wr S_n$.

In section 2, by using the expression for $p_n^{(\delta)}(x)$ as a specialized Jacobi Polynomial, we easily obtain an explicit formula for its discriminant, which is composed of all the primes in the interval $[2, 4n+2\delta-1]$; we can then prove Theorem 1.6. We compute the Newton Polygons of $\mathscr{J}_n^{\pm}(x)$ at all primes $p > n$ in section 3. In section 4, we prove Theorem 1.7 by exploiting the tame ramification of primes exceeding n, as determined by the slopes of the Newton polygons at these primes. We remark that in practice it is easy, for any large enough n, to find a plethora of prime pairs $(\ell, 2\ell+\epsilon)$ or $(\ell, 2\widehat{\ell}+\epsilon)$ with ℓ in the range indicated in Theorem 1.7; note that for $\epsilon = 1$ this is the case of Sophie Germain primes. It is likely well-known to experts that the Hardy-Littlewood conjectures imply that such prime pairs always exist for large enough n, and that the number of such pairs goes to infinity as n grows, but we were not able to find this in the literature. We therefore discuss the case of prime pairs $(\ell, 2\ell + \epsilon)$ in the final section to establish Theorem 1.8 (see Theorem 5.2). We establish Theorem 1.9(a) by a computation in Pari checking that every n in the indicated range is close enough to an appropriate prime of $\pm$-Sophie Germain type, and Theorem 1.9(b) via a computation in Magma.

2. Discriminant Formula

It is well-known that the Galois group of a degree n irreducible polynomial $f(x) \in \mathbf{Q}[x]$ is contained in A_n if and only if $\mathrm{disc}(f)$ is a square in $\mathbf{Q}^{\times}$. In this section we will compute the discriminant for $\mathscr{J}_n^{(\pm 1/2, 0)}(x)$ and prove that it is not a rational square.

Lemma 2.1. *For $n > 1$ and $\epsilon \in \{\pm 1\}$, the discriminant of $\mathscr{J}_n^{\epsilon}(x)$ is given by the formula*

$$\mathrm{disc}\, \mathscr{J}_n^{\epsilon}(x) = 2^{n^2-n} \prod_{k=1}^{n} k^{2k-1}(2k+\epsilon)^{k-1}(2k+2n+\epsilon)^{n-k}.$$

Proof. It is known [23, Thm. 6.71] that the discriminant $D_n(\alpha, \beta)$ of the Jacobi polynomial $P_n^{(\alpha,\beta)}(x)$ is equal to

$$D_n(\alpha, \beta) = 2^{-n(n-1)} \prod_{k=1}^{n} k^{k-2n+2}(k+\alpha)^{k-1}(k+\beta)^{k-1}(n+k+\alpha+\beta)^{n-k}.$$

Thus, for $P_n^{(\pm 1/2,0)}(x)$ we get

$$\begin{aligned} D_n(\pm 1/2, 0) &= 2^{-n(n-1)} \prod_{k=1}^{n} k^{2k-2n+1}(k \pm 1/2)^{k-1}(n+k \pm 1/2)^{n-k} \\ &= 2^{-2n(n-1)} \prod_{k=1}^{n} k^{1-2(n-k)}(2k \pm 1)^{k-1}(2n+2k \pm 1)^{n-k}. \end{aligned}$$

Taking into account the fact that the discriminant of $n!2^n P_n^{(\pm 1/2,0)}(x)$ is equal to $(n!2^n)^{2(n-1)} D_n(\pm 1/2, 0)$, and writing $n!^{2(n-1)}$ as $\prod_{k=1}^{n} k^{2(n-1)}$, we find

$$\operatorname{disc} n!2^n P_n^{(\pm 1/2,0)}(x) = \prod_{k=1}^{n} k^{2k-1}(2k \pm 1)^{k-1}(2n+2k \pm 1)^{n-k}.$$

Finally, recall that $J_n^{(\alpha,\beta)}(x) = P_n^{(\alpha,\beta)}(2x+1)$. Since the discriminant is invariant under translation, we apply the formula $\operatorname{disc}(f(2x)) = 2^{\deg f(\deg f - 1)} \operatorname{disc}(f(x))$ to arrive at

$$\operatorname{disc} \mathscr{J}_n^{\pm}(x) = \operatorname{disc} n!2^n J_n^{\pm}(x) = 2^{n^2-n} \prod_{k=1}^{n} k^{2k-1}(2k \pm 1)^{k-1}(2k+2n \pm 1)^{n-k},$$

which is what we wanted to prove. □

To see that the discriminant of $\mathscr{J}_n^{(\pm 1/2,0)}(x)$ is not a rational square, we will use the following Lemma on the distribution of primes modulo 4, which is a simple consequence of Ramaré-Rumely [20] together with a computer calculation.

Lemma 2.2. *For all $x \geq 9$, the interval $[x, 2x-5]$ contains at least one prime congruent to 1 modulo 4 and at least one prime congruent to 3 modulo 4.*

Proof. See [7, Thm. 1]. □

Proposition 2.3. *For all $n \geq 2$, and $\epsilon \in \{\pm 1\}$, the discriminant of $\mathscr{J}_n^{\epsilon}(x)$ is not a square in $\mathbf{Q}^{\times}$.*

Proof. From Lemma 2.1, we have

$$\operatorname{disc} \mathscr{J}_n^{\epsilon}(x) = 2^{n^2-n} \prod_{k=1}^{n} k^{2k-1}(2k+\epsilon)^{k-1}(2k+2n+\epsilon)^{n-k}.$$

According to Lemma 2.2, for all $n > 6$, the interval $[2n+2+\epsilon, 4n-2+\epsilon]$ contains a prime p congruent to $2+\epsilon \bmod 4$. When we write p in the form

$$p = 2k_0 + 2n + \epsilon, \qquad 1 \leq k_0 \leq n-1,$$

we find that the p-valuation of disc $\mathscr{J}_n^{\epsilon}(x)$ is $n - k_0$. But since $p = 2k_0 + 2n + \epsilon \equiv 2 + \epsilon \bmod 4$, $n + k_0$ is odd, hence so is $n - k_0$. Consequently, disc $\mathscr{J}_n^{\epsilon}(x)$ has odd p-valuation, hence cannot be a rational square. The cases $2 \leq n \leq 6$ are easily checked by hand. □

3. Newton Polygons

In this section we will compute the Newton polygons of $\mathscr{J}_n^{\pm}(x)$ at primes $p > n$, giving us information on the ramification indices for these primes in fields obtained by adjoining a root of the polynomial. In Section 4 we will then use these ramification data to give easily verified numerical criteria for showing that these polynomials have large Galois groups.

We write $\mathtt{NP}_p(f)$ for the p-adic Newton Polygon of a polynomial $f \in \mathbf{Q}[x]$; for more details on Newton Polygons, we refer the reader to [8], whose conventions we use, namely for a degree n polynomial $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbf{Q}[x]$, $\mathtt{NP}_p(f)$ is the lower convex hull of the points

$$\{(j, \operatorname{ord}_p a_j) \mid 0 \le j \le n\}.$$

A short but excellent account is also given in [6].

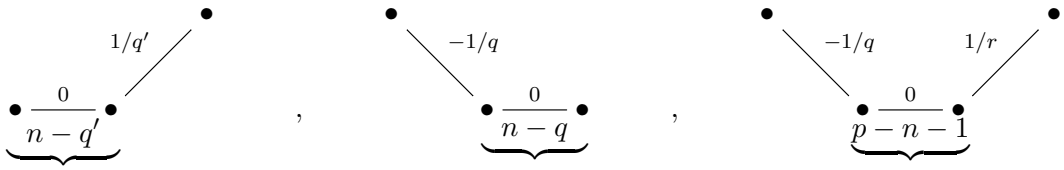
Proposition 3.1. *Fix an integer $n \ge 2$ and $\epsilon \in \{\pm 1\}$. For a prime $p > n$, define $q = (p-\epsilon)/2$, $q' = 2n+1-q$, $r = q'-p$. If $p > 4n+\epsilon$, then $\mathtt{NP}_p(\mathscr{J}_n^{\epsilon}(x))$ is trivial, i.e. it consists of a single slope 0 segment of length n. For primes p in the interval $n < p \le 4n+\epsilon$, the p-adic Newton polygon of $\mathscr{J}_n^{\epsilon}(x)$ can be described as follows:*

(a) If $2n+\epsilon < p \le 4n+\epsilon$, then $\mathtt{NP}_p(\mathscr{J}_n^{\epsilon}(x))$ consists of
- *a length $n-q'$ segment of slope 0, and;*
- *a length q' segment of of slope $1/q'$.*

(b) If $(4n+\epsilon)/3 < p \le 2n+\epsilon$, then $\mathtt{NP}_p(\mathscr{J}_n^{\epsilon}(x))$ consists of
- *a length q segment of slope $-1/q$, and;*
- *a length $n-q$ segment of slope 0.*

(c) If $n < p \le (4n+\epsilon)/3$, then $\mathtt{NP}_p(\mathscr{J}_n^{\epsilon}(x))$ consists of
- *a length q segment of slope $-1/q$, and;*
- *a length $p-n-1$ segment of slope 0, and;*
- *a length r segment of slope $1/r$.*

Schematically, the Newton polygon for p in the intervals $(2n+\epsilon, 4n+\epsilon]$, $((4n+\epsilon/3, 2n+\epsilon]$, and $(n, (4n+\epsilon)/3]$ is given as follows:



Proof. Recall that

$$\mathscr{J}_n^{\epsilon}(x) = \sum_{j=0}^{n} \binom{n}{j} (\!(2j+\epsilon)\!)_n x^j,$$

where

$$(\!(2j+\epsilon)\!)_n = \prod_{k=1}^{n} (2j+2k+\epsilon) = (2j+\epsilon+2)(2j+\epsilon+4)\cdots(2j+\epsilon+2n).$$

Since $p > n$, we have $\operatorname{ord}_p \binom{n}{j} = 0$ for all $j = 0, \ldots, n$. Therefore, it suffices to pay attention to the p-adic valuation of $a_j^{(\epsilon)} := (\!(2j+\epsilon)\!)_n$ for the purposes of computing the Newton polygon at $p > n$. We first make a general observation on the computation of this valuation, namely:

Observation 1. If $a_j^{(\epsilon)}$ is divisible by p, then $2j+2k+\epsilon = \mu p$ for a unique pair μ, k with $\mu \in \{1,3\}$ and $k \in \{1, \ldots, n\}$.

To see this, we note that a) $a_j^{(\epsilon)}$ is a product of n consecutive odd positive integers, none of which exceeds $4n+\epsilon$; b) we have $5p > 5n > 4n+\epsilon$ since $p > n$; and, finally c) p and $3p$ cannot both occur simultaneously as factors in the product defining $a_j^{(\epsilon)}$, since $3p - p = 2p > 2n$.

For $\mu = 1$, we note that

$$p = 2q+\epsilon = 2j+2k+\epsilon \text{ if and only if } j+k = q.$$

Thus, p is one of the factors in the product defining $a_j^{(\epsilon)}$ if and only if $\max(0, q-n) \le j \le q-1$. For the case of $\mu = 3$, we compute similarly that

$$3p = 6q + 3\epsilon = 2j + 2k + \epsilon \text{ if and only if } j + k = q + p.$$

Thus, $3p$ is one of the factors in the product defining $a_j^{(\epsilon)}$ if and only if $\max(0, q+p-n) \le j \le \min(n, q+p-1)$. We have therefore demonstrated the following:

Observation 2. Suppose $j \in \{0, 1, 2, \ldots, n\}$. If $q - n \le j \le q-1$ or $q+p-n \le j \le q+p-1$, then $\operatorname{ord}_p a_j^{(\epsilon)} = 1$. Otherwise, $\operatorname{ord}_p a_j^{(\epsilon)} = 0$.

If $p > 4n+\epsilon$, then clearly $\operatorname{ord}_p a_j^{(\epsilon)}$ vanishes for all j so the Newton polygon is trivial. We are now ready to proceed by splitting the proof into cases according to the various intervals within $(n, 4n+\epsilon]$ to which p belongs. First suppose that $2n + \epsilon < p \le 4n + \epsilon$. We note that since $q' + q = 2n + 1$, we have $q - n - 1 = n - q'$. Therefore, from Observation 2, we find that $a_j^{(\epsilon)}$ has p-adic valuation 0 for $1 \le j \le n - q'$ and p-adic valuation 1 for $n - q' + 1 \le j \le n$. Thus, the p-adic Newton polygon of $\mathscr{J}_n^{\epsilon}(x)$ has a length $(n - q')$ segment of slope 0 and a length q' segment of slope $1/q'$.

We move to the case where $(4n + \epsilon)/3 < p \le 2n + \epsilon$. From Observation 2, we find that $a_j^{(\epsilon)}$ has p-adic valuation 1 for $1 \le j \le q - 1$ and p-adic valuation 0 for $q \le j \le n$. Thus, the Newton polygon of $\mathscr{J}_n^{\epsilon}(x)$ has a slope $-1/q$ segment of length q and a length $n - q$ segment of slope 0.

Finally, suppose p lies in the range $n < p \le (4n + \epsilon)/3$. By Observation 2, we have $\operatorname{ord}_p a_j^{(\epsilon)}$ is 0 for j in the interval $q \le j \le q + p - n - 1$ and 1 for the other values of j in $\{0, 1, 2, \ldots, n\}$. This finishes the proof of the Proposition. □

Remark. The first two cases of the above Proposition give an alternate means of obtaining the irreducibility results of Holt [11], [12] mentioned in the introduction. The last case, giving Newton polygons with slopes of opposite sign, gives new information on degrees of factors of Legendre polynomials via a result of Bush-Hajir [4]; for the reader's convenience, we record the result we need in a simplified form.

Lemma 3.2 (Lemma 2.5 of [4])**.** *Suppose r is the length of the slope zero segment of $\mathtt{NP}_p(f(x))$ where $f(x) \in \mathbf{Q}[x]$ and s is the maximum of the absolute values of slopes of $\mathtt{NP}_p(f(x))$. If $g(x) \in \mathbf{Q}[x]$ is a degree d divisor of $f(x)$, then d does not belong to the interval $(r, 1/s)$.*

Theorem 3.3. *Suppose $n > 1$, $\epsilon \in \{\pm 1\}$ and $\mathscr{J}_n^{\epsilon}(x)$ has a factor of degree $d \ge 1$ in $\mathbf{Q}[x]$.*

(a) If $p = (2n + \epsilon) + 2s$ is a prime exceeding $2n + \epsilon$, where $1 \le s \le n$, then d does not belong to the interval $[s, n - s]$.

(b) If $p = (2n + \epsilon) - 2(t - 1)$ is a prime not exceeding $2n + \epsilon$ where $1 \le t \le (n + \epsilon)/3$, then d does not belong to the interval $[t, n - t]$.

(c) If $p = n + u$ is a prime exceeding n where $1 \le u \le (n + \epsilon)/3$, then d does not belong to the interval $[u, (n + \epsilon - 3u)/2]$.

Proof. Each of these follows easily via an application of Lemma 3.2 to the Newton polygon determinations of Proposition 3.1; the details are left to the reader. □

We can use the above Theorem to recover a result of Holt [12], completed by Wahab [24].

Corollary 3.4. *(a) Suppose $n > 10$, $\epsilon \in \{\pm 1\}$, and there is a prime p which satisfies*

$$2n + \epsilon - 2 \le p \le 2n + \epsilon + 4.$$

Then $\mathscr{J}_n^{\epsilon}(x)$ is irreducible over $\mathbf{Q}$.

(b) Suppose p is an odd prime and m is an integer in the interval $p-4 \le m \le p+3$. Then $L_m(x)$ is irreducible over $\mathbf{Q}$.

Proof. We begin with (a). If $p > 2n+\epsilon$, we write $p = 2n+\epsilon+2s$ with $s = 1$ or 2. Then by Theorem 3.3(a), if $\mathscr{J}_n^\epsilon(x)$ is reducible, it has a linear factor. But by Wahab [24, Cor. 3.5], $P_{2n+\delta}(x)$, where $\delta = (\epsilon+1)/2$, does not have a quadratic factor, hence $\mathscr{J}_n^\epsilon(x)$ does not have a linear factor. For $p \le 2n+\epsilon$, the proof is the same except that we use Theorem 3.3(b) with $t = 1$ or 2. We derive (b) directly from (a) via Lemma 1.3. □

4. Galois Properties

We are finally ready to address the Galois theory of the polynomials under consideration.

4.1. **General Considerations.** As before, we write $m = 2n+\delta$, $\delta \in \{0,1\}$, $\epsilon = (-1)^{\delta+1}$. We seek to understand the Galois group of $L_m(x)$, paying close attention to the fact that

$$(-2)^n n! L_m(x) = \mathscr{J}_n^\epsilon(-x^2).$$

Let $\Gamma = \mathrm{Gal}_{\mathbf{Q}}(L_m(x))$ and $G = \mathrm{Gal}_{\mathbf{Q}}(\mathscr{J}_n^\epsilon(x))$ so that G is a quotient of Γ. If the roots of $\mathscr{J}_n^\epsilon(x)$ are $\theta_1, \ldots, \theta_n$, then the roots of $L_m(x)$ are

$$\pm\sqrt{-\theta_1}, \ldots, \pm\sqrt{-\theta_n}.$$

Thus, the splitting field F of $L_m(x)$ is an elementary abelian extension of degree 2^k ($k \le n$) over the splitting field K of $\mathscr{J}_n^\epsilon(x)$.

In other words, the conjectured irreducibility of $L_m(x)$ and of $\mathscr{J}_n^\epsilon(x)$ tells us that there is an exact sequence

$$1 \longrightarrow (S_2)^k \longrightarrow \Gamma \longrightarrow G \longrightarrow 1.$$

Note that Γ is a subgroup of the wreath product $S_2 \wr G$. According to Conjecture 1.5, we expect, based on numerical evidence, not only that G is isomorphic to S_n but that Γ/G is "full," meaning $k = n$ in all cases. We should note that Lemma 1.3 implies $k > 1$. We do not enter into a further discussion of the interesting question of determining Γ/G but note only that it is equivalent to the determination of its Kummer dual, namely the subgroup of $K^\times/(K^\times)^2$ generated by the image of $\langle -\theta_1, \ldots, -\theta_n\rangle$ where $K = \mathbf{Q}(\theta_1, \ldots, \theta_n)$ is the splitting field of $\mathscr{J}_n^\epsilon(x)$. While we do not currenty have an efficient method for verifying that Γ/G is as large as possible for a given m, we have checked this using Magma for $m \le 120$.

By contrast, we can use the results of the previous section to give a simple numerical criterion for confirming the conjecture on G. This criterion is easily checked for any given m; moreover, standard conjectures in analytic number theory predict that this criterion holds for all m as we will see in Theorem 5.2.

4.2. **Jordan's Criterion.** Our main technique is to extract information about the size of the Galois group from the slopes of the Newton polygons at well-chosen primes. The basic tool is *Jordan's Criterion*: a transitive subgroup of S_n containing a p-cycle where p is a prime in the range $n/2 < p < n-2$ contains A_n (see for example Wielandt [26]). Following [9, def. 5.1], we denote by $\mathcal{N}_f$ the *Newton index* of $f(x) \in \mathbf{Q}[x]$, namely the least common multiple of the denominators (in lowest terms) of all slopes of $\mathtt{NP}_p(f(x))$ as p ranges over all primes. The main theorem of Newton polygons tells us the slopes of $\mathtt{NP}_p(f(x))$ are the negatives of p-adic valuations of the roots of f, hence their denominators are ramification indices. We can therefore extract information about the Galois group from the Newton polygon as follows (see [8] and [9] for more details).

Theorem 4.3 ([9])**.** *Given an irreducible polynomial $f \in \mathbf{Q}[x]$, $\mathcal{N}_f$ divides the order of the Galois group of f. Moreover, if $\mathcal{N}_f$ has a prime divisor q in the range $n/2 < q < n-2$, where n is the degree of f, then the Galois group of f contains A_n.*

4.4. **Tame Ramification.** Proposition 3.1 tells us that all primes p in the range $n < p < 4n + \epsilon$ ramify in the splitting field of $\mathscr{J}_n^\epsilon(x)$; we note that since p does not divide $n!$, all these primes are tamely ramified. We are now ready to extract Galois-theoretic information from this Newton polygon data via Theorem 4.3.

Theorem 4.5. *Suppose $n > 1$ and $\epsilon \in \{\pm 1\}$. Every prime p in the interval $(n, 4n + \epsilon]$ yields a decomposition of the number $2n + 1$ as*

$$2n + 1 = q + q' \qquad \text{where } q = (p - \epsilon)/2.$$

We have:

(a) If p is a prime in the range $n < p \leq 2n + \epsilon$, then q divides $\#\operatorname{Gal}_{\mathbf{Q}} \mathscr{J}_n^\epsilon(x)$; and
(b) If p is a prime in the range $2n + \epsilon < p \leq 4n + \epsilon$ then q' divides $\#\operatorname{Gal}_{\mathbf{Q}} \mathscr{J}_n^\epsilon(x)$.

Proof. Suppose first $p \in (n, 2n + \epsilon]$. Then, by Theorem 3.1, the p-adic Newton Polygon of $\mathscr{J}_n^\epsilon(x)$ has $-1/q$ as a slope, so by Theorem 4.3, q divides the order of its Galois group. Similarly, if $p \in (2n + \epsilon, 4n + \epsilon]$, then the p-adic Newton Polygon of $\mathscr{J}_n^\epsilon(x)$ has $1/q'$ as a slope, hence q' divides the order of its Galois group. □

We can now prove Theorem 1.7.

Proof of Theorem 1.7. We take case (a) first where by assumption there is a prime ℓ in $(^{(n+1)}/_2, n-2)$ such that $2\ell + \epsilon$ is prime. We put $p = 2\ell + \epsilon$, and $q = \ell$. We note that $p \in (n, 2n - 4 + \epsilon)$ so we can apply case (a) of Theorem 4.5 in conjunction with Jordan's criterion and Theorem 1.6 to conclude that the Galois group of $\mathscr{J}_n^\epsilon(x)$ is S_n. For case (b), we put $p = 2\widehat{\ell} + \epsilon$. In the notation of Theorem 4.5, we get $q' = \ell$ and $q = \widehat{\ell}$. We have $p \in (2n + 6 + \epsilon, 3n + 1 + \epsilon)$, so case (b) of Theorem 4.5 applies to show that $\ell = q'$ divides the order of $\operatorname{Gal}_{\mathbf{Q}} \mathscr{J}_n^\epsilon(x)$. We can then finish as before, applying Jordan's criterion and Theorem 1.6, to conclude that this Galois group is S_n. □

5. Hardy-Littlewood Conjectures

Standard conjectures in analytic number theory predict the existence of prime pairs (q', p) and (q, p) as in Theorem 4.5 for all large enough n. We were not able to find an appropriate reference for this type of result in the literature, so we work out the details for the case of prime pairs $q, 2q + \epsilon$, which is enough to establish Theorem 1.8.

A Sophie Germain prime is a prime q such that $2q + 1$ is prime; we're not aware of a name for primes q such that $2q - 1$ is prime. It is not known whether there are infinitely many prime pairs $q, 2q + \epsilon$ for either value of $\epsilon \in \{\pm 1\}$ but heuristic arguments for their density has a long history culminating in the beautiful conjectures of Hardy and Littlewood. We will establish that these conjectures imply that for every large enough n, the criterion of Theorem 1.7 (a) holds, i.e. there is a prime q in $(^{(n+1)}/_2, n - 2)$ such that $2q + \epsilon$ is also prime.

Let

$$\pi_{\mathrm{sg}}^{(\epsilon)}(x) = |\{2 \leq q \leq x \mid q \text{ and } 2q + \epsilon \text{ are both prime}\}|.$$

Hardy and Littlewood [10] put forward the following conjecture.

Conjecture 5.1. *[[10, Conj. D]] Suppose a, b are fixed coprime positive integers, k is a positive integer coprime to a and to b, and just one of k, a, b is even. Let $\pi_{a,b,k}(x)$ be the number of prime pairs (p, p') with $p' < x$ such that $ap' - bp = k$. Then*

$$\pi_{a,b,k}(x) \sim \frac{2C_2}{a} \frac{x}{(\log x)^2} \prod_{r \mid abk} \frac{r-1}{r-2},$$

where the product is over the odd prime divisors r of abk and C_2 is defined by

$$C_2 := \prod_{\text{odd primes } p} \left(1 - \frac{1}{(p-1)^2}\right).$$

Theorem 5.2. *Suppose $\epsilon \in \{\pm 1\}$.*

(a) Conjecture 5.1 implies that

$$\pi_{sg}^{(\epsilon)}(x) \sim C_2 \frac{x}{(\log x)^2}.$$

(b) Conjecture 5.1 implies that for every n exceeding some absolute constant n_0, the interval $(^{(n+1)}/_2, n-2)$ contains a prime q such that $2q+\epsilon$ is prime.

(c) Conjecture 5.1 implies that for $n \geq n_0$ with n_0 as above, the Galois group of $\mathscr{J}_n^{\epsilon}(x)$, assumed irreducible, is S_n.

Proof. (a) If we take $(a,b,k) = (1,2,1)$ in Conjecture 5.1, then we are counting prime $p' < x$ such that $p' - 2p = 1$ i.e. we are counting the number of Sophie-Germain primes $p < x/2$, so $\pi_{\text{sg}}^{(1)}(x) \sim \pi_{1,2,1}(x/2)$.

If we take $(a,b,k) = (2,1,1)$, then we are counting primes $p' < x$ such that $2p' - p = 1$, i.e. we are counting primes $p' < x$ such that $2p'-1$ is prime, so $\pi_{\text{sg}}^{(-1)}(x) \sim \pi_{2,1,1}(x)$. Thus, from Conjecture 5.1, we find the following asymptotic expansions predicted by Hardy and Littlewood:

$$\begin{aligned} \pi_{1,2,1}(x/2) &\sim 2C_2 \frac{x/2}{(\log(x/2))^2} \\ \pi_{2,1,1}(x) &\sim \frac{2C_2}{2} \frac{x}{((\log x)^2}. \end{aligned}$$

We conclude that $\pi_{\text{sg}}^{(\epsilon)}(x) \sim C_2\ x/(\log x)^2$, which, incidentally, is independent of ϵ.

(b) Let us put

$$E_{\text{sg}}^{(\epsilon)}(x) := \pi_{\text{sg}}^{(\epsilon)}(x) - C_2 \frac{x}{(\log x)^2}.$$

According to Hardy-Littlewood, $E_{\text{sg}}^{(\epsilon)}(x)$ is in $o(x/(\log x)^2)$, hence so is $E_{\text{sg}}^{(\epsilon)}(x/2)$. Thus,

$$\pi_{\text{sg}}^{(\epsilon)}(x) - \pi_{\text{sg}}^{(\epsilon)}(x/2) = \left[C_2 x \left(\frac{1}{(\log x)^2} - \frac{1/2}{(\log(x/2)^2}\right)\right] + \left[E_{\text{sg}}^{(\epsilon)}(x) - E_{\text{sg}}^{(\epsilon)}(x/2)\right].$$

The first (main) term of the right hand side is of size $x/(\log x)^2$ whereas the second term is of order of magnitude $o(x/(\log x)^2)$. Hence, for any positive integer k, there exists a bound $n_0(k)$ such that for all $x \geq n_0(k)$, $\pi_{\text{sg}}^{(\epsilon)}(x) - \pi_{\text{sg}}^{(\epsilon)}(x/2) > k$. Taking $k = 4$, say, we conclude that for $n \geq n_0(4)$, the interval $(^{(n+1)}/_2, n-2)$ contains a prime q such that $2q+\epsilon$ is prime. It is reasonable to expect that $E_{\text{sg}}^{(\epsilon)}(x)$ is of order of magnitude $O(x/(\log x)^3)$. An explicit O-constant in such an estimate would then allow one to give a specific value for n_0. Computations on the computer indicate that optimal values for n_0 are 26 if $\epsilon = 1$ and 82 if $\epsilon = -1$.

(c) This is clear from (b), Theorem 4.5, and and the proof of Theorem 1.7. □

Remark. The existence of prime pairs (q', p) such that $q' \in (\frac{(n+1)}{2}, n-2)$ and $p = 2(2n+1-q') + \epsilon$ as in Theorem 1.7(b) can be analyzed in a similar manner using [10, Conj. C].

Prime distribution results are still quite far from establishing any conjectures of Hardy-Littlewood type beyond Dirichlet's theorem. It is clear though that Theorem 1.7 can in practice verify Conjecture 1.5(a) for any given value of n very quickly. To demonstrate this, we provide some computational evidence on the existence of desired prime pairs (q', p) or (q, p) in the desired ranges. Using precomputed tables of primes in PARI, a relatively quick computation finds a desired (q', p)

or (q,p) for all n in the range $26 \le n \le 10^9$. The plenitude of such pairs in this range can be gleaned from the following representative chart showing the growth of the number of such pairs for eight sample values of n. In the column marked $\#\ell$, we record the number of primes in the interval $(^{(n+1)}/_2, n-2)$. In the notation of Theorem 1.7, the columns marked $\#2\ell+1$ and $\#2\widehat{\ell}+1$ correspond to the number of primes of the given form for prime ℓ in the specified range. These give instances of prime pairs (q,p) and (q',p) respectively, in the notation of Theorem 4.5. Columns 3 and 4 correspond to the choice $\epsilon = 1$, while the last two columns give the same counts for the case of $\epsilon = -1$.

		$\epsilon = +1$	$\epsilon = +1$	$\epsilon = -1$	$\epsilon = -1$
n	$\#\ell$ prime	$\#2\ell+1$ prime	$\#2\widehat{\ell}+1$ prime	$\#2\ell-1$ prime	$\#2\widehat{\ell}-1$ prime
10	1	0	1	1	0
100	10	3	3	2	2
1 000	73	12	16	14	13
10 000	560	75	75	80	82
100 000	4 459	501	473	494	560
1 000 000	36 960	3 422	4 049	3 452	3 401
10 000 000	316 066	25 375	24 435	25 418	24747
100 000 000	2 760 321	193 572	205 460	193 968	188 438
1 000 000 000	24 491 667	1 533 184	1 494 514	1 531 559	1 539 939

For the purposes of numerical verification, it can be useful to invert the point of view. Namely, if we assume Stieltjes' conjecture, we can think of each prime pair $(q, 2q+\epsilon)$ as a "certificate" for the Galois group of $\mathscr{J}_n^{(\epsilon/,0)}(x)$ being S_n for many n: it is so as long as $^{(n+1)}/_2 < q < n-2$, i.e. for all n belonging to $[q+3, 2q-2]$. For instance, the Sophie Germain prime 29 is a ramification index for the prime $59 = 2 \cdot 29 + 1$ in a root field of $\mathscr{J}_n^+(x)$ for all n in $[32, 56]$ and therefore exhibits a (tame) 29-cycle in some inertial subgroup of the Galois group for each of these integers n. Thus, to ensure that criterion (a) of Theorem 1.7 applies to every n up to a given bound, it's enough to check that consecutive primes of ϵ-Sophie Germain type are sufficiently close to each other. We can state this more precisely as follows.

Lemma 5.3. *Let $\epsilon \in \{\pm 1\}$. Consider the increasing sequence*

$$q_1^{(\epsilon)} < q_2^{(\epsilon)} < \ldots < q_k^{(\epsilon)} < \ldots$$

of all primes q satisfying $2q+\epsilon$ is prime. Suppose $u < v$ are positive integers such that for all k in $[u,v]$ we have $q_{k+1} \le 2q_k - 4$. Then for every n in $[q_u + 3, 2q_v - 2]$, the Galois group of $\mathscr{J}_n^{\epsilon}(x)$, assumed irreducible, is S_n.

We used the above Lemma to check case (a) of Theorem 1.7 applies for both $\epsilon = +1$ and $\epsilon = -1$ and all n in the range $26 \le n \le 10^9$. Also, as mentioned above, we used Magma to check the (irreducibility and) Galois group of $L_{2n+\delta}(x)$ for small values of n. Parts (a) and (b) of Theorem 1.9 summarize the results of our numerical computations in Pari and Magma, respectively.

6. Mod p Factorizations

In her 1924 dissertation, Ille [14] states a beautiful factorization property modulo primes for Legendre polynomials, which she attributed to her advisor Schur, but she did not provide a proof. Here is the statement of the result.

Theorem 6.1. *Let p be an odd prime number and let m be a positive integer whose base-p expansion is given by*

$$m = a_0 + a_1 p + \cdots + a_r p^r, \qquad 0 \le a_i < p \text{ for } i = 0, 1, \ldots, r.$$

Then the reduction mod p of the Legendre polynomial $P_m(x)$ admits the factorization

$$P_m(x) \equiv P_{a_0}(x)P_{a_1}(x)^p \cdots P_{a_r}(x)^{p^r} \bmod p.$$

As far as we know, the first published proof appears in Wahab [24, Theorem 6.1]. Wahab's advisor, Carlitz wrote a paper [5] on the more general subject of factorizations of orthogonal polynomials modulo integers less than the degree and called the factorization formula for Legendre polynomials a "Schur congruence." The name has been generally adopted, and polynomial families satisfying such congruences have been studied more broadly; see, for example, [1] and [19].

We recently discovered that in 1913, Holt stated this property for Legendre polynomials in a notice [13] to the London Mathematical Society; it does not appear that Holt published a subsequent paper with more details, though that was his intention. Thus, unfortunately his congruence went unnoticed for some time. It's probably too late to change the name "Schur congruence" to "Holt-Schur congruence" but since Holt laid much of the foundation for the study of Stjeltjes' conjecture, we thought we should point out that many years prior to Ille's thesis, Holt had discovered the Schur congruence and indicated that he had a proof. His earlier papers contained special cases.

Recall that $P_m(x)$ is an even polynomial if m is even and an odd polynomial if m is odd, so for every $m \geq 0$, the polynomial

$$L_m(x) = \begin{cases} P_m(x) & \text{if } m \text{ is even;} \\ P_m(x)/x & \text{if } m \text{ is odd.} \end{cases}$$

is an even polynomial of degree $2\lfloor m/2 \rfloor$.

Theorem 6.2. *Suppose $\epsilon \in \{\pm 1\}$, $n \geq 4$ and $n = u+p$ where p is a prime in the range $n/2 < p \leq n$.*

(1) If $(2n+3)/3 \leq p \leq n$ or, equivalently, if $0 \leq u \leq (p-3)/2$, then

$$J_n^\epsilon(x) \equiv J_u^\epsilon(x) \left(J_1^-(x)\right)^p \bmod p, \qquad \text{and}$$
$$J_n^\epsilon(x - 1/3) \equiv (3/2) J_u^\epsilon(x - 1/3)\ x^p \bmod p.$$

(2) Suppose $p \neq 2, 5$. If $n/2 < p \leq (2n+1)/3$ or, equivalently, if $(p-1)/2 \leq u < p$, then

$$J_n^\epsilon(x) \equiv x^{(p-\epsilon)/2} J^{-\epsilon}_{u+\delta-(p+1)/2}(x) \left(J_1^+(x)\right)^p \bmod p \text{ and}$$
$$J_n^\epsilon(x - 3/5) \equiv (5/2) x^p (x - 3/5)^{(p-\epsilon)/2} J^{-\epsilon}_{u+\delta-(p+1)/2}(x - 3/5) \bmod p.$$

Proof. Let $m = 2n + \delta \geq 8$ where $\delta = (\epsilon + 1)/2 \in \{0, 1\}$.

We begin with part (1). We have $m - 2p = 2n + \delta - 2p = 2u + \delta$. Note that by the constraint on u, we have $2u + \delta < p$. Thus, by Theorem 6.1,

$$L_{2n+\delta}(x) \equiv L_{2u+\delta}(x) L_2(x)^p \bmod p.$$

Since $L_{2k+\delta}(x) = (-1)^k J_k^\epsilon(-x^2)$, we have

$$(-1)^n J_n^\epsilon(-x^2) \equiv (-1)^u J_u^\epsilon(-x^2) \left(-J_1^-(-x^2)\right)^p \bmod p.$$

Noting that $n = u + p$ makes the signs on both sides match up, we conclude that

$$J_n^\epsilon(-x^2) - J_u^\epsilon(-x^2) \left(J_1^-(-x^2)\right)^p$$

is identically 0 as a polynomial over $\mathbf{F}_p$, hence

$$J_n^\epsilon(x) \equiv J_u^\epsilon(x) \left(J_1^-(x)\right)^p \bmod p.$$

The second congruence follows from the first one by noting that $J_1^-(x) = (1 + 3x)/2$ and applying Fermat's congruence.

For part (2), let $p \in ({}^{n}/_{2}, {}^{(2n+1)}/_{3}]$ so that the following are valid base-p expansions:

$$n = u \cdot p^0 + 1 \cdot p^1$$
$$m = (2u + \delta - p) \cdot p^0 + 3 \cdot p^1.$$

The Holt-Schur factorization gives us

$$P_m(x) \equiv P_{2u+\delta-p}(x) P_3(x)^p \bmod p.$$

This translates into the L-factorzation as

$$x^\delta L_m(x) \equiv x^{1-\delta} L_{2u+\delta-p}(x)(xL_3(x))^p \bmod p,$$

where the term $x^{1-\delta}$ comes from the fact that $2u+\delta-p = 2v+(1-\delta)$ where $v = u+\delta-(p+1)/2$. As before, we now use the fact that the L-polynomials are even to get

$$(-1)^n J_n^\epsilon(-x^2) \equiv x^{p+1-2\delta}(-1)^v J_v^{-\epsilon}(-x^2)(-J_1^+(-x^2))^p \bmod p.$$

Recalling $n = u + p$ and $2\delta - 1 = \epsilon$, and writing $x^{p+1-2\delta} = (-1)^{(p+1-2\delta)/2}(-x^2)^{(p-\epsilon)/2}$, we find

$$J_n^\epsilon(-x^2) - (-x^2)^{(p-\epsilon)/2} J_v^{-\epsilon}(-x^2)(J_1^+(-x^2))^p$$

vanishes identically over $\mathbf{F}_p$, hence

$$J_n^\epsilon(x) \equiv x^{(p-\epsilon)/2} J_v^{-\epsilon}(x)(J_1^+(x))^p \bmod p.$$

The second congruence follows from the first one by noting that $J_1^+(x) = (3+5x)/2$.

□

7. Wild primes

The results of the previous section afford us a new path by which to try to establish for a given n and ϵ that J_n^ϵ has Galois group S_n. Namely, one observes by numerical investigation that primes p very close to, but not exceeding, n, tend to be wildly ramified in a root field of $J_n^\epsilon(x)$; of course, as before, we assume that J_n^ϵ is irreducible. When p is wildly ramified, it divides a ramification index, hence the order of the group, allowing us to conclude that the Galois group is S_n via Jordan's criterion. Using the results of the previous section, we will develop a numerical criterion for a prime p to be wildly ramified in a root field of $J_n^\epsilon(x)$. We illustrate this in particular for $n = p+3$ where $p \geq 13$ is a prime satisfying $p \equiv 1 \bmod 4$ in which case we can prove, assuming only that $J_{p+3}^\epsilon(-1/3)$ is not divisible by p^2, both that $J_{p+3}^\epsilon(x)$ is irreducible, and that it has Galois group S_{p+3}. We present numerical data on how often this condition holds.

Theorem 7.1. *Suppose $\epsilon \in \{\pm 1\}$ and $n = p + u > 12$ where p is a prime in the range $2n/3 < p < n-2$. If*

$$v_p(J_n^\epsilon(-1/3)) = 1 \text{ and } v_p(J_u^\epsilon(-1/3)) = 0,$$

then the Newton Polygon of $J_n^\epsilon(x - 1/3)$ at p consists of a slope 0 segment of length u and a slope $-1/p$ segment of length p. If, additionally, $J_n^\epsilon(x)$ has no factor in $\mathbf{Q}[x]$ of degree $\leq u$, then $J_n^\epsilon(x)$ is irreducible over $\mathbf{Q}$ and has Galois group S_n.

Proof. From Theorem 6.2, we have

$$J_n^\epsilon(x) \equiv J_u^\epsilon(x) J_1^-(x)^p \bmod p,$$

and so

$$J_n^\epsilon(x - 1/3) \equiv \frac{3}{2}\, x^p\, J_u^\epsilon(x - 1/3) \bmod p.$$

Let us write

$$J_n^\epsilon(x - 1/3) = \sum_{j=0}^{n} A_j x^j, \qquad J_u^\epsilon(x - 1/3) = \sum_{j=0}^{u} a_j x^j.$$

We see immediately that

$$A_i \equiv 0 \bmod p \text{ for } i = 0, 1, 2, \ldots p-1.$$

Moreover, $v_p(A_p) = v_p(a_0) = v_p(J_u^\epsilon(-1/3)) = 0$. Since $v_p(A_n) = v_p(\binom{2n+\epsilon}{n}) = 0$, we conclude that the corners of the Newton Polygon of $J_n^\epsilon(x - 1/3)$ are $(0,1)$, $(p,0)$, and $(n,0)$, giving a slope 0 segment of length u and a slope $-1/p$ segment of length p. The shape of this Newton polygon dictates that in any factorization of $J_n^\epsilon(x - 1/3)$, at least one of the factors must have degree at most u; if no such factors exist, then $J_n^\epsilon(x-1/3)$, and therefore also $J_n^\epsilon(x)$, is irreducible. Moreover, in the field obtained by adjoining a root of this polynomial, p is wildly ramified. By Theorem 4.3, the Galois closure of this field has Galois group containing A_n and is therefore S_n by Proposition 2.3. □

Corollary 7.2. *Fix $\epsilon \in \{\pm 1\}$ and an integer $u \geq 3$. Let $B(u)$ be the largest prime dividing $J_u^\epsilon(-1/3)$. For every sufficiently large prime p, specifically for $p > \max(2u, B(u))$, if $J_{p+u}^\epsilon(x)$ does not have a factor in $\mathbf{Q}[x]$ of degree $\leq u$, then $J_{p+u}^\epsilon(x)$ is irreducible. Under this assumption, if, furthermore, $v_p(J_{p+u}^\epsilon(-1/3)) < 2$, then the Galois group of $J_{p+u}^\epsilon(x)$ is S_{p+u}.*

In the case $u = 3$ in the above Corollary, for "half" the primes p, we can prove both irreducibility and fullness of the Galois group assuming only the condition on p^2 not dividing the value of $J_{p+3}^\epsilon(-1/3)$. To do so, we need to make use of a 2-adic Newton polygon as well as the p-adic one. We first recall the computation, first made by Wahab [24, Theorem 3.1], of the 2-adic Newton polygon of $P_m(2x+1)$.

Theorem 7.3 (Wahab)**.** *Let m be a positive integer with base 2 expansion*

$$m = 2^{e_1} + 2^{e_2} + \ldots + 2^{e_r}, \qquad e_1 > e_2 > \cdots > e_r \geq 0.$$

Then the vertices of the 2-adic Newton polygon of $P_m(2x+1)$ are

$$(0,0), (2^{e_1}, 1), (2^{e_1} + 2^{e_2}, 2), (2^{e_1} + 2^{e_2} + 2^{e_3}, 3), \ldots, (m, r).$$

Thus, this Newton polygon consists of r segments with slopes

$$m_i = \frac{1}{2^{e_i}}, \qquad i = 1, \ldots, r.$$

Corollary 7.4. *Suppose $\epsilon \in \{\pm 1\}$ and n is a positive integer. Let $m = 2n + \delta$ where $\delta = (\epsilon+1)/2$. Write the 2-adic expansion of n as*

$$n = 2^{k_1} + 2^{k_2} + \ldots + 2^{k_r}, \qquad k_1 > k_2 > \cdots > k_r \geq 0.$$

Then,

(1) The 2-adic Newton polygon of $L_m(2x+1)$ consists of r segments with slopes

$$m_i = \frac{1}{2^{k_i+1}}, \qquad i = 1, \ldots, r.$$

(2) Any factor in $\mathbf{Q}[x]$ of $L_m(x)$ has degree divisible by 2^{k_r+1}.

(3) Any factor of $J_n^\epsilon(x)$ in $\mathbf{Q}[x]$ has degree divisible by 2^{k_r}.

Proof. (1) If $\epsilon = -1$ so that $m = 2n$, then the base 2 expansion of m is simply

$$m = 2^{k_1+1} + 2^{k_2+1} + \ldots + 2^{k_r+1}.$$

Since $L_m(x) = P_m(x)$ in this case, (1) follows immediately from Theorem 7.3. Now suppose $\epsilon = 1$, giving

$$m = 2^{k_1+1} + 2^{k_2+1} + \ldots + 2^{k_r+1} + 2^0.$$

In this case, $P_m(2x+1) = (2x+1)L_m(2x+1)$, so the Newton polygon of $P_m(2x+1)$ is the Minkowski sum of the Newton polygon of $L_m(2x+1)$ and that of $2x+1$, which is simply a slope 1 segment of length 1. By Theorem 7.3, the Newton polygon of $L_m(2x+1)$ thus has the claimed slopes.

(2) It suffices to prove that if $L_m(x)$ has an irreducible factor $g(x)$ of degree d in $\mathbf{Q}[x]$, then 2^{k_r+1} divides d. Note that $g(2x+1)$ is an irreducible degree d factor of $L_m(2x+1)$. Consider the number field $\mathbf{Q}(\alpha)$ where α is a root of of $g(2x+1)$; its degree d decomposes as a sum $d = \sum_j e_j f_j$ where e_j and f_j are, respectively, the ramification index and residual degree corresponding to the distinct embeddings $\mathbf{Q}(\alpha) \hookrightarrow \mathbf{Q}_2(\alpha)$. It suffices to show that 2^{k_r+1} divides each e_j. This follows from Coleman [6, Corollary p. 185] but since the argument is elementary and elegant, we give the details. Since α is a root of $L_m(2x+1)$, its valuation is the negative of one of the slopes of the 2-adic Newton polygon of $L_m(2x+1)$, i.e. it is $-1/2^{k_i+1}$ for some $1 \leq i \leq r$ by (1). Since the denominator of this valuation is the ramification index e_j, and since $k_i \geq k_r$ for $i = 1, \ldots, r$, we have shown that 2^{k_r+1} divides e_j for each j. Hence d is divisible by 2^{k_r+1} and we are done.

(3) Suppose $J_n^\epsilon(x)$ has a factor over $\mathbf{Q}$ of degree e. Recall that $L_m(x) = (-1)^n J_n^\epsilon(-x^2)$, hence $L_m(x)$ has a rational factor of degree $2e$, so by (2), $2^{k_r+1} | 2e$, i.e. 2^{k_r} divides e.

□

Theorem 7.5. *Suppose $\epsilon \in \{\pm 1\}$ and $n = p+3$ where $p \geq 13$ is a prime satisfying $p \equiv 1 \bmod 4$. If*

$$v_p(J_n^\epsilon(-1/3)) = 1,$$

then $J_n^\epsilon(x)$ is irreducible over $\mathbf{Q}$ and has Galois group S_n.

Proof. By Theorem 7.1, the Newton polygon at p has a slope 0 segment of length 3 and one of length p. By Cor. 7.4, every factor has degree divisible by 4, so there is no factor of degree less than 4, hence irreducibility (note that the hypothesis on n means that $k_r = 2$ in the statement of Cor. 7.4). The rest follows from Corollary 7.2. □

We tested the condition $v_p(J_{p+3}^\epsilon(-1/3)) < 2$ for primes $p < 18,637$. In this range, there are only three exceptions: $(p, \epsilon) = (59, 1)$, $(p, \epsilon) = (3191, -1)$ and $(p, \epsilon) = (12799, 1)$. In all these cases the valuation was 2. We do not have an explanation as to why these exceptions occur, hence we do not have a good sense whether there will be infinitely many exceptions or not. However, the advantage of this approach is that when the condition does hold, we do not need to assume irreducibility of the polynomial, but can instead derive it from the given hypotheses. In the case of $n = p+3$ where $p \equiv 3 \bmod 4$, we do not yet know how to rule out the quadratic and cubic factors.

We conclude with an alternative approach to verifying the condition that $v_p(J_{p+3}^\epsilon(-1/3)) < 2$ that may prove more amenable to computation for large n. Using the recursion relations for the Jacobi polynomials, we may write

$$J_n^{(\alpha,\beta)}(x) = C(\alpha, \beta, x) J_{n-3}^{(\alpha,\beta)}(x) + Q(\alpha, \beta, x) J_{n-4}^{(\alpha,\beta)}(x),$$

where C and Q are cubic and quadratic polynomials in x, respectively. Under the specializations $\alpha = \pm 1/2$, $\beta = 0$ and specifically in degree $n = p+3$, we get the following explicit expressions :

$$J_{p+3}^\epsilon(x) = C^\epsilon(x) J_p^\epsilon(x) + Q^\epsilon(x) J_{p-1}^\epsilon(x), \tag{1}$$

where

$$\begin{aligned}C^+(x) &= \frac{(4p+3)(4p+5)(4p+7)(4p+9)(4p+11)(4p+13)}{8(p+1)(p+2)(p+3)(2p+3)(2p+5)(2p+7)}x^3\\ &+ \frac{3(4p+3)(4p+5)(4p+7)(4p+9)(4p+11)(8p^2+28p+7)}{8(p+1)(p+2)(p+3)(2p+3)(2p+5)(2p+7)(4p+1)}x^2\\ &+ \frac{5(4p+5)(4p+7)(4p+9)(32p^4+224p^3+488p^2+336p+63)}{8(p+1)(p+2)(p+3)(2p+3)(2p+5)(2p+7)(4p+1)}x\\ &+ \frac{(4p+7)(8p^2+28p+15)(32p^4+224p^3+520p^2+448p+105)}{8(p+1)(p+2)(p+3)(2p+3)(2p+5)(2p+7)(4p+1)}\end{aligned}$$

$$\begin{aligned}C^-(x) &= \frac{(4p+1)(4p+3)(4p+5)(4p+7)(4p+9)(4p+11)}{8(p+1)(p+2)(p+3)(2p+1)(2p+3)(2p+5)}x^3\\ &+ \frac{3(4p+1)(4p+3)(4p+5)(4p+7)(4p+9)(8p^2+20p-5)}{8(p+1)(p+2)(p+3)(2p+1)(2p+3)(2p+5)(4p-1)}x^2\\ &+ \frac{5(4p+3)(4p+5)(4p+7)(32p^4+160p^3+200p^2-9)}{8(p+1)(p+2)(p+3)(2p+1)(2p+3)(2p+5)(4p-1)}x\\ &+ \frac{(4p+5)(8p^2+20p+3)(32p^4+160p^3+232p^2+80p-15)}{8(p+1)(p+2)(p+3)(2p+1)(2p+3)(2p+5)(4p-1)}\end{aligned}$$

$$\begin{aligned}Q^+(x) &= \frac{-p(2p+1)(4p+5)(4p+7)(4p+9)(4p+11)(4p+13)}{4(p+1)(p+2)(p+3)(2p+3)(2p+5)(2p+7)(4p+1)}x^2\\ &+ \frac{-p(2p+1)(4p+7)(4p+9)(4p+11)(8p^2+36p+33)}{2(p+1)(p+2)(p+3)(2p+3)(2p+5)(2p+7)(4p+1)}x\\ &+ \frac{-3p(2p+1)(4p+9)(4p^2+18p+17)(4p^2+18p+19)}{4(p+1)(p+2)(p+3)(2p+3)(2p+5)(2p+7)(4p+1)}\end{aligned}$$

$$\begin{aligned}Q^-(x) &= \frac{-p(2p-1)(4p+3)(4p+5)(4p+7)(4p+9)(4p+11)}{4(p+1)(p+2)(p+3)(2p+1)(2p+3)(2p+5)(4p-1)}x^2\\ &+ \frac{-p(2p-1)(4p+5)(4p+7)(4p+9)(8p^2+28p+17)}{2(p+1)(p+2)(p+3)(2p+1)(2p+3)(2p+5)(4p-1)}x\\ &+ \frac{-3p(2p-1)(4p+7)(4p^2+14p+9)(4p^2+14p+11)}{4(p+1)(p+2)(p+3)(2p+1)(2p+3)(2p+5)(4p-1)}.\end{aligned}$$

Since $J_p^\epsilon(x) \equiv J_1^-(x)^p \bmod p$, we will introduce an auxiliary polynomial $E_p^\epsilon(x)$ by writing $J_p^\epsilon(x) = J_1^-(x)^p + pE_p^\epsilon(x)$. Substituting this expression into (1) and then evaluating at $x = -1/3$ gives us (recall $J_1^-(-1/3) = 0$):

$$\begin{aligned}J_{p+3}^\epsilon(x) &= C^\epsilon(x)J_1^-(x)^p + pC^\epsilon(x)E_p^\epsilon(x) + Q^\epsilon(x)J_{p-1}^\epsilon(x);\\ J_{p+3}^\epsilon(-1/3) &= pC^\epsilon(-1/3)E_p^\epsilon(-1/3) + Q^\epsilon(-1/3)J_{p-1}^\epsilon(-1/3).\end{aligned}$$

We therefore seek a criterion for which the right side of the previous equation is not divisible by p^2 (note p divides the content of $Q^\epsilon(x)$). Dividing by p, we can make this into a mod p criterion:

$$C^\epsilon(-1/3)E_p^\epsilon(-1/3) \not\equiv (1/p)Q^\epsilon(-1/3)J_{p-1}^\epsilon(-1/3) \bmod p.$$

Proposition 7.6. *For a prime $p > 3$, we have $v_p(J^{\epsilon}_{p+3}(-1/3)) < 2$ if and only if*

$$-35E_p^+(-1/3) \not\equiv 38J_{p-1}^+(-1/3) \text{ for } \epsilon = 1, \text{ and}$$
$$-5E_p^-(-1/3) \not\equiv 21J_{p-1}^-(-1/3) \text{ for } \epsilon = -1.$$

Acknowledgments. We are grateful to Emmanuel Kowalski for helpful correspondence. We would also like to thank the anonymous referee for a careful reading and helpful suggestions.

References

[1] J.-P. Allouche, G. Skordev, G., Schur congruences, Carlitz sequences of polynomials and automaticity. Discrete Math. **214** (2000), no. 1-3, 2149.
[2] J. Bourgain, Z. Rudnick, On the nodal sets of toral eigenfunctions, Invent. Math. **185** (2011), 199-237.
[3] 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.
[4] M. Bush, F. Hajir. An irreducibility lemma. J. Ramanujan Math. Soc. **23** (2008), no. 1, 33-41.
[5] L. Carlitz, Congruence properties of the polynomials of Hermite, Laguerre and Legendre, Math. Z. **59**, (1954), 474-483.
[6] R. Coleman, On the Galois groups of exponential Taylor polynomials, Enseign. Math. **33**, (1987), 183-189.
[7] J. Cullinan, F. Hajir. Primes of prescribed congruence class in short intervals. INTEGERS **12** (2012) #A56.
[8] F. Gouvea, p-adic Numbers. An introduction. Second edition. Universitext. Springer-Verlag, Berlin, 1997.
[9] F. Hajir. Algebraic properties of a family of generalized Laguerre polynomials. Canad. J. Math. **61** (2009), no. 3, 583-603.
[10] 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.
[11] J.B. Holt. The irreducibility of Legendre's polynomials. Proc. London Math. Soc. **11** (1912) 351-356.
[12] J.B. Holt. On the irreducibility of Legendre's polynomials. Proc. London Math. Soc. **12** (1912) 126-132.
[13] J.B. Holt, The irreducibility of Legendre's polynomials (Third Paper). Proc. London Math. Soc. Recrods of Proceedings at Meetings, Session November 1912 - June, 1913 **12** (1913), p. xxxi-xxxii.
[14] H. Ille, Zur Irreduzibilität der Kugelfunctionen, Jbuch.der Dissertationen, Berlin(1924).
[15] A-M. Legendre, Recherches sur l'attraction des sphéroïdes homogènes, Mémoires de Mathématiques et de Physique, présentés à l'Académie Royale des Sciences, par divers savans, et lus dans ses Assemblées, Tome X, pp. 411-435 (Paris, 1785).
[16] R. F. McCoart, Irreducibility of certain classes of Legendre polynomials, Duke Mathematical Journal **28** no. 2 (1961), 239-246.
[17] I.G. Melnikov, On irreducibility of Legendre polynomials, Ukrainskii Matematiceskii Zurnal (Kiev), vol. **8** (1956), 26-33.
[18] P. Morton, Legendre polynomials and complex multiplication, I, J. Number Theory **130**. no. 8 (2010), 1718-1731.
[19] T. D. Noe, On the Divisibility of Generalized Central Trinomial Coefficients. J. Integer Seq. **9**, Article 06.2.7, 2006.
[20] O. Ramaré, R. Rumely. Primes in arithmetic progressions. Math. Comp. **65** (1996), no. 213, 397-425.
[21] I. Schur, *Gessammelte Abhandlungen*, Vol. 3, Springer, 1973
[22] T. J. Stieltjes, Letter No. 275 of Oct. 2, 1890. In: Correspondence de Hermite et Stieltjes, vol. 2, Gauthier-Villars, Paris (1905).
[23] G. Szegö, Orthogonal Polynomials, 4th ed. Providence, RI: Amer. Math. Soc., 1975.
[24] J.H. Wahab. New cases of irreducibility for Legendre polynomials. Duke Math. J. **19**, (1952) 165-176.
[25] J.H. Wahab. New cases of irreducibility for Legendre polynomials. II. Duke Math. J. **27**, (1960) 481-482.
[26] 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