TRISECTION, PYTHAGOREAN ANGLES, AND GAUSSIAN INTEGERS

PETER J. KAHN

Abstract. Pythagorean angles, that is angles with rational sines and cosines, provide an interesting environment for studying the question of characterizing trisectable angles. The main result of this paper shows that a Pythagorean angle is trisectable if and only if it is three times some other Pythagorean angle. Using the Euclidean parametrization of Pythagorean angles, this result allows an effective listing of all trisectable Pythagorean angles. The arguments of the paper describe and use many of the interesting properties of the Gaussian integers.

Department of Mathematics
Cornell University
Ithaca, New York 14853
July 21, 2011

1. Introduction

For well over two thousand years, the problem of finding, for each angle α, a construction by unmarked straight-edge and compass that produces an angle β such that $\alpha = 3\beta$ lingered in a sort of purgatory of mathematics problems, often misunderstood, never resolved. This is the famous Greek angle-trisection problem; an α for which a β can be constructed as indicated is said to be *trisectable*.*

Then in 1837, the French genius and polymath P.L. Wantzel, building on earlier work by Arabic and Italian mathematicians, gave a definitive solution [W], which, while *negative* from the viewpoint of the original problem, opened the door to new, interesting questions. He obtained a necessary and sufficient algebraic criterion for deciding whether an angle having cosine a is trisectable: namely, to rephrase only slightly, that the polynomial

$$x^3 - 3x - 2a$$

have a zero in the field $\mathbb{Q}(a)$ of all rational functions of a.

This criterion leads to the possibility of constructing many examples of trisectable and non-trisectable angles and of determining the density of the set of trisectable angles in various restricted sets of angles [K]. We denote the set of all trisectable angles by Tri.

This paper looks at the question of angle trisectability for angles that have a pedigree even more venerable than that of the trisection problem. We represent an angle by a point on the unit circle S^1 in the complex plane $\mathbb{C}$, and we let Π denote the subset of S^1 consisting of all points with rational real and imaginary parts. We call these angles *Pythagorean* because the acute angles in Π are precisely those that occur in right triangles with integer side-lengths, the triples of such side-lengths being commonly called *Pythagorean triples*. With a few well-known exceptions, Pythagorean angles have been the longest known and most

*Usually β is visualized to be smaller than α. However, we identify angles modulo 2π, so if γ is any multiple of $2\pi/3$, we have $\alpha = 3\beta = 3(\beta + \gamma)$. See the remark after the Main Theorem below.

intensively studied of all angles. They provide a perfect laboratory, as it were, for studying the problem of angle trisection.

Complex multiplication in S^1 (i.e., angle addition) makes Π into a countable subgroup of S^1, known to be isomorphic to the direct sum of a cyclic group of order four and a countably-generated free-abelian group(cf. the appendix).

The group Π is closed under the map $z \mapsto z^3$, which gives a homomorphism $Q : \Pi \to \Pi$ (easily seen to be injective, cf. Proposition 4.1). The image $Q(\Pi)$ obviously consists of countably many trisectable angles in Π, i.e., $Q(\Pi) \subseteq \Pi \cap Tri$. Our main result shows that these are the *only* angles in Π that are trisectable:

Main Theorem. $Q(\Pi) = \Pi \cap Tri$.

Remark: Note that, for a given trisectable angle α in Π, this theorem will not always produce a β in Π that "looks" as though it trisects α. For example, if α is the acute trisectable angle (in complex notation) $(117+44i)/125$, then the unique angle in Π trisecting it is the *obtuse* angle $(-3+4i)/5$.

By applying the Main Theorem to a well-known parametrization of Pythagorean angles (cf., §3), we obtain an effective means for listing all trisectable Pythagorean angles:

Corollary. *Let (M, N) be a pair of relatively prime non-negative integers, not both zero,let u be one of the numbers in $\{1, -1, i, -i\}$, and define the angle $z \in \Pi$ by the equation*

$$z = u \cdot \frac{(M+Ni)^6}{|M+Ni|^6}.$$

Then z represents a trisectable angle in Π, and every trisectable angle in Π can be obtained in this way.

When $z \notin \{1, -1, i, -i\}$, the pair (M, N) and the number u are uniquely determined by z. Otherwise, (M, N) may be chosen arbitrarily to equal $(1, 0)$ or $(0, 1)$ with u then determined by this choice and z.

Our arguments are algebraic, and most of the facts needed for them are known to intermediate students of algebra and number theory. We give an exposition that assumes what is normally covered in an introductory undergraduate algebra course. In particular, from this introductory standpoint, we introduce various facts about the ring $\mathbb{Z}[i]$ of Gaussian integers not normally covered in such algebra courses. The ring $\mathbb{Z}[i]$ has beautiful features that are particularly well adapted for studying Pythagorean angles, as we shall show.

I want to thank Dr. Catherine M. Wagner for many helpful conversations and suggestions during the course of this work.

2. The Ring of Gaussian Integers

The set of complex numbers $a + bi$, with a and b ordinary integers, comprise a subring of the complex field $\mathbb{C}$ called the ring of *Gaussian integers*. It is often denoted $\mathbb{Z}[i]$ (the ring of integers $\mathbb{Z}$ with the complex number $i = \sqrt{-1}$ adjoined), but we denote it more briefly by Γ. The field of fractions of Γ consists of the complex numbers $r + si$, with r and s ordinary rational numbers. It is often denoted $\mathbb{Q}(i)$ (the subfield of $\mathbb{C}$ obtained by adjoining i to the field of rationals $\mathbb{Q}$) and is called the field of Gaussian numbers..

The algebraic properties of Γ are closely analogous to those of its subring $\mathbb{Z}$. We assume that the reader is familiar with the properties of $\mathbb{Z}$. We shall list those properties of $\mathbb{Z}$ that are important for us and then indicate such modifications as may be needed to apply to Γ.

1) Division : Given $x, d \in \mathbb{Z}$, with $d \neq 0$, there exist $q, r \in \mathbb{Z}$ such that

$$x = qd + r \quad \text{and} \quad |r| < |d|. \tag{1}$$

2) Greatest common divisor: Given x and y in $\mathbb{Z}$, not both zero, there exists a common divisor of x and y divisible by every common divisor of x and y. This is called a greatest common divisor of x and y (gcd) and may be denoted as (x, y). It is unique up to sign. Moreover, there exist $a, b \in \mathbb{Z}$ such that $(x, y) = ax + by$.

3) Prime factorization: Every integer $n \notin \{-1, 0, 1\}$ can be factored as a product of prime integers, which factorization is unique except for the order of the factors and their signs.

It is often convenient to work with ideals in a ring R, examples of which are the sets xR consisting of all ring multiples of some ring element x (called a generator of the ideal). The ideals xR are called *principal*. A generator x of a principal ideal is unique up to multiplication by an invertible element of R, which is usually called a *unit* in R. Two ring elements x and y that satisfy $x = uy$, u a unit, are said to be *associates* or *associated*. To indicate this, we may write $x \sim y$.

4) Principal ideal domain: Every ideal in $\mathbb{Z}$ is a principal ideal. It is a prime ideal if and only if its generator is a prime integer.

5) Prime factorization of ideals: Every non-zero ideal in $\mathbb{Z}$ factors into a product of prime ideals, which factorization is unique except for the order of the factors.

Notice, by comparing properties 3) and 5), that when we pass from integers to ideals, we avoid the mildly unpleasant non-uniqueness in 3) that is due to sign ambiguity.

These properties are all consequences of the division property, which, in turn, can be proved by induction.

The ring Γ has versions of all of these features of $\mathbb{Z}$.

6) Division : The division property holds in Γ as stated, provided the absolute values $|r|$ and $|y|$ are understood in the sense of absolute values of complex numbers $|u + iv| = (u^2 + v^2)^{1/2}$. It is usually convenient, and loses no generality, to replace $|r|$ and $|y|$ by $|r|^2$ and $|y|^2$, because these last are integers, whereas, in general, $|r|$ and $|y|$ are not.

7) Greatest common divisor: The notions of divisor and gcd are the same in Γ as in $\mathbb{Z}$. However, the "uniqueness up to sign" of the gcd in $\mathbb{Z}$ must be understood more broadly in Γ.

The numbers ± 1 in $\mathbb{Z}$ are precisely the units of $\mathbb{Z}$. The units in Γ are the numbers $1, -1, i, -i$, which form a cyclic group with respect to multiplication. We denote this group by U.

In questions of divisibility, uniqueness in both $\mathbb{Z}$ and Γ is always understood "up to multiplication by a unit," i.e. up to associates. Because Γ has more units than $\mathbb{Z}$, uniqueness becomes slightly more awkward.

Any two Gaussian integers x and y, not both of which are zero, have gcd's. All these gcd's are associated. We may denote any one of them as (x, y) despite the ambiguity of this notation.

As in the case of $\mathbb{Z}$, for any elements x and y of Γ, not both zero, we have elements c and d of Γ and a formula $(x, y) = cx + dy$.

We say that x and y are relatively prime when x and y have no prime factors in common. This is equivalent to saying that (x, y) equals a unit. If x and y are ordinary integers, then one checks easily that they are relatively prime in $\mathbb{Z}$ if and only if they are relatively prime in Γ. We state the following lemma for later use.

Lemma 2.1. *Suppose that $z = a + bi \in \Gamma$, with a and b relatively prime in $\mathbb{Z}$. Then either z and its complex conjugate $\overline{z}$ are relatively prime in Γ, or $(z, \overline{z}) = \pm(1 \pm i)$.*

Proof. Let x be a gcd of z and $\overline{z}$. Then x divides $z + \overline{z} = 2a$ and $-i(z - \overline{z}) = 2b$. It follows that x divides 2. But x cannot equal ± 2, since this would contradict the relative primality of a and b. So, x must equal a unit or one of the prime divisors $\pm(1 \pm i)$ of 2. □

8) Prime factorization: Prime factorization holds in Γ just as in $\mathbb{Z}$, with uniqueness up to the order of factors and associates.

9) Principal ideal domain: The PID property holds for Γ, which means that every ideal in Γ is principal. As in the case of $\mathbb{Z}$, a principal ideal in Γ is prime if and only if its generator is a prime element of Γ.

10) Prime factorization of ideals: Prime factorization of ideals holds in Γ just as in $\mathbb{Z}$.

Properties $7) - 10)$ are consequences of property 6). This last may be proved, for any $x, d \in \Gamma, d \neq 0$ by choosing $q \in \Gamma$ so that $|(x/d) - q|^2 < 1$ (cf. equation (1)).

Now let I be any ideal of $\mathbb{Z}$, and define I_Γ to be its *extension* to Γ: that is, I_Γ is the set of all sums of products of the form mx, where $m \in I$ and $x \in \Gamma$. This is easily checked to be an ideal of Γ satisfying $I_\Gamma \cap \mathbb{Z} = I$. If we use property 4) of $\mathbb{Z}$ to write $I = n\mathbb{Z}$, for some ordinary integer n, then clearly $I_\Gamma = n\Gamma$.

Important caveat: The integer n may be prime in $\mathbb{Z}$ but not prime in Γ. Therefore, I may be prime without the extension I_Γ being prime. For example 2 is prime in $\mathbb{Z}$, but $2 = (1 + i)(1 - i)$, so 2 is not prime in Γ. On the other hand, 3 is prime in both $\mathbb{Z}$ and Γ. This kind of phenomenon is fundamental in algebraic number theory.

The following lemma and corollary expand on and clarify this caveat via some facts that are well-known in number theory but often appear imbedded in other more general arguments.

Lemma 2.2. *Let p be a positive, odd prime in $\mathbb{Z}$, and let π be a divisor of p that is prime in Γ. Then, the following statements are equivalent.*

(a) *p is prime in Γ.*
(b) *$\pi \sim \overline{\pi}$.*
(c) *$\pi \sim$ some prime in $\mathbb{Z}$.*
(d) *$\pi \sim p$.*
(e) *The polynomial $x^2 + 1$ has no zeros in the field $\mathbb{Z}/p\mathbb{Z}$.*
(f) *$p \equiv 3 (\mod 4)$.*
(g) *$p \neq a^2 + b^2$, for any $a, b \in \mathbb{Z}$.*

Proof. We shall prove the implications $(b) \implies (c) \implies (d) \implies (a) \implies (e) \implies (f) \implies (g) \implies (b)$.

We first note that associates of a prime are prime and every $p \in \mathbb{Z}$ that is prime in Γ is prime in $\mathbb{Z}$.

$(b) \implies (c)$: Set $\pi = a + bi$. If $\pi \sim \overline{\pi}$, then either $\pi = \pm\overline{\pi}$ or $\pi = \pm i \cdot \overline{\pi}$. If $\pi = \pm\overline{\pi}$, one sees immediately that $a = 0$ or $b = 0$, implying that $\pi \sim b$ or $\pi \sim a$. Suppose the former. Then, b is prime in Γ, hence prime in $\mathbb{Z}$. This implies (c). Similarly when $\pi \sim a$. We show that the other possibility, namely $\pi = \pm i \cdot \overline{\pi}$, cannot occur. For if it did, then we could immediately compute that $a = \pm b$, which implies that either π or $\overline{\pi}$ equals $a(1 + i)$. It would follow that $\pi\overline{\pi} = 2a^2$. But both π and $\overline{\pi}$ divide the odd prime p, so we could conclude that $2a^2$ divides p^2 (in Γ, hence in $\mathbb{Z}$), a contradiction.

$(c) \implies (d)$: If $\pi \sim$ some prime in $\mathbb{Z}$, say q, then q divides p, so $q = \pm p$, hence $q \sim p$. Therefore, $\pi \sim p$.

$(d) \implies (a)$: Since π is a prime in Γ and $\pi \sim p$, p is a prime in Γ.

$(a) \implies (e)$: If p is prime in Γ, then $\Gamma/p\Gamma$ is a finite integral domain, hence a field, implying that $x^2 + 1$ has at most two roots in $\Gamma/p\Gamma$. Now, in fact, $\pm i$ are zeros of $x^2 + 1$ in Γ, so the classes $\pm[i]$ they represent in $\Gamma/p\Gamma$ are zeros of $x^2 + 1$. These classes are distinct, hence they are the only zeros of $x^2 + 1$ in $\Gamma/p\Gamma$. Since $\mathbb{Z}/p\mathbb{Z}$ is a subfield of $\Gamma/p\Gamma$, and since $\pm[i] \notin \mathbb{Z}/p\mathbb{Z}$, $x^2 + 1$ has no zeros in $\mathbb{Z}/p\mathbb{Z}$.

$(e) \implies (f)$: The multiplicative group of non-zero elements of $\mathbb{Z}/p\mathbb{Z}$ is well-known to be cyclic of order $p - 1$. (E.g., see the discussion of the roots of unity of a field in [H] or in [W]). Let g be a generator of this group. Since the group has order $p-1$, we have $g^{p-1} = [1]$ but $h = g^{(p-1)/2} \neq [1]$, where $[1]$ is the residue class of the integer 1 in $\mathbb{Z}/p\mathbb{Z}$. Since $h^2 = [1]$ and $h \neq [1]$, we must have $h = -[1]$. Now, $(p - 1)/2$ cannot be an even number. For if it equals 2ℓ, then, we compute that $(g^\ell)^2 = h = -[1]$, contradicting the fact that $x^2 + 1$ has no zeros in $\mathbb{Z}/p\mathbb{Z}$. So, $(p - 1)/2$ is odd, which is equivalent to $p \equiv 3(\mod 4)$.

$(f) \implies (g)$: Suppose $p = a^2 + b^2$, for some a and b in $\mathbb{Z}$. We may assume that $0 < a, b < p$. Reducing the equation $\mod p$ and dividing by the residue class $[b^2]$ of b^2, we get an equation $[c]^2 + [1] = [0]$ in $\mathbb{Z}/p\mathbb{Z}$, for some integer c. It follows that $[c]^4 = [1]$ in $\mathbb{Z}/p\mathbb{Z}$, implying that 4 divides $p - 1$, the order of the group of invertible elements in $\mathbb{Z}/p\mathbb{Z}$. This contradicts $p \equiv 3(\mod 4)$.

$(g) \implies (b)$: Set $\pi = a + bi$, and suppose that $\pi \not\sim \overline{\pi}$. We know that π is a prime divisor of p, and so, passing to conjugates, $\overline{\pi}$ is a prime divisor of $\overline{p} = p$. Since these two prime divisors are not associates, they both appear in a prime factorization of p, i.e., the positive integer $a^2 + b^2 = \pi \cdot \overline{\pi}$ divides p. Since π is not a unit, $a^2 + b^2 \geq 2$. It follows that we must have $a^2 + b^2 = p$, contradicting (g).

This concludes the proof of the lemma. □

Remark. The proof of (g) $\implies$ (b) above shows that if $p \equiv 1(\mod 4)$ (equivalently, $\pi \not\sim \overline{\pi}$), then $p = \pi\overline{\pi}$.

3. Pythagorean angles

For any field F, the multiplicative group of invertible (i.e., non-zero) elements is denoted by F^*. The countable abelian group Π can be defined as the intersection $\mathbb{Q}(i)^* \cap S^1$, where S^1 is the subgroup of $\mathbb{C}^*$ consisting of numbers of unit length. We describe the structure of Π in some detail in the appendix.

An arbitrary element z of Π, that is, a Pythagorean angle, may be uniquely written as

$$z = \frac{a + bi}{c},$$

where a, b, c are pairwise relatively prime integers, c is an *odd, positive integer*, and $c^2 = a^2 + b^2$. (If c were even, the last equation would force both a and b to be even as well.) In this section we derive a variant of the well-known Euclidean parametrization of z. The proof will provide preparation for the proof of the main theorem.

Proposition 3.1. *Let z and a, b, c be as above.*

(a) (Existence): *There exist non-negative, relatively prime integers m and n and a unit $u \in \Gamma$ such that*

$$a + bi = u(m^2 - n^2 + 2mni), \tag{2}$$

$$c = m^2 + n^2. \tag{3}$$

(b) (Uniqueness): *We continue with the notation of* (a). *If $z \notin \{1, -1, i, -i\}$, then the integers m and n and the unit u are uniquely determined by z. If $z \in \{1, -1, i, -i\}$, then $z = a + bi$, and the pair m, n can equal either $1, 0$ or $0, 1$, with the unit u then determined by the equation $u = z/(m + ni)$.*

Remark. It is immediate from definitions that every complex number of the form

$$\frac{u(m^2 - n^2 + 2mni)}{m^2 + n^2} = u \cdot \frac{(m + ni)^2}{|m + ni|^2} \tag{4}$$

belongs to Π, for any integers m and n, not both 0, and any unit u.

The integers m and n in the proposition must have different parity (since c is odd). This condition is not required in this remark, but note that if m and n have the same parity, the numerator and the denominator in (4) will both be even.

Proof. (a) We have $c^2 = a^2 + b^2 = (a + bi)(a - bi)$. Since gcd $(a, b) = 1$, Lemma 2.1 implies that $(a + bi, a - bi) \in U$ or $(a + bi, a - bi) = \pm(1 \pm i)$. If the latter were true, it would follow that 2 divides $(a + bi)(a - bi) = c^2$, contradicting the fact that c is odd. Therefore, $a + bi$ and $a - bi$ are relatively prime in Γ.

We now factor into primes in Γ the principal ideals $(a + bi)\Gamma$ and $c\Gamma$:

$$(a + bi)\Gamma = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}, \tag{5}$$

$$c\Gamma = \mathfrak{q}_1^{f_1} \cdots \mathfrak{q}_s^{f_s}, \tag{6}$$

where the $\mathfrak{p}_i$'s are distinct prime ideals, as are the $\mathfrak{q}_j$'s . From the equation $c^2 = (a+bi)(a-bi)$, we get

$$\mathfrak{q}_1^{2f_1} \cdots \mathfrak{q}_s^{2f_s} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r} \overline{\mathfrak{p}}_1^{e_1} \cdots \overline{\mathfrak{p}}_r^{e_r}, \tag{7}$$

where $\overline{\mathfrak{p}}_i$ is the ideal obtained from $\mathfrak{p}_i$ by conjugating all the elements. Because $a + bi$ and $a - bi$ are relatively prime, all the $\mathfrak{p}_i$ are distinct from all the $\overline{\mathfrak{p}}_j$, so both sides of (7) give irredundant prime factorizations of the same ideal. By the uniqueness of prime factorization of ideals in Γ, we can conclude:

(a) s=2r,

(b) After relabeling the subscripts of the $\mathfrak{q}_j$'s, we have:

(i) $\mathfrak{p}_i = \mathfrak{q}_i, \quad i = 1, \ldots, r.$

(ii) $\overline{\mathfrak{p}}_i = \mathfrak{q}_{r+i}, \quad i = 1, \ldots, r.$

(iii) $2f_i = e_i, \quad i = 1, \ldots, r.$

Now consider the ideal $\mathfrak{m} = \mathfrak{p}_1^{f_1} \cdots \mathfrak{p}_r^{f_r}$. Since Γ is a PID, we may write $\mathfrak{m} = (m + ni)\Gamma$, where we may multiply the generator by a unit if necessary so as to insure that both m and n are non-negative. Thus we have

$$(a + bi)\Gamma \quad = \quad \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r} = \mathfrak{m}^2 = ((m + ni)\Gamma)^2 = (m^2 - n^2 + 2mni)\Gamma, \tag{8}$$

from which statement (a)(1) of the proposition follows immediately.

The equation $c\Gamma = \mathfrak{m}\overline{\mathfrak{m}} = (m^2 + n^2)\Gamma$ immediately implies statement (a)(2).

Finally, if the integers m and n had a common prime factor in $\mathbb{Z}$, that factor would also divide a and b, contrary to hypothesis. This concludes the proof of (a).

(b) When $z \in \{1, -1, i, -i\}$, the proof is a direct check, which we omit. So, we may suppose that $a \neq 0$ and $b \neq 0$. We let $m + ni$ be as in the proof of part (a), and we suppose that M and N are non-negative integers and v is a unit in Γ such that

$$a + bi = v((M^2 - N^2) + 2MNi).$$

Note that because $a \neq 0$ and $b \neq 0$, all the integers m, n, M, N are *strictly* positive.

We have $u(m + ni)^2 = v(M + Ni)^2$, or, setting $w = v/u$,

$$\left(\frac{m + ni}{M + Ni}\right)^2 = w.$$

We claim that $w \neq \pm i$. For if $w = i$, then, since $i = (1 + i)^2/2$,

$$\frac{m + ni}{M + Ni} = \pm\frac{1 + i}{\sqrt{2}} \notin \mathbb{Q}(i),$$

a contradiction. A similar argument applies when we suppose $w = -i$, with $1 - i$ replacing $1 + i$. Therefore,

$$(m + ni)^2 = \pm(M + Ni)^2,$$

which yields one of the following four possibilities:

$$m + ni = \begin{cases} M + Ni \\ -M - Ni \\ -N + Mi \\ N - Mi \end{cases}.$$

The last three choices all contradict our positivity condition on m, n, M, N. So $m = M$ and $n = N$. The equality $u = v$ follows immediately.

This concludes our proof of the uniqueness statement (b) and the proof of the proposition. □

4. Trisecting angles in Π

Let $Q : \mathbb{Q}(i)^* \to \mathbb{Q}(i)^*$ be the homomorphism defined by cubing: $Q(z) = z^3$, for $z \in \mathbb{Q}^*$. Q preserves elements of length 1, so $Q(\Pi) \subseteq \Pi$. Of course, every element in $Q(\Pi)$ is trisectable , i.e., $Q(\Pi) \subseteq \Pi \cap Tri$, where, we recall, Tri is the set of all trisectable angles.

Proposition 4.1. *Q is injective.*

Proof. The only cube root of unity in $\mathbb{Q}(i)^*$ is 1. □

Main Theorem. $Q(\Pi) = \Pi \cap Tri$.

Proof. It suffices to show that every $z \in \Pi \cap Tri$ is in $Q(\Pi)$. When $z \in U = \{1, -1, i, -i\}$ (which is obviously contained in $\Pi \cap Tri$), z is a cube, since Q maps U bijectively onto itself. So, for the rest of the proof, we may assume that $z = (a + bi)/c$ as in Proposition 3.1 with $a \neq 0$ and $b \neq 0$. Recall that a, b, c are pairwise relatively prime, and c is odd and positive. According to Proposition 3.1, there are unique positive integers m and n and a unique unit u in Γ such that

$$a + bi = u(m^2 - n^2 + 2mni) \tag{9}$$

$$c = m^2 + n^2. \tag{10}$$

We now use the fact that $z \in Tri$. Applying Wantzel's criterion as stated in the Introduction, we may conclude that the polynomial $x^3 - 3x - 2a/c$ has a zero in the field of rational functions of a/c, i.e., in $\mathbb{Q}$. So, let $r/s \in \mathbb{Q}$ be such a zero. We may assume that r and s are relatively prime and $s > 0$ without loss of generality. So, evaluating the polynomial at r/s, we obtain

$$\frac{r^3 - 3s^2 r}{s^3} = \frac{2a}{c}. \tag{11}$$

We apply equations (9) and (10) to (11):

$$\frac{r^3 - 3s^2 r}{s^3} = \frac{A}{m^2 + n^2}, \tag{12}$$

where

$$A = \begin{cases} \pm 2(m^2 - n^2), & \text{if } u = \pm 1, \text{ resp.} \\ \mp 4mn, & \text{if } u = \pm i, \text{ resp.} \end{cases}$$

We observe that any gcd $(A, m^2 + n^2)$ in $\mathbb{Z}$ is odd because $m^2 + n^2$ is odd. If p were an odd prime divisor of $(A, m^2 + n^2)$, we could conclude, for each of the four possible expressions for A, that p is a common divisor of m and n, a contradiction.

Therefore, both fractions appearing in equation (12) are in lowest terms, implying that

$$r^3 - 3s^2 r = A \tag{13}$$

$$s^3 = (m + ni)(m - ni)\ . \tag{14}$$

We now consider a prime power factorization of s in $\mathbb{Z}$:

$$s = p_1^{j_1} \cdots p_t^{j_t}, \tag{15}$$

where each p_i is odd because $s^3 = m^2 + n^2$ is odd. The j_i are all ≥ 1. Note that no prime p_i can be a prime in Γ because if it were, referring to the equation for s^3 above, it would have to divide either $m + ni$ or $m - ni$, hence divide both m and n, a contradiction. Therefore, by Lemma 2.2 and the subsequent remark, all the primes p_i are $\equiv 1 (\mod 4)$, and each ideal $p_i\Gamma$ factors as $\mathfrak{a}_i\overline{\mathfrak{a}}_i$, where $\mathfrak{a}_i$ and $\overline{\mathfrak{a}}_i$ are distinct prime ideals. Note, for each i, h, with $i \neq h$, we may conclude that $\mathfrak{a}_i$ is distinct from $\mathfrak{a}_h$ and $\overline{\mathfrak{a}}_h$, because $\mathfrak{a}_i \cap \mathbb{Z} = p_i\mathbb{Z}$ and $\mathfrak{a}_h \cap \mathbb{Z} = \overline{\mathfrak{a}}_h \cap \mathbb{Z} = p_h\mathbb{Z}$. So,

$$s\Gamma = \mathfrak{a}_1^{j_1} \cdots \mathfrak{a}_t^{j_t} \overline{\mathfrak{a}}_1^{j_1} \cdots \overline{\mathfrak{a}}_t^{j_t} \tag{16}$$

is an irredundant factorization into powers of prime ideals in Γ. Therefore, using equations (14) and (16), we get

$$((m + ni)\Gamma)((m - ni)\Gamma) = (s^3)\Gamma = (s\Gamma)^3 = \mathfrak{a}_1^{3j_1} \cdots \mathfrak{a}_t^{3j_t} \overline{\mathfrak{a}}_1^{3j_1} \cdots \overline{\mathfrak{a}}_t^{3j_t}, \tag{17}$$

with the right hand side an irredundant prime power factorization.

The numbers $m+ni$ and $m-ni$ are relatively prime by exactly the same argument that we used in the proof of Proposition 3.1 (a) to show that $a+bi$ and $a-bi$ are relatively prime. Therefore, referring to (17), we may, without losing generality, relabel the subscripts and, if necessary, relabel some $\mathfrak{a}_i$ as $\overline{\mathfrak{a}}_i$ and vice versa so that $\mathfrak{a}_1, \ldots, \mathfrak{a}_t$ all divide $(m+ni)\Gamma$ and $\overline{\mathfrak{a}}_1, \ldots, \overline{\mathfrak{a}}_t$ all divide $(m-ni)\Gamma$. Thus, we get

$$(m+ni)\Gamma = \mathfrak{a}_1^{3j_1} \cdots \mathfrak{a}_t^{3j_t}.$$

Since Γ is a PID, there is a non-zero $y \in \Gamma$ such that

$$y\Gamma = \mathfrak{a}_1^{j_1} \cdots \mathfrak{a}_t^{j_t},$$

and, consequently $(m+ni)\Gamma = (y\Gamma)^3 = y^3\Gamma$. This means that $m+ni = vy^3$, for some unit v. But, since Q induces an automorphism of U, $v = w^3$ for some unique $w \in U$. So, setting $x = wy \in \Gamma$,

$$m+ni = x^3 = Q(x). \tag{18}$$

We now define a homomorphism $S : \mathbb{Q}(i)^* \to \Pi$ by

$$S(\zeta) = \frac{\zeta^2}{|\zeta|^2},$$

and we apply it to equation (18):

$$\frac{m^2-n^2+2mni}{m^2+n^2} = SQ(x) = QS(x), \tag{19}$$

where we use the fact that Q and S commute.

Therefore, using equations (9) and (10), we get

$$z = \frac{a+bi}{c} = u\frac{m^2-n^2+2mni}{m^2+n^2} = uQS(x).$$

Again, since Q is bijective on U, we may write $uQS(x) = Q(u_1S(x))$, for some $u_1 \in U$, showing that $z \in Q(\Pi)$. This concludes the proof of the theorem. □

The proof of the Corollary to the Main Theorem is an easy consequence of the Main Theorem and its proof, together with Proposition 3.1.

References

[E] E. J. Eckert. *The Group of Primitive Pythagorean Triangles*, Math. Magazine, 57, n.1 (1984), pp. 22-27.

[HW] G.H.Hardy and E.M.Wright. "An Introduction to the Theory of Numbers," Sixth Edition, (2008) Oxford University Press.

[H] I.N. Herstein."Topics in Algebra," [more recent data]

[K] P. Kahn. *Trisectable and Non-trisectable Angles,* preprint, Nov. 2010, http://arxiv.org/abs/1108.2793.

[S] Th. Skolem. *On the Existence of a Multiplicative Basis for an Algebraic Number Field*, Norske Vid. Selsk Forh., 20, (1948), pp. 4-7.

[V] B.L. Van der Waerden, "Modern Algebra," [more recent data]

[W] P.L. Wantzel. *Recherches sur les moyens de reconnâitre si un Problème de Géometrie peut se résoudre avec la règle et le compas.* Journal de Mathématiques Pures et Appliquées 1 (2) (1837) 366-372.

[Z] P Zanardo and U. Zannier. *The Group of Pythagorean Triples in Number Fields*, Annali di Matematica pura ed applicata (IV), Vol. CLIX (1991), pp. 81-88.

Appendix: The group $\Pi \cap Tri$

A 1948 paper of Th. Skolem [S], deriving from work of his in 1923, is the first to present the abelian-group structure of the multiplicative group F^* of an algebraic number field F, from which the structure of Π can be easily deduced. E.Eckert [E] uses observations similar to Skolem's, together with geometric arguments, to describe a close variant of Π. P.Zanardo and U.Zannier generalize this [Z].

Here we describe the structure of Π and $\Pi \cap Tri$ based on the work in the preceding sections. Proofs using the methods of this paper can be supplied without much difficulty:

(a) The order four cyclic group U is the torsion subgroup of Π and of $\Pi \cap Tri$.
(b) Let $p_1, p_2, p_3, \ldots$ be a listing of the integer primes $\equiv 1(\mod 4)$. (There are infinitely many of these, [HW], Theorem 14.) For each p_k, we have $p_k = \pi_k \cdot \overline{\pi}_k$ (cf. the remark following Lemma 2.2), where π_k and $\overline{\pi}_k$ are non-associated primes in Γ. Set $\lambda_k = \pi_k/\overline{\pi}_k$. Then the numbers λ_k form a basis of a free-abelian subgroup A of Π, and the numbers λ_k^3 form a basis of a free-abelian subroup $B \subseteq A$.
(c) The set $\{i, \lambda_1, \lambda_2, \ldots\}$ is a basis for the direct sum $UA = \Pi$ (where we are writing these abelian groups multiplicatively, in accord with the conventions in this paper).
(d) The set $\{i, \lambda_1^3, \lambda_2^3, \ldots\}$ is a basis for the direct sum $UB = \Pi \cap Tri$.