The Tangent Analogues of the Chebyshev Polynomials

Jack S. Calcut

November 10, 2008

1 Introduction

We study the tangent analogues $\tan(n \arctan x)$ of the Chebyshev polynomials from an algebraic viewpoint. They are rational functions of a pleasant form and enjoy several noteworthy properties: a useful composition law, their numerators $p_n(x)$ split into the minimal polynomials of the numbers $\tan k\pi/n$, they define the elements of the Galois groups of these minimal polynomials, and their algebraic and number theoretic properties strongly parallel those of the roots of unity. We give a complete factorization of the polynomials $p_n(x)$ in $\mathbb{Z}[x]$, give several applications, and list some open problems.

2 Tangent Rational Functions

For each natural number n define

$$F_n(x) = \tan(n \arctan x). \tag{1}$$

These functions are the tangent analogues of the Chebyshev polynomials of the first kind for cosine. They were known to John Bernoulli as early as 1712 [16, pp. 193–195], appear explicitly in Euler's 1748 work [8, pp. 217–218], were used by Carlitz and Thomas [4, p. 792], and were rediscovered independently by the author as an undergraduate [1]. Define

$$p_n(x) = \mathrm{Im}(1+ix)^n \quad \text{and} \quad q_n(x) = \mathrm{Re}(1+ix)^n, \tag{2}$$

then

$$F_n(x) = \frac{p_n(x)}{q_n(x)}. \tag{3}$$

There are several ways to verify (3) and we mention two of them. First, the tangent angle addition formula and the recursions

$$\begin{aligned} p_{n+1}(x) &= xq_n(x) + p_n(x) \\ q_{n+1}(x) &= q_n(x) - xp_n(x) \end{aligned}$$

establish (3) by induction (see [1]). Second, let $\theta = \arctan x$ and apply De Moivre's formula:

$$\begin{aligned} F_n(x) = \frac{\sin n\theta}{\cos n\theta} &= \frac{1}{i}\frac{(\cos\theta + i\sin\theta)^n - (\cos\theta - i\sin\theta)^n}{(\cos\theta + i\sin\theta)^n + (\cos\theta - i\sin\theta)^n} \\ &= \frac{1}{i}\frac{(1+ix)^n - (1-ix)^n}{(1+ix)^n + (1-ix)^n} = \frac{\mathrm{Im}(1+ix)^n}{\mathrm{Re}(1+ix)^n}. \end{aligned}$$

If $n > 0$, then

$$F_{-n}(x) = -F_n(x) = -\frac{p_n(x)}{q_n(x)}.$$

Therefore, for each integer n, $F_n(x)$ is a rational function with integer coefficients. For example

$$F_1(x) = \frac{x}{1}, \quad F_2(x) = \frac{2x}{1-x^2}, \quad F_3(x) = \frac{3x-x^3}{1-3x^2},$$
$$F_4(x) = \frac{4x-4x^3}{1-6x^2+x^4}, \quad \text{and} \quad F_5(x) = \frac{5x-10x^3+x^5}{1-10x^2+5x^4}.$$

Clearly $p_n(x)$ is the alternating sum of the odd power terms in the binomial expansion $(1+x)^n$ and $q_n(x)$ is the alternating sum of the even power terms.

Remark 1. *The Chebyshev polynomials of the first kind $T_n(x) = \cos(n \arccos x)$ are integer polynomials. The analogous functions for sine are not in general polynomials or rational functions.*

Fix a natural number n and define for each integer k

$$r_k = \tan \frac{k\pi}{n}. \tag{4}$$

Strictly speaking, r_k depends on n, but n will be clear from context. Clearly r_k is determined by the congruence class $[k]_n \in \mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ since tangent has period π and r_k exists unless $[k]_n = [n/2]_n$. Equations (1) and (3) imply that the roots of $p_n(x)$ are the distinct real numbers (4), say with $k = 0, 1, \ldots, n-1$ if n is odd and further $k \neq n/2$ if n is even. Therefore, each of the numbers (4) is algebraic over $\mathbb{Q}$ of degree at most $\deg p_n(x)$. Geometrically, the numbers (4) are the slopes of the lines through the origin and the $2n$th roots of unity as in Figure 1. This naturally organizes

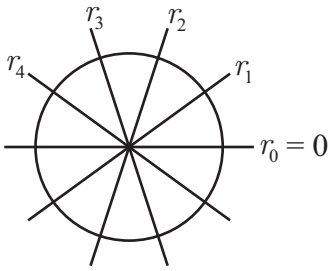


Figure 1: $n = 5$.

the roots r_k in a counterclockwise manner. If $4|n$, then

$$r_{n/4} = 1 \text{ and } r_{3n/4} = -1. \tag{5}$$

Similarly, $q_n(x)$ has roots $\tan k\pi/2n$ where $k = 1, 3, \ldots, 2n-1$ if n is even and further $k \neq n$ if n is odd. Thus, for fixed n, $p_n(x)$ and $q_n(x)$ have real, distinct, and simple roots, and $F_n(x) = p_n(x)/q_n(x)$ is reduced.

The nth roots of unity form a multiplicative cyclic group. Analogously, the tangent functions enjoy the following easily verified properties:

$$F_i \circ F_j(x) = F_{ij}(x) \quad \text{and} \tag{6}$$

$$F_i(r_j) = r_{ij}, \tag{7}$$

where i and j are arbitrary integers and $n \in \mathbb{N}$ is fixed for the r_j. Equation (6) will be called the *composition law*. Note that the composition law does not hold precisely when $F_j(x)$ does not exist and i is even, in which case $F_i \circ F_j(x)$ does not exist and $F_{ij}(x) = 0$. The composition law provides a natural proof that $p_n(x)$ has only the obvious rational roots (compare [1]).

Proposition 1. *The rational roots of $p_n(x)$ are $x = 0$ if $4 \nmid n$ and $x = 0$ and $x = \pm 1$ if $4|n$.*

Proof. The stated numbers are obviously roots and the result is clear if $n \leq 2$. So, write $n = s_1 s_2 \cdots s_j > 2$ a product of positive primes. We proceed by induction on j with the inductive hypothesis: the possible rational roots of $p_n(x)$ are $x = 0$ and $x = \pm 1$ and of $q_n(x)$ are $x = \pm 1$.

If $j = 1$, then n is an odd prime and the rational root theorem (RRT) implies that the possible rational roots of $p_n(x)$ are $x = 0$, $x = \pm 1$, and $x = \pm n$. Substituting $x = \pm n$ into $p_n(x) = 0$ implies $n|1$, a contradiction. Similar reasoning proves the $j = 1$ case for $q_n(x)$.

Assume $j > 1$. Suppose $p_n(x) = 0$ with x rational. Then, $F_n(x) = 0$ and by the composition law (6) either $F_{n/s_1}(x)$ exists and $F_{s_1}\left(F_{n/s_1}(x)\right) = 0$, or $F_{n/s_1}(x)$ does not exist and $s_1 = 2$. The former implies $p_{s_1}\left(F_{n/s_1}(x)\right) = 0$, where $F_{n/s_1}(x)$ is rational since x is rational and F_{n/s_1} is a rational function with integer coefficients. Thus, $F_{n/s_1}(x) = 0$ or $F_{n/s_1}(x) = \pm 1$ by induction. $F_{n/s_1}(x) = 0$ implies $p_{n/s_1}(x) = 0$ and $x = 0$ or $x = \pm 1$ by induction. $F_{n/s_1}(x) = \pm 1$ implies $p_{n/s_1}(x) = \pm q_{n/s_1}(x)$ and $x = \pm 1$ by the RRT. On the other hand, if $F_{n/s_1}(x)$ does not exist, then $q_{n/s_1}(x) = 0$ and $x = \pm 1$ by induction. The inductive step is proven for $p_n(x)$. Next, suppose $q_n(x) = 0$ with x rational. Then, $F_n(x)$ does not exist and by the composition law either $F_{n/s_1}(x)$ does not exist or $q_{s_1}\left(F_{n/s_1}(x)\right) = 0$ where $F_{n/s_1}(x)$ is rational. The former implies $q_{n/s_1}(x) = 0$ and $x = \pm 1$ by induction. The latter implies $F_{n/s_1}(x) = \pm 1$ by induction, so $p_{n/s_1}(x) = \pm q_{n/s_1}(x)$ and $x = \pm 1$ by the RRT. The proof is complete. □

Corollary 1. *The rational values of the tangent function at rational multiples of π are 0 and ± 1.*

Proof. Suppose $\tan k\pi/n = x$ is rational where $k \in \mathbb{Z}$ and $n \in \mathbb{N}$. Then

$$0 = \tan k\pi = \tan\left(n \arctan x\right) = \frac{p_n(x)}{q_n(x)}$$

and so x is a rational root of $p_n(x)$. Now apply Proposition 1. □

Remark 2. *There exist other proofs of Corollary 1 (see [2]).*

3 Algebraic Degree and Galois Groups

Lemma 1. *Let $n > 2$ and $(k, n) = 1$. Let $\psi(x)$ be a minimal polynomial of r_k over $\mathbb{Q}$. Then*

$$\mathbb{Q}(r_k) = \mathbb{Q}(r_1)$$

is the splitting field of $p_n(x)$ and of $\psi(x)$ over $\mathbb{Q}$. In particular, $\mathbb{Q}(r_k)$ is a Galois extension of $\mathbb{Q}$.

Proof. If r_j exists, then by (7)

$$r_j = F_j(r_1) \in \mathbb{Q}(r_1) \tag{8}$$

since F_j is a rational function with integer coefficients. In particular, $\mathbb{Q}(r_1)$ is the splitting field of $p_n(x)$ over $\mathbb{Q}$. Write $ak + bn = 1$ for integers a and b. Then

$$r_1 = F_a(r_k) \in \mathbb{Q}(r_k). \tag{9}$$

Equations (8) and (9) imply that $\mathbb{Q}(r_k) = \mathbb{Q}(r_1)$. Finally, $\psi(x)|p_n(x)$ in $\mathbb{Q}[x]$ since $\psi(x)$ is minimal and they share a root. The result follows. □

Lemma 2. *Let $n > 2$ and $(k, n) = 1$. Then each $\sigma \in \mathrm{Gal}\,(\mathbb{Q}(r_k)/\mathbb{Q})$ is induced by some F_m where $(m, n) = 1$. In particular, $\mathrm{Gal}\,(\mathbb{Q}(r_k)/\mathbb{Q})$ is abelian. Additionally, if $4|n$, then $m \equiv 1 \mod 4$.*

Proof. Let $\sigma \in \mathrm{Gal}\,(\mathbb{Q}(r_k)/\mathbb{Q})$. Such an automorphism permutes the roots of $p_n(x)$ and so

$$\sigma(r_1) = r_m = F_m(r_1)$$

for some m. Now, $\mathbb{Q}(r_k) = \mathbb{Q}(r_1)$ has a basis $\left\{1, r_1, r_1^2, \ldots, r_1^{d-1}\right\}$ over $\mathbb{Q}$ where $d = [\mathbb{Q}(r_1) : \mathbb{Q}]$. Therefore σ is completely determined by $[m]_n$ and we say that σ is *induced by* F_m. Notice that $\sigma \in \mathrm{Gal}\,(\mathbb{Q}(r_k)/\mathbb{Q})$ commutes with each rational function F_i. By (7), σ acts on each r_j by

$$\sigma(r_j) = \sigma\left(F_j(r_1)\right) = F_j(\sigma(r_1)) = F_j(r_m) = r_{mj}.$$

It follows that $\mathrm{Gal}\,(\mathbb{Q}(r_k)/\mathbb{Q})$ is abelian. The inverse of σ is induced by say F_l. Hence, $r_{lm} = r_1$ and $(m, n) = 1$. Finally if $4|n$, then σ must fix $1 = r_{n/4}$ which implies $m \equiv 1 \mod 4$. □

Remark 3. *The restriction $(m, n) = 1$ parallels the same restriction for the nth roots of unity. The restriction $m \equiv 1 \mod 4$ is special to the tangent numbers r_k and comes from the line of slope 1. As we will show, these obvious restrictions are all of the restrictions. In other words, as with the roots of unity,* the Galois groups here are as large as possible.

We need a technical result.

Lemma 3. *The discriminant Δ_n of $p_n(x)$ is*

$$\Delta_n = \begin{cases} 2^{(n-1)(n-2)} n^n & \text{if } n \text{ is odd} \\ 2^{(n-1)(n-2)} n^{n-2} & \text{if } n \text{ is even.} \end{cases}$$

To avoid interruption, Lemma 3 is proved in Section 7.

If $f(x) \in \mathbb{Z}[x]$ and $p > 1$ is prime, then let $\overline{f(x)}$ denote the image of $f(x)$ in $\mathbb{Z}_p[x]$ under the natural ring epimorphism.

Lemma 4. *Let n be natural and $p > 2$ prime such that $(p, n) = 1$. Then $\overline{p_n(x)} \in \mathbb{Z}_p[x]$ has simple roots.*

Proof. It suffices to show that the discriminant of $\overline{p_n(x)}$ is nonzero. The discriminant of $\overline{p_n(x)}$ equals $\Delta_n \mod p$ (see [17, pp. 82–88]) which is nonzero by Lemma 3 since $p > 2$ and $(p, n) = 1$. □

Remark 4. *The analogous result for $x^n - 1$ is easier, since $\overline{x^n - 1}$ and its formal derivative $\overline{nx^{n-1}}$ are clearly coprime in $\mathbb{Z}_p[x]$.*

Lemma 5. *Let $n > 2$ and $p > 2$ prime such that $(p, n) = 1$ and $p \equiv 1 \mod 4$. Then r_p is a root of any minimal polynomial of r_1 over $\mathbb{Q}$.*

It is remarkable that Dirichlet's beautiful argument for roots of unity and cyclotomic polynomials [12, pp. 51-52] may be recast in the present context.

Proof. Let $h(x)$ be a minimal polynomial of r_1 over $\mathbb{Q}$. Then $h(x)|p_n(x)$ in $\mathbb{Q}[x]$ since $p_n(r_1) = 0$. By Gauss' lemma [6, p. 86] we may assume $h(x)$ is *primitive*, that is $h(x) \in \mathbb{Z}[x]$ is not the zero polynomial and the greatest common divisor of its coefficients is 1. So

$$p_n(x) = f(x)h(x) \tag{10}$$

for some $f(x) \in \mathbb{Z}[x]$. The roots of $p_n(x)$ are distinct, so suppose by way of contradiction that $f(r_p) = 0$. By (7), $f\left(F_p(r_1)\right) = 0$ where $q_p(r_1) \neq 0$. Let $d = \deg f$ and let $g(x) \in \mathbb{Z}[x]$ be the polynomial obtained by clearing denominators in

$$q_p(x)^d f\left(F_p(x)\right).$$

Note that $g(r_1) = 0$. Thus $h(x)|g(x)$ in $\mathbb{Q}[x]$. As $h(x)$ is primitive, $h(x)|g(x)$ in $\mathbb{Z}[x]$. Write

$$k(x)h(x) = g(x)$$

for some $k(x) \in \mathbb{Z}[x]$. Projecting to $\mathbb{Z}_p[x]$ we have

$$\overline{q_p(x)} = \overline{1} \quad \text{and} \quad \overline{p_p(x)} = \overline{x^p}$$

where the latter uses $p \equiv 1 \mod 4$ (this is a crucial point; if $p \equiv 3 \mod 4$, then $\overline{p_p(x)} = \overline{-x^p}$ and the proof unravels.). Recall Fermat's little theorem and exploit the Frobenius homomorphism to obtain

$$\overline{k(x)}\,\overline{h(x)} = \overline{g(x)} = \overline{f\left(x^p\right)} = \overline{f(x)}^p.$$

Note that $\overline{h(x)}$ has positive degree by (10) and since $p_n(x)$ has leading coefficient ± 1 or $\pm n$. Unique factorization in $\mathbb{Z}_p[x]$ implies that some irreducible factor of $\overline{h(x)}$ with positive degree divides $\overline{f(x)}$. Hence, $\overline{p_n(x)} = \overline{f(x)}\,\overline{h(x)}$ has a multiple root contradicting Lemma 4. □

Up until this point all arguments have been elementary. The following lemma will employ Dirichlet's theorem [7, 15] on primes in arithmetic progressions.

Lemma 6. *Let n and k be coprime naturals. If $4|n$, then assume further that $k \equiv 1 \mod 4$. Then there exists a prime $p > 2$ such that $(p, n) = 1$, $p \equiv k \mod n$, and $p \equiv 1 \mod 4$.*

Proof. First, assume $4|n$ so $k \equiv 1 \mod 4$. By Dirichlet's theorem there exist infinitely many primes in the arithmetic progression $4na + k$. Any such prime $p > \max\{2, n\}$ behaves as desired.

Next, assume $n = 4m + 2$. Case 1. $k \equiv 1 \mod 4$. The previous argument proves this case. Case 2. $k \equiv 3 \mod 4$. Let $K = k + n$, so $(K, n) = 1$ and $K \equiv 1 \mod 4$. Case 1 applied to K

yields a prime $p > 2$ such that $(p, n) = 1$, $p \equiv K \equiv k \mod n$, and $p \equiv 1 \mod 4$, proving Case 2.

Finally, assume n is odd. The system of congruences $X \equiv 1 \mod 4$ and $X \equiv k \mod n$ has a solution $l > 0$ by the Chinese remainder theorem. The progression $4na + l$ contains infinitely many primes by Dirichlet's theorem. Any such prime $p > 2$ behaves as desired. □

Corollary 2. *Let $n > 2$ and let $h(x)$ be a minimal polynomial of r_1 over $\mathbb{Q}$. Then r_k is a root of $h(x)$ provided $(k, n) = 1$ and, in case $4|n$, $k \equiv 1 \mod 4$.*

Proof. Without loss, assume $k > 0$. By Lemma 6 there exists a prime $p > 2$ such that $(p, n) = 1$, $p \equiv k \mod n$, and $p \equiv 1 \mod 4$. Lemma 5 implies $r_p = r_k$ is a root of $h(x)$. □

If $4|n$, then

$$H_n = \{[m]_n \mid (m, n) = 1 \text{ and } m \equiv 1 \mod 4\} \tag{11}$$

is a well-defined subgroup of $\mathbb{Z}_n^\times$ of index 2 and order

$$|H_n| = \varphi(n)/2. \tag{12}$$

Theorem 1. *Let $n > 2$ and $(k, n) = 1$. Then*

$$\deg_{\mathbb{Q}} r_k = \begin{cases} \varphi(n) & \text{if } 4 \nmid n \\ \varphi(n)/2 & \text{if } 4|n \end{cases} \tag{13}$$

and

$$\mathrm{Gal}\,(\mathbb{Q}(r_k)/\mathbb{Q}) \cong \begin{cases} \mathbb{Z}_n^\times & \text{if } 4 \nmid n \\ H_n & \text{if } 4|n. \end{cases}$$

Proof. We have $\deg_{\mathbb{Q}} r_k = [\mathbb{Q}(r_k) : \mathbb{Q}] = |\mathrm{Gal}\,(\mathbb{Q}(r_k)/\mathbb{Q})|$. The stated degree (13) is an upper bound for $\deg_{\mathbb{Q}} r_k$ by Lemma 2 and equations (11) and (12) and is a lower bound by Lemma 1 and Corollary 2. This proves (13). By Lemma 2 each $\sigma \in \mathrm{Gal}\,(\mathbb{Q}(r_k)/\mathbb{Q})$ is induced by some F_m so naturally we define

$$\begin{aligned} \Phi : Aut_{\mathbb{Q}}\mathbb{Q}\,(r_k) &\to \mathbb{Z}_n^\times \\ \sigma &\mapsto [m]_n \end{aligned}$$

which is a well-defined injective homomorphism. Corollary 2 implies Φ is surjective if $4 \nmid n$ and maps onto H_n if $4|n$. □

Remark 5. *In [13, pp. 33–41] Niven proved that if $n > 2$, $n \neq 4$, and $(k, n) = 1$, then*

$$\deg_{\mathbb{Q}} \left(\tan \frac{2k\pi}{n} \right) = \begin{cases} \varphi(n) & \text{if } 4 \nmid n \\ \varphi(n)/2 & \text{if } n \equiv 4 \mod 8 \\ \varphi(n)/4 & \text{if } n \equiv 0 \mod 8. \end{cases} \tag{14}$$

The reader may verify that (13) *and* (14) *agree. Niven's proof has the advantage of being independent of a difficult result (for us, Dirichlet's theorem), but it is somewhat ad hoc and lacks insight, and the resulting statement* (14) *is clumsier than* (13). *With the present approach the Galois groups* $\mathrm{Gal}\,(\mathbb{Q}(r_k)/\mathbb{Q})$ *and* (13) *emerge naturally, the factor of* 2 *in* (13) *is transparent (slope* 1 *must be*

fixed), and deep parallels are revealed between the tangent numbers r_k and roots of unity especially in the proof of Lemma 5.

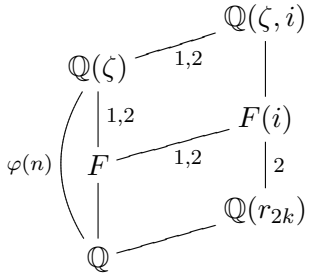
Pedagogically minded readers may be interested in the following natural approach to Theorem 1 which avoids Dirichlet's theorem. The material on the functions $F_n(x)$ preceding Remark 3, which is intuitive and elementary, should be presented first (Proposition 1 may be safely omitted). At this point, one has naturally motivated necessary restrictions on the relevant Galois groups and it remains only to prove they are sufficient. One option is to employ Niven's approach [13, pp. 33–41]. Here is another option that applies to cosine and sine as well. Fix $n > 2$ and let $\zeta = \exp 2\pi i/n$. Then $\mathrm{Gal}\,(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong \mathbb{Z}^+$ by Dirichlet's argument [12, pp. 51-52]. Complex conjugation is a nontrivial automorphism in $\mathrm{Gal}\,(\mathbb{Q}(\zeta)/\mathbb{Q})$ since $n > 2$. Let $(k, n) = 1$. The cosine proof is the simplest: as $\cos 2k\pi/n = (\zeta^k + \zeta^{-k})/2$ we see that $\mathbb{Q}(\cos 2k\pi/n) \subset \mathbb{Q}(\zeta)$ is the fixed field of complex conjugation and so $\deg_{\mathbb{Q}} \cos 2k\pi/n = \varphi(n)/2$. Next we outline the proof for tangent, the proof for sine being similar. If $n \neq 4$, then

$$\tan 2k\pi/n = \frac{1}{i}\frac{\zeta^k - \zeta^{-k}}{\zeta^k + \zeta^{-k}}.$$

Define

$$F = \mathbb{Q}\left(\frac{\zeta^k - \zeta^{-k}}{\zeta^k + \zeta^{-k}}\right)$$

and consider the lattice of fields



(15)

Strictly speaking, the node $\mathbb{Q}(\zeta, i)$ is unnecessary, but it is the natural overfield and its inclusion makes a pretty picture. In each of the three cases $4 \nmid n$, $n \equiv 0 \mod 8$, and $n \equiv 4 \mod 8$ one determines the upper left vertical degree and the middle diagonal degree using elementary field theory. The result is equation (14)*. This proves* (13) *and the proof of Theorem 1 follows as above verbatim.*

4 Complete Factorization of $p_n(x)$ in $\mathbb{Q}[x]$

Lemma 7. *Let $n > 2$ and $k \in \mathbb{Z}$ such that r_k exists. Let $\mathcal{G} = \mathrm{Gal}\,(\mathbb{Q}(r_k)/\mathbb{Q})$. Then*

$$\prod_{\sigma \in \mathcal{G}} (x - \sigma(r_k)) \tag{16}$$

is the monic minimal polynomial of r_k over $\mathbb{Q}$.

Proof. It suffices to show that $\mathbb{Q}(r_k)$ is a Galois extension of $\mathbb{Q}$ and this follows from Lemma 1 applied to k/n reduced to lowest terms. □

Fix $n > 2$. For each positive divisor $d \neq 2$ of n define

$$\psi_d(x) = \prod_{[j]_d \in \mathbb{Z}_d^+} (x - r_{j \cdot n/d}). \tag{17}$$

If $4|d$, then define

$$\psi_d^+(x) = \prod_{[j]_d \in H_d} (x - r_{j \cdot n/d}) \quad \text{and} \tag{18}$$

$$\psi_d^-(x) = \prod_{[j]_d \in H_d} (x - r_{-j \cdot n/d}). \tag{19}$$

Notice that $r_{j \cdot n/d} = \tan j\pi/d$. This explains the condition $d \neq 2$ in (17) and shows that the polynomials (17)–(19) are actually independent of n. Lemma 7 and Theorem 1 imply that if $4 \nmid d$, then (17) is the monic minimal polynomial of $r_{n/d}$ and if $4|d$, then (18) and (19) are the monic minimal polynomials of $r_{n/d}$ and $r_{-n/d}$ respectively.

Lemma 8. *If $d \neq e$, then $\psi_d(x)$ and $\psi_e(x)$ have no common roots. If $4|d$, then $\psi_d^+(x)$ and $\psi_d^-(x)$ have no common roots and $\psi_d(x) = \psi_d^+(x)\psi_d^-(x)$.*

Proof. First write $d = (d,e)d'$, $e = (d,e)e'$, and $n = (d,e)d'e'n'$. If $\psi_d(x)$ and $\psi_e(x)$ share the root $r_{jn/d} = r_{kn/e}$ where $(j,d) = 1$ and $(k,e) = 1$, then $(d,e)d'e'|je' - kd'$. Hence $d' = e' = 1$ proving the first part. Next, let $4|d$. If $r_{jn/d} = r_{-kn/d}$ is a common root where $j, k \equiv 1 \mod 4$, then $j \equiv -k \mod 4$ a contradiction. The last part is clear. □

Remark 6. *Equations* (17)–(19) *admit equivalent definitions with the products over suitable classes in $\mathbb{Z}_n^+$. In the tower of fields*

$$\mathbb{Q} \subseteq \mathbb{Q}(r_{n/d}) \subseteq \mathbb{Q}(r_1) \tag{20}$$

$\mathbb{Q}(r_{n/d})$ is a stable intermediate field, $\mathrm{Gal}\left(\mathbb{Q}(r_{n/d})/\mathbb{Q}\right)$ *permutes the roots of a minimal polynomial of $r_{n/d}$ transitively, and each $\tau \in \mathrm{Gal}\left(\mathbb{Q}(r_{n/d})/\mathbb{Q}\right)$ extends to some $\sigma \in \mathrm{Gal}\left(\mathbb{Q}(r_1)/\mathbb{Q}\right)$ by the fundamental theorem of Galois theory. In the present cases, extendability may be shown directly. For instance if $d|n$ are naturals and $(j,d) = 1$, then there exists an integer l such that $[l]_d = [j]_d$ and $(l,n) = 1$ (proof: l must have the form $l = j + md$ for some m; let m be the product of the primes dividing n but not dividing d or j.).*

Theorem 2. *A complete factorization of $p_n(x)$ into irreducibles in $\mathbb{Q}[x]$ is*

$$p_n(x) = \pm \prod_{d|n} \psi_d(x) \quad \text{if } (n,4) = 1, \tag{21}$$

$$p_n(x) = \pm n \prod_{2 \neq d|n} \psi_d(x) \quad \text{if } (n,4) = 2, \text{ and} \tag{22}$$

$$p_n(x) = \pm n \prod_{\substack{4 \nmid d|n \\ d \neq 2}} \psi_d(x) \prod_{4|d|n} \psi_d^+(x) \prod_{4|d|n} \psi_d^-(x) \quad \text{if } (n,4) = 4. \tag{23}$$

Proof. For (21), n is odd and $p_n(x)$ has leading coefficient ± 1 and degree n. The product in (21) has all simple roots by Lemma 8 and has degree $\sum_{d|n} \varphi(d) = n$. The proofs of (22) and (23) are similar. □

5 Complete Factorization of $p_n(x)$ in $\mathbb{Z}[x]$

We begin by stating some elementary results that will be used below without explicit mention. A nonzero polynomial is *primitive* provided it lies in $\mathbb{Z}[x]$ and the greatest common divisor of its coefficients is 1. The product of primitive polynomials is primitive [6, p. 85]. Every nonzero $f(x) \in \mathbb{Q}[x]$ may be written uniquely in the form $f(x) = c\widehat{f}(x)$ where $c \in \mathbb{Q}^+$ and $\widehat{f}(x)$ is primitive [6, p. 86]; c is called the *content* of $f(x)$ and content is multiplicative.

The goal of this section is to prove following two results.

Proposition 2. *Each $\psi_d(x)$ and $\psi_d^{\pm}(x)$ is primitive, unless $d = 2p^a$ for some odd prime p and $a > 0$ in which case $\psi_d(x) \notin \mathbb{Z}[x]$ and $p\psi_d(x)$ is primitive.*

Theorem 3. *The factorization* (21) *is a factorization into irreducibles in $\mathbb{Z}[x]$. If $n = 2p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}$ where each $a_j > 0$ and the p_j are distinct odd primes, then*

$$p_n(x) = \pm 2 \prod_{\substack{2 \neq d \mid n \\ d \neq 2p_j^b}} \psi_d(x) \prod_{\substack{1 \leq j \leq k \\ 1 \leq i \leq a_j}} p_j \psi_{2p_j^{a_i}}(x) \tag{24}$$

is a factorization into irreducibles in $\mathbb{Z}[x]$. If $n = 2^a p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}$ where $a > 1$, each $a_j > 0$, and the p_j are distinct odd primes, then

$$p_n(x) = \pm 2^a \prod_{\substack{4 \nmid d \mid n \\ d \neq 2p_j^b}} \psi_d(x) \prod_{\substack{1 \leq j \leq k \\ 1 \leq i \leq a_j}} p_j \psi_{2p_j^{a_i}}(x) \prod_{4 \mid d \mid n} \psi_d^+(x) \prod_{4 \mid d \mid n} \psi_d^-(x) \tag{25}$$

is a factorization into irreducibles in $\mathbb{Z}[x]$.

The proof of these results comprises the rest of this section.

Lemma 9. *If d is odd, then $\psi_d(x)$ is primitive.*

Proof. If $e|d$, then write $\psi_e(x) = c_e\widehat{\psi_e}(x)$ where $c_e \in \mathbb{Q}^+$ and $\widehat{\psi_e}(x)$ is primitive. As d is odd, $p_d(x)$ has leading coefficient ± 1 and is primitive. By (21), $p_d(x) = \left(\prod_{e|d} c_e\right)\left(\pm \prod_{e|d} \widehat{\psi_e}(x)\right)$ and so $\prod_{e|d} c_e = 1$. Comparing leading coefficients in $p_d(x) = \pm \prod_{e|d} \widehat{\psi_e}(x)$, we see that each $\widehat{\psi_e}(x)$ is monic. Each $\psi_e(x)$ is monic as well, so each $c_e = 1$ and $\psi_e(x) = \widehat{\psi_e}(x)$ is primitive. □

Lemma 10. *If $n = 2^a m$ where m is odd, then the content of $p_n(x)$ is 2^a.*

Proof. First, $p_k(x)$ is primitive for every odd k and $q_k(x)$ is primitive for every k. Next

$$p_{2k}(x) = 2p_k(x)q_k(x) \tag{26}$$

by (3) and (6). The result follows by repeated application of (26). □

Lemma 11. *Let $k > 1$ be an integer and $f(x) = g(x) \cdot kh(x)$ where $f(x)$ and $g(x)$ are primitive and $h(x) \in \mathbb{Q}[x]$. Then $h(x) \notin \mathbb{Z}[x]$ and $kh(x)$ is primitive.*

Proof. Both results follow from simple content arguments. □

Lemma 12. *Let $n = 2p^a$ where $p > 0$ is an odd prime and $a > 0$. Then for each $d = 2p^b$, $1 \le b \le a$, we have $\psi_d \notin \mathbb{Z}[x]$ and $p\psi_d(x)$ is primitive.*

Proof. We proceed by induction on a. First, assume $a = 1$ so $n = 2p$. Then by (22) we have

$$p_n(x) = \pm n\psi_1(x)\psi_p(x)\psi_{2p}(x)$$

where $\psi_1(x) = x$ and $\psi_p(x)$ are primitive by Lemma 9 and the content of $p_n(x)$ is 2 by Lemma 10. Hence

$$\pm\frac{1}{2}p_n(x) = [\psi_1(x)\psi_p(x)] \cdot p\psi_{2p}(x)$$

and the result follows by Lemma 11.

Next, let $a > 1$ and $n = 2p^a$. Then using (22) we have

$$\pm\frac{1}{2}p_n(x) = \left[\prod_{0\le i\le a} \psi_{p^i}(x) \prod_{1\le i\le a-1} p\psi_{2p^i}(x)\right] \cdot p\psi_{2p^a}(x)$$

where each polynomial in the products in brackets is primitive by Lemma 9 or induction. The result follows by Lemma 11. □

Taking stock, Lemmas 9 and 12 prove Proposition 2 for odd d and $d = 2p^a$ respectively. These results, (21), and (22) prove Theorem 3 for odd n and $n = 2p_1^{a_1}$.

Lemma 13. *Let $f(x) = g(x)\prod_{i=1}^k h_i(x)$ where $f(x)$ and $g(x)$ are primitive and each $h_i(x) \in \mathbb{Q}[x]$ is monic. Then each $h_i(x)$ is primitive.*

Proof. The hypotheses imply that $f(x)$ and $g(x)$ have equal leading coefficients. For each i write $h_i(x) = c_i\widehat{h_i}(x)$ where $c_i \in \mathbb{Q}^+$ and $\widehat{h_i}(x)$ is primitive. Then $f(x) = (\prod c_i)\left(g(x)\prod \widehat{h_i}(x)\right)$ and $\prod c_i = 1$. Comparing leading coefficients in $f(x) = g(x)\prod \widehat{h_i}(x)$, we see that each $\widehat{h_i}(x)$ is monic. As $h_i(x) = c_i\widehat{h_i}(x)$ and $h_i(x)$ is monic, each $c_i = 1$. The result follows. □

Equation (22) implies (24) holds as a polynomial identity in $\mathbb{Q}[x]$. We have already shown each term in the second product in (24) is primitive, and therefore so is their product. Divide (24) by 2, the content of $p_n(x)$, and note that $\pm p_n(x)/2$ and the second product in (24) have equal leading coefficients. Lemma 13 now implies that each term in the first product in (24) is primitive. An almost identical argument applies to each term in the first, third, and fourth products in (25). This completes the proof of Theorem 3 and Proposition 2.

Remark 7. *Proposition 2 provides an effective and rigorous procedure to produce these integer minimal polynomials using suitably precise floating point arithmetic on a computer: evaluate the desired product* (17), (18), *or* (19), *if $d = 2p^a$ for some odd prime p and $a > 0$, then further multiply the polynomial by p, and finally round each coefficient to the nearest integer. In practice, an alternative is to use a computer algebra system such as MAGMA to factor an appropriate $p_n(x)$ over $\mathbb{Z}$ and then pick out the correct irreducible factor by inspection.*

6 Applications and Questions

6.1 Rational and Quadratic Irrational Values $\tan k\pi/n$

We compute exactly the values $\tan k\pi/n$ of degree 1 or 2 over $\mathbb{Q}$. We may assume $(k,n) = 1$ and $0 \le k\pi/n < \pi$. Theorem 1 and the well-known inequality $\varphi(n) \ge \sqrt{n/2}$ reduce this to a finite problem. The trivial cases $n = 1$ and $n = 2$ are inspected directly. The rational values are $\tan 0 = 0$, $\tan \pi/4 = 1$, and $\tan 3\pi/4 = -1$, in agreement with Corollary 1 above. For degree 2, we find $n = 2, 3, 6, 8, 12$. The pertinent values of k and corresponding minimal polynomials are

$$\begin{aligned} x^2 - 3 &\text{ for } n = 3 \text{ and } k = 1, 2, \\ 3x^2 - 1 &\text{ for } n = 6 \text{ and } k = 1, 5, \\ x^2 + 2x - 1 &\text{ for } n = 8 \text{ and } k = 1, 5, \\ x^2 - 2x - 1 &\text{ for } n = 8 \text{ and } k = 3, 7, \\ x^2 - 4x + 1 &\text{ for } n = 12 \text{ and } k = 1, 5, \text{ and} \\ x^2 + 4x + 1 &\text{ for } n = 12 \text{ and } k = 7, 11. \end{aligned}$$

Therefore, the quadratic irrational values are:

$$\begin{array}{lll} \tan \pi/3 = \sqrt{3} & \tan 2\pi/3 = -\sqrt{3} & \tan \pi/6 = \sqrt{3}/3 \\ \tan 5\pi/6 = -\sqrt{3}/3 & \tan \pi/8 = \sqrt{2} - 1 & \tan 3\pi/8 = \sqrt{2} + 1 \\ \tan 5\pi/8 = -\sqrt{2} - 1 & \tan 7\pi/8 = 1 - \sqrt{2} & \tan \pi/12 = 2 - \sqrt{3} \\ \tan 5\pi/12 = \sqrt{3} + 2 & \tan 7\pi/12 = -\sqrt{3} - 2 & \tan 11\pi/12 = \sqrt{3} - 2 \end{array}$$

Recently Cha [5, p. 16] used the above to give a nontrivial example where the so-called Grand Simplicity Hypothesis for function fields may be verified.

6.2 Higher Degree Irrationalities and Expression by Real Radicals

Using elementary properties of $\varphi(n)$ and (13) it is easy to see that $\deg_{\mathbb{Q}} r_k$ is always even. Next one may ask for numbers $\tan k\pi/n$ of degree 4 over $\mathbb{Q}$. These have $n = 5, 10, 16, 20, 24$ and $(k,n) = 1$. The cases $n = 5$ and $n = 10$ correspond to biquadratic polynomials. First, $\tan \pi/5$ has minimal polynomial $x^4 - 10x^2 + 5$ and $\tan \pi/5 = \sqrt{5 - 2\sqrt{5}}$. So, there is a 36–54–90 triangle with opposite side lengths $\sqrt{5 - 2\sqrt{5}}$, 1, and $\sqrt{6 - 2\sqrt{5}}$. Note that this example may be obtained simply from the most basic properties of the rational functions in the beginning of Section 2. A student may be introduced to applications of these functions with minimal background and perhaps may be enticed to study number and field theory to learn more. Second, $\tan \pi/10$ has minimal polynomial $5x^4 - 10x^2 + 1$ and $\tan \pi/10 = \sqrt{1 - 2\sqrt{5}/5}$. So, there is an 18–72–90 triangle with opposite side lengths $\sqrt{1 - 2\sqrt{5}/5}$, 1, and $\sqrt{2 - 2\sqrt{5}/5}$.

This raises the question: which numbers $\tan k\pi/n$ are expressible by real radicals? The Galois groups $\mathrm{Gal}\,(\mathbb{Q}(r_k)/\mathbb{Q})$ are all abelian by Lemma 2 and hence are solvable. Therefore the numbers $\tan k\pi/n$ may all be expressed by radicals. However, expressions by *real* radicals are rarely possible. If an irreducible polynomial $f(x) \in \mathbb{Q}[x]$ has all real roots and any root can be constructed from

$\mathbb{Q}$ by a combination of field operations and real mth roots, then $\deg f(x)$ is a power of 2 and the Galois group of $f(x)$ over $\mathbb{Q}$ is a 2-group [11]. If $n = 7$, then $\deg \tan \pi/7 = \varphi(7) = 6$ and $\tan \pi/7$ is not expressible by real radicals. This question is related to compass and straightedge constructions and further investigation is left to the reader.

6.3 Algebraic Integers

Niven raised the question of which numbers $\tan k\pi/n$ are algebraic integers when he mentioned that $2\tan \pi/6$ is not an algebraic integer [13, p. 38]. To see this, $\tan \pi/6$ has minimal polynomial $3x^2 - 1$ and so $2\tan \pi/6$ has minimal polynomial $3x^2 - 4$. For another example, $\tan \pi/50$ is not an algebraic integer since it has minimal polynomial

$$5x^{20} - 450x^{18} + 9725x^{16} - 76600x^{14} + 253450x^{12} - 369260x^{10} + 250850x^8 - 78200x^6 + 9745x^4 - 290x^2 + 1.$$

Therefore, $2\tan \pi/50$ is not an algebraic integer either by the following lemma.

Lemma 14. *Let $\alpha \in \mathbb{C}$ be algebraic over $\mathbb{Q}$ of degree D and with minimal polynomial $h(x) = \sum_{j=0}^{D} a_j x^j \in \mathbb{Z}[x]$. If $0 \neq m \in \mathbb{Z}$, then $m\alpha$ has minimal polynomial $g(x) = \sum_{j=0}^{D} m^{D-j} a_j x^j \in \mathbb{Z}[x]$.*

Remark 8. *Even if $h(x)$ is primitive, $g(x)$ need not be primitive: take $\alpha = 1/2$ and $m = 2$.*

Proof. Any nonzero rational multiple of α has degree D over $\mathbb{Q}$ and so any minimal polynomial of $m\alpha$ over $\mathbb{Q}$ has degree D. Now $0 = h(\alpha) = \sum a_j m^{-j} (m\alpha)^j$ and the result follows by multiplying through by m^D. □

Corollary 3. *The number $r_k = \tan k\pi/n$ with $(k, n) = 1$ is an algebraic integer if and only if n is not of the form $2p^a$ for some odd prime p and $a > 0$. Further, if $n = 2p^a$ and $0 \neq m \in \mathbb{Z}$, then mr_k is an algebraic integer if and only if $p|m$.*

Proof. The first assertion is immediate by Proposition 2. For the second assertion, r_k has primitive minimal polynomial $p\psi_{2p^a}(x)$ by Proposition 2 and (17). The leading coefficient of $p\psi_{2p^a}(x)$ is p and some coefficient is not divisible by p. By Lemma 14, a minimal polynomial $g(x) \in \mathbb{Z}[x]$ of mr_k is obtained from $p\psi_{2p^a}(x)$ by multiplying each non-leading coefficient by a positive power of m. Therefore p factors out of $g(x)$ yielding a monic integer minimal polynomial of mr_k if and only if $p|m$. □

Remark 9. *Carlitz and Thomas [4] obtained the partial result that $\tan k\pi/n$ with $(k, n) = 1$ is an algebraic integer provided n is odd or $4|n$.*

6.4 Signed Binomial Polynomials

A *signed binomial polynomial* (SBP) is a polynomial of the form

$$\sum_{i=0}^{m} \varepsilon_i \binom{m}{i} x^i \tag{27}$$

where each $\varepsilon_i \in \{-1, 1\}$. That is, expand $(1+x)^m$, collect like powers, and change any subset of the $m + 1$ signs. Two infinite families of SBPs emerge naturally from the functions $F_n(x)$. Before we

present them let us make some preliminary observations. Define $R(m)$ to be the number of SBPs of degree m that are reducible in $\mathbb{Q}[x]$. The interesting point is that there are no known general irreducibilty criteria for polynomials that take the *signs* of the coefficients into account. Bounds on $R(m)$ must be obtained by other means.

If $m > 1$, then $R(m) \geq 4$ by taking all the same signs and strictly alternating signs. If m is odd, then one may exploit the symmetry of the binomial coefficients to obtain reducible SBPs with factors $x-1$ or $x+1$ as follows. Let $m = 2j+1 > 1$ and consider the SBP (27). By symmetry, (27) has 1 as a root if and only if

$$\sum_{i=0}^{j} (\varepsilon_i + \varepsilon_{2j+1-i}) \binom{m}{i} = 0 \tag{28}$$

and (27) has -1 as a root if and only if

$$\sum_{i=0}^{j} (-1)^i (\varepsilon_i - \varepsilon_{2j+1-i}) \binom{m}{i} = 0 \tag{29}$$

where each $\varepsilon_i \pm \varepsilon_{2j+1-i} \in \{-2, 0, 2\}$. The substitutions

$$\begin{aligned} \varepsilon_i + \varepsilon_{2j+1-i} &= 2\delta_i \\ (-1)^i (\varepsilon_i - \varepsilon_{2j+1-i}) &= 2\delta_i \end{aligned} \tag{30}$$

for $1 \leq i \leq j$ show that solutions to

$$\sum_{i=0}^{j} \delta_i \binom{m}{i} = 0 \tag{31}$$

with each $\delta_i \in \{-1, 0, 1\}$ correspond to SBPs (27) having 1 or -1 as a root. This correspondence is a bijection except for the possibility that some solution δ to (31) may correspond to a SBP having 1 and -1 as roots (i.e. both (28) and (29) are satisfied). By (30), this does not occur if some $\delta_i = 0$. Equation (31) has the obvious solution $\delta = \vec{0}$ (i.e. all $\delta_i = 0$) which corresponds to 2^{j+1} distinct solutions to each of (28) and (29). Hence, if $m = 2j+1 > 1$ is odd, then $R(m) \geq 2^{j+2}$.

It is not clear how to produce more reducible or irreducible SBPs. Using MAGMA and a few weeks computing time on multiple Sun Fire V20z nodes of an AMD64 cluster we collected the data in Table 1. In particular the lower bound $R(m) \geq 2^{j+2}$ for $m = 2j+1$ is tight if $1 < m \leq 27$,

m	1	3	5	7	9	11	13	15	17	19	21	23	25	27
$R(m)$	0	8	16	32	64	128	288	512	1024	2048	4096	8192	16384	32768

m	2	4	6	8	10	12	14	16	18	20	22	24	26	28
$R(m)$	4	4	12	12	8	8	32	4	12	16	8	104	16	8

Table 1: The number $R(m)$ of reducible signed binomial polynomials of degree $m \leq 28$.

except when $m = 13$. This anomaly is completely explained by the fact that if $m = 13$, then (31) has, in addition to the obvious solution $\delta = \vec{0}$, the two solutions $\delta = \pm[0, 0, 0, -1, 1, 1, -1]$ each

corresponding to 2^3 distinct solutions to (28) and (29) for a total of $2 \cdot 2^7 + 2 \cdot 2^3 + 2 \cdot 2^3 = 288$ reducible SBPs.

Again computing with MAGMA for several weeks we obtained all exceptional solutions to (31) for $m = 2j + 1 \leq 23$ as in Table 2. It appears that these exceptional solutions are more than a

j	$\pm\delta$
6	$[0,0,0,1,-1,-1,1]$
14	$[0,0,0,0,0,0,0,1,-1,0,1,1,-1,0,0]$
15	$[0,0,0,1,-1,0,0,-1,-1,0,-1,1,1,-1,-1,1]$ $[0,0,0,1,-1,0,0,-1,-1,1,0,1,0,1,0,-1]$
16	$[0,0,0,0,0,0,0,0,0,0,0,0,1,-1,-1,1,0]$
17	$[1,-1,1,-1,1,-1,1,-1,1,-1,1,1,0,-1,-1,1,0,0]$ $[1,-1,1,-1,1,-1,1,-1,1,-1,1,-1,1,-1,-1,1,0,0]$
20	$[0,0,0,0,0,1,0,1,0,0,0,1,-1,1,0,-1,0,-1,1,0,0]$ $[0,0,0,0,0,1,0,1,0,0,0,1,-1,-1,1,-1,0,-1,1,0,0]$ $[0,0,0,0,0,1,-1,1,1,1,0,-1,0,1,0,-1,-1,1,0,0,0]$ $[0,0,0,0,0,1,-1,1,1,1,0,-1,0,-1,1,-1,-1,1,0,0,0]$
23	$[0,0,0,0,0,0,0,0,0,0,0,1,0,0,-1,0,-1,-1,1,0,0,0,0,0]$

Table 2: Exceptional solutions to (31) for $1 \leq j \leq 23$ and $m = 2j + 1$.

small number anomaly.

Having introduced SBPs, let us explain their relation to the tangent functions. The two infinite

n	$q_n(x) - p_n(x)$	$q_n(x) + p_n(x)$
1	$1 - x$	$1 + x$
2	$1 - 2x - x^2$	$1 + 2x - x^2$
3	$1 - 3x - 3x^2 + x^3$	$1 + 3x - 3x^2 - x^3$
4	$1 - 4x - 6x^2 + 4x^3 + x^4$	$1 + 4x - 6x^2 - 4x^3 + x^4$

Table 3: Two infinite families of signed binomial polynomials.

families of SBPs in Table 3 emerge naturally from the functions $F_n(x)$. Moreover, we may determine exactly when each is irreducible.

Lemma 15. *The SBPs $q_n(x) \pm p_n(x)$ are irreducible if and only if $n = 2^j$ for some j.*

Proof. As in (26), we have

$$\frac{p_{2n}(x)}{q_{2n}(x)} = \frac{2p_n(x)q_n(x)}{(q_n(x) - p_n(x))(q_n(x) + p_n(x))}.$$

Therefore

$$p_{4n}(x) = 2p_{2n}(x)(q_n(x) - p_n(x))(q_n(x) + p_n(x)). \tag{32}$$

As $q_n(x)$ is even and $p_n(x)$ is odd, α is a root of $q_n(x) - p_n(x)$ if and only if $-\alpha$ is a root of $q_n(x)+p_n(x)$. Therefore (32) implies that $\tan \pi/4n$ is a root of one of the polynomials $q_n(x)-p_n(x)$ or $q_n(x) + p_n(x)$ and $\tan(4n-1)\pi/4n$ is a root of the other. Both of these numbers have degree $\varphi(4n)/2$ over $\mathbb{Q}$ by (13) and both of these polynomials has degree n. So, they are irreducible if and only if and only if $\varphi(4n)/2 = n$ and this occurs if and only if n is a power of 2. □

In particular, when n is not a power of two these polynomials yield four new reducible SBPs in addition to the obvious four. Hence if $n \neq 2^j$, then $R(m) \geq 8$. Table 1 shows that for $m = 10, 12, 22, 28$ these are the only reducible SBPs. That is, of the $536,870,912$ SBPs of degree 28 the reducible ones are exactly the ones with the same signs, strictly alternating signs, and doubly alternating signs as in Table 1.

Notice that ± 1 are roots of (32). If n is odd, then ± 1 are roots of the polynomials in Table 3. If n is even, then ± 1 are roots of $p_{2n}(x)$ and (32) shows that ± 1 are not roots of the polynomials in Table 3. In particular, these yield examples of reducible SBPs without 1 or -1 as a root.

We close with some open problems.

Conjecture 1. *There does not exist a SBP of odd degree having both* 1 *and* -1 *as roots. Equivalently, every signed sum of the first half of the elements in an odd row of Pascal's triangle (compare* (31)*) is nonzero.*

Conjecture 2. *A SBP of odd degree is reducible over* $\mathbb{Q}$ *if and only if it has* 1 *or* -1 *as a root.*

Conjecture 3. $\lim_{m\to\infty} \frac{R(m)}{2^{m+1}} = 0$.

Conjecture 4. *There exist infinitely many even* m *for which* $R(m) = 8$. *In particular,* $R(m) \not\to \infty$ *as* $m \to \infty$.

7 The Discriminant of $p_n(x)$

This section proves Lemma 3. Fix $n \in \mathbb{N}$ and $\zeta = \exp \pi i/n$, a primitive $2n$th root of unity. If $z \in \mathbb{C}$, then $|z| = (z\overline{z})^{1/2}$ denotes the modulus of z. We have

$$x^{2n} - 1 = \prod_{k=0}^{2n-1} \left(x - \zeta^k\right) \quad \Longrightarrow \quad \sum_{j=0}^{n-1} x^{2j} = \prod_{k=1}^{n-1} \left(x - \zeta^k\right)\left(x - \zeta^{n+k}\right).$$

Evaluating the latter at $x = 1$ yields

$$n = \prod_{k=1}^{n-1} \left(1 - \zeta^{2k}\right) = \zeta^{n(n-1)/2} \prod_{k=1}^{n-1} \left(\zeta^{-k} - \zeta^k\right).$$

Taking the modulus yields

$$n = \left| \prod_{k=1}^{n-1} \left(\zeta^{-k} - \zeta^k\right) \right|. \tag{33}$$

Recalling that

$$r_k = \tan\frac{k\pi}{n} = \frac{1}{i}\frac{\zeta^k - \zeta^{-k}}{\zeta^k + \zeta^{-k}},$$

we obtain the modulus of the product of the nonzero roots of $p_n(x)$:

$$\left|\prod_{\substack{k=1\\k\neq n/2}}^{n-1} r_k\right| = \left|\prod_{\substack{k=1\\k\neq n/2}}^{n-1} \frac{\zeta^k - \zeta^{-k}}{\zeta^k + \zeta^{-k}}\right| = \left|\prod_{\substack{k=1\\k\neq n/2}}^{n-1} \frac{\zeta^{-k} - \zeta^{k}}{\zeta^{-k} + \zeta^{k}}\right|. \tag{34}$$

The value of (34) equals the absolute value of the constant coefficient of the monic polynomial $\pm p_n(x)/x$ if n is odd and $\pm p_n(x)/nx$ if n is even. The value of the former is n and the value of the latter is 1. These values, equations (33) and (34), and $\left|\zeta^{-n/2} - \zeta^{n/2}\right| = 2$ imply that

$$\left|\prod_{\substack{k=1\\k\neq n/2}}^{n-1} \left(\zeta^{-k} + \zeta^{k}\right)\right| = \begin{cases} 1 & \text{if } n \text{ is odd} \\ n/2 & \text{if } n \text{ is even.} \end{cases} \tag{35}$$

Next, we compute the following product that is intimately related to the discriminant (see [17, pp. 82–88]):

$$\delta_n = \prod_{r_k \neq r_l} (r_k - r_l)^2,$$

where the product is taken over pairs of distinct roots of $p_n(x)$. The roots of $p_n(x)$ are real and distinct so $\delta_n > 0$. Thus, we may compute δ_n using the modulus. If n is odd, then

$$\begin{aligned}
\delta_n &= \prod_{0\leq k<l\leq n-1} |r_k - r_l|^2 \\
&= \prod_{0\leq k<l\leq n-1} \left|\frac{2}{i}\frac{\zeta^{k-l} - \zeta^{l-k}}{\left(\zeta^k + \zeta^{-k}\right)\left(\zeta^l + \zeta^{-l}\right)}\right|^2 \\
&= 2^{(n-1)(n-2)} \frac{\left|\prod_{k=1}^{n-1}\left(\zeta^{-k} - \zeta^{k}\right)^{2(n-k)}\right|}{\left|\prod_{k=1}^{n-1}\left(\zeta^k + \zeta^{-k}\right)\right|^{2n-2}} && (36) \\
&= 2^{(n-1)(n-2)} \left|\prod_{k=1}^{n-1}\left(\zeta^{-k} - \zeta^{k}\right)^{n}\right| && (37) \\
&= 2^{(n-1)(n-2)} n^n. && (38)
\end{aligned}$$

Equation (36) combined the obvious $n(n-1)$ factors of 2 with the $2(n-1)$ factors of $\zeta^0 + \zeta^{-0} = 2$ from the denominator and collected the remaining equal terms in the numerator and denominator respectively. Equation (37) collected some equal terms in the numerator, namely $\zeta^{-(n-k)} - \zeta^{n-k} = \zeta^{-k} - \zeta^{k}$, and noted that the denominator in (36) equals 1 by (35). Equation (38) used (33). If n

is even, then

$$\begin{aligned}
\delta_n &= \prod_{\substack{0\le k<l\le n-1\\ k,l\neq n/2}} (r_k - r_l)^2 \\
&= \prod_{\substack{0\le k<l\le n-1\\ k,l\neq n/2}} \left| \frac{2}{i} \frac{\zeta^{k-l} - \zeta^{l-k}}{\left(\zeta^k + \zeta^{-k}\right)\left(\zeta^l + \zeta^{-l}\right)} \right|^2 \\
&= 2^{(n-1)(n-2)} \frac{\left|\prod_{k=1}^{n-1} \left(\zeta^{-k} - \zeta^k\right)\right|^{n-2}}{\left|\prod_{\substack{k=0\\ k\neq n/2}}^{n-1} \left(\zeta^{-k} + \zeta^k\right)\right|^{2n-4}} \qquad (39) \\
&= 2^{(n-1)(n-2)} \frac{n^{n-2}}{2^{2n-4}\left(n/2\right)^{2n-4}} \qquad (40) \\
&= 2^{(n-1)(n-2)} n^{2-n}.
\end{aligned}$$

Equation (39) was obtained similarly to equations (36) and (37). Equation (40) used (33) in the numerator and collected factors of 2 and used (35) in the denominator. Summarizing, we have

$$\delta_n = \begin{cases} 2^{(n-1)(n-2)} n^n & \text{if } n \text{ is odd} \\ 2^{(n-1)(n-2)} n^{2-n} & \text{if } n \text{ is even.} \end{cases}$$

The discriminant Δ_n of $p_n(x)$ is obtained by multiplying δ_n by the leading coefficient of $p_n(x)$ raised to the power $2\deg p_n(x) - 2$ (see [17, p. 82]). If n is odd, then this has no effect. If n is even, then

$$\begin{aligned}
\Delta_n &= (\pm n)^{2n-4} \delta_n \\
&= 2^{(n-1)(n-2)} n^{n-2}.
\end{aligned}$$

Therefore, the discriminant of $p_n(x)$ equals

$$\Delta_n = \begin{cases} 2^{(n-1)(n-2)} n^n & \text{if } n \text{ is odd} \\ 2^{(n-1)(n-2)} n^{n-2} & \text{if } n \text{ is even.} \end{cases}$$

This completes the proof of Lemma 3.

Acknowledgments. The author thanks Gregory Johnson, Vince Vatter, and Sophie Huczynska for helpful conversations.

References

[1] J. S. Calcut, Single rational arctangent identities for π, *Pi Mu Epsilon J.*, **11** (1999) 1–6.

[2] J. S. Calcut, Gaussian integers and arctangent identities for pi, *Amer. Math. Monthly* to appear 1–20.

[3] J. S. Calcut, Grade school triangles, submitted preprint (2008).

[4] L. Carlitz and J. Thomas, Rational tabulated values of trigonometric functions, *Amer. Math. Monthly* **69** (1962) 789–793.

[5] B. Cha, Chebyshev's bias in function fields, *Compositio Mathematica* to appear.

[6] A. Clark, *Elements of Abstract Algebra*, Dover, New York, 1971, reprinted 1984.

[7] L. Dirichlet, Beweis des Satzes, dafs jede unbegrentze arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält, *Abhandlungen der Königlichen Preussischen Akademie der Wissenschaften zu Berlin* (1837) 45-81; English translation by R. Stephan (2008) arXiv:0808.1408v1.

[8] L. Euler, *Introductio in Analysin Infinitorum, Tomus Primus*, Lausannae, M. M. Bousquet, 1748; English translation by J. D. Blanton, *Introduction to Analysis of the Infinite, Book I*, Springer-Verlag, New York, 1988.

[9] C. F. Gauss, *Werke. Band II*, Königlichen Gesellschaft der Wissenschaften zu Göttingen, Göttingen, 1863.

[10] T. Hungerford, *Algebra*, Springer-Verlag, New York, 1974.

[11] I. Isaacs, Solution of polynomials by real radicals, *Amer. Math. Monthly* **92** (1985) 571–575.

[12] J. S. Milne, Fields and Galois Theory (Version 4.21), *Notes* (2008) available at http://www.jmilne.org/math/.

[13] I. Niven, *Irrational Numbers*, Carus Mathematical Monographs, no. 11, Mathematical Association of America, Washington, DC, 1997; fourth printing, 1956.

[14] J. Olmsted, Rational values of trigonometric functions, *Amer. Math. Monthly* **52** (1945) 507–508.

[15] A. Selberg, An elementary proof of Dirichlet's theorem about primes in an arithmetic progression, *Ann. of Math. (2)* **50** (1949) 297–304.

[16] J. Stillwell, *Mathematics and Its History*, Springer-Verlag, New York, 1989.

[17] B. L. van der Waerden, *Modern Algebra*, Vol. 1, Second Ed., Ungar, New York, 1949.

Department of Mathematics, Michigan State University, East Lansing, MI 48824
jack@math.msu.edu