Arithmetic Properties of the Legendre Polynomials

John Cullinan

&

Farshid Hajir

October 6, 2013

Introduction and Definitions

Introduction and Definitions

$(P_m(x))_{m \geqslant 0}$ orthogonal family on $[-1, 1]$

Introduction and Definitions

$(P_m(x))_{m \geqslant 0}$ orthogonal family on $[-1, 1]$

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

Introduction and Definitions

$(P_m(x))_{m \geqslant 0}$ orthogonal family on $[-1, 1]$

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

Solution $y = P_m(x)$ to the Legendre differential equation

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

Introduction and Definitions

$(P_m(x))_{m\geqslant 0}$ orthogonal family on $[-1,1]$

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

Solution $y = P_m(x)$ to the Legendre differential equation

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

$P_m(-x) = (-1)^m P_m(x)$

Define

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

Applications to Number Theory

Applications to Number Theory

...as the Hasse invariant

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

for the Legendre-form elliptic curve $E_\lambda : y^2 = x(x-1)(x-\lambda)$ over $\mathbf{F}_p$, where $p = 2m+1$.

Applications to Number Theory

...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 $p = 2m+1$.

...when $m = (p-1)/2$ is odd, the class number of $\mathbf{Q}(\sqrt{-p})$ is one-third the number of linear factors of $P_m(x)$ over $\mathbf{F}_p$.

Applications to Number Theory

...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 $p = 2m+1$.

...when $m = (p-1)/2$ is odd, the class number of $\mathbf{Q}(\sqrt{-p})$ is one-third the number of linear factors of $P_m(x)$ over $\mathbf{F}_p$.

Thus, the irreducibility of $P_m(x)$ would imply that the class number of $\mathbf{Q}(\sqrt{-p})$ is "governed" by the number field cut out by a root of $P_m(x)$, specifically by how the prime p splits in it.

Stieltjes' Conjecture

Stieltjes' Conjecture

In a letter to Hermite (1890):

Conjecture. $P_{2n}(x)$ and $P_{2n+1}(x)/x$ are irreducible over $\mathbf{Q}$.

Stieltjes' Conjecture

In a letter to Hermite (1890):

$\boxed{\textbf{Conjecture. } P_{2n}(x) \text{ and } P_{2n+1}(x)/x \text{ are irreducible over } \mathbb{Q}.}$

Some cases of Stieltjes' conjecture have been verified by Holt, Ille, Melnikov, Wahab, McCoart.

Roughly:

If m or $m/2$ is within a few units of a prime number, then $L_m(x)$ is irreducible over $\mathbb{Q}$.

Setup

Convenient form of the polynomials

Setup

Convenient form of the polynomials

$(\!(\alpha)\!)_n \stackrel{\text{def}}{=} (\alpha+2)(\alpha+4)\cdots(\alpha+2n)$

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

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

$$(-2)^n n!\, L_m(x) = J_n^{\epsilon}(-x^2).$$

Galois Groups

Galois Groups

Assume the $L_m(x)$ are irreducible over $\mathbf{Q}$. What is Gal $L_m(x)$?

Galois Groups

Assume the $L_m(x)$ are irreducible over $\mathbf{Q}$. What is Gal $L_m(x)$?

We conjecture: (recall $\delta \in \{0, 1\}$)

1. Gal $L_{2n+\delta}(x) \simeq S_2 \wr S_n$
2. Gal $J_n^{\epsilon}(x) \simeq S_n$

We'll focus on #2.

Galois Groups

Assume the $L_m(x)$ are irreducible over $\mathbf{Q}$. What is Gal $L_m(x)$?

We conjecture: (recall $\delta \in \{0, 1\}$)

1. Gal $L_{2n+\delta}(x) \simeq S_2 \wr S_n$
2. Gal $J_n^\epsilon(x) \simeq S_n$

We'll focus on #2.

Theorem

The discriminant of J_n^ϵ is not a square in $\mathbf{Q}^\times$.

$$\operatorname{disc} J_n^\epsilon(x) = 2^{n^2-n} \prod_{k=1}^{n} k^{2k-1}(2k+\epsilon)^{k-1}(2k+2n+\epsilon)^{n-k}$$

Newton Polygons and a Criterion of Jordan

Newton Polygons and a Criterion of Jordan

Jordan's Criterion: a transitive subgroup of S_n containing a p-cycle (p prime) in the range $n/2 < p < n-2$ contains A_n.

Newton Polygons and a Criterion of Jordan

Jordan's Criterion: a transitive subgroup of S_n containing a p-cycle (p prime) in the range $n/2 < p < n-2$ contains A_n.

The cycle type of certain elements of the Galois Group can be detected by the (least common multiples of the denominators of the slopes of) the Newton polygon at p, as p ranges over all primes.

Tame Evidence

From the Newton Polygon:

All primes p in the range $n < p < 4n + \epsilon$ ramify in the splitting field of $J_n^\epsilon(x)$; since $p \nmid n!$, all these primes are <u>tamely ramified</u>.

Tame Evidence

From the Newton Polygon:

All primes p in the range $n < p < 4n + \epsilon$ ramify in the splitting field of $J_n^{\epsilon}(x)$; since $p \nmid n!$, all these primes are tamely ramified.

Theorem

Every prime p in the interval $(n, 4n + \epsilon]$ yields a decomposition of the number $2n + 1$ as

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

We have:

(a) *If p is a prime in the range $n < p \leqslant 2n + \epsilon$, then q divides $\#\,\mathrm{Gal}\ J_n^{\epsilon}(x)$; and*

(b) *If p is a prime in the range $2n + \epsilon < p \leqslant 4n + \epsilon$ then q' divides $\#\,\mathrm{Gal}\ J_n^{\epsilon}(x)$.*

Tame Evidence

Tame Evidence

Theorem

The Hardy-Littlewood conjecture implies that $J_n^{\epsilon}(x)$ (assuming irreducibility) has Galois group S_n.

Tame Evidence

Theorem

The Hardy-Littlewood conjecture implies that $J_n^{\epsilon}(x)$ (assuming irreducibility) has Galois group S_n.

Additionally, for $n \leqslant 10^{10}$ we compute the number of instances of pairs (q, p) and (q', p) that allow us to conclude $\mathrm{Gal} \simeq S_n$ (roughly 10^7 such pairs).

Wild Primes and Mod p Factorization

Wild Primes and Mod p Factorization

Write $m = a_0 + a_1 p + \cdots + a_r p^r$. Then

Wild Primes and Mod p Factorization

Write $m = a_0 + a_1 p + \cdots + a_r p^r$. Then

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

Wild Primes and Mod p Factorization

Write $m = a_0 + a_1 p + \cdots + a_r p^r$. Then

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

Ille (in her 1924 dissertation) attributes this to Schur (no proof); Holt proved special cases 1912 (but stated it earlier). First proof by Wahab in 1952.

Wild Primes and Mod p Factorization

Write $m = a_0 + a_1 p + \cdots + a_r p^r$. Then

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

Ille (in her 1924 dissertation) attributes this to Schur (no proof); Holt proved special cases 1912 (but stated it earlier). First proof by Wahab in 1952.

Theorem

Let $n \geqslant 4$ and $n = u + p$ where $n/2 < p \leqslant n$.

1. *If $0 \leqslant u \leqslant (p-3)/2$, then*

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

2. *If $(p-1)/2 \leqslant u < p$, then*

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

Wild Evidence

p very close to n tend to be wildly ramified in a root field of $J_n^{\epsilon}(x)$.

p is wildly ramified $\to$ p divides a ramification index $\to$ $p \mid \#Gal$.

Jordan $\to$ Gal $\supset A_n$.

Wild Evidence

p very close to n tend to be wildly ramified in a root field of $J_n^\epsilon(x)$.

p is wildly ramified $\to$ p divides a ramification index $\to$ $p \mid \#\mathrm{Gal}$.

Jordan $\to$ Gal $\supset A_n$.

Theorem

Let $n = p + 3$ *where* $p \geqslant 13$ *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.

Wild Evidence

p very close to n tend to be wildly ramified in a root field of $J_n^{\epsilon}(x)$.

p is wildly ramified $\to$ p divides a ramification index $\to$ $p \mid \#\mathrm{Gal}$.

Jordan $\to$ Gal $\supset A_n$.

Theorem

Let $n = p + 3$ *where* $p \geqslant 13$ *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*.*

Exceptions?

Wild Evidence

p very close to n tend to be wildly ramified in a root field of $J_n^\epsilon(x)$.

p is wildly ramified $\to$ p divides a ramification index $\to$ $p \mid \#\mathrm{Gal}$.

Jordan $\to$ Gal $\supset A_n$.

Theorem

Let $n = p + 3$ *where* $p \geqslant 13$ *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*.*

Exceptions?

For $p < 18,637$:

three exceptions: $(p, \epsilon) \in \{(59, 1), (3191, -1), (12799, 1)\}$.

In all these cases the valuation equals 2.