Rose-Hulman Undergraduate Mathematics Journal

Volume 22
Issue 2

Article 3

A Proof of a Generalization of Niven's Theorem Using Algebraic Number Theory

Caroline Nunn
University of Maryland, College Park, jnunn@umd.edu

A Proof of a Generalization of Niven's Theorem Using Algebraic Number Theory

Cover Page Footnote

This paper is the result of independent research conducted under the supervision of Larry Washington, without whom this paper would not have been possible. I especially appreciate the many helpful comments he gave during the editing process. Thank you to the whole MMDG Math Discussion Group for helping to motivate me; specifically, thanks to Jason Lee for help with combinatorics and Jamie Jorgensen for introducing me to Niven's theorem.

Rose-Hulman Undergraduate Mathematics Journal
VOLUME 22, ISSUE 2, 2021

A Proof of a Generalization of Niven's Theorem Using Algebraic Number Theory

By *Caroline Nunn*

Abstract. Nivens theorem states that the sine, cosine, and tangent functions are rational for only a few rational multiples of π. Specifically, for angles θ that are rational multiples of π, the only rational values of $\sin(\theta)$ and $\cos(\theta)$ are 0, $\pm\frac{1}{2}$, and ± 1. For tangent, the only rational values are 0 and ± 1. We present a proof of this fact, along with a generalization, using the structure of ideals in imaginary quadratic rings. We first show that the theorem holds for the tangent function using elementary properties of Gaussian integers, before extending the approach to other imaginary quadratic rings. We then show for which rational multiples of π the squares of the sine, cosine, and tangent functions are rational, providing a generalized form of Nivens theorem. We end with a discussion of a few related combinatorial identities.

1 Introduction

The identity

$$(1+i)^4 = -4 \tag{1}$$

gives an example of a complex number (specifically, a Gaussian integer) which, when raised to an integral power, gives a real number. This is, by itself, rather unremarkable; however, a search for other examples shows that, aside from trivial cases, multiples, and conjugates, this number appears to be the only Gaussian integer with this property. In fact, this is true:

Theorem 1.1. *Let $\alpha \in \mathbb{Z}[i]$ be a nonzero Gaussian integer such that there exists $n \in \mathbb{Z}^+$ and $c \in \mathbb{Z}$ with $\alpha^n = c$.*[1] *Then α is an integer multiple of either a unit or an associate of $1+i$.*

This result follows from a classic theorem on trigonometric functions that was included in Ivan Niven's famous book *Irrational Numbers* [6]. This theorem can be stated as follows:

Mathematics Subject Classification. 11R04
Keywords. Number Theory, Algebraic Number Theory, Trigonometry

[1] Here and throughout this paper, $\mathbb{Z}^+$ denotes the positive integers. In particular, $0 \notin \mathbb{Z}^+$.

Theorem 1.2 (Lehmer, Olmsted, Niven)**.**

$$\sin(\pi\mathbb{Q}) \cap \mathbb{Q} = \cos(\pi\mathbb{Q}) \cap \mathbb{Q} = \left\{0, \pm\tfrac{1}{2}, \pm 1\right\} \tag{2}$$

and

$$\tan(\pi\mathbb{Q}) \cap \mathbb{Q} = \{0, \pm 1\}. \tag{3}$$

Theorem 1.1 follows easily from eq. (3): let $\alpha = a + bi$ be a Gaussian integer. For α to have the desired property, we must have that $\theta = \arctan(b/a)$ is a rational multiple of π. This is because α may be written in polar form as $\pm|\alpha|e^{i\theta}$, so for $\alpha^k = (\pm|\alpha|)^k e^{ik\theta}$ to be real, $k\theta$ must be an integer multiple of π, meaning θ is a rational multiple of π. However, this method of proof requires trigonometry, while our original question was purely algebraic and did not make any reference to trigonometric functions. This suggests that there might be a method of proving this result without reference to trigonometry.

In fact, as we will see in **Corollary 2.5**, **Theorem 1.1** is equivalent to Niven's theorem, at least in the case of the tangent function. This means that an algebraic proof of **Theorem 1.1** gives a new approach to proving the tangent part of Niven's theorem. Finding such an algebraic proof is the focus of section section 2.

In section 3 we generalize the method of section section 2 to quadratic rings other than the Gaussian integers. This can be seen to imply a generalized form of Niven's theorem. Specifically, we are able to classify when the tangent of a rational multiple of π is the square of a rational number. The Pythagorean trigonometric identities allow us to extend this result to the other trigonometric functions. Section 4 gives a few related combinatorial identities.

Niven's original proof [6] also uses algebraic number theory, but the approach is different. Niven first proves a result of D. H. Lehmer [5]; namely, that for integers $k \geq 0$, $n > 2$ with $\gcd(k, n) = 1$, the number $2\cos(2\pi k/n)$ is an algebraic integer of degree $\phi(n)/2$, where $\phi(n)$ is Euler's ϕ–function. Niven's theorem then follows for cosine noting that $\phi(n) = 2$ if and only if $n = 3$, 4, or 6. Niven then extends this result in a modified form to the sine and tangent functions, thus proving the full theorem.

For other proofs, see [1, 3, 7, 8].

2 Proof of Niven's theorem for the tangent function

The Gaussian integers $\mathbb{Z}[i] = \{\alpha \in \mathbb{C} \mid \alpha = a + bi, a, b \in \mathbb{Z}\}$ are a special subset of the complex numbers with properties similar to the regular integers. To distinguish between regular integers and Gaussian integers, we will always refer to $\mathbb{Z}[i]$ as "Gaussian", reserving "integer" for $\mathbb{Z}$. Note that $\mathbb{Z}[i]$ is a ring and recall the following definitions from ring theory:

Definition 2.1. A **unit** is an element of a ring whose multiplicative inverse is also in the same ring. Two numbers α and β are called **associates** if there exists a unit u such that $\alpha = u\beta$.

The units of $\mathbb{Z}[i]$ are $\{1, i, -1, -i\}$. So for any $\alpha \in \mathbb{Z}[i]$, the set of associates of α is given by $\{\alpha, i\alpha, -\alpha, -i\alpha\}$.

Lemma 2.2. *Let $\alpha \neq 0$ be a Gaussian integer that is an associate of its complex conjugate. Then α is an integer multiple of 1, i, or $1 \pm i$.*

Proof. Let $\alpha = a + bi$. The associates of α are $\{a + bi, -b + ai, -a - bi, b - ai\}$, and the conjugate of α is $a - bi$. If $a - bi = a + bi$, then $b = 0$, so $\alpha = a$ is an integer. If $a - bi = -a - bi$, then $a = 0$, so $\alpha = bi$ is an integer multiple of i. Finally, if $a - bi = \pm b \mp ai$, we find by comparing real and imaginary parts that $b = \pm a$. Then $\alpha = a \pm ai$ is an integer multiple of $1 \pm i$. □

An analogue of unique factorization holds in $\mathbb{Z}[i]$. However, because of the fact that any element can be trivially factored, for example, as $\alpha = -i(i\alpha)$, we must be careful about what we mean by "unique factorization".

Definition 2.3. An element α of a ring is called **irreducible** if α is not a unit and for all β and γ in the ring with $\alpha = \beta\gamma$, one of β or γ must be a unit. A **prime** element is an irreducible element π with the following property: if $\pi \mid \alpha\beta$, then $\pi \mid \alpha$ or $\pi \mid \beta$.

Proposition 2.4. *All irreducible elements of $\mathbb{Z}[i]$ are prime. Furthermore, each nonzero element of $\mathbb{Z}[i]$ may be written in the form $\pi_1 \cdots \pi_n$, where $\pi_1, ..., \pi_n$ are prime. This factorization is unique up to reordering and replacement by associates.*

For a proof, see [4], Corollary 18.10 and Theorem 18.12. Now we are ready to prove **Theorem 1.1**.

*Proof (of **Theorem 1.1**).* Let $\alpha = a + bi$, where a and b are integers with $\gcd(a, b) = 1$. Suppose there exists a positive integer n and an integer c such that $\alpha^n = c$. Let π be a prime factor of α. Then since $\alpha \mid c$, we have $\pi \mid c$. This means that there exists a ρ such that $\pi\rho = c$. Taking conjugates, we find $\bar{\pi}\bar{\rho} = \bar{c} = c$. Therefore, $\bar{\pi} \mid c$. Since $c = \alpha^n$ and $\bar{\pi}$ is prime, $\bar{\pi} \mid \alpha$. Suppose for a contradiction that π and $\bar{\pi}$ are relatively prime. Then $\pi\bar{\pi} \mid \alpha$. But $\pi\bar{\pi}$ is an integer, and since $\gcd(a, b) = 1$, α has no integer factors. Therefore π and $\bar{\pi}$ are not relatively prime and so, since they are both primes, must be associates. By **Lemma 2.2**, π is an associate of $1 + i$ (note that $1 - i = -i(1 + i)$ is an associate of $1 + i$). Therefore, α must be a unit times a power of $1 + i$. However, since $2 \mid 2i = (1 + i)^2$ and α is assumed to have no integer factors, we find that α is either a unit or an associate of $1 + i$.

For α where $\gcd(a, b) > 1$, the result follows from the previous result using $\alpha' = \alpha / \gcd(a, b)$. □

Corollary 2.5. $\tan(\pi\mathbb{Q}) \cap \mathbb{Q} = \{0, \pm 1\}$.

Proof. Suppose $\tan(\pi m/n) = b/a$, where $a, b, m, n \in \mathbb{Z}$. Let $\alpha = a + bi$. Note that α is a Gaussian integer, so any positive power of α is also a Gaussian integer. Then $\alpha = \pm re^{i\pi m/n}$, where $r = \sqrt{a^2+b^2}$, so $\alpha^n = (\pm r)^n e^{i\pi m} = (-1)^m (\pm r)^n$. Then α^n is a real number and a Gaussian integer, so is an integer. This means that α is an integer multiple of either a unit or $1+i$, i.e., α is either $a+0i$ or $a \pm ai$. Then $\tan(\pi m/n)$ is either 0 or ± 1. □

3 Niven generalized

The Gaussian integers can be generalized as follows:

Definition 3.1. A **quadratic field** is a field extension of the rational numbers given by $\mathbb{Q}(\sqrt{d}) = \{x + y\sqrt{d} \mid x, y \in \mathbb{Q}\}$, where d is a square-free integer. If $d > 0$, the quadratic field is said to be **real**, otherwise, it is **imaginary**. The **ring of algebraic integers** in $\mathbb{Q}(\sqrt{d})$, denoted $\mathcal{O}_d$, is defined as the intersection of $\mathbb{Q}(\sqrt{d})$ with the algebraic integers, that is, roots of polynomials over the integers with leading coefficient 1. As the name implies, this set is a ring.

For example, $\mathbb{Q}[i]$ is a quadratic field with $d = -1$, and its ring of algebraic integers is the Gaussian integers. We will describe the ring of algebraic integers for arbitrary quadratic fields later in **Proposition 3.4**. Again, we will always refer to algebraic integers as algebraic integers and refer to regular integers as "integers".

Proposition 3.2. *Let $\alpha \neq 0$ be an element of a real quadratic field $K = \mathbb{Q}(\sqrt{d})$ such that there exists $n \in \mathbb{Z}^+$ and $c \in \mathbb{Q}$ with $\alpha^n = c$. Then α is rational or a rational multiple of $\sqrt{d}$.*

Proof. Suppose for contradiction that $\alpha = (a + b\sqrt{d})$ for rational $a \neq 0$, $b \neq 0$. It suffices to show that α^n is irrational for positive a and b, since if α is rational so are $-\alpha$, $\bar{\alpha}$, and $-\bar{\alpha}$. Let $a_n + b_n\sqrt{d} = (a + b\sqrt{d})^n$. Expanding the right hand side with the binomial theorem, we find that $b_n > 0$, since it is a sum of positive numbers. Since α^n was assumed to be rational, we have found that $\sqrt{d} = (\alpha^n - a_n)/b_n$ is rational, a contradiction. Hence, one of a or b must equal 0. □

For imaginary quadratic fields, we can extend the argument used to prove **Theorem 1.1**. However, the argument must be modified to account for the failure of unique factorization in arbitrary quadratic rings. Recall that a set $\mathfrak{a}$ is called an ideal of a ring R if $\mathfrak{a}$ is an additive subgroup of R with the property that if $\alpha \in \mathfrak{a}$, we have $\alpha\beta \in \mathfrak{a}$ for all $\beta \in R$. If there exists an $\alpha \in R$ such that $\mathfrak{a} = \{\alpha r : r \in R\}$, we say that $\mathfrak{a}$ is *principal* and write $\mathfrak{a} = \langle\alpha\rangle$. We denote by $N(\mathfrak{a})$ the index of $\mathfrak{a}$ as a subgroup of the additive group of the ring, that is, $N(\mathfrak{a}) = [\mathcal{O}_d : \mathfrak{a}]$.

Ideals can be multiplied; for ideals $\mathfrak{a}$ and $\mathfrak{b}$, the ideal $\mathfrak{ab}$ is defined to be the smallest ideal containing products of elements of $\mathfrak{a}$ and $\mathfrak{b}$. We have $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$. Note that in

a quadratic ring, $\langle N(\mathfrak{a})\rangle = \mathfrak{a}\bar{\mathfrak{a}}$, where $\bar{\mathfrak{a}}$ is the ideal obtained by conjugating each element of $\mathfrak{a}$. For ideals $\mathfrak{a}$ and $\mathfrak{c}$, if there exists an ideal $\mathfrak{b}$ such that $\mathfrak{a}\mathfrak{b} = \mathfrak{c}$, we say $\mathfrak{a} \mid \mathfrak{c}$. Equivalently, $\mathfrak{a} \mid \mathfrak{c}$ if $\mathfrak{c} \subseteq \mathfrak{a}$. When $\mathfrak{c} = \langle\gamma\rangle$ is a principal ideal, we write $\mathfrak{a} \mid \gamma$. An ideal $\mathfrak{p}$ is said to be *prime* if it has the property that $\mathfrak{p} \mid \mathfrak{a}\mathfrak{b}$ implies $\mathfrak{p} \mid \mathfrak{a}$ or $\mathfrak{p} \mid \mathfrak{b}$. While factorization of elements is not unique in general, an ideal of $\mathcal{O}_d$ can always be uniquely factored into prime ideals. For a proof, see [9, 2].

Lemma 3.3. *Let $\alpha \neq 0$ be an algebraic integer in a quadratic field K with no integer factors other than ± 1 such that there exists $n \in \mathbb{Z}^+$ and $c \in \mathbb{Z}$ with $\alpha^n = c$. Then any prime ideal factor $\mathfrak{p}$ of $\langle\alpha\rangle$ satisfies $\mathfrak{p} = \bar{\mathfrak{p}}$.*

Proof. Let $\mathcal{O}_d$ be the ring of algebraic integers in the quadratic field $K = \mathbb{Q}(\sqrt{d})$, and let α be an element of $\mathcal{O}_d$ with no nontrivial integer factors (i.e., the only integer factors are 1 and -1) such that $\alpha^n = c$ for some positive integer n and integer c. Let $\mathfrak{p}$ be a prime ideal factor of $\langle\alpha\rangle$. Since $\mathfrak{p} \mid \alpha$ and $\alpha \mid c$, we have $\mathfrak{p} \mid c$. Taking conjugates, we find $\bar{\mathfrak{p}} \mid \bar{c} = c$. Since $c = \alpha^k$ and $\bar{\mathfrak{p}}$ is prime, $\bar{\mathfrak{p}} \mid \alpha$. Suppose for a contradiction that $\mathfrak{p} \neq \bar{\mathfrak{p}}$. Then $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ are distinct prime ideal factors of $\langle\alpha\rangle$ and $\mathfrak{p}\bar{\mathfrak{p}} \mid \alpha$. Since $\mathfrak{p}\bar{\mathfrak{p}} = \langle N(\mathfrak{p})\rangle$, we have $N(\mathfrak{p}) \mid \alpha$. Then $N(\mathfrak{p})$ is a nontrivial integer factor of α, a contradiction. Therefore, all prime ideal factors of $\langle\alpha\rangle$ satisfy $\mathfrak{p} = \bar{\mathfrak{p}}$. □

To pin down exactly which α have the desired property, we need to know a little bit more about the ring of algebraic integers in quadratic fields. Recall that d is a square-free integer.

Proposition 3.4. *Let $K = \mathbb{Q}(\sqrt{d})$ and let $\mathcal{O}_d$ be the ring of algebraic integers in K. Then*

(a) $\mathcal{O}_d = \mathbb{Z}[\theta]$, where $\theta = \sqrt{d}$ if $d \not\equiv 1 \pmod 4$ or $\theta = \frac{1+\sqrt{d}}{2}$ if $d \equiv 1 \pmod 4$.

(b) For $d < 0$, the group of units in $\mathcal{O}_d$ is generated by i if $d = -1$, by $\frac{1+\sqrt{-3}}{2}$ if $d = -3$, or by -1 otherwise.

(c) For a principal ideal $\langle\alpha\rangle$, $N(\langle\alpha\rangle) = |N(\alpha)| = |\alpha\bar{\alpha}| = |x^2 - dy^2|$, where $\alpha = x + y\sqrt{d}$.

For a proof, see [9, 2].

Lemma 3.5. *Let $\mathfrak{p} \neq 0$ be a prime ideal of the ring of algebraic integers in a quadratic field $K = \mathbb{Q}(\sqrt{d})$. If $\mathfrak{p} = \bar{\mathfrak{p}}$, then either $\mathfrak{p} = \langle p\rangle$ for a rational prime p, or $N(\mathfrak{p}) = p$ for some rational prime p with either $p \mid d$ or $p = 2$. If $N(\mathfrak{p}) = p$ and $d \equiv 1 \pmod 4$, then $p \neq 2$.*

For a proof, see Theorem 8.3 and Table 3 of [2]. We remark that a prime ideal $\mathfrak{p}$ is said to be ramified if $\mathfrak{p}^2 = \langle p\rangle$ for some prime integer p. These are exactly the ideals with $\mathfrak{p} = \bar{\mathfrak{p}}$ and $N(\mathfrak{p}) = p$ that occur in the second part of **Lemma 3.5**. We are now ready to classify exactly which prime ideals can appear in the factorization of $\langle\alpha\rangle$, where α is an algebraic integer with the desired property.

Lemma 3.6. *Let $\langle\beta\rangle = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ with $r \geq 1$ be a principal ideal in the ring of algebraic integers of an imaginary quadratic field $K = \mathbb{Q}(\sqrt{d})$ where $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are distinct ramified prime ideals. Then β is an associate of $\sqrt{d}$ or, when $d = -1$, an associate of $1 + i$.*

Proof. Let $\mathcal{O}_d$ be the ring of algebraic integers in the imaginary quadratic field $\mathbb{Q}(\sqrt{d})$. Let $p_i = N(\mathfrak{p}_i)$. Since $\mathfrak{p}_i$ is ramified, p_i is prime and either divides d or equals 2 by **Lemma 3.5**. If $d \equiv 1 \pmod 4$, then $p_i \neq 2$. Since each prime $p_i = N(\mathfrak{p}_i) = \mathfrak{p}_i\bar{\mathfrak{p}}_i = \mathfrak{p}_i^2$ and $\mathfrak{p}_i \neq \mathfrak{p}_j$ when $i \neq j$, unique factorization gives $p_i \neq p_j$.

Because the norm is multiplicative, $N(\beta) = N(\mathfrak{p}_1 \cdots \mathfrak{p}_r) = p_1 \cdots p_r$. In particular, by the above, the prime factors of $N(\beta)$ are contained in the prime factors of d and do not repeat. Therefore, $N(\beta)$ is at most $2|d|$, or $|d|$ in the case that $d \equiv 1 \pmod 4$.

When $d \not\equiv 1 \pmod 4$, we have $\beta = m + n\sqrt{d}$ for some integers m and n. Then $N(\beta) = m^2 + |d|n^2 = p_1 \cdots p_r$. Note that $n \neq 0$ since otherwise m^2 would be a nonempty product of distinct primes, which is impossible. So $|d| \leq N(\beta) \leq 2|d|$. Because the prime factors of $N(\beta)$ are contained in the prime factors of d and 2, $N(\beta)$ is either $|d|$ or $2|d|$. If $N(\beta) = d$, we must have $m = 0$, so $\langle\beta\rangle = \langle\sqrt{d}\rangle$. For $N(\beta) = 2|d|$, we must have $n^2 = 1$ (otherwise $N(\beta)$ is too large). Then $m^2 + |d| = 2|d|$ implies that $|d| = m^2$. Since d is square-free, $d = -1$. Then $\langle\beta\rangle = \langle 1 + i\rangle$.

In the case $d \equiv 1 \pmod 4$, a similar analysis may be carried out, but with $\beta = m + n\frac{1+\sqrt{d}}{2}$. Again, $n \neq 0$, so $N(\beta) = (m + n/2)^2 + |d|n^2/4 \geq (1 + |d|)/4$, since either $|n| \geq 2$ or $|n| = 1$ and $|m + n/2| \geq 1/2$. The only odd prime less than 4 is 3, so, since $(1 + |d|)/4 \leq N(\beta) \leq |d|$, we have $N(\beta) = |d|$ or $N(\beta) = |d|/3$. If $N(\beta) = |d|$, we know from size considerations that $|n|$ is at most 2. If $n = \pm 2$, we must have $m = \mp 1$, so we find $\langle\beta\rangle = \langle\sqrt{d}\rangle$. If $n = \pm 1$, let $k = 2m + n = 2m \pm 1$. Then $N(\beta) = (k^2 + |d|)/4 = |d|$, so $k^2 = 3|d|$. Since d is square-free, we must have $d = -3$ and $k = \pm 3$, meaning $\langle\beta\rangle = \left\langle \frac{\pm 3 \pm \sqrt{-3}}{2} \right\rangle = \langle\sqrt{-3}\rangle$. If $N(\beta) = |d|/3$, we must have $n^2 = 1$ (again, because otherwise $N(\beta)$ is too large). Let $k = 2m + n = 2m \pm 1$. Then $N(\beta) = (k^2 + |d|)/4 = |d|/3$, meaning $|d| = 3k^2$. Since d is square-free, we have $d = -3$, in which case the corresponding ideal $\left\langle \frac{1+\sqrt{-3}}{2} \right\rangle = \mathcal{O}_{-3}$ is the entire ring, and is therefore not a nonempty product of prime ideals. □

Thus we have found that there is exactly one principal ideal $\langle\beta\rangle$ in each imaginary quadratic ring $\mathcal{O}_d$ satisfying the hypotheses of **Lemma 3.6**. Figure 1, Figure 2, and Figure 3 illustrate this ideal for a few values of d. In each diagram, the ring of algebraic integers for $\mathbb{Q}(\sqrt{d})$ is represented by points in the complex plane. The ideal $\langle\beta\rangle$ is shown with blue + symbols, with the generators as green * symbols. The units of the ring are shown with magenta × symbols.

The two exceptional cases, $\mathbb{Z}[i]$ and $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$, are shown, along with the ring $\mathbb{Z}[\sqrt{-2}]$, which is intended to represent the general case.

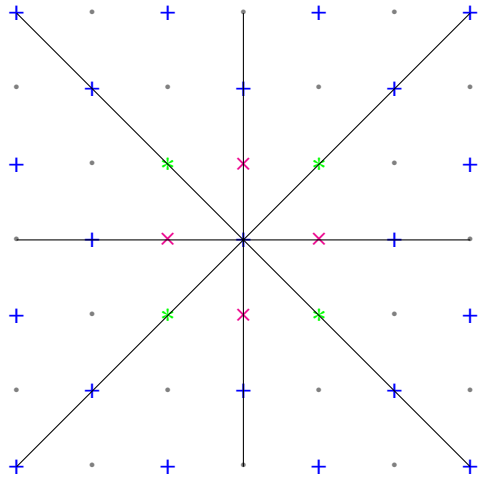

Figure 1: $\mathbb{Z}[i]$

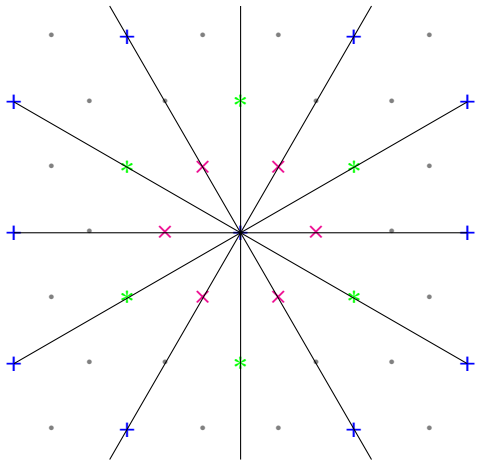

Figure 2: $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$

Theorem 3.7. *Let $\alpha \neq 0$ be an element of a quadratic field $K = \mathbb{Q}(\sqrt{d})$ such that there exists $n \in \mathbb{Z}^+$ and $c \in \mathbb{Q}$ with $\alpha^n = c$. Then α is a rational multiple of one of 1, i, $1 \pm i$, $\frac{1\pm\sqrt{-3}}{2}$, $\frac{3\pm\sqrt{-3}}{2}$, or $\sqrt{d}$.*

Proof. In the case of real quadratic fields, the theorem follows from **Proposition 3.2**. For imaginary quadratic fields, it suffices to show that the theorem is true for algebraic integers, since every element of a quadratic field is a rational multiple of an algebraic integer. In this case, since c is a power of an algebraic integer, it is an algebraic integer. It is also rational, so $c \in \mathbb{Z}$.

Let $\mathcal{O}_d$ be the ring of algebraic integers in the imaginary quadratic field $K = \mathbb{Q}(\sqrt{d})$ in which α is an element. Let a be the largest integer factor of α and let $\beta = \alpha/a$. If β is a unit, we are done, since the units of β are given by **Proposition 3.4**. Otherwise, by **Lemma 3.3**, we know that $\langle\beta\rangle$ factors as $\mathfrak{p}_1 \cdots \mathfrak{p}_r$, where each $\mathfrak{p}_i$ is a distinct prime ideal satisfying $\mathfrak{p}_i = \bar{\mathfrak{p}}_i$. Since a is the largest integer factor of α, $\mathfrak{p}_i$ cannot be a principal ideal generated by a rational prime and is therefore ramified. Thus $\langle\beta\rangle$ satisfies the conditions of **Lemma 3.6**, so β is an associate of $\sqrt{d}$ or, in the case that $d = -1$, an associate of $1 + i$.

In summary, $\langle\alpha\rangle$ must factor as either $\langle a\rangle$, $\langle a\rangle\langle\sqrt{d}\rangle$, or $\langle a\rangle\langle 1 + i\rangle$, with a an integer. Thus, α/a is a unit times 1, $\sqrt{d}$, or $1+i$. The units of $\mathcal{O}_d$ are ± 1, $\pm i$ for $d = -1$, and $\frac{\pm 1\pm\sqrt{-3}}{2}$ for $d = -3$. The theorem follows (note that $\frac{3\pm\sqrt{-3}}{2}$ is an associate of $\sqrt{-3}$). □

In Figure 1, Figure 2, and Figure 3, the points α lying along a black line are exactly the points that satisfy $\alpha^n = c$ for some $n \in \mathbb{Z}^+$ and $c \in \mathbb{Z}$.

Theorem 3.8 (Generalized Niven's theorem)**.** *Let $\theta \in \pi\mathbb{Q}$. If $\tan^2\theta$ is rational, then θ is an integer multiple of $\pi/6$ or $\pi/4$. The same result holds for $\sin^2\theta$ and $\cos^2\theta$.*

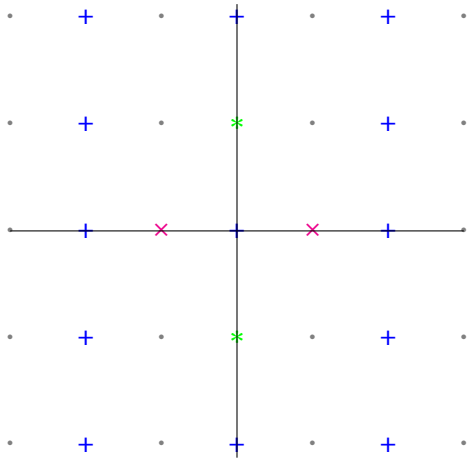

Figure 3: $\mathbb{Z}[\sqrt{-2}]$

Proof. Suppose $\tan^2\theta$ is rational, where $\theta = \pi m/n$ is a rational multiple of π. Then $\tan\theta = b\sqrt{d}/a$, with $a, b, d \in \mathbb{Z}$ and $d > 0$ square-free. Let $\alpha = a + ib\sqrt{d}$. We have $\alpha = \pm re^{i\pi m/n}$ where $r = \sqrt{a^2 + db^2}$, so $\alpha^n = (\pm r)^n e^{i\pi m} = (-1)^m (\pm r)^n$. Then α^n is a real number and is in $\mathcal{O}_{-d}$ and is therefore an integer. By **Theorem 3.7**, α is a rational number times one of 1, $1 \pm i$, $1 \pm \sqrt{-3}$, or $3 \pm \sqrt{-3}$. Thus θ is an integer multiple of $\pi/6$ or $\pi/4$.

This result can be extended to sin and cos using the identity $\tan^2\theta + 1 = \sec^2\theta$. Suppose $\cos^2\theta$ is rational with $\theta \in \pi\mathbb{Q}$. Then $\tan^2\theta = 1 - 1/\cos^2\theta$ is rational, so θ is an integer multiple of $\pi/6$ or $\pi/4$. (Note that this argument does not work for θ that are odd multiples of $\pi/2$; however, $\cos(\pi/2) = 0$ is rational.) The result holds for sin since $\sin(\pi/2 - \theta) = \cos\theta$. □

4 Combinatorial Identities

We end with a discussion of certain combinatorial identities that may be derived from our result. Specifically, the equations

$$\begin{aligned}(1+i)^4 &= -4,\\ \left(1+\sqrt{-3}\right)^3 &= -8,\\ \left(3+\sqrt{-3}\right)^6 &= -1728,\end{aligned}$$

together with the binomial theorem (taking real and imaginary parts of the resulting sum) provide the following six combinatorial identities:

$(1+i)^{4n}$	$\sum_{k=0}^{2n}\binom{4n}{2k}(-1)^k=(-4)^n$	$\sum_{k=0}^{2n-1}\binom{4n}{2k+1}(-1)^k=0$
$\left(1+\sqrt{-3}\right)^{3n}$	$\sum_{k=0}^{\lfloor 3n/2\rfloor}\binom{3n}{2k}(-3)^k=(-8)^n$	$\sum_{k=0}^{\lceil 3n/2\rceil-1}\binom{3n}{2k+1}(-3)^k=0$
$\left(3+\sqrt{-3}\right)^{6n}$	$\sum_{k=0}^{3n}\binom{6n}{2k}(-1)^k 3^{6n-k}=(-1728)^n$	$\sum_{k=0}^{3n-1}\binom{6n}{2k+1}(-1)^k 3^{6n-k-1}=0$

This suggests a general method of deriving combinatorial identities from complex identities; however, **Theorem 3.7** shows that these are essentially the only examples.

References

[1] Curtis D. Bennett, A. M. W. Glass, and Gábor J. Székely. Fermat's last theorem for rational exponents. *American Mathematical Monthly*, 111(4):322–329, 2004. https://www.jstor.org/stable/4145241.

[2] Keith Conrad. Factoring in quadratic fields. https://kconrad.math.uconn.edu/blurbs/gradnumthy/quadraticgrad.pdf.

[3] Jörg Jahnel. When is the (co)sine of a rational angle equal to a rational number? 2010. https://arxiv.org/abs/1006.2938.

[4] James S. Kraft and Lawrence C. Washington. *An Introduction to Number Theory with Cryptography*. CRC Press, 2nd edition, 2018.

[5] D. H. Lehmer. A note on trigonometric algebraic numbers. *American Mathematical Monthly*, 40(3):165–166, 1933. https://www.jstor.org/stable/2301023.

[6] Ivan Niven. *Irrational Numbers*. The Mathematical Association of America, 1956.

[7] J. M. H. Olmsted. Rational values of trigonometric functions. *American Mathematical Monthly*, 52(9):507–508, 1945. https://www.jstor.org/stable/2301023.

[8] Norman Schaumberger. A classroom theorem on trigonomtric irrationalities. *Two-Year College Mathematics Journal.*, 5(1):73–76, 1974. https://www.jstor.org/stable/3026991.

[9] Ian Stewart and David Tall. *Algebraic Number Theory and Fermat's Last Theorem*. AK Peters, Ltd., 3rd edition, 2002.

Caroline Nunn
University of Maryland, College Park
jnunn@umd.edu