Rationality and the Tangent Function

J. S. Calcut

1. Introduction

The irrational nature of values of the circular trigonometric functions at rational multiples of pi (angles with rational degree measure) has been well studied [**L1, N, O, U, CT**]. The tangent function takes a secondary role in these treatments. This is unfortunate since, *"...the tan function may be considered more fundamental than either cos or sin"* (Stillwell [**S2**], p. 156). Arguments for this view include: the tangent function is essentially slope, cosine and sine may be expressed in terms of tangent ([**S2**], p. 156), and cotangent admits probably the simplest imaginable sum displaying periodicity:

$$\pi \cot \pi x = \sum_{n \in \mathbb{Z}} \frac{1}{x-n}$$

a formula due to Euler ([**E**], p. 149, see also [**S2**], p. 151).

This paper aims to reveal the geometric and algebraic significance of the irrational nature of the numbers $\tan k\pi/n$. For example, unique factorization of Gaussian integers yields a very natural proof that the only rational values of $\tan k\pi/n$ are 0 and ± 1 (Corollary 1 in Section 2). In all, we give four proofs of this fact. Several applications of this fact appear in Section 2.

The numbers $\tan k\pi/n$, $\cos k\pi/n$ and $\sin k\pi/n$ are algebraic over $\mathbb{Q}$ and the study of their degrees has been popular in the literature. Section 3, included for completeness, determines these degrees in a unified fashion. This implies a result of Niven (Corollary 5) that the only rational values of the circular trigonometric functions at rational multiples of pi are the well known values. Applications to Hilbert's third problem and rational triangles are discussed in Section 4.

A sequence of rational functions are introduced in Section 5 that are the tangent analogues of the Chebyshev polynomials of the first kind. These functions take a pleasant form and enjoy several noteworthy properties: a useful composition law, their numerators 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 parallel those of the roots of unity. Section 5 concludes with Theorem 1, which

determines the degrees of the numbers $\tan k\pi/n$ in an enlightening way. The appearance of certain factors of two in Niven's approach are made transparent.

These results are used in Section 6 to determine the Galois groups of the numbers $\tan k\pi/n$ and factor completely the numerators of the tangent rational functions. Simple applications include the exact values of numbers $\tan k\pi/n$ that are quadratic irrationals and the solution of the $36-54-90$ triangle. Section 6 also discusses the expression of the numbers $\tan k\pi/n$ by real radical, which numbers $\tan k\pi/n$ are algebraic integers, and presents some open problems.

Section 7 proves a technical result (Lemma 6) used in Section 5.

Properties of the circular trigonometric functions used below are rigorously founded on elementary geometry as developed, for example, in Moise's text [**Mo**]. These functions are defined using the notions of slope and arc length on the unit circle C in the Cartesian plane. Their usual domains and so forth may then be deduced. In particular, semicircles in C have arc length π, so tangent has period π and domain $D=\mathbb{R}-\{\pi/2+k\pi \mid k\in\mathbb{Z}\}$. If the real numbers α, β, and $\alpha+\beta$ lie in D, then a direct geometric argument proves the tangent angle addition formula:

$$\tan(\alpha+\beta)=\frac{\tan\alpha+\tan\beta}{1-\tan\alpha\tan\beta}.$$

Throughout, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ denote the ring of integers and the fields of rational, real and complex numbers respectively. The natural numbers $\mathbb{N}$ consist of the positive integers.

2. Gaussian Integers and Tangent

The ring of Gaussian integers $\mathbb{Z}[i]$ is the integer lattice $\{a+bi \mid a,b\in\mathbb{Z}\}$ in $\mathbb{C}$. Unique factorization in $\mathbb{Z}[i]$ refines unique factorization in $\mathbb{Z}$ and yields:

PROPOSITION 1. *Let $z=a+bi$ be a Gaussian integer. There is a natural number n such that $z^n\in\mathbb{Z}$ iff $a=0$, $b=0$ or $a=\pm b$.*

The proof is below. First, recall some basic facts about the Gaussian integers. For a lively introduction to the Gaussian integers, see [**S2**], pp. 227-236. Regard $\mathbb{Z}\subset\mathbb{Z}[i]$ as the Gaussian integers with zero imaginary part. The units in $\mathbb{Z}[i]$ are ±1 and $\pm i$. The norm $N(a+bi)=a^2+b^2$ of a Gaussian integer is multiplicative: $N(wz)=N(w)N(z)$ for all w,z. $\mathbb{Z}[i]$ is a square lattice in $\mathbb{C}$ and this geometry[1] implies the division property: if w and $z\neq0$ are Gaussian integers, then there exist Gaussian integers α and ρ such that $w=\alpha z+\rho$ and $N(\rho)<N(z)$. The division property ensures that the Euclidean algorithm terminates after finitely many steps and produces the GCD of two Gaussian

[1]Stillwell explains clearly the relationship between the square shape of the lattice $\mathbb{Z}[i]$ and unique factorization ([**S2**], pp. 230-232, see also [**S3**], pp. 164-168). He also shows how the lack of unique factorization in the ring $\mathbb{Z}\left[\sqrt{-5}\right]$ follows from the shape of a certain sublattice that forms a nonprincipal ideal ([**S2**], pp. 243-245, see also [**S3**], pp. 173-175). Failure of unique factorization for certain rings is relevant to an old, but important, faulty proof of Fermat's last theorem [**S3**], p. 171.

integers. This implies $\mathbb{Z}[i]$ has unique factorization. Fermat's two squares theorem implies the classification of Gaussian primes. The primes in $\mathbb{Z}[i]$ break into two disjoint classes:

Type 1: unit multiples of ordinary primes $p \equiv 3 \bmod 4$, and

Type 2: unit multiples of $a+bi$ with $N(a+bi)$ an ordinary prime.

Primes $a+bi$ of Type 1 have a or b equal to zero and primes of Type 2 have a and b both nonzero. Clearly, $z = a+bi$ is a Gaussian prime iff its complex conjugate $\overline{z} = a-bi$ is as well. Indeed, $z = uv$ iff $\overline{z} = \overline{u}\,\overline{v}$. Conjugation preserves the type of a Gaussian prime. It is easy to see that $z = a+bi$ and $\overline{z}$ are associates if and only if $a = 0$, $b = 0$, or $a = \pm b$. The following observation is key to the proof of Proposition 1.

LEMMA 1. *Let z be a Gaussian integer and m an ordinary integer such that $z|m$, then $\overline{z}|m$. If, in addition, z is a Type 2 Gaussian prime that is not an associate of $1+i$, then $\overline{z}$ is a prime divisor of m that is not an associate of z.*

PROOF. $z|m$ implies $\overline{z}|\overline{m} = m$ since $m \in \mathbb{Z}$. The rest follows from the preceding paragraph. □

PROOF OF PROPOSITION 1. Only the forward direction requires proof. Let n be a natural number such that $z^n \in \mathbb{Z}$. The Gaussian integer z admits a factorization into primes:

$$z = p_1 p_2 \cdots p_j q_1 q_2 \cdots q_k$$

where the p_i are of Type 1 and the q_i are of Type 2. At the expense of including a unit factor u, assume each $p_i \in \mathbb{Z}$ and collect the associates of $1+i$ into a term $(1+i)^l$ for some nonnegative integer l. After relabeling:

$$z = u p_1 p_2 \cdots p_j q_1 q_2 \cdots q_k (1+i)^l.$$

If $k = 0$, the result follows. Otherwise, $q_k|z^n$ and Lemma 1 implies $\overline{q_k}$ is a prime divisor of z^n that is not an associate of q_k. By unique factorization, $k \geq 2$ and we may relabel (possibly changing the unit u) so that $q_{k-1} = \overline{q_k}$. Noting that $\overline{q_k} q_k$ is an ordinary integer, the Gaussian integer $w = z/(\overline{q_k} q_k)$ has $k-2$ prime factors of Type 2 and $w^n \in \mathbb{Z}$. By induction on k:

$$z = U p_1 p_2 \cdots p_j (\overline{q_2} q_2)(\overline{q_4} q_4) \cdots (\overline{q_k} q_k)(1+i)^l$$

which is the product of a unit, ordinary integers, and a nonnegative integer power of $(1+i)$. The result follows. □

In the following corollaries of Proposition 1, $k \in \mathbb{Z}$ and $n \in \mathbb{N}$.

COROLLARY 1. *The only rational values of $\tan k\pi/n$ are 0 and ± 1.*

PROOF. Suppose $\tan k\pi/n = b/a$ where $b \in \mathbb{Z}$ and $a \in \mathbb{N}$. Then, $\arg(a+bi)^n = n \arg(a+bi) = n(k\pi/n)$, which, modulo 2π, equals 0 or π. Thus, $(a+bi)^n \in \mathbb{Z}$ and Proposition 1 implies $\tan k\pi/n = 0$ or $\tan k\pi/n = \pm 1$. □

Similar reasoning shows that Corollary 1 is equivalent to Proposition 1.

It is common to use the series[2]:

$$\arctan x = x - \frac{x^3}{3} + \frac{x^5}{5} - \frac{x^7}{7} + \frac{x^9}{9} - \cdots$$

with rational arguments to compute decimal digits of π. Of course, one desires $|x|$ to be small for faster convergence.

COROLLARY 2. *Identities of the form* $n \arctan x = k\pi$ *with* $x \in \mathbb{Q}$ *have* $x = 0$ *or* $x = \pm 1$. *In particular,* $\pi = 4 \arctan 1$ *is the most efficient such identity for computing* π.

There exist more efficient identities for π of a similar form, provided one agrees to make two or more arctangent evaluations. For example, Klingenstierna's formula from 1730 (see [**L2**], p. 662 and [**Wr2**], p. 646):

$$\pi = 32 \arctan \frac{1}{10} - 4 \arctan \frac{1}{239} - 16 \arctan \frac{1}{515}.$$

Such identities, called Machin-like formulas in honor of Machin's celebrated identity:

$$\pi = 16 \arctan \frac{1}{5} - 4 \arctan \frac{1}{239}$$

have been extensively studied [**G, St, WW, Wr1, L2, Wr2**]. There is a measure of efficiency of such identities due to Lehmer [**L2**]. Apparently, only Størmer's 1893 work ([**St**], Theorem 5, p. 27) explicitly mentions the nonexistence result in the previous corollary. The author independently obtained this result as an undergraduate [**C**]. Størmer's work uses unique factorization in $\mathbb{Z}[i]$ to produce all such rational arctangent identities for π.

COROLLARY 3. *The acute angles in a right triangle with rational side lengths are never rational multiples of* π.

PROOF. Suppose triangle $\triangle ABC$ has C a right angle, rational side lengths a, b, c opposite angles A, B, C respectively, and angle B is a rational multiple of π. Then $\tan B = b/a$ is rational and equals $+1$ by Corollary 1 since $a, b, c > 0$. The Pythagorean theorem implies $2a^2 = c^2$, a familiar contradiction. □

Stillwell obtains the previous corollary using our tack above [**S3**], pp. 168-169.

We close this section with a seemingly unrelated application. Let X be the space obtained from the unit square $[0,1]^2 \subset \mathbb{R}^2$ by deleting all points with both coordinates rational except $(0,0)$ and $(1,1)$. The Baire category theorem implies the existence of a smooth path in X from $(0,0)$ to $(1,1)$. For an explicit example:

COROLLARY 4. *There is a smooth path in* X *from* $(0,0)$ *to* $(1,1)$.

[2]The Indian mathematician and astronomer Madhava apparently discovered this series in the 14th century. Gergory independently rediscovered it in 1668. It is now a special case of Taylor's infamous 1715 theorem known to all calculus students.

PROOF. Define $\gamma : [0,1] \to [0,1]^2$ by $\gamma(t) = (t, (4/\pi)\arctan t)$. If γ passes through a rational point, then $y = (4/\pi)\arctan t$ is rational for some rational $t \in [0,1]$. This implies $t = \tan y\pi/4$ is rational and $t = 0$ or $t = 1$ by Corollary 1. Therefore, γ is a smooth (in fact, analytic) path in X as desired. □

The reader may enjoy producing more such paths, for example using any transcendental number $\alpha > 0$.

3. Algebraic Degrees

The numbers $\tan k\pi/n$ are usually irrational by Corollary 1. How irrational are these numbers? They are algebraic over $\mathbb{Q}$, as are the corresponding numbers for cosine and sine. In particular, none of the values in the usual trigonometric tables are transcendental. For completeness, we present a proof of the following result.

PROPOSITION 2. *Let $n > 2$ be a natural number and k an integer such that $(k,n) = 1$. In the sine and tangent cases, assume that $n \neq 4$. Then, the algebraic degree over $\mathbb{Q}$ of:*

$$\cos\frac{2k\pi}{n} \text{ is } \varphi(n)/2,$$

$$\sin\frac{2k\pi}{n} \text{ is } \begin{cases} \varphi(n) & \text{if} \quad 4 \nmid n \\ \varphi(n)/2 & \text{if} \quad n \equiv 0 \bmod 8 \\ \varphi(n)/4 & \text{if} \quad n \equiv 4 \bmod 8 \end{cases}, \text{ and}$$

$$\tan\frac{2k\pi}{n} \text{ is } \begin{cases} \varphi(n) & \text{if} \quad 4 \nmid n \\ \varphi(n)/4 & \text{if} \quad n \equiv 0 \bmod 8 \\ \varphi(n)/2 & \text{if} \quad n \equiv 4 \bmod 8 \end{cases}.$$

The remainder of this section is devoted to proving Proposition 2. Recall that the Euler totient function $\varphi(n)$ is by definition the number of integers j such that $1 \leq j \leq n$ and $(j,n) = 1$. In particular, $\varphi(n)$ equals the order of $\mathbb{Z}_n^\times$, the multiplicative group of units in the ring $\mathbb{Z}_n$. The factor of two in the numerator of $2k\pi/n$ relates the pertinent algebraic numbers more directly to nth roots of unity.

The natural approach to Proposition 2 presented here uses basic field theory [**A, H**] and likely was known to Kronecker and Sylvester, although the author knows no reference. The cosine result, a common exercise in algebra texts, and the sine result were proved by Lehmer [**L1**] using symmetric polynomials. The tangent result was proved by Niven [**N**], pp. 38-41, using a somewhat ad hoc extension of the cosine and sine results.

Fix a natural number $n > 2$ and let $\zeta = \exp 2\pi i/n$, a primitive nth root of unity. The splitting field of $x^n - 1 \in \mathbb{Q}[x]$ is the cyclotomic extension $\mathbb{Q}(\zeta)$ of $\mathbb{Q}$. It is well known that this Galois extension has dimension $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$ and its Galois group $Aut_{\mathbb{Q}}\mathbb{Q}(\zeta) = \{\zeta \mapsto \zeta^k | (k,n) = 1\}$, being canonically isomorphic to $\mathbb{Z}_n^\times$, is abelian. Indeed, ζ^k is a primitive nth root of unity if and only if $(k,n) = 1$. The elegant proof of these facts, utilizing unique factorization in $\mathbb{Z}_p[x]$ for primes $p \nmid n$ and exploiting the Frobenius homomorphism, is due to Dedekind (1857) and is often erroneously attributed to Gauss (see Milne's discussion [**M**], pp. 49-51). An automorphism in $Aut_{\mathbb{Q}}\mathbb{Q}(\zeta)$ permutes the roots of

$x^n - 1$ (the nth roots of unity), so such a map is uniquely determined by the congruence class modulo n of an integer k where $\zeta \mapsto \zeta^k$. This automorphism has an inverse $\zeta \mapsto \zeta^j$, which implies $(k,n) = 1$. Therefore, only the maps $\zeta \mapsto \zeta^k$ with $(k,n) = 1$ have a chance of being automorphisms in $Aut_{\mathbb{Q}}\mathbb{Q}(\zeta)$. One interpretation of the fact that $Aut_{\mathbb{Q}}\mathbb{Q}(\zeta) = \left\{\zeta \mapsto \zeta^k \middle| (k,n) = 1\right\}$ is: *the Galois group $Aut_{\mathbb{Q}}\mathbb{Q}(\zeta)$ is as large as possible.* Section 5 ahead shows that this philosophy holds for the tangent numbers as well. This is reminiscent of a Taylor series expansion of an analytic function naturally seeking the largest possible radius of convergence. Note that complex conjugation is a nontrivial automorphism in $Aut_{\mathbb{Q}}\mathbb{Q}(\zeta)$ since $\overline{\zeta} = \zeta^{-1} = \zeta^{n-1}$ and $n > 2$. Also, since $Aut_{\mathbb{Q}}\mathbb{Q}(\zeta)$ is abelian, all of its subgroups are automatically normal.

Let k be an integer such that $(k,n) = 1$. Then:

$$\cos\frac{2k\pi}{n} = \frac{\zeta^k + \zeta^{-k}}{2} \in \mathbb{Q}(\zeta)$$

is algebraic over $\mathbb{Q}$ since $\mathbb{Q}(\zeta)$ is an algebraic extension of $\mathbb{Q}$. Plainly, $\mathbb{Q} \subset \mathbb{Q}\left(\zeta^k + \zeta^{-k}\right) \subset \mathbb{Q}(\zeta)$.

Claim 1. *$\mathbb{Q}\left(\zeta^k + \zeta^{-k}\right)$ is the fixed field of complex conjugation.*

Proof. Let $\sigma \in Aut_{\mathbb{Q}}\mathbb{Q}(\zeta)$ be $\zeta \mapsto \zeta^j$ where $(j,n) = 1$ and $1 \leq j < n$. Clearly, σ fixes $\mathbb{Q}\left(\zeta^k + \zeta^{-k}\right)$ iff $\zeta^{jk} + \zeta^{-jk} = \zeta^k + \zeta^{-k}$. Taking real parts, this is equivalent to $\zeta^{jk} = \zeta^k$ or $\zeta^{jk} = \zeta^{(n-1)k}$, which is equivalent to $j = 1$ or $j = n-1$. □

Thus, $\mathbb{Q}\left(\zeta^k + \zeta^{-k}\right) = \mathbb{Q}\left(\zeta + \zeta^{-1}\right)$ since each is the fixed field of complex conjugation. $\mathbb{Q}\left(\zeta + \zeta^{-1}\right)$ is denoted $\mathbb{Q}^+(\zeta)$ and is called the maximal real subfield of $\mathbb{Q}(\zeta)$. By the fundamental theorem of Galois theory:

$$\left[\mathbb{Q}(\zeta) : \mathbb{Q}^+(\zeta)\right] = \left|Aut_{\mathbb{Q}^+(\zeta)}\mathbb{Q}(\zeta)\right| = 2.$$

Now, $\mathbb{Q}\left(\left(\zeta^k + \zeta^{-k}\right)/2\right) = \mathbb{Q}^+(\zeta)$ and the degree of $\cos 2k\pi/n$ over $\mathbb{Q}$ equals $[\mathbb{Q}^+(\zeta) : \mathbb{Q}]$. As $[\mathbb{Q}(\zeta) : \mathbb{Q}] = [\mathbb{Q}(\zeta) : \mathbb{Q}^+(\zeta)]\,[\mathbb{Q}^+(\zeta) : \mathbb{Q}]$, one has $[\mathbb{Q}^+(\zeta) : \mathbb{Q}] = \varphi(n)/2$, proving the cosine result.

Moving to sine, again let $(k,n) = 1$. Then:

$$\sin\frac{2k\pi}{n} = \frac{\zeta^k - \zeta^{-k}}{2i}.$$

The appearance of i makes this and the tangent case a little more subtle. Nevertheless, $\mathbb{Q}(\zeta, i)$ is an algebraic extension of $\mathbb{Q}$ and $\sin 2k\pi/n \in \mathbb{Q}(\zeta, i)$ is therefore algebraic over $\mathbb{Q}$. Plainly, $\mathbb{Q} \subset \mathbb{Q}\left(\zeta^k - \zeta^{-k}\right) \subset \mathbb{Q}(\zeta)$.

Claim 2. *$\mathbb{Q}\left(\zeta^k - \zeta^{-k}\right)$ is the fixed field of the identity if $4 \nmid n$ and is the fixed field of $\zeta \mapsto -\zeta^{-1}$ if $4|n$.*

Proof. Let $\sigma \in Aut_{\mathbb{Q}}\mathbb{Q}(\zeta)$ be $\zeta \mapsto \zeta^j$ where $1 \leq j < n$. Clearly, σ fixes $\mathbb{Q}\left(\zeta^k - \zeta^{-k}\right)$ iff $\zeta^{jk} - \zeta^{-jk} = \zeta^k - \zeta^{-k}$. Taking imaginary parts, this is equivalent to $\zeta^{jk} = \zeta^k$ (i.e. $j = 1$) or $\zeta^{jk} = -\zeta^{-k}$. The latter implies $-1 = \zeta^{(j+1)k}$, so $n = 2m$ is even and $j = m - 1$ or

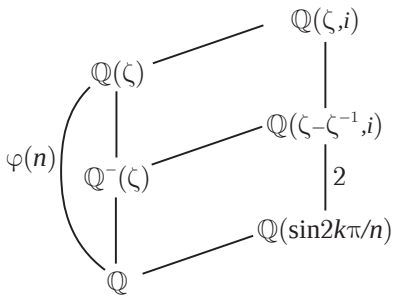

FIGURE 1. Lattice of fields for sine.

$j = n-1$. If $j = n-1$, then σ does not fix $\zeta^k - \zeta^{-k}$. If $j = m-1$, then σ fixes $\zeta^k - \zeta^{-k}$. This σ lies in $Aut_{\mathbb{Q}}\mathbb{Q}(\zeta)$ iff $(m-1, 2m) = 1$, which is equivalent to $4|n$. □

In case $4|n$, the automorphism $\zeta \mapsto -\zeta^{-1}$ is trivial iff $n = 4$. This explains the hypothesis that $n \neq 4$.

Thus, $\mathbb{Q}\left(\zeta^k - \zeta^{-k}\right) = \mathbb{Q}\left(\zeta - \zeta^{-1}\right)$ since each is the fixed field of the same subgroup of $Aut_{\mathbb{Q}}\mathbb{Q}(\zeta)$. $\mathbb{Q}\left(\zeta - \zeta^{-1}\right)$ is denoted $\mathbb{Q}^-(\zeta)$ and is called the maximal imaginary subfield of $\mathbb{Q}(\zeta)$. By the fundamental theorem of Galois theory:

$$\left[\mathbb{Q}(\zeta) : \mathbb{Q}^-(\zeta)\right] = \begin{cases} 1 & \text{if} \quad 4 \nmid n \\ 2 & \text{if} \quad 4|n \end{cases}.$$

Before we complete the proof for sine, we record a few basic facts.

CLAIM 3. *If E is an extension field of $\mathbb{Q}$ containing $\zeta = \exp 2\pi i/n$ and $\omega = \exp 2\pi i/m$, then E contains $\exp 2\pi i/L$ where $L = LCM(n, m)$.*

PROOF. Let $d = (m, n)$ and write $m = da$ and $n = db$. Let x and y be integers such that $xa + yb = 1$. Then, E contains $\zeta^x \omega^y = \exp 2\pi i/L$. □

CLAIM 4. *The primitive roots of unity in $\mathbb{Q}(\zeta)$ are precisely the primitive nth roots if n is even and the primitive $2n$th roots if n is odd. In particular, $i \in \mathbb{Q}(\zeta)$ iff $4|n$.*

PROOF. If $n = 2m+1$, then $\mathbb{Q}(\zeta)$ contains $-\zeta^{m+1} = \exp(2\pi i/(4m+2))$, showing $\mathbb{Q}(\zeta)$ contains the $2n$th roots of unity. For arbitrary n, suppose $\mathbb{Q}(\zeta)$ contains a primitive mth root of unity. Then, $\exp 2\pi i/m \in \mathbb{Q}(\zeta)$ and so $\omega = \exp 2\pi i/L \in \mathbb{Q}(\zeta)$ where $L = LCM(n, m)$ by Claim 3. Hence, $\mathbb{Q}(\zeta) = \mathbb{Q}(\omega)$ and $[\mathbb{Q}(\zeta) : \mathbb{Q}] = [\mathbb{Q}(\omega) : \mathbb{Q}]$, implying $\varphi(n) = \varphi(L)$. This is true iff $L = n$, or n is odd and $L = 2n$. □

CLAIM 5. *$i \in \mathbb{Q}^-(\zeta)$ iff $n \equiv 4 \bmod 8$.*

PROOF. Either condition implies $4|n$ by Claim 4. Thus, $\sigma : \zeta \mapsto -\zeta^{-1} = \zeta^{n/2-1}$ is nontrivial in $Aut_{\mathbb{Q}^-(\zeta)}\mathbb{Q}(\zeta)$ by Claim 2, and $i \in \mathbb{Q}^-(\zeta)$ iff i is fixed by σ. As $\sigma(i) = i^{n/2-1}$, this is equivalent to $n \equiv 4 \bmod 8$. □

The lattice of fields in Figure 1 will complete the proof for sine. Strictly speaking, the node $\mathbb{Q}(\zeta, i)$ is unnecessary, but $\mathbb{Q}(\zeta, i)$ is the natural overfield and its inclusion makes a pretty picture. In each of the three cases $4 \nmid n$, $n \equiv 0 \bmod 8$ and $n \equiv 4 \bmod 8$, one fills in certain degrees in the figure. Claim 2 and its subsequent comments give the degree of the upper left vertical extension. Then, $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$ implies the degree of the lower left vertical extension. Claim 5 gives the degree of the middle diagonal extension. The real field $\mathbb{Q}(\sin 2k\pi/n)$ does not contain i, but adjoining i produces $\mathbb{Q}\left(\zeta - \zeta^{-1}, i\right)$. Hence, the lower right vertical extension is degree two. One now deduces the degree of the bottom diagonal extension and the sine result follows.

Finally, for tangent let $(k, n) = 1$. Then:

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

This number exists iff $n \neq 4$, which explains the hypothesis that $n \neq 4$. As $\tan 2k\pi/n \in \mathbb{Q}(\zeta, i)$, it is algebraic over $\mathbb{Q}$. Define:

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

and note that $\mathbb{Q} \subset F \subset \mathbb{Q}(\zeta)$.

Claim 6. *F is the fixed field of the identity if $4 \nmid n$ and is the fixed field of $\zeta \mapsto -\zeta$ if $4|n$.*

Proof. Let $\sigma \in Aut_{\mathbb{Q}}\mathbb{Q}(\zeta)$ be $\zeta \mapsto \zeta^j$ where $1 \leq j < n$. Clearly, σ fixes F iff σ fixes $\left(\zeta^k - \zeta^{-k}\right) / \left(\zeta^k + \zeta^{-k}\right)$. Equivalently, $\zeta^{2(j-1)k} = 1$. This is equivalent to $n|2(j-1)$ since $(k, n) = 1$, and hence is equivalent to $j = 1$, or $n = 2m$ is even and $j = m + 1$. In the latter case, $\sigma \in Aut_{\mathbb{Q}}\mathbb{Q}(\zeta)$ iff $(m + 1, 2m) = 1$. This is equivalent to $4|n$. □

Thus, $F = \mathbb{Q}\left(\left(\zeta - \zeta^{-1}\right) / \left(\zeta + \zeta^{-1}\right)\right)$ since each is the fixed field of the same subgroup of $Aut_{\mathbb{Q}}\mathbb{Q}(\zeta)$. By the fundamental theorem of Galois theory:

$$[\mathbb{Q}(\zeta) : F] = \begin{cases} 1 & \text{if} \quad 4 \nmid n \\ 2 & \text{if} \quad 4|n \end{cases}.$$

Claim 7. *$i \in F$ iff $n \equiv 0 \bmod 8$.*

Proof. Either condition implies $4|n$ by Claim 4. Thus, $\sigma : \zeta \mapsto -\zeta = \zeta^{n/2+1}$ is nontrivial in $Aut_F\mathbb{Q}(\zeta)$ by Claim 6, and $i \in F$ iff $i = \sigma(i) = i^{n/2+1}$. This is equivalent to $n \equiv 0 \bmod 8$. □

In Figure 1, replace $\mathbb{Q}^-(\zeta)$ with F, $\mathbb{Q}\left(\zeta - \zeta^{-1}, i\right)$ with $F(i)$, and $\mathbb{Q}(\sin 2k\pi/n)$ with $\mathbb{Q}(\tan 2k\pi/n)$. This figure and Claims 6 and 7 imply the tangent result. The proof of Proposition 2 is complete.

4. Applications of Proposition 2

Proposition 2 and inspection of the trivial cases $n \leq 4$ imply:

COROLLARY 5 ([**N**], p. 41). *The only rational values of the circular trigonometric functions at rational multiples of* π *are* 0, $\pm 1/2$ *and* ± 1 *for cosine and sine,* 0 *and* ± 1 *for tangent and cotangent, and* ± 1 *and* ± 2 *for secant and cosecant.*

The tangent part of this corollary provides an alternate proof of Corollary 1 and hence reproves the main results in Section 2. The cosine part is used in the solution of Hilbert's third problem on equidecomposability of polyhedra. The unfamiliar reader will enjoy Stillwell's exposition [**S2**], pp. 159-169.

The rational values of $\cos 2k\pi/n$ with $0 \leq 2k\pi/n < \pi$ are $\cos 0 = 1$, $\cos \pi/3 = 1/2$, $\cos \pi/2 = 0$ and $\cos 2\pi/3 = -1/2$. A triangle is *rational* provided it has rational side lengths and its angles are rational multiples of π.

COROLLARY 6. *If* $\triangle ABC$ *is rational, then it is equilateral.*

PROOF. Each angle of $\triangle ABC$ has rational cosine by the law of cosines, hence has measure $\pi/3$, $\pi/2$ or $2\pi/3$. The angle sum is π and the result follows. □

5. Tangent Rational Functions

For each natural n, define:

$$F_n(x) = \tan(n \arctan x).$$

These functions are the tangent analogues of the Chebyshev polynomials of the first kind for cosine and are rational functions with integer coefficients. They were known to John Bernoulli as early as 1712 [**S1**], pp. 193-195, appear explicitly in Euler's 1748 work [**E**], pp. 217-218, were used in essence in [**CT**], p. 792, and were rediscovered independently by the author [**C**].

Recall that:

$$\begin{aligned} \tan\theta &= \frac{1}{i}\frac{e^{i\theta} - e^{-i\theta}}{e^{i\theta} + e^{-i\theta}} = \frac{1}{i}\frac{e^{2i\theta} - 1}{e^{2i\theta} + 1} \text{ and} \\ \arctan x &= \frac{1}{2i}\ln\frac{1+ix}{1-ix} \end{aligned}$$

using the usual branch cut for arctangent with range $(-\pi/2, \pi/2)$ for real x. Therefore:

$$\begin{aligned} F_n(x) &= \tan\frac{1}{2i}\ln\left(\frac{1+ix}{1-ix}\right)^n \\ &= \frac{\left[(1+ix)^n - (1-ix)^n\right]/2i}{\left[(1+ix)^n - (1-ix)^n\right]/2} \\ &= \frac{p_n(x)}{q_n(x)}. \end{aligned}$$

The last two lines define the integer polynomials:

$$\begin{aligned} p_n(x) &= \operatorname{Im}(1+ix)^n = \sum_{k=0}^{\lfloor (n-1)/2 \rfloor} (-1)^k \binom{n}{2k+1} x^{2k+1} \\ q_n(x) &= \operatorname{Re}(1+ix)^n = \sum_{k=0}^{\lfloor n/2 \rfloor} (-1)^k \binom{n}{2k} x^{2k}. \end{aligned}$$

For example:

$$F_1(x) = \frac{x}{1}, \qquad F_2(x) = \frac{2x}{1-x^2}, \qquad F_3(x) = \frac{3x-x^3}{1-3x^2},$$

$$F_4(x) = \frac{4x-4x^3}{1-6x^2+x^4}, \qquad F_5(x) = \frac{5x-10x^3+x^5}{1-10x^2+5x^4}.$$

REMARK 1. *The Chebyshev polynomials of the first kind* $T_n(x) = \cos(n \arccos x)$ *are integer polynomials, while the analogous functions* $\sin(n \arcsin x)$ *for sine are not in general polynomials or rational functions. Indeed,* $\sin(2 \arcsin x) = 2x\sqrt{1-x^2}$ *is not a rational function on any open interval. The coefficient pattern for* $F_n(x)$ *is particularly simple.*

It follows that $p_n(x)$ has roots $r_k = \tan k\pi/n$, where $k = 0, 1, \ldots, n-1$ if n is odd and further $k \neq n/2$ if n is even. 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. So, 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. Clearly, $r_k = \tan k\pi/n$ exists iff k/n is not of the form $(2j+1)/2$ for integral j. If r_k exists, then it is algebraic over $\mathbb{Q}$ of degree at most n since it is a root of $p_n(x)$. The roots r_k are the slopes of the lines through the origin and the $2n$th roots of unity. This naturally organizes the roots r_k in a counterclockwise manner. Subscripts of the r_k are read modulo n, since tangent has period π. If $4|n$, then $r_{n/4} = 1$ and $r_{3n/4} = -1$.

REMARK 2. *As in* [**C**]*, one may show* $F_n(x) = p_n(x)/q_n(x)$ *by induction using the tangent angle addition formula and the recursions:*

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

The following composition law, employed below for real arguments x, is quite useful.

LEMMA 2. *If* n *and* m *are natural numbers, then* $F_{nm}(x) = F_n \circ F_m(x)$*, except when* $F_m(x)$ *does not exist and* n *is even, in which case* $F_{nm}(x) = 0$ *and* $F_n \circ F_m(x)$ *is undefined.*

PROOF. If $F_m(x)$ exists, then:

$$\begin{aligned} F_n \circ F_m(x) &= \tan(n \arctan(\tan m \arctan x)) \\ &= \tan(nm \arctan x) \\ &= F_{nm}(x). \end{aligned}$$

Otherwise, $q_m(x) = 0$, $m \arctan x = \pi/2 + k\pi$ for some integer k, and:

$$F_{nm}(x) = \tan(nm \arctan x) = \tan(n\pi/2)$$

which vanishes for n even and is undefined for n odd. □

This composition law facilitates our third proof of Corollary 1 (compare [**C**]). The following implies Corollary 1 since the numbers $\tan k\pi/n$ are roots of $p_n(x)$.

COROLLARY 7. *For natural n, the possible rational roots of $p_n(x)$ are $x = 0$ and $x = \pm 1$.*

PROOF. The result is clear if $n \leq 2$. Write $n = s_1 s_2 \cdots s_j$, 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 $x = \pm 1$.

Base Case: let $j = 1$. 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 $x = \pm n$. If $x = \pm n$ is a root, then the form of the polynomial $p_n(x)$ quickly implies the contradiction $n|1$. Similar reasoning proves the base case for $q_n(x)$.

Inductive Step: let $j > 1$. Suppose $p_n(x) = 0$ with x rational. Then, $F_n(x) = 0$ and by the composition law (Lemma 2) 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. □

For fixed natural n, the rational functions F_i act nicely on the r_j.

LEMMA 3. *If i is natural and j is an integer, then $F_i(r_j) = r_{ij}$.*

PROOF. If n is even and $j \equiv n/2 \bmod n$ or $ij \equiv n/2 \bmod n$, then $F_i(r_j)$ and r_{ij} are both undefined. Otherwise, without loss assume that $0 \leq j < n$. Then, $F_j(r_1) = r_j$ and $F_i(r_j) = F_i(F_j(r_1)) = F_{ij}(r_1) = r_{ij}$ by the composition law (Lemma 2). □

For the moment, fix a natural number $n > 2$ (so r_1 exists) and an integer k such that $r_k = \tan k\pi/n$ exists. Let $\psi(x)$ denote a minimal polynomial of r_k over $\mathbb{Q}$, which is irreducible, separable and divides $p_n(x)$ in $\mathbb{Q}[x]$ since $p_n(r_k) = 0$. Notice that $r_k = F_k(r_1) \in \mathbb{Q}(r_1)$ since F_k is a quotient of integer polynomials and $q_k(r_1) \neq 0$. Therefore, $\mathbb{Q}(r_k) \subset \mathbb{Q}(r_1)$. Assume further that $(k, n) = 1$. Choose integers $a > 0$ and b such that $ak + bn = 1$. Then, $ak \equiv 1 \bmod n$ and $F_a(r_k) = r_1$. Hence, $r_1 \in \mathbb{Q}(r_k)$ and $\mathbb{Q}(r_k) = \mathbb{Q}(r_1)$. In particular, $[\mathbb{Q}(r_k) : \mathbb{Q}] = [\mathbb{Q}(r_1) : \mathbb{Q}]$. It follows that all r_j lie in $\mathbb{Q}(r_k)$, and $\mathbb{Q}(r_k)$ is

the splitting field of $\psi(x)$. The extension $\mathbb{Q}(r_k)$ of $\mathbb{Q}$ is therefore Galois and has dimension $d = \deg \psi(x) \leq n$.

Still assuming $(k,n) = 1$, an automorphism $\sigma \in Aut_{\mathbb{Q}}\mathbb{Q}(r_k)$ permutes the roots of $\psi(x)$. These roots are a subset of the roots of $p_n(x)$, so $\sigma(r_1) = r_m$ for some integer m. Now, $\mathbb{Q}(r_k) = \mathbb{Q}(r_1)$ has a basis $1, r_1, r_1^2, \ldots r_1^{d-1}$ over $\mathbb{Q}$. Therefore, σ is completely determined by the congruence class of m modulo n. Without loss, assume $m > 0$. Since $\sigma(r_1) = r_m = F_m(r_1)$, we say that σ is induced by F_m. Notice that σ commutes with each F_i since σ is a field automorphism fixing $\mathbb{Q}$ and F_i is a rational function with integer coefficients. By Lemma 3, σ acts by multiplication by m on the subscripts of each r_j:

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

It follows that the Galois group $Aut_{\mathbb{Q}}\mathbb{Q}(r_k)$ is abelian. The inverse of σ is induced by, say, F_l. Hence, $r_{lm} = r_1$ and $(m,n) = 1$. This is the first obvious restriction on m so that F_m induces an automorphism in $Aut_{\mathbb{Q}}\mathbb{Q}(r_k)$, and parallels the same fact for nth roots of unity. The other obvious restriction here is if $4|n$, then $r_{n/4} = 1$ and σ must fix $r_{n/4}$.

LEMMA 4. *If $n > 2$ is natural and $(k,n) = 1$, then each $\sigma \in Aut_{\mathbb{Q}}\mathbb{Q}(r_k)$ is induced by some F_m where $(m,n) = 1$. Further, if $4|n$, then $m \equiv 1 \bmod 4$.*

PROOF. The first part was shown above. If $4|n$, then σ preserves $1 = r_{n/4}$. Thus, $mn/4 \equiv n/4 \bmod n$ which implies $m \equiv 1 \bmod 4$. □

These turn out to be all of the restrictions! Later, the number of m allowed by Lemma 4 will be needed.

LEMMA 5. *If $4|n$, then $\varphi(n)/2$ natural numbers m satisfy: $m < n$, $(m,n) = 1$ and $m \equiv 1 \bmod 4$.*

PROOF. The $\varphi(n)$ naturals $m < n$ with $(m,n) = 1$ break into $A_1 = \{m \equiv 1 \bmod 4\}$ and $A_3 = \{m \equiv 3 \bmod 4\}$. The map $m \mapsto -m \bmod n$ is a bijection $A_1 \to A_3$. □

Showing the restrictions in Lemma 4 are sufficient parallels the argument for nth roots of unity, but is more subtle. A technical result is needed.

LEMMA 6. *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 6 is proved in Section 7. The energetic reader may take the proof as a fun exercise.

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

LEMMA 7. *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. The discriminant of $p_n(x)$ equals the resultant of $p_n(x)$ and its formal derivative, up to a constant that is a power of the leading coefficient of $p_n(x)$ [**W**], pp. 82-88. The resultant is the determinant of a certain matrix whose entries are zero and the coefficients of $p_n(x)$ and $p_n'(x)$. The discriminant of $\overline{p_n(x)}$ is computed in the same way. Therefore, the discriminant of $\overline{p_n(x)}$ equals $\Delta_n \bmod p$, which does not vanish since $p \neq 2$ and $(p,n)=1$. This implies $\overline{p_n(x)}$ has no multiple roots. □

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 8. *Let $n>2$ be natural and $p>2$ prime such that $(p,n)=1$ and $p \equiv 1 \bmod 4$. Then, r_p is a root of the minimal polynomial of r_1 over $\mathbb{Q}$.*

PROOF. The assumption that $n>1$ simply ensures that $r_1 = \tan \pi/n$ exists. Let $h(x) \in \mathbb{Q}[x]$ be a minimal polynomial of r_1 over $\mathbb{Q}$, which divides $p_n(x)$ in $\mathbb{Q}[x]$ since $p_n(r_1)=0$. By Gauss' lemma, one may assume $h(x) \in \mathbb{Z}[x]$ is primitive and $p_n(x) = f(x)h(x)$ for $f(x) \in \mathbb{Z}[x]$. The roots of $p_n(x)$ are distinct, so suppose by way of contradiction that $f(r_p)=0$. By Lemma 3, $f(F_p(r_1))=0$ where $q_p(r_1) \neq 0$ since $(p,n)=1$. Let $d = \deg f$ and $g(x) \in \mathbb{Z}[x]$ be the polynomial obtained by clearing denominators in:

$$q_p(x)^d f(F_p(x)).$$

Note that $g(r_1)=0$. Thus, the minimal polynomial $h(x)$ of r_1 divides $g(x)$ in $\mathbb{Q}[x]$. As $h(x)$ is primitive, $h(x)$ divides $g(x)$ in $\mathbb{Z}[x]$. Write $k(x)h(x) = g(x)$ for $k(x) \in \mathbb{Z}[x]$. Project to $\mathbb{Z}_p[x]$, where $\overline{q_p(x)} = \overline{1}$ since $p \left| \binom{p}{j} \right.$ as p is prime. Also, $\overline{p_p(x)} = \overline{x^p}$ since $p \equiv 1 \bmod 4$ (this is a key point; if $p \equiv 3 \bmod 4$, then $\overline{p_p(x)} = \overline{-x^p}$ and the proof unravels). Recall Fermat's little theorem and exploit the Frobenius homomorphism to obtain:

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

Note that $\overline{h(x)}$ has positive degree, since $h(r_1)=0$ implies $\deg h(x) > 0$, $h(x) | p_n(x)$ in $\mathbb{Z}[x]$, $p_n(x)$ has highest power term $\pm x^n$ or $\pm n x^{n-1}$, and $(p,n)=1$. 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 7. □

The following produces primes p with desired properties.

LEMMA 9. *Let n and k be coprime naturals. If $4|n$, assume further that $k \equiv 1 \bmod 4$. Then, there exists a prime $p>2$ such that $(p,n)=1$, $p \equiv k \bmod n$ and $p \equiv 1 \bmod 4$.*

PROOF. First, assume $4|n$, so $k \equiv 1 \bmod 4$. Look at the arithmetic progression $4na+k$ where a varies over $\mathbb{N}$. Notice that $(k,4n)=1$. By Dirichlet's theorem [**D, S**], there exist infinitely many primes in this progression. Let $p>2$ be any such prime that is coprime to n (e.g. choose $p > \max\{2,n\}$). The prime p behaves as desired.

Next, assume $n = 4m+2$. Case 1. $k \equiv 1 \bmod 4$. The previous argument proves this case. Case 2. $k \equiv 3 \bmod 4$. Let $K = k+n$, which satisfies $(K,n)=1$ and $K \equiv 1 \bmod 4$. Thus, Case 1 applied to K gives a prime $p>2$ such that $(p,n)=1$, $p \equiv K \equiv k \bmod n$ and $p \equiv 1 \bmod 4$, proving Case 2.

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

COROLLARY 8. *Let $n>2$ be natural and $h(x)$ 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 $4|n$, $k \equiv 1 \bmod 4$.*

PROOF. Without loss, assume $k>0$. Lemma 9 gives a prime $p>2$ such that $(p,n)=1$, $p \equiv k \bmod n$ and $p \equiv 1 \bmod 4$. Lemma 8 implies $r_p = r_k$ is a root of $h(x)$. □

We have obtained:

THEOREM 1. *If $n>2$ is natural and k is an integer such that $(k,n)=1$, then the degree of $\tan k\pi/n$ over $\mathbb{Q}$ is $\varphi(n)$ if $4 \nmid n$ and $\varphi(n)/2$ if $4|n$.*

PROOF. The degree of $\tan k\pi/n$ over $\mathbb{Q}$ is $[\mathbb{Q}(r_k):\mathbb{Q}] = [\mathbb{Q}(r_1):\mathbb{Q}]$ since $\mathbb{Q}(r_k) = \mathbb{Q}(r_1)$. Upper bounds for $[\mathbb{Q}(r_1):\mathbb{Q}]$ are given by Lemmas 4 and 5, namely $\varphi(n)$ if $4 \nmid n$ and $\varphi(n)/2$ if $4|n$. These are also lower bounds by Corollary 8 and Lemma 5. □

Theorem 1 is true as stated for $n=1$. If $n=2$, the hypothesis should be that $\tan k\pi/n$ exists (i.e. k is even), and then the conclusion is true.

Theorem 1 reproves the tangent result in Proposition 2. The reader may verify the results are indeed the same. Theorem 1 provides our fourth proof of Corollary 1. The factor of two when $4|n$ is simply due to the fact that $r_{n/4}=1$, thus explaining Niven's factors of two [**N**], p. 39. The cognoscenti will note that the sufficiency of the restrictions listed in Lemma 4, proved here using Dirichlet's theorem, also follows from the degrees of the tangent numbers in Proposition 2. In particular, the use of Dirichlet's theorem may be avoided. The present argument, however, reveals deeper algebraic parallels between the tangent numbers and roots of unity.

6. Applications of Section 5

The results in the previous section allow us to determine the Galois groups of the extensions $\mathbb{Q}(r_k)$ over $\mathbb{Q}$ and split $p_n(x)$ into irreducibles in $\mathbb{Q}[x]$. Other applications and some open problems follow. Recall that $\mathbb{Z}_n^\times$ is the multiplicative group of units in $\mathbb{Z}_n$. If $4|n$, then let H denote the index two subgroup $\{j|\,(j,n)=1, j \equiv 1 \bmod 4\}$ of $\mathbb{Z}_n^\times$ (see Lemma 5).

COROLLARY 9. *Let $n>2$ be natural and k an integer such that $(k,n)=1$. Then, the Galois group $Aut_{\mathbb{Q}}\mathbb{Q}(r_k)$ is naturally isomorphic to $\mathbb{Z}_n^\times$ if $4 \nmid n$ and to H if $4|n$.*

PROOF. As $\mathbb{Q}(r_k) = \mathbb{Q}(r_1)$, we may assume $k=1$. Each $\sigma \in Aut_{\mathbb{Q}}\mathbb{Q}(r_1)$ is induced by some F_m where m is unique modulo n and $(m,n)=1$; define $\mu : Aut_{\mathbb{Q}}\mathbb{Q}(r_1) \to \mathbb{Z}_n^\times$ by $\sigma \mapsto m \bmod n$. It is easy to see that μ is a group homomorphism. Let $h(x)$ be a minimal polynomial of r_1 over $\mathbb{Q}$. The roots of $h(x)$ were determined in Corollary 8 and Theorem 1, and $Aut_{\mathbb{Q}}\mathbb{Q}(r_1)$ permutes these roots transitively. Therefore, μ maps onto $\mathbb{Z}_n^\times$ if $4 \nmid n$

and onto H if $4|n$. $Aut_{\mathbb{Q}}\mathbb{Q}(r_1)$ has the same cardinality as its image under μ, so μ is an isomorphism onto its image. □

COROLLARY 10. *Let $n > 2$ be natural and k an integer such that $r_k = \tan k\pi/n$ exists. The roots of a minimal polynomial of r_k over $\mathbb{Q}$ are precisely the numbers r_{jk} where j is any integer such that $(j, n) = 1$ and, in case $4|n$, $j \equiv 1 \bmod 4$.*

PROOF. Note that we are not assuming $(k, n) = 1$. Let $\psi(x)$ be a minimal polynomial of r_k over $\mathbb{Q}$. Clearly, $\mathbb{Q}(r_k) \subset \mathbb{Q}(r_1)$. $\mathbb{Q}(r_k)$ is the splitting field of $\psi(x)$ over $\mathbb{Q}$, so $\mathbb{Q}(r_k)$ is Galois (and stable) over $\mathbb{Q}$. Thus, any $\sigma \in Aut_{\mathbb{Q}}\mathbb{Q}(r_1)$ maps $\mathbb{Q}(r_k)$ into itself and permutes the roots of $\psi(x)$. Hence, the numbers in the statement of the corollary are indeed roots of $\psi(x)$. The converse follows similarly, since $Aut_{\mathbb{Q}}\mathbb{Q}(r_k)$ permutes the roots of $\psi(x)$ transitively and any $\tau \in Aut_{\mathbb{Q}}\mathbb{Q}(r_k)$ extends to some $\sigma \in Aut_{\mathbb{Q}}\mathbb{Q}(r_1)$. □

Notice that if $4 \nmid n$ and $2 \neq d|n$, then $r_{n/d}$ and $r_{-n/d}$ are roots of the same minimal polynomial by Corollary 10, since $(n-1)\, n/d \equiv -n/d \bmod n$ and $(n-1, n) = 1$. If $4|n$, then this is not always true.

COROLLARY 11. *Let $n > 2$ be natural. Suppose $4|d$ and $d|n$. Then, $r_{n/d}$ and $r_{-n/d}$ are not roots of the same minimal polynomial over $\mathbb{Q}$.*

PROOF. Otherwise, there is an integer j such that $j \equiv 1 \bmod 4$ and $jn/d \equiv -n/d \bmod n$ by Corollary 10. Then, $d|j+1$ and $j \equiv 3 \bmod 4$, a contradiction. □

The factorization of $p_n(x)$ over $\mathbb{Q}$ is now straightforward. The irreducible factors of $p_n(x)$ roughly correspond to divisors of n. The factorization is simplest for odd n.

Fix $n > 2$ odd. Let d be a positive divisor of n. Define:

$$\psi_d(x) = \prod (x - r_{jn/d}) \tag{6.1}$$

where the product is over distinct values $jn/d \bmod n$ for integers j such that $(j, n) = 1$.

COROLLARY 12. *$\psi_d(x) \in \mathbb{Q}[x]$ is irreducible and has degree $\varphi(d)$.*

PROOF. The coefficients of $\psi_d(x)$ are symmetric polynomials in the roots $r_{jn/d}$. Every $\sigma \in Aut_{\mathbb{Q}}\mathbb{Q}(r_1)$ permutes these $r_{jn/d}$ by Corollary 10, and therefore fixes the coefficients of $\psi_d(x)$. The fixed field of $Aut_{\mathbb{Q}}\mathbb{Q}(r_1)$ is $\mathbb{Q}$, and so $\psi_d(x) \in \mathbb{Q}[x]$. The degree of $r_{n/d} = \tan \pi/d$ is $\varphi(d)$ by Theorem 1. The number of terms in the product 6.1 equals the number of roots of a minimal polynomial of $r_{n/d}$ by Corollary 10, which equals $\deg r_{n/d} = \varphi(d)$. Thus, $\psi_d(x)$ is irreducible. □

In particular, $\psi_d(x)$ is a monic minimal polynomial of $r_{n/d}$ over $\mathbb{Q}$. Note that $d = 1$ corresponds to the factor $\psi_1(x) = x$ of $p_n(x)$.

LEMMA 10. *$\psi_d(x)$ and $\psi_e(x)$ have a common root iff $d = e$.*

PROOF. If they share a common root, then they have identical roots and $r_{n/e}$ is a root of $\psi_d(x)$. Corollary 10 implies there is an integer j such that $(j, n) = 1$ and $jn/d \equiv n/e \bmod n$. This implies $j/d - 1/e \in \mathbb{Z}$ and $je/d \in \mathbb{Z}$. As $d|n$ and $(j, n) = 1$, we get $d|e$. By symmetry, $e|d$ and $d = e$. □

The product:

$$\prod_{d|n} \psi_d(x) \in \mathbb{Q}[x] \tag{6.2}$$

has degree $\sum_{d|n} \varphi(d) = n = \deg p_n(x)$ since n is odd, and has the same roots as $p_n(x)$. The leading coefficient of $p_n(x)$ is ± 1. Therefore, 6.2 equals $\pm p_n(x) \in \mathbb{Z}[x]$ and 6.2 is the factorization of $\pm p_n(x)$ into monic irreducibles in $\mathbb{Q}[x]$ (in fact, in $\mathbb{Z}[x]$ by Gauss' lemma).

The previous discussion applies to the case $(n, 4) = 2$ with minor changes. In this case, $r_{n/2}$ does not exist. The product:

$$\prod_{d|n, d\neq 2} \psi_d(x) \in \mathbb{Q}[x] \tag{6.3}$$

has degree $\sum_{d|n,d\neq 2} \varphi(n) = n - 1 = \deg p_n(x)$ since n is even, and has the same roots as $p_n(x)$. The leading coefficient of $p_n(x)$ is $\pm n$. Therefore, 6.3 equals $\pm p_n(x)/n \in \mathbb{Q}[x]$ and 6.3 is the factorization of $\pm p_n(x)/n$ into monic irreducibles in $\mathbb{Q}[x]$.

Finally, assume $4|n$. Again, $r_{n/2}$ does not exist. Further, if $4|d$, then $r_{n/d}$ and $r_{-n/d}$ each have degree $\varphi(d)/2$ by Theorem 1, and are not roots of the same minimal polynomial by Corollary 11. Therefore, $\psi_d(x)$ splits into two irreducible polynomials in $\mathbb{Q}[x]$, namely $\prod (x - r_{jn/d})$ and $\prod (x - r_{-jn/d})$ where the products are over the same values as 6.1 except $j \equiv 1 \bmod 4$. It is easy to sum the degrees and see that again we have split the monic polynomial $\pm p_n(x)/n$ into monic irreducibles in $\mathbb{Q}[x]$.

It is important to note that the above method for obtaining the desired irreducible polynomials is both constructive and proved to be valid. In practice, it is convenient to factor the polynomials $p_n(x)$ (that have a very simple form) using a computer algebra system such as MAGMA, and then pick out by inspection the desired irreducible factor.

One may use these minimal polynomials to compute exactly some of the values $r_k = \tan k\pi/n$. As an example, we determine all of the numbers $\tan k\pi/n$ with degree two or less over $\mathbb{Q}$. Tangent has period π, so assume $(k, n) = 1$ and $0 \leq k\pi/n < \pi$. Using Theorem 1, we find the values of n corresponding to degrees one and two, namely $n = 1, 4$ and $n = 3, 6, 8, 12$ respectively. The rational values (degree one) are $\tan 0 = 0$, $\tan \pi/4 = 1$ and $\tan 3\pi/4 = -1$. For degree two, the pertinent values of k and corresponding minimal polynomials are:

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

Therefore, the quadratic irrational values are precisely:

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

This complete list has recently been used by B. Cha to give a nontrivial example where the Grand Simplicity Hypothesis for function fields may be verified [**Cha**], p. 16.

The number $\tan \pi/5$ has minimal polynomial x^4-10x^2+5, and so $\tan \pi/5 = \sqrt{5-2\sqrt{5}}$. In particular, we get the $36-54-90$ right triangle with opposite side lengths $\sqrt{5-2\sqrt{5}}$, 1 and $\sqrt{6-2\sqrt{5}}$. We do not advocate having students memorize this triangle in an elementary geometry course. It could, however, provide a useful example and an open ended challenge for curious students.

The Galois groups $Aut_{\mathbb{Q}}\mathbb{Q}\left(\tan k\pi/n\right)$ are all abelian (Corollary 9) and hence are solvable. Thus, the numbers $\tan k\pi/n$ may all be expressed by radicals. These numbers are real, so one may expect expressions by real radicals. Such expressions are rarely possible. If an irreducible polynomial $f\left(x\right) \in \mathbb{Q}\left[x\right]$ has all real roots and any root can be constructed from $\mathbb{Q}$ by a combination of field operations and real mth roots, then $\deg f$ is a power of 2 and the Galois group of $f\left(x\right)$ over $\mathbb{Q}$ is a 2-group [**I**]. If $n=7$, then $\deg \tan \pi/7 = \varphi\left(7\right) = 6$ and $\tan \pi/7$ is not expressible by real radicals. One may ask which numbers $\tan k\pi/n$ admit expressions by real radicals. This question is related to compass and straightedge constructions. Investigation is left to the reader.

Niven pointed out that $2\tan k\pi/n$ is not always an algebraic integer and mentioned $2\tan \pi/6$ [**N**], 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:

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

Therefore, $2\tan \pi/50$ is not an algebraic integer either (one easily obtains the minimal polynomial of 2α from that of α; note that 2α is not algebraic integer is a stronger statement than α is not an algebraic integer). As a doable challenge for the reader, we ask whether $\tan \pi/n$ is an algebraic integer iff n is not of the form $2p^k$ where p is an odd prime and k is a natural number. Note that above, $50 = 2 \cdot 5^2$.

We close this section with some open questions. Notice that:

$$\begin{aligned} F_{2n}\left(x\right) &= F_2\left(F_n\left(x\right)\right) = \frac{2p_n\left(x\right)/q_n\left(x\right)}{1-\left(p_n\left(x\right)/q_n\left(x\right)\right)^2} \\ &= \frac{2p_n\left(x\right)q_n\left(x\right)}{\left(q_n\left(x\right)-p_n\left(x\right)\right)\left(q_n\left(x\right)+p_n\left(x\right)\right)} \end{aligned}$$

and so:

$$\begin{aligned} p_{2n}(x) &= 2p_n(x)\,q_n(x) \\ q_{2n}(x) &= [q_n(x)-p_n(x)]\,[q_n(x)+p_n(x)] \\ p_{4n}(x) &= 2p_{2n}(x)\,[q_n(x)-p_n(x)]\,[q_n(x)+p_n(x)]\,. \end{aligned}$$

Examples of the polynomials in square brackets are:

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

These are examples of *signed binomial polynomials*, since they are obtained from $(1+x)^m$ by changing some signs. The sign patterns are $+--++--\cdots$ and $++--++\cdots$ respectively. If $n=2^j$, then $\deg(q_n(x)\pm p_n(x))=2^j$ and $\deg\tan\pi/4n=2^j$ by Theorem 1. Hence, these examples are irreducible over $\mathbb{Q}$. The usual irreducibility criteria do not seem to apply to $q_n(x)\pm p_n(x)$. Only the geometric significance of the numbers $\tan k\pi/n$ allowed us to conclude that the polynomials in these two families are irreducible. A similar phenomenon occurs with the cyclotomic polynomials. One is left wanting general irreducibility criteria that take the signs of the coefficients into account. A natural question is: *given $m>0$, which signed binomial polynomials are irreducible?*

For natural m, define $R(m)$ to be the number of monic signed binomial polynomials of degree m that are reducible in $\mathbb{Q}[x]$. Clearly, $R(m)\geq 2$ if $m>1$ by taking all $+$ and strictly alternating signs. Using MAGMA, one finds:

m	1	3	5	7	9	11	13	15	17	19	21	23	25	27
$R(m)$	0	4	8	16	32	64	144	256	512	1024	2048	4096	8192	16384

m	2	4	6	8	10	12	14	16	18	20	22	24	26	28
$R(m)$	2	2	6	6	4	4	16	2	6	8	4	52	8	4

This suggests that $R(m)/2^m$ tends to zero quickly and most signed binomial polynomials are irreducible. Does $R(m)$ tend to infinity as m tends to infinity? The experimentalist may seek an odd anomaly greater than 13.

CONJECTURE 1. *For all but finitely many odd natural numbers m, $R(m)=2^{(m+1)/2}$.*

For even m, we leave the reader to speculate.

7. The Discriminant of $p_n(x)$

This section proves Lemma 6 from Section 5. Fix $n\in\mathbb{N}$ and $\zeta=\exp\pi i/n$, a primitive $2n$th root of unity. If $z\in\mathbb{C}$, then let $|z|=(z\overline{z})^{1/2}$ denote the modulus of z. We have:

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

Evaluating the latter at $x = 1$ gives:

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

Taking the modulus gives:

$$n = \left| \prod_{k=1}^{n-1} \left(\zeta^{-k} - \zeta^{k}\right) \right|. \tag{7.1}$$

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 $p_n(x)$:

$$\left| \prod_{\substack{k=1 \\ k \neq n/2}}^{n-1} r_k \right| = \left| \prod_{\substack{k=1 \\ k \neq n/2}}^{n-1} \frac{\zeta^k - \zeta^{-k}}{\zeta^k + \zeta^{-k}} \right| = \left| \prod_{\substack{k=1 \\ k \neq n/2}}^{n-1} \frac{\zeta^{-k} - \zeta^{k}}{\zeta^{-k} + \zeta^{k}} \right|. \tag{7.2}$$

This equals the modulus 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 former value is n and the latter value is 1. Combining these values with equations 7.1 and 7.2, and noting that $\left|\zeta^{-n/2} - \zeta^{n/2}\right| = 2$, one obtains:

$$\left| \prod_{\substack{k=1 \\ k \neq n/2}}^{n-1} \left(\zeta^{-k} + \zeta^{k}\right) \right| = \begin{cases} 1 & \text{if} \quad n \text{ is odd} \\ \frac{n}{2} & \text{if} \quad n \text{ is even} \end{cases}. \tag{7.3}$$

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

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

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:

$$\begin{aligned}
\delta_n &= \prod_{0\leq k<l\leq n-1} |r_k - r_l|^2 \\
&= \prod_{0\leq k<l\leq n-1} \left| \frac{2}{i} \frac{\zeta^{k-l} - \zeta^{l-k}}{\left(\zeta^k + \zeta^{-k}\right)\left(\zeta^l + \zeta^{-l}\right)} \right|^2 \\
&= 2^{(n-1)(n-2)} \frac{\left| \prod_{k=1}^{n-1} \left(\zeta^{-k} - \zeta^k\right)^{2(n-k)} \right|}{\left| \prod_{k=1}^{n-1} \left(\zeta^k + \zeta^{-k}\right) \right|^{2n-2}} \qquad (7.4) \\
&= 2^{(n-1)(n-2)} \left| \prod_{k=1}^{n-1} \left(\zeta^{-k} - \zeta^k\right)^n \right| \qquad (7.5) \\
&= 2^{(n-1)(n-2)} n^n. \qquad (7.6)
\end{aligned}$$

Equation 7.4 combined the obvious $n(n-1)$ factors of two 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 7.5 collected some equal terms in the numerator (e.g. $\zeta^{-(n-k)} - \zeta^{n-k} = \zeta^{-k} - \zeta^k$) and noted that the denominator in 7.4 equals one by 7.3. Equation 7.6 used 7.1. If n is even, then:

$$\begin{aligned}
\delta_n &= \prod_{\substack{0\leq k<l\leq n-1 \\ k,l\neq n/2}} (r_k - r_l)^2 \\
&= \prod_{\substack{0\leq k<l\leq n-1 \\ k,l\neq n/2}} \left| \frac{2}{i} \frac{\zeta^{k-l} - \zeta^{l-k}}{\left(\zeta^k + \zeta^{-k}\right)\left(\zeta^l + \zeta^{-l}\right)} \right|^2 \\
&= 2^{(n-1)(n-2)} \frac{\left| \prod_{k=1}^{n-1} \left(\zeta^{-k} - \zeta^k\right) \right|^{n-2}}{\left| \prod_{\substack{k=0 \\ k\neq n/2}}^{n-1} \left(\zeta^{-k} + \zeta^k\right) \right|^{2n-4}} \qquad (7.7) \\
&= 2^{(n-1)(n-2)} \frac{n^{n-2}}{2^{2n-4}\left(n/2\right)^{2n-4}} \qquad (7.8) \\
&= 2^{(n-1)(n-2)} n^{2-n}.
\end{aligned}$$

Equation 7.7 was obtained in a similar way as 7.4 and 7.5. Equation 7.8 used 7.1 in the numerator, and collected factors of two and used 7.3 in the denominator.

Summarizing, we have:

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

To obtain the discriminant Δ_n of $p_n(x)$ from δ_n, one multiplies δ_n by the leading coefficient of $p_n(x)$ raised to the power $2 \deg p_n(x) - 2$ (see [**W**], 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:

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

This completes the proof of Lemma 6.

References

[A] Artin, E., *Galois Theory*, edited and supplemented by A. Milgram, Dover, New York, 1998.

[C] Calcut, J., *Single rational arctangent identities for* π, Pi Mu Epsilon J., Vol. 11, No. 1, Fall 1999, 1-6.

[CT] Carlitz, L. and Thomas, J., *Rational tabulated values of trigonometric functions*, Amer. Math. Monthly **69**, October 1962, 789-793.

[Cha] Cha, B., *Chebyshev's bias in function fields*, preprint, 2006.

[D] Dirichlet, L., *Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen erhält*, 1837.

[E] Euler, L., *Introduction to Analysis of the Infinite*, Book I (English translation of 1748 original), Springer-Verlag, 1988.

[G] Gauss, C. F., *Werke*, (Göttingen 1863; Second Ed. 1876) Vol. 2, 499-502.

[H] Hungerford, T., *Algebra*, Springer, GTM **73**, 1974.

[I] Isaacs, I., *Solution of polynomials by real radicals*, Amer. Math. Monthly **92**, No. 8, 1985, 571-575.

[L1] Lehmer, D., *A note on trigonometric algebraic numbers*, Amer. Math. Monthly **40**, March 1933, 165-166.

[L2] Lehmer, D., *On arccotangent relations for* π, Amer. Math. Monthly **45**, No. 10, December, 1938, 657-664.

[M] Milne, J.S., *Fields and Galois Theory*, Notes, Version 4.00, February 19, 2005, available at: http://www.jmilne.org/math/.

[Mo] Moise, E., *Elementary geometry from an advanced standpoint*, Second Edition, Addison-Wesley Pub. Co., 1974.

[N] Niven, I., *Irrational Numbers*, Carus Math. Monographs **11**, MAA, 1956.

[O] Olmsted, J., *Rational values of trigonometric functions*, Amer. Math. Monthly **52**, 1945, 507-508.

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

[S1] Stillwell, J., *Mathematics and Its History*, UTM, Springer-Verlag, 1989.

[S2] Stillwell, J., *Numbers and Geometry*, UTM, Springer-Verlag, 1998.

[S3] Stillwell, J., *Yearning for the Impossible: The Surprising Truths of Mathematics*, A K Peters, Ltd., 2006.

[St] Størmer, C., *Sur l'application de la théorie des nombres entiers complexes à la solution en nombres rationnels* $x_1x_2\cdots x_n\ c_1c_2\cdots c_n$ *de l'équation:* $c_1\arctan x_1+c_2\arctan x_2+\cdots+c_n\arctan x_n$, Archiv for Mathematik og Naturvidenskab, B., XIX, no. 3, 1896, 3-96.

[U] Underwood, R., *On the irrationality of certain trigonometric functions*, Amer. Math. Monthly **28**, 1921, 374-376.

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

[WW] Weber, H. and Wellstein, J., *Enzyklopädie der Elementarmathematik*, B.G. Teubner, Leipzig, 1922, 528-529.

[Wr1] Wrench, Jr., J., *On the derivation of arctangent equalities*, Amer. Math. Monthly **45**, No. 2, February, 1938, 108-109.

[Wr2] Wrench, Jr., J., *The evolution of extended decimal approximations to* π, The Math. Teacher, Vol. 53, December, 1960, 644-650.

University of Texas at Austin
E-mail address: jack@math.utexas.edu
URL: http://www.ma.utexas.edu/users/jack/