THE DENSITY OF THE SET OF TRISECTABLE ANGLES

PETER J. KAHN

Department of Mathematics
Cornell University
Ithaca, New York 14853
December 23, 2010
Revised July 22, 2011

Abstract. It has been known for almost 200 years that some angles cannot be trisected by straightedge and compass alone. This paper studies the set of such angles as well as its complement $\mathcal{T}$, both regarded as subsets of the unit circle S^1. It is easy to show that both are topologically dense in S^1 and that $\mathcal{T}$ is contained in the countable set $\mathcal{A}$ of all angles whose cosines (or, equivalently, sines) are algebraic numbers (Corollary 3.2). Thus, $\mathcal{T}$ is a very "thin" subset of S^1. Pushing further in this direction, let K be a real algebraic number field, and let $\mathcal{T}_K$ denote the set of trisectable angles with cosines in K. We conjecture that the "computational density" of $\mathcal{T}_K$ in K is zero and prove this when K has degree ≤ 2 (cf. §1.2 and Theorem 4.1). The techniques are elementary, involving some field theory and some counting arguments.

1. Introduction

In 1837, P.L. Wantzel proved that there exist angles that cannot be trisected by strict use of straightedge and compass alone [Wan] (see also, §1.1 below for further discussion). An easy observation based on his argument (Cor. 3.2) shows that the cosine of each trisectable angle must be an algebraic number, and thus the trisectable angles comprise merely a countable subset of the unit circle S^1. This paper pushes further in the direction of showing how rare trisectable angles are. To this end, we let $\mathcal{A} \subset S^1$ be the countable set of all angles with algebraic cosines and let $\mathcal{T} \subseteq \mathcal{A}$ be the subset of trisectables. The main result of this paper (Theorem 1.1 or Theorem 4.1) provides evidence for the conjecture that $\mathcal{T}$ is a very "thin" subset of $\mathcal{A}$.

Statements of our results will be given at the end of this introduction, as will a description of how the remainder of the paper is organized. First, however, we present some context for the angle trisection problem.

1.1. **A thumbnail history of the angle trisection problem.** The classical angle trisection problem, which originated with Greek mathematicians in the 5th century B.C.E., requires that for each angle α one find a geometric procedure that starts with α and ends with $\alpha/3$. From that period on, numerous solutions to the problem have been given [Dud], many of them very ingenious. None of these, however, make exclusive use of the simple straightedge and compass, requiring instead auxiliary devices: e.g., marks on the straightedge, special curves, such as the Quadratrix of Hippias and the Conchoid of Nicomedes [Dud], and other devices, such as the "Shoemaker's knife"[Hen].

A purist strain in Greek geometry, said to originate with Plato and encoded in the axiomatics of Euclid's *Elements*, devalued the use of such auxiliary methods in geometric constructions. Hence constructions using only compass and straightedge have been called Euclidean [Dud]. What has come to be called "the angle trisection problem" in subsequent times is the problem of finding, for each α, a *Euclidean* geometric construction that starts with α and produces $\alpha/3$.

A *Euclidean geometric construction* may be described more precisely as a finite sequence of steps starting with at least two distinct points in the plane such that each step is a construction of one of the following two types: (1) If two distinct points exist at a prior step, then the line they determine or the circle centered at one of them and passing through the other may be constructed. (2) If two lines, two circles, or a line and a circle exist at a prior step, then their points of intersection, if any, may be constructed.

In this paper, all further references to constructions, trisections, trisectability, and the like, will assume the Euclidean restriction.

After many failed efforts at solving the Euclidean angle trisection problem, it became widely believed, even in Euclid's time, that a solution was impossible. However, this belief was not supported by proof.

Further progress on the Euclidean angle trisection problem was not achieved until the development of trigonometry and algebra by Arab mathematicians. Around 1430, the Arab mathematician Al-Kāshī showed that the trisectability of a given angle α is related to the solvability of a certain cubic polynomial [Hog]. Presumably, this is essentially the polynomial $q(x, b)$ described in the following paragraph, which derives from the trigonometric identity expressing $\sin(\alpha)$ in terms of $\sin(\alpha/3)$. In 1569, the Italian mathematician Rafael Bombelli independently demonstrated the same connection between trisectability and algebraic solvability [Bor]. However, with both Al Kāshī and Bombelli, the concepts of "trisectability" and "solvability" remain unclear. Neither mathematician gives an algebraic criterion for Euclidean constructibility. Nor does either specify what kind of algebraic solutions he has in mind. Finally, neither makes a claim to having proved the impossibility of solving the trisection problem. Nevertheless, despite these gaps, the connection these mathematicians obtain between

the purely geometric problem and an algebraic one was a major breakthrough that foreshadowed the ultimate solution

This solution was finally and decisively achieved by the French mathematician Pierre-Laurent Wantzel (1814-1848) [Wan], as stated at the outset of this paper. By that time, the connection between trisectability and properties of the cubic polynomial $q(x,b) = 4x^3 - 3x + b$ must have been well known, because Wantzel uses the polynomial without further comment. The parameter b represents the sine of a given angle α, and one of the roots of $q(x,b)$ is $\sin(\alpha/3)$. Wantzel demonstrates that constructible quantities must be zeros of irreducible polynomials of degree a power of two, and he uses this criterion to deduce that α is trisectable if and only if $q(x,b)$ is reducible over the field $\mathbb{Q}(b)$. (To be sure, he does not use the language of fields, since the concept of a field was not fully developed until the 1850's.) Since there are many b in the interval $[-1,1]$ for which $q(x,b)$ is *not* reducible over $\mathbb{Q}(b)$, there are, correspondingly, many angles for which there is no Euclidean trisection procedure (cf. **Corollary 2.2**).

1.2. **Some terminology, statements of results and organization of the paper.**

For technical convenience in our work and in the statements of results, we shall replace $\sin(\alpha)$ by $2\cos(\alpha)$. This amounts to replacing the polynomial $q(x,b)$ by the polynomial $p(x,a) = x^3 - 3x - a$, which we use throughout the rest of this paper. Here the parameter a represents $2\cos(\alpha)$. Wantzel's argument applies equally well to $p(x,a)$, so we can rephrase his result as: *α is trisectable if and only if $p(x,a)$ is reducible over the field $\mathbb{Q}(a)$.*

Next, we normalize our discussion by using the Cartesian plane $\mathbb{R}^2$, with its usual terminology and notation. Points in $\mathbb{R}^2$ will be called *constructible* if they can be obtained from the set of points $\{(0,0),(1,0)\}$ by a Euclidean construction. More generally, given any set $S \subseteq \mathbb{R}^2$ that contains $\{(0,0),(1,0)\}$, any point for which there is a construction starting with points in S is said to be *constructible over S*. The set of all such points will be denoted by $C(S)$. An angle α is identified in the usual way with the point $(\cos(\alpha),\sin(\alpha))$ on the unit circle S^1, which allows us to talk about *constructible angles*. α is said to be *trisectable* if $\alpha/3 \in C(\{(0,0),(1,0),\alpha\})$ [*]. Since this last relation bears no obvious connection to the relation $\alpha \in C(\{(0,0),(1,0)\})$, there is no reason to suppose that a trisectable angle need be constructible.

Some examples are in order. First note that the following angles are *constructible*: $\alpha = \pi/3$; $\beta_n = \pi/2^n$; $\gamma_n = \pi/3\cdot 2^n$; $\epsilon_n = \pi/2^n + \pi/3$. The reasons are: α is the angle in an equilateral triangle; β_n can be obtained from π, which is obviously constructible, by repeated bisection; γ_n can be obtained from α by repeated bisection; $\epsilon_n = \beta_n + \alpha$. Here, n is any non-negative integer.

[*]The notation "$\alpha/3$" here represents 1/3 of α in angular measure and should not be confused with scalar multiplication of the point α by the scalar 1/3. A similar caveat applies to the examples of angles that we give later.

Now, $\alpha = \pi/3$ is the most commonly presented example of a *non-trisectable* angle: for $2\cos(\pi/3) = 1$, and $p(x, 1)$ is easily shown to be irreducible. Therefore, we may conclude that ϵ_n is not trisectable: for if it were, then starting with ϵ_n we could construct $\epsilon_n/3 = \gamma_n + \alpha/3$, and from that we could subtract γ_n, obtaining $\alpha/3$. Since ϵ_n is constructible, we could conclude that $\alpha/3$ is constructible, hence, *a fortiori* constructible over $\{(0, 0), (1, 0), \alpha\}$, which was just shown to be impossible.

By the same arguments, we could conclude that all angles of the form $k\beta_n$ are trisectable, k an arbitrary integer, and all angles of the form $k\beta_n + \alpha$ are non-trisectable. Both these sets are countable, dense subsets of the unit circle. Of course, all of these examples are constructible.

At this point it becomes convenient to focus our attention away from the angles themselves and toward their cosines. Consider any number $a \in [-2, 2]$. We call a a *trisection number* if there is a trisectable angle α such that $a = 2\cos(\alpha)$, and we denote the set of all trisection numbers by Tri. As we show in Corollary 3.2 (and have already mentioned earlier), $Tri \subseteq \mathbb{A}$, where $\mathbb{A}$ is the set of algebraic numbers. For any real algebraic number field K, we define the *density* of $Tri \cap K$ in $[-2, 2] \cap K$ in §4, and we denote it by $\delta_K(Tri)$.

Conjecture 1. $\delta_K(Tri) = 0$.

Theorem 1.1 (Main result)**.** *Conjecture 1 is true when K is the field of rational numbers $\mathbb{Q}$ or a real quadratic field.*

Now we present a selection of other results in the paper which may be of independent interest.

The following three results in §§3.2, 3.3 give further examples of non-trisectable angles :

Corollary 3.2 *α is non-trisectable whenever* $\cos(\alpha)$ *is transcendental. Therefore,* Tri *is countable and the set of non-trisectable angles is uncountable.*

Proposition 3.2 *If a is a non-zero square in $\mathbb{Q}$, then $a \notin Tri$.*

Proposition 3.3 *Let r and s be any non-zero integers prime to each other and to* 3*. Then $p(x, 3r/s)$ is irreducible over $\mathbb{Q}$. Hence, $3r/s \notin Tri$.*

Lest the reader be left wondering whether there are any non-trisectable angles with irrational algebraic cosines, we prove the following result in Appendix C about the non-trisectable angles $\pi/3 + \pi/2^n$:

Theorem The numbers $\cos(\pi/3 + \pi/2^n)$ are algebraic of degree 2^n.

Proposition 3.4, together with its addendum, implies that *there exist a countable number of trisectable angles that are not constructible.*

Theorem 4.1 *Let K be a real number field of degree $k \leq 2$. Then*

$$\delta_K(R) \quad is \quad \mathcal{O}(R^{-\frac{2}{3}(k+1)}).$$

Here $\delta_K(R)$ counts the number of trisection numbers in K that have height $\leq R$ and divides this by the number of members of $[-2, 2] \cap K$ of height $\leq R$. See §4 for the definition of height and further notation. Using the usual definition of the big "$\mathcal{O}$" notation, it is clear that Theorem 4.1 implies Theorem 1.1.

In § 5, we estimate the number of relatively prime positive integer k-tuples $(a_1, \ldots, a_k)$ satisfying $a_i \leq n_i$, where $\mathbf{n} = (n_1, \ldots, n_k)$ is a k-tuple of positive real numbers (**Theorem 5.2)**. This generalizes a theorem of Lehmer and Sittinger [Sit]. A consequence of this theorem is an asymptotic relation, which is easier to state than the theorem itself:

$$|C(k, \mathbf{n})| \sim \frac{n_1 \cdot \ldots \cdot n_k}{\zeta(k)}.$$

The term on the left denotes the number of integer k-tuples $(a_1, \ldots, a_k)$ being counted and ζ denotes the Riemann zeta function. See § 5 for further definitions.

Finally, in Appendix A, we prove some results about n-section of angles, by which we mean a Euclidean construction that starts with an angle α and produces the angle α/n.

Theorem A.1 *Suppose n is a positive integer such that for any given angle α, there is a Euclidean construction that starts with α and ends with α/n. Then, n has the form 2^k, for some non-negative integer k.*

Therefore, for any n not a power of 2, there exist non-n-sectable angles. But can we assert, as in the case of non-trisectable angles, that, for fixed n (not a power of 2), the set of all non-n-sectable angles is dense in S^1, or similarly for the set of all n-sectable angles?

In general, this may not be so easy. However, we can assert this to be the case for special n:

Propositions A.1 and A.2: *If n is an odd positive integer such that $2\pi/n$ can be constructed (i.e., the regular polygon of n sides can be constructed), then there exists a countable dense subset of S^1 consisting of n-sectable angles and a countable dense subset of S^1 consisting of non-n-sectable angles.*

As is well known, Gauss showed that $2\pi/n$ can be constructed provided $\phi(n)$ is a power of 2. Here, ϕ denotes the Euler phi function. Among odd integers n for which Gauss's condition holds are the integers $n = 3, 5, 17, 257, 65537$.

All of the angles in these two propositions have cosines that are algebraic numbers. The transcendental case is covered by the following theorem in Appendix A, which extends Corollaries 3.1 and 3.2 of the main text.

Theorem A.2 *Suppose that $\cos(\alpha)$ is transcendental and that n is a positive integer that is not a power of 2. Then α is not n-sectable. Therefore, the set of all non-n-sectable angles is uncountable, and the set of all n-sectable angles is countable.*

The paper has three main parts. First, Sections 1 - 3 consist of background and several results that produce classes of examples of both trisectable and non-trisectable angles. Second, Sections 4 - 7 prove our main result on density (the precise version of which is Theorem 4.1). The proof involves a variety of counting and estimation arguments, including a generalization of a theorem of Lehmer. Third, the Appendix contains miscellaneous supplementary results. One section (Appendix B) shows that our main result is independent of choice of basis. Another section (Appendix A) extends some of the results of Sections 2 and 3 to the case of n-section of angles. And, finally, Appendix C shows that the algebraic number $\cos(\pi/3 + \pi/2^n)$ has degree 2^n.

At this point, I wish to thank Ravi Ramakrishna for a number of helpful conversations and suggestions. I also wish to thank George Wilson and Michael Nussbaum for their help with the Italian article on Bombelli [Bor]. Michael Nussbaum's assistance was particularly helpful in enabling me to assess Bombelli's contribution to the angle trisection problem. Finally, I wish to thank Benjamin Kahn and Kay Wagner for some interesting questions. These are answered in Theorems A.1 and A.2.

Contents

2. Basic facts about constructibility and trisectability

Most of the results described in subsections 2.1 and 2.2 are either well known or easily derivable. They are presented here as background for the reader.

2.1. **Constructible points and numbers.** The basic facts about constructible points and numbers are carefully described in various classical texts (e.g., [Wae], [Cou]), so we give only a brief outline here.

Let S be a subset of $\mathbb{R}^2$. We have already defined the set of points $C(S)$ constructible over S in §1.2. We shall now identify in the usual way the field $\mathbb{R}$ of real numbers with the set of all points in $\mathbb{R}^2$ of the form $(x, 0)$. If $S \subseteq \mathbb{R}$, then we call the elements of $C_{\mathbb{R}}(S) = C(S) \cap \mathbb{R}$ *numbers constructible over* S (or simply *constructible numbers* when $S = \{(1, 0), (0, 1)\}$).

Because the four elementary operations of arithmetic can be realized by Euclidean constructions, it follows that the sets $C(S)$ are closed under these operations, so these sets are subfields of $\mathbb{R}$. Furthermore, it follows directly from definitions that $C_{\mathbb{R}}(C_{\mathbb{R}}(S)) = C_{\mathbb{R}}(S)$. Thus, we lose no generality by assuming that S itself is already a subfield of $\mathbb{R}$. The further equality $C_{\mathbb{R}}(S) \times C_{\mathbb{R}}(S) = C(S)$ shows that we lose no information about points constructible over S by focusing on numbers constructible over S.

The field $C_{\mathbb{R}}(\mathbb{Q})$ is called the field of *constructible numbers*, and its subfields are called *constructible fields*. It follows from our comments above that if K is a constructible field, then $C_{\mathbb{R}}(\mathbb{Q}) = C_{\mathbb{R}}(K)$.

Now consider some Euclidean construction over S. By elementary plane geometry, the coordinates of each newly constructed point are zeros of polynomial equations of degree at most two, and the coefficients in each such equation are rational functions of the coordinates of points that have already been constructed over S. This description leads immediately to the following fundamental algebraic fact about constructible numbers:

Theorem 2.1. *Let K be a subfield of $\mathbb{R}$. A real number x belongs to $C_{\mathbb{R}}(K)$ (i.e., is constructible over K) if and only if there is a finite tower of real, quadratic field extensions*

$$K = K_0 \subset K_1 \subset \ldots \subset K_n,$$

such that $x \in K_n$.

It follows immediately that $C_{\mathbb{R}}(\mathbb{Q})$ is a real subfield of the field $\mathbb{A}$ of algebraic numbers.

Suppose that the real number b is constructible over the real field K and that $K = K_0 \subset \ldots \subset K_n$ is a tower as above with $b \in K_n$. Then, by Theorem 2.1, the minimal polynomial of b over K must have degree of the form 2^k for some $k \leq n$. When $K = \mathbb{Q}$, this is called the *degree of b*. Therefore, every $b \in C_{\mathbb{R}}(\mathbb{Q})$ has degree a power of 2.

2.2. **Trisectable angles.** We recall that the angle α is *trisectable* if the angle $\alpha/3$ is constructible over the set $\{(0, 0), (1, 0), \alpha\}$

We set $a = 2\cos(\alpha)$. It is easy to see that $\alpha/3$ is constructible over $\{(0, 0), (1, 0), \alpha\}$ if and only if $\cos(\alpha/3)$ is constructible over the field $\mathbb{Q}(\cos(\alpha))$ or, equivalently, $2\cos(\alpha/3)$ is constructible over the field $\mathbb{Q}(2\cos(\alpha)) = \mathbb{Q}(a)$. This second formulation is often slightly more convenient for our algebraic computations. We use either formulation without further comment.

It is possible for the angle α to be constructible without being trisectable (e.g., $\pi/3$, as mentioned in the introduction) and to be trisectable without being constructible. We give examples of the latter in §3.4.

We now invoke a standard trigonometric identity to relate the quantities $2\cos(\alpha)$ and $2\cos(\alpha/3)$:

$$2\cos(\alpha) = (2\cos(\alpha/3))^3 - 3(2\cos(\alpha/3)). \tag{1}$$

That is, using $a = 2\cos(\alpha)$, as above, $2\cos(\alpha/3)$ is a zero of the monic polynomial

$$p(x, a) = x^3 - 3x - a \in \mathbb{Q}(a)[x].$$

Theorem 2.2. *The angle α is trisectable if and only if $p(x, a)$ is reducible over the field $\mathbb{Q}(a)$, where $a = 2\cos(\alpha)$.*

As indicated in our introduction, an equivalent fact was demonstrated by Wantzel. We provide a modern version of his proof here for the reader's convenience.

Proof. $\Leftarrow$: Assume that $2\cos(\alpha/3)$ is constructible over $\mathbb{Q}(\cos(\alpha)) = \mathbb{Q}(a)$. Then , by Theorem 1, the minimal polynomial f of $2\cos(\alpha/3)$ over $\mathbb{Q}(a)$ has degree 2^n , for some integer n. Thus, the degree of f is not equal to 0 or 3. Since f divides $p(x, a)$, $p(x, a)$ is reducible in $\mathbb{Q}(a)[x]$.

$\Rightarrow$: If $p(x, a)$ is reducible over $\mathbb{Q}(a)$, it factors as the product of a linear term and a quadratic term in $\mathbb{Q}(a)[x]$. Since $2\cos(\alpha/3)$ is a zero of $p(x, a)$, by the foregoing trig identity, it must be a zero of one of the factors. Therefore, in either case, it is constructible over $\mathbb{Q}(a)$, by Theorem 1, and so α is trisectable. □

Corollary 2.3. *$\pi/3$ is not trisectable, which means that it is impossible to find a Euclidean trisection construction for each angle.*

Proof. When $\alpha = \pi/3$, we have $2\cos(\alpha) = 1$, so that $p(x, a) = x^3 - 3x - 1$. The reader can easily check by a direct computational argument that this polynomial is irreducible over $\mathbb{Q}(1) = \mathbb{Q}$. Alternatively, we give an argument that uses Eisenstein's criterion [Wae]. The polynomial $f(x) = p(x - 1, 1) = x^3 + 3x^2 - 3$ satisfies the conditions of Eisenstein's Theorem. Therefore, $f(x)$ is irreducible. It follows that $p(x, 1) = f(x + 1)$ is irreducible. Now apply the preceding theorem. □

3. Examples of trisectable and non-trisectable angles

3.1. **Multiples of π.** As we already indicated in the introduction, every integral multiple of $\pi/2^n$ is *both* trisectable *and* constructible and these form a countable, dense subset of S^1. Indeed, it is easy to see that the set of all angles that are both trisectable and constructible form a dense *subgroup* of S^1 under angle addition. It follows from Corollary 3.2 that this subgroup is countable. We do not make use of the group structure in this paper.

R. C. Yates [Yat] proves the following easy generalization of the fact that the integer multiples of $\pi/2^n$ are trisectable.

Proposition 3.1. *Suppose that the integer k is not a multiple of 3. Then every multiple of π/k is trisectable.*

Proof. Since k is relatively prime to 3, there are integers a and b such that $3a+bk = 1$. Multiply both sides of this equation by $\pi/3k$: $a(\pi/k) + b\pi/3 = \pi/3k$. Since π/k is given and $\pi/3$ is constructible, it follows that $\pi/3k$ can be constructed from π/k.† □

Suppose now that α is a constructible angle that is trisectable and β is a non-trisectable angle. Then $\alpha+\beta$ cannot be trisectable. For if it were, then, starting with β, we could construct $\alpha + \beta$, hence $(\alpha + \beta)/3$, and from that, $\beta/3$, contradicting the non-trisectability of β.

Since we have shown above that there is a countable dense subset of S^1 consisting of angles that are constructible and trisectable, and since we have seen that non-trisectable angles exist, this shows that *the set of non-trisectable angles contains a countable subset that is dense in S^1*. Shortly, we demonstrate a much stronger result.

3.2. **Trisection numbers and the countability of the set of trisectable angles.** We give further examples of non-trisectable angles. First, we restate the definition of a *trisection number* for emphasis.

Definition 1. *A* trisection number *is any real number of the form $2\cos(\alpha)$, for some trisectable angle α. We denote the set of all trisection numbers* Tri.

We begin with the following lemma.

Lemma 3.1. *Let t be an indeterminate. The polynomial $p(x,t) \in \mathbb{Q}(t)[x]$ is irreducible.*

Proof. Suppose the conclusion is false. Then $p(x,t)$ has a zero in $\mathbb{Q}(t)$, which we may write as A/B, where A and B are relatively prime polynomials in $\mathbb{Q}[t]$. The equation $p(A/B,t) = 0$ implies that $A(A^2 - 3B^2) = tB^3$, and this, in turn implies that $B|A^2$, which is impossible unless B is a unit in $\mathbb{Q}[t]$, i.e., a non-zero constant polynomial, which we may absorb in A. Therefore, $p(A,t) = 0$, which implies $A \neq 0$ and $A|t$. So, either there is a non-zero rational number c such that $A = c$ or there is a non-zero c such that $A = ct$. Either choice gives a non-trivial algebraic relation satisfied by t over $\mathbb{Q}$, $p(A,t) = 0$, which is impossible. □

See the proof of Theorem A.2 in Appendix A for an alternative proof of this lemma that uses Eisenstein's criterion.

Since $\mathbb{Q}(a) \equiv \mathbb{Q}(t)$ when a is transcendental, the following corollary is immediate:

Corollary 3.1. *$p(x,a)$ is irreducible over $\mathbb{Q}(a)$, for every transcendental a.*

†Yates gives a faulty proof of the inverse of this proposition. He succeeds only in proving that if k is a multiple of 3 *and* if π/k is constructible, then it is not trisectable

Corollary 3.2. *α is non-trisectable whenever* $\cos(\alpha)$ *is transcendental. Therefore,* Tri *is countable and the number of non-trisectable angles is uncountable.*

Proof. Let $a = 2\cos(\alpha)$ and $b = 2\cos(\alpha/3)$. We have shown that the following assertions are equivalent: α is non-trisectable; b is not constructible over $\mathbb{Q}(a)$; $p(x, a)$ is irreducible over $\mathbb{Q}(a)$. Thus, by Corollary 3.1, when a is transcendental, α is not trisectable. Therefore, *Tri* is a subset of $\mathbb{A} \cap \mathbb{R}$, and so it is countable. Since $\alpha \mapsto a$ is at most $2 - 1$ and is onto $[-2, 2]$, the set of non-trisectable α is uncountable. □

This corollary shows that to find a trisectable angle α (or rather, to find the corresponding number $2\cos(\alpha) = a$), we can require, without loss of generality, that we search for a among the *algebraic numbers. Therefore, we assume throughout the rest of this paper that a is algebraic.*

In Appendix A, we generalize Corollary 3.2 to the case of n-sectable and non-n-sectable angles, for every n that is not a power of 2.

3.3. **Non-trisectable angles with rational cosines.** We now focus on the numbers $a = 2\cos(\alpha)$ to describe some examples of non-trisectable angles. The next two results display countably many examples of *rational* $a \in [-2, 2]$ that are not trisection numbers. Contrast these with the non-trisectable angles $\frac{\pi}{3} + \frac{\pi}{2^n}$, whose cosines are constructible numbers of arbitrarily high degree over $\mathbb{Q}$ (cf. Appendix C).

Proposition 3.2. *If a is a non-zero square in $\mathbb{Q} \cap [-2, 2]$ then $a \notin$* Tri.

Proof. Let E be the projective elliptic curve whose affine equation is $y^2 = x^3 - 3x$. It is well known that the set of rational points on E form a finitely-generated abelian group of rank 0 and torsion group $\mathbb{Z}_2$ (e.g., see [Hus], pp.33-35). That is, the only rational points on E are $[0, 0, 1]$ and $[0, 1, 0]$, the point at infinity. It follows that there is no non-zero rational c such that $c^2 = x^3 - 3x$ has a rational solution. So, $p(x, c^2)$ is irreducible over $\mathbb{Q} = \mathbb{Q}(c^2)$, for all non-zero, rational c. The result now follows from Theorem 2 by restricting to non-zero, rational c such that $c^2 \leq 2$. □

Proposition 3.3. *Let r and s be any non-zero integers prime to each other and to* 3. *Then $p(x, 3r/s)$ is irreducible over $\mathbb{Q}$. Hence, no such $3r/s$ in $[-2, 2]$ belongs to Tri.*

Proof. The irreducibility of $p(x, 3r/s)$ is an immediate consequence of the Eisenstein Criterion and the Gauss Lemma. □

Remarks: a) Any real number field K (i.e., subfield of $\mathbb{R}$ of finite degree over $\mathbb{Q}$) whose integers admit unique factorization can be used in place of $\mathbb{Q}$ in this proposition, provided 3 is a prime in the ring of integers of K.

b) The foregoing results show that both $K \cap Tri$ and $(K \cap [-2, 2]) \setminus (K \cap Tri)$ are big subsets of $K \cap [-2, 2]$ for many real number fields K. In the next few sections, we show in a number of cases that $K \cap Tri$ is much the smaller of the two.

3.4. **Non-constructible trisection numbers.** We conclude with a family of examples of real number fields containing countably many trisection numbers that are not constructible. We remind the reader that these correspond to trisectable angles that are not constructible.

First, it will be convenient to make use of the polynomial function $f : \mathbb{R} \to \mathbb{R}$ given by the equation $f(x) = x^3 - 3x$, so that, for each real x and a, $p(x, a) = f(x) - a$. Set $y = f(x)$. It is easy to check that if $-2 \leq x \leq 2$ (resp, $x < -2$, $x > 2$), then $-2 \leq y \leq 2$ (resp., $y < -2$, $y > 2$). It follows immediately that $f([-2, 2]) = [-2, 2]$ (resp., $f^{-1}([-2, 2]) = [-2, 2]$, so that $f(S \cap [-2, 2]) = f(S) \cap [-2, 2]$ (resp., $f^{-1}(S \cap [-2, 2]) = f^{-1}(S) \cap [-2, 2]$) for every S. The following lemma will be useful for our later computations. We leave the easy verification to the reader.

Lemma 3.2. *Let K be any subfield of $\mathbb{R}$. Then $Tri \cap K \subseteq f(K \cap [-2, 2])$.*

The following proposition now forms the basis for the examples just mentioned.

Proposition 3.4. *Let K be a finite, constructible extension of $\mathbb{Q}$, and let F be a real, finite extension of K such that $[F : K]$ is prime to 2 and 3. Then: (a) $Tri \cap F = f(F \cap [-2, 2])$; (b) No element of $f(F \setminus K)$ is constructible. In particular, when $F \neq K$, $f(F \setminus K)$ contains a countable infinity of trisection numbers that are not constructible.*

Proof. (a) By the lemma, it suffices to prove that $Tri \cap F \supseteq f(F \cap [-2, 2])$. So, choose any $a \in f(F \cap [-2, 2]) = f(F) \cap [-2, 2]$. That is, a is in $[-2, 2]$ and is of the form $a = b^3 - 3b$, for some $b \in F$. The degree d of b over $K(a)$ divides $[K(b) : K]$, which, in turn, divides the odd number $[F : K]$. Since b is a zero of $p(x, a) \in K(a)[x]$, d cannot be greater than 3. Since it is odd and prime to 3, it must equal 1, so $K(a) = K(b)$. By construction, $p(x, a)$ is reducible over $K(b)$, so it is reducible over $K(a)$. Now, since $a \in [-2, 2]$, we may write a as $a = 2\cos(\alpha)$, for some angle α. Then $2\cos(\alpha/3)$ is a zero of $p(x, a)$ by the definition of $p(x, a)$. We now argue as in the proof of Theorem 2.2. Since $p(x, a)$ factors into the product of a linear and a quadratic polynomial over $K(a)$, and since $2\cos(\alpha/3)$ is a zero of one of these, Theorem 2.1 implies that $2\cos(\alpha/3)$ is constructible over $K(a)$.

Now let $\mathbb{Q} = L_0 < L_1 < \ldots < L_n = K$ be a tower of real quadratic extensions, which exists by the hypothesis on K. Then, $\mathbb{Q}(a) = L_0(a) \leq \ldots \leq L_n(a) = K(a)$ is a tower of real field extensions, each at most quadratic. It follows that $2\cos(\alpha/3)$ is constructible over $\mathbb{Q}(a)$, which shows that α is trisectable.

Therefore, $a = 2\cos(\alpha) \in Tri \cap F$, as required.

(b) Now suppose that $b \in F \setminus K$, and set $a = f(b)$, as above. The argument in (a) shows that $K(a) = K(b)$, so, in particular $a \notin K$. Therefore $[K(a) : K] \neq 1$. Further, $[K(a) : K]$ is odd, since it divides $[F : K]$. Therefore, by Theorem 2.1, a is not constructible over K. So it is not constructible over $\mathbb{Q}$. Since $F \cap [-2, 2] \setminus K$ is infinite, and f is at most three to one, $f(F \cap [-2, 2] \setminus K)$ is an infinite set of trisection numbers (by part (a)) none of which is constructible.

□

Addendum to Proposition 3.4: *Let K be any real number field and m any positive integer. There exists an extension F of K such that $[F : K] = m$. When m is odd, we may choose the extension to be real.*

Therefore, there exist many instances of constructible fields K and extensions F of K as described by Proposition 3.4 , i.e., the proposition is not vacuous.

We thank Ravi Ramakrishna for suggesting the following proof of the addendum, which we give in three steps.

Step 1: Let R be the ring of integers of K, and choose any proper prime ideal $\mathfrak{p} \subset R$. Let S be the localization $R_{\mathfrak{p}}$ of R at $\mathfrak{p}$, and let $\mathfrak{q}$ be the extension of $\mathfrak{p}$ to S.

Step 2: $\mathfrak{q}$ is the unique maximal ideal of the local ring S. The non-zero ideals of S are precisely the non-negative powers of $\mathfrak{q}$, all of which are distinct. Choose any $q \in \mathfrak{q} \setminus \mathfrak{q}^2$. Since S is a Dedekind domain, the ideal (q) equals a unique non-negative power of $\mathfrak{q}$, which must be the first power. Therefore, S is a principal ideal domain.

Step 3: By Step 2, we may apply Eisenstein's criterion to the polynomial $x^m - q \in S[x]$, concluding that it is irreducible. Since K is the field of fractions of S, Gauss's Lemma implies that $x^m - q$ is irreducible in $K[x]$. Letting c be any zero of $x^m - q$ (real, if m is odd), the field $F = K(c)$ satisfies the desired condition.

4. The density of $K \cap Tri$ in $K \cap [-2, 2]$: preliminaries and an overview

We have seen that the set *Tri* of trisection numbers consists of real algebraic numbers in $[-2, 2]$, i.e., $Tri \subseteq \mathbb{A} \cap \mathbb{R} \cap [-2, 2]$. As a step toward getting more information about the global structure of *Tri*, we specialize to a number field $K \subset \mathbb{A} \cap \mathbb{R}$, and we attempt to compute the density of $Tri \cap K$ in $K \cap [-2, 2]$.

4.1. **Height and density.** One way to define density in this context is to make use of a so-called *height function*

$$h_K : K \to (0, \infty).$$

The definition of h_K that we have in mind is a simplified version of what is used in Diophantine Geometry (cf. [Lan]). We begin by choosing a fixed $\mathbb{Q}$-vector space basis $\mathcal{V} = \{v_1, v_2, \ldots v_k\}$ of K.

Lemma 4.1. *Every $x \in K$ can be written uniquely as*

$$x = (a_1 v_1 + \ldots + a_k v_k)/b, \tag{2}$$

for integers $a_1, \ldots, a_k, b$ satisfying

(a) *$b > 0$ and*
(b) *$a_1, \ldots a_k, b$ have no prime factors in common.*

We leave the proof to the reader.

Then, using (2), we define

$$h_K(x) = \max\{|a_1|, \ldots, |a_k|, b\}. \tag{3}$$

For any real, positive R, the set

$$B_K(R) \stackrel{def}{=} h_K^{-1}(0, R]$$

is finite, and so, its cardinality $|B_K(R)|$ is a non-negative integer. Clearly, if $\mathcal{R}$ is any unbounded subset of $(0, \infty)$, then

$$\bigcup_{R \in \mathcal{R}} B_K(R) = K.$$

For sufficiently large R, *the density* $\delta_K(R)$ of *Tri* in $B_K(R) \cap [-2, 2]$ is defined to be the ratio

$$\delta_K(R) = \frac{|Tri \cap B_K(R) \cap [-2, 2]|}{|B_K(R) \cap [-2, 2]|}. \tag{4}$$

Alternatively, it might be called the relative frequency of occurrence of elements of Tri in $B_K(R) \cap [-2, 2]$. If the limit $\lim_{R \to \infty} \delta_K(R)$ exists, we call it the *density* of *Tri* in $K \cap [-2, 2]$, and we denote it by $\delta_K(Tri)$. It can be viewed as the probability that a randomly selected element of $K \cap [-2, 2]$ belongs to Tri. We now

Conjecture 1 (Main Conjecture) $\delta_K(Tri) = 0$.

Note that the definitions of h_K and $B_K(R)$ depend on the choice of $\mathcal{V}$. And so our density function depends on this choice. It is not hard, however, to show that the height function corresponding to another choice of basis will be commensurate to the first. This enables us to show that if Conjecture 1 holds for one choice of basis, it will hold for any other. We present some details of this discussion in Appendix B. Here we simply proceed with the definitions arising from a fixed $\mathcal{V}$.

Next, we wish to describe our computational strategy for estimating the densities (4). This will make use of some standard "estimation language," which we briefly spell out for the reader's convenience.

4.2. **Estimation.** We are interested in estimating values of real-valued functions as the arguments get large. Usually this is done for functions with some standard domain, such as the real numbers or the integers. However, we need to look at a broader class of domains. Accordingly, we let X be a locally-compact Hausdorff space with countable basis, and we let $\mathcal{F}$ denote the set of (not necessarily continuous) real-valued functions f on X such that $f^{-1}(0)$ has compact closure.

Let $f, g \in \mathcal{F}$, with $g > 0$ outside some compact set. Then f is said to be $\mathcal{O}(g)$ if the ratios $|f(x)|/g(x)$ are defined and bounded for all x outside some compact set. If f_1 is also in $\mathcal{F}$, such that $f - f_1$ is $\mathcal{O}(g)$, then we may express this by writing $f = f_1 + \mathcal{O}(g)$.

This notation has a number of simple consequences. For example:

(a) If f is $\mathcal{O}(g)$, $f_1, g_1 \in \mathcal{F}$, and if $|f_1| \leq |f|$ and $g \leq g_1$, then f_1 is $\mathcal{O}(g_1)$.
(b) If f_i is $\mathcal{O}(g_i)$, $i = 1, 2, \ldots, m$, then $f_1 \cdot f_2 \cdot \ldots \cdot f_m$ is $\mathcal{O}(g_1 \cdot g_2 \cdot \ldots \cdot g_m)$.
(c) If f_i and g_i are as in (b), and if $c_1, c_2, \ldots, c_m$ are real numbers that are not all zero, then $\Sigma_{i=1}^m c_i f_i$ is $\mathcal{O}(\Sigma_{i=1}^m |c_i| g_i)$.

Although the "big $\mathcal{O}$" notation gives only a very crude connection between the values $f(x)$ and $g(x)$ as x gets large in X, even this can sometimes be useful. For example, let us write $\lim_{x\to\infty} f(x) = L$, for some real number L, if, for each positive integer n, there is a compact subset C_n of X such that the relation $|f(x)-L| \in [0, 1/n)$ holds outside of C_n. Now suppose that f is $\mathcal{O}(g)$ and $\lim_{x\to\infty} g(x) = 0$. It then follows that $\lim_{x\to\infty} f(x) = 0$.

A more refined estimation relation, namely that of asymptotic approximation, may be defined as follows. Let f and g belong to $\mathcal{F}$. Then $f(x)/g(x)$ is defined outside some compact set, and the expression $\lim_{x\to\infty}(f(x)/g(x))$ makes sense. We say that f is asymptotic to g, written $f \sim g$, provided that $\lim_{x\to\infty} f(x)/g(x) = 1$. It is easy to check that $\sim$ defines an equivalence relation on $\mathcal{F}$.

Assuming additionally that $g > 0$ outside some compact set, it is easy to check that $f \sim g$ implies that f is $\mathcal{O}(g)$. So $\sim$ is a finer relation than big $\mathcal{O}$.

However, big $\mathcal{O}$ can be used to obtain $\sim$ under some circumstances. Namely, choose any $f, g \in \mathcal{F}$, with $g > 0$ outside some compact set, and let $f_1 = f + \mathcal{O}(g)$. Assume that $\lim_{x\to\infty}(g(x)/f(x)) = 0$. It then follows that there exist a positive constant M and a compact set $C \subseteq X$ such that

$$-Mg/f \leq 1 - f_1/f \leq Mg/f$$

outside C. This implies, first, that $f_1 \in \mathcal{F}$ and, second, that $f_1 \sim f$.

4.3. **The Computational Strategy.** Although the steps that we use in working toward a proof of Conjecture 1 are mostly of an elementary computational nature, the overall structure of the argument is intricate, and so we give here a brief overview.

4.3.1. *The numerator $|Tri \cap B_K(R) \cap [-2, 2]|$ of (4).* The set Tri appearing in the numerator of (4) is not computationally easy to work with, so we replace it by a larger set that is more computationally amenable. In particular, we use the function $f : \mathbb{R} \to \mathbb{R}$ of §4— $f(x) = x^3 - 3x$— and Lemma 1 of §4 to conclude that

$$Tri \cap B_K(R) \cap [-2, 2] \subseteq f(K) \cap B_K(R).$$

Therefore,

$$\delta_K(R) \leq \frac{|f(K) \cap B_K(R)|}{|B_K(R) \cap [-2, 2]|}. \tag{5}$$

We shall show that the right hand side of inequality (5) goes to zero as $R \to \infty$, so we do not lose anything by this replacement in our effort to prove Conjecture 1 .

4.3.2. *The key computations for the numerator of (5).* We see from equation (2) that K can be identified with the set of all integer $(k + 1)$-tuples $(a_1, \ldots, a_k, b)$ such that $b > 0$ and $a_1, \ldots, a_k, b$ are relatively prime. It is not hard to rewrite f using this identification. $B_K(R)$ has a simple description in this notation, but a description of the intersection $f(K) \cap B_K(R)$ involves $k+1$ polynomial inequalities in $a_1, a_2, \ldots, a_k, b$, and so it is fairly complex.

When k is small, specifically, when $k \leq 2$, however, we are able to use the inequalities to find a function $S : (0, \infty) \to (0, \infty)$ such that

$$S \quad \text{is} \quad \mathcal{O}(R^{1/3}) \tag{6}$$

and

$$f(K) \cap B_K(R) \subseteq f(B_K(S)). \tag{7}$$

The proof of (7) follows a similar pattern for each number field K but details and specific bounds depend on the degree and discriminant of K. These proofs will occupy all of §7.

Using the inequality for the density above, we then get

$$\begin{aligned} \delta_K(R) &\leq \frac{|f(B_K(S))|}{|B_K(R) \cap [-2,2]|} \\ &\leq \frac{|B_K(S)|}{|B_K(R) \cap [-2,2]|}. \end{aligned} \tag{8}$$

4.3.3. *The denominator* $|B_K(R) \cap [-2,2]|$. The description of $B_K(R)$ leads immediately to an estimate for $|B_K(R)|$. Indeed, as we shall see in §6.1,

$$|B_K(R)| \sim \frac{(2R)^k R}{\zeta(k+1)},$$

where ζ is the classical Riemann zeta function. This will follow by generalizing an argument of Sittinger that proves a theorem of Lehmer (cf. [Sit] and §5). This asymptotic relation implies that

$$|B_K(R)| \leq \frac{(2R)^{k+1}}{\zeta(k+1)}, \tag{9}$$

for sufficiently large R.

However, even though the subset $B_K(R) \cap [-2,2]$ is easy to describe in terms of $a_1, \ldots, a_k, b$ and the basis $\mathcal{V}$, its cardinality cannot be easily estimated. For example, we do not have good information about how the relatively prime, positive integer $k+1$-tuples are distributed throughout the subset $\mathbb{N}^{k+1} \subset \mathbb{R}^{k+1}$, where $\mathbb{N}$ is the set of natural numbers, so we cannot proceed via some sort of volume computation.

However, since our goal is a very crude estimation, we can circumvent this problem by defining a (relatively small) subset

$$Q(R) \subseteq B_K(R) \cap [-2,2], \tag{10}$$

for which we can prove that

$$|Q(R)| \sim \frac{2^k R^{k+1}}{(k+1)^{k+1} ||\mathcal{V}|| \zeta(k+1)}. \tag{11}$$

Here $||\mathcal{V}||$ is a positive constant depending only on the basis $\mathcal{V}$— in particular, *not* on R. This will occupy §6.2. It follows from (11) that

$$|Q(R)| \geq \frac{2^{k-1}R^{k+1}}{(k+1)^{k+1}||\mathcal{V}||\zeta(k+1)}, \tag{12}$$

for sufficiently large R.

Therefore, using (8), (9), (10), and (12), we have

$$\begin{aligned} \delta_K(R) &\leq \frac{|B_K(S)|}{|Q(R)|} \\ &\leq \frac{(2S)^{k+1}(k+1)^{k+1}||\mathcal{V}||}{2^{k-1}R^{k+1}} \\ &= 4||\mathcal{V}||\left(\frac{(k+1)S}{R}\right)^{k+1}. \end{aligned} \tag{13}$$

Since S is $\mathcal{O}(R^{1/3})$, by (6),

$$\left(\frac{(k+1)S}{R}\right)^{k+1} \quad \text{is} \quad \mathcal{O}(R^{-\frac{2}{3}(k+1)}), \tag{14}$$

which implies the following result.

Theorem 4.1. *Let K be a real number field of degree $k \leq 2$. Then,*

$$\delta_K(R) \quad \textit{is} \quad \mathcal{O}(R^{-\frac{2}{3}(k+1)}). \tag{15}$$

This clearly implies Theorem 1.1. We state its extension to all real number fields:

Conjecture 2. *: $\delta_K(R)$ is $\mathcal{O}(R^{-\frac{2}{3}(k+1)})$, for any real, degree k extension K of $\mathbb{Q}$.*

We now begin the proofs of the above results.

5. A generalization of Lehmer's Theorem

Choose integers k and n, with $k \geq 2$ and $n \geq 1$, and let $Q(k,n)$ be the set of all relatively prime k-tuples of positive integers $\leq n$. As before, we make use of the Riemann zeta function ζ.

Theorem 5.1 (D. Lehmer, 1900)**.** *Fix the integer k. Then*

$$|Q(k,n)| \sim \frac{n^k}{\zeta(k)}.$$

In more recent work [Sit], B.D. Sittinger has shown that

$$|Q(k,n)| = \frac{n^k}{\zeta(k)} + \mathcal{O}(f_k(n)), \tag{16}$$

where $f_k(n) = n\ln(n)$, when $k = 2$, and $f_k(n) = n^{k-1}$, when $k > 2$. Equation (16) immediately implies Theorem 5.1 (cf. §4.2).

We will generalize (16) in two ways. First, we replace n by a k-tuple $\mathbf{n} = (n_1, \ldots, n_k)$, and second, we allow each n_i to be an *arbitrary real* number ≥ 1. Let $Q(k, \mathbf{n})$ be the set of all relatively prime k-tuples of positive integers $(a_1, \ldots, a_k)$ such that each $a_i \leq n_i$, where $\mathbf{n}$ satisfies the conditions just given.

We think of $Q(k, \mathbf{n})$ as a generalized "cube" with sides of length n_i. The set $Q(k, n)$ appearing in (16) represents the case in which all side-lengths equal a given positive integer n.

It will now be convenient to introduce the notion of *eccentricity* of $Q(k, \mathbf{n})$. We define this as follows:

$$e(Q(k, \mathbf{n})) = \frac{\max\{n_1, \ldots, n_k\}}{\min\{n_1, \ldots, n_k\}}. \tag{17}$$

Clearly, $e(Q(k, \mathbf{n})) \geq 1$, with equality holding if and only if all n_i are equal. For any real number $E \geq 1$, let $\mathcal{C}_E^k$ denote the set of all $\mathbf{n} \in \mathbb{R}^k$ such that each $n_i \geq 1$ and $e(Q(k, \mathbf{n})) \leq E$. This set inherits a locally-compact topology from $\mathbb{R}^k$; we may call it the *space of k-cubes of eccentricity $\leq E$*.

Next, we let $\gamma(\mathbf{n})$ denote the geometric mean of the the n_i comprising $\mathbf{n}$, i.e.,

$$\gamma(\mathbf{n}) = (n_1 \cdot \ldots \cdot n_k)^{1/k}. \tag{18}$$

We use this to define a function $f_k(\mathbf{n})$ as follows:

$$f_k(\mathbf{n}) = \begin{cases} \gamma(\mathbf{n}) \ln(\gamma(\mathbf{n})) & : \quad k = 2 \\ \gamma(\mathbf{n})^{k-1} & : \quad k > 2. \end{cases} \tag{19}$$

Clearly this gives one reasonable way to generalize the definition of the same-named function appearing in (16).

We can now state the desired generalization:

Theorem 5.2. *Fix k and choose a real number $E \geq 1$. Then, for $\mathbf{n}$ ranging over $\mathcal{C}_E^k$, we have*

$$|Q(k, \mathbf{n})| = \frac{n_1 \cdot \ldots \cdot n_k}{\zeta(k)} + \mathcal{O}(f_k(\mathbf{n})).$$

An easy computation that follows directly from the definitions shows that

$$\lim_{\mathbf{n} \to \infty} (f_k(\mathbf{n}) / n_1 \cdot \ldots \cdot n_k) = 0.$$

According to §4.2, Theorem 5.2 then implies that

$$|C(k, \mathbf{n})| \sim \frac{n_1 \cdot \ldots \cdot n_k}{\zeta(k)}. \tag{20}$$

The remainder of this section is devoted to a proof of Theorem 5.2.

5.1. **The integral case.** We begin by proving an analog of the theorem in which $\mathbf{n}$ ranges over the integral k-tuples in $\mathcal{C}_E^k$. That is, $\mathbf{n}$ ranges over $\mathcal{C}_E^k \cap \mathbb{Z}^k$. The proof follows that of Sittinger's proof of (16), with modifications to take into account the fact that not all the n_i are equal.

To simplify the notation in the computation, we adopt the following convention: whenever we have a k-tuple of reals, say $(z_1, \ldots, z_k)$, we shall write $\pi(z_i)$ to denote the product $z_1 \cdot \ldots \cdot z_k$.

Using the inclusion-exclusion principle, we compute

(21)
$$|Q(k,\mathbf{n})| = \pi(n_i) - \sum_{p_1} \pi([n_i/p_1]) + \sum_{p_1<p_2} \pi([n_i/p_1p_2]) - \sum_{p_1<p_2<p_3} \pi([n_i/p_1p_2p_3]) + \ldots,$$

where $[\ \ ]$ denotes the greatest integer function and the p_i range over the set of primes. Note that each of the terms $[n_i/p_1 \ldots p_r]$ is zero when either r is sufficiently large or some p_i is sufficiently large. Therefore the expression on the right hand side reduces to a finite sum. As Sittinger does in his special case, we consolidate (21) by using the Möbius function μ:

$$|Q(k,\mathbf{n})| = \sum_{j=1}^{\infty} \mu(j)\pi([n_i/j]). \tag{22}$$

Clearly the summands for which $j > \min\{n_1 \ldots, n_k\}$ all vanish.We now need a lemma to help evaluate the products $\pi([n_i/j])$.

Lemma 5.1. *For any $\mathbf{x} = (x_1, \ldots, x_k)$ in $\mathcal{C}_E^k$, set*

$$\phi(\mathbf{x}) = \pi(x_i)/\min\{x_1, \ldots, x_k\}.$$

Let $\mathbf{y} = \mathbf{y}(\mathbf{x})$ be any function $\mathcal{C}_E^k \to \mathcal{C}_E^k$ satisfying $|x_i - y_i| \leq 1$ for all $i = 1, \ldots, k$. Then

$$\pi(x_i) = \pi(y_i) + \mathcal{O}(\phi(\mathbf{x})).$$

We give a proof at the end of this section.

Corollary 5.1. *Let $\mathbf{x}$ and $\mathbf{y}$ be as in Lemma 5.1. Then,*

$$\pi(x_i) = \pi(y_i) + \mathcal{O}(\gamma(\mathbf{x})^{k-1}).$$

Proof. Choose any $\mathbf{y}$ as in Lemma 5.1. The lemma implies that

$$\frac{|\pi(x_i) - \pi(y_i)|}{\phi(\mathbf{x})} \tag{23}$$

is bounded for all $\mathbf{x} \in \mathcal{C}_E^k$. Now, $\max\{x_1, \ldots, x_k\}/E \geq \gamma(\mathbf{x})/E$. Therefore, by our eccentricity assumption, $\min\{x_1, \ldots, x_k\} \geq \max\{x_1, \ldots, x_k\}/E \geq \gamma(\mathbf{x})/E$. It follows that $\phi(\mathbf{x}) \leq E\pi(x_i)/\gamma(\mathbf{x}) = E\gamma(\mathbf{x})^{k-1}$. Combining this with (23,) we conclude that

$$\frac{|\pi(x_i) - \pi(y_i)|}{\gamma(\mathbf{x})^{k-1}}$$

is bounded, as desired. □

We now return to our proof of Theorem 5.2 by applying Corollary 5.1 to the case in which

$$x_i = \frac{n_i}{j} \quad \text{and} \quad y_i = \left[\frac{n_i}{j}\right],$$

assuming that $j \leq \min\{n_1, \ldots, n_k\}$. Note that

$$\gamma(n_1/j, \ldots, n_k/j) = \gamma(n_1, \ldots, n_k)/j.$$

Therefore, 5.1 yields

$$\pi([n_i/j]) = \pi(n_i/j) + \mathcal{O}(\gamma(\mathbf{n})^{k-1}/j^{k-1}). \tag{24}$$

Feeding this into equation (22) (and recalling that we may assume that $j \leq \min\{n_1, \ldots, n_k\}$ and that the Möbius function μ assumes only the values 0 and ± 1), we get

$$\begin{aligned} |Q(k, \mathbf{n})| &= \sum_{j=1}^{m} \mu(j)\pi(n_i)/j^k + \sum_{j=1}^{m} \mu(j)(\pi([n_i/j]) - \pi(n_i/j)) \\ &= \sum_{j=1}^{m} \mu(j)\pi(n_i)/j^k + \mathcal{O}(\sum_{j=1}^{m} |\mu(j)|(\gamma(\mathbf{n})^{k-1}/j^{k-1}) \\ &= \pi(n_i) \sum_{j=1}^{m} \mu(j)/j^k + \mathcal{O}(\gamma(\mathbf{n})^{k-1} \sum_{j=1}^{m} 1/j^{k-1}), \end{aligned} \tag{25}$$

where $m = \min\{n_1, \ldots, n_k\}$.

Next, Sittinger observes that, by the definition of the zeta function,

$$\sum_{j=1}^{m} \mu(j)/j^k = 1/\zeta(k) - \sum_{j=m+1}^{\infty} \mu(j)/j^k,$$

with the tail dominated by

$$\int_m^\infty \frac{dt}{t^k} = \frac{1}{(k-1)m^{k-1}}.$$

(Recall that throughout this section, we are assuming that $k \geq 2$.)

Therefore, setting $M = \max\{n_1, \ldots, n_k\}$,

$$\begin{aligned} \pi(n_i) \sum_{j=m+1}^{\infty} \mu(j)/j^k &\leq \frac{m\pi(n_i)}{(k-1)m^k} \\ &\leq \frac{m\pi(n_i)E^k}{(k-1)M^k} \\ &\leq \frac{E^k m}{k-1} \\ &\leq \frac{E^k}{k-1} \cdot \gamma(\mathbf{n}). \end{aligned} \tag{26}$$

Next, we compute

$$\mathcal{O}(\gamma(\mathbf{n})^{k-1}\sum_{j=1}^{m} 1/j^{k-1})$$

by observing that

$$\sum_{j=1}^{m}\frac{1}{j^{k-1}} \text{ is dominated by } 1+\int_1^m \frac{dt}{t^{k-1}},$$

which is

$$\begin{cases} \mathcal{O}(\ln(\gamma(\mathbf{n})), & k=2, \\ \mathcal{O}(1), & k>2. \end{cases}$$

Therefore,

$$\mathcal{O}(\gamma(\mathbf{n})^{k-1}\sum_{j=1}^{m} 1/j^{k-1}) \quad \text{is} \quad \begin{cases} \mathcal{O}(\gamma(\mathbf{n})\ln(\gamma(\mathbf{n})), & k=2, \\ \mathcal{O}(\gamma(\mathbf{n})^{k-1}), & k>2. \end{cases} \tag{27}$$

Combining (25), (26), and (27), we obtained the desired result when $\mathbf{n}$ ranges over $\mathcal{C}_E^k \cap \mathbb{Z}^k$.

Our next task is to derive from this the result for general $\mathbf{n}$.

5.2. **The case of general real k-tuple $\mathbf{n}$.** Choose any $\mathbf{n}$ in $\mathcal{C}_E^k$ and set

$$[\mathbf{n}] = ([n_1], \ldots, [n_k]).$$

It is not hard to check that $[\mathbf{n}] \in \mathcal{C}_{2E}^k \cap \mathbb{Z}^k$.

By what was proved in the integral case,

$$|Q(k,\mathbf{m})| = \frac{\pi(m_i)}{\zeta(k)} + \mathcal{O}(f_k(\mathbf{m})),$$

for $\mathbf{m}$ ranging over $\mathcal{C}_{2E}^k \cap \mathbb{Z}^k$.

It will be convenient to reformulate this as follows: *There exists a constant H, depending only on E and k, such that*

$$|\,|Q(k,\mathbf{m})| - \frac{\pi(m_i)}{\zeta(k)}| \le H \cdot f_k(\mathbf{m}), \tag{28}$$

for $\mathbf{m}$ ranging over $\mathcal{C}_{2E}^k \cap \mathbb{Z}^k$.

Clearly, $[n_i] \le n_i$, so that $f_k([\mathbf{n}]) \le f_k(\mathbf{n})$. Further, it is immediate from the definition that $Q(k,[\mathbf{n}]) = Q(k,\mathbf{n})$. Therefore, replacing $\mathbf{m}$ by $[\mathbf{n}]$ in inequality (28) and using the foregoing observations, we get

$$|\,|Q(k,\mathbf{n})| - \frac{\pi([n_i])}{\zeta(k)}| \le H \cdot f_k(\mathbf{n}). \tag{29}$$

Finally, by Corollary 5.1, there is a constant H', depending only on k, such that

$$|\pi(n_i) - \pi([n_i])| \le H' \cdot \gamma(\mathbf{n})^{k-1}.$$

Dividing this last inequality by $\zeta(k)$, adding the result to (29) and using the definition of $f_k(\mathbf{n})$, it follows that

$$|\,|Q(k,\mathbf{n})| - \frac{\pi(n_i)}{\zeta(k)}| \leq H'' \cdot f_k(\mathbf{n}),$$

where H'' is a constant depending only on E and k. This translates to the desired statement involving big $\mathcal{O}$.

It remains to prove Lemma 5.1.

5.3. **Proof of Lemma 5.1.** We begin with the identity

$$\pi(x_i) - \pi(y_i) = \sum_{h=1}^{k} (x_h - y_h) y_1 \cdot \ldots \cdot y_{h-1} x_{h+1} \cdot \ldots \cdot x_k, \tag{30}$$

which can be proved by induction on k or by a simple algebraic manipulation. Equation (30) holds for all elements x_i, y_j in any commutative ring.

Next, since the hypothesis of the lemma states that $|x_i - y_i| \leq 1$, for all i, (30) implies that

$$|\pi(x_i) - \pi(y_i)| \leq \sum_{h=1}^{k} (1+x_1) \cdot \ldots \cdot (1+x_{h-1}) \cdot x_{h+1} \cdot \ldots \cdot x_k. \tag{31}$$

We may write

$$(1+x_1) \cdot \ldots \cdot (1+x_{h-1}) = 1 + \sigma_1^{h-1}(x_1, \ldots, x_{h-1}) + \ldots + \sigma_{h-1}^{h-1}(x_1, \ldots, x_{h-1}),$$

where σ_a^{h-1} is the a^{th} elementary symmetric function in $h-1$ variables. Therefore,

$$|\pi(x_i) - \pi(y_i)| \leq \sum_{h=1}^{k} \sum_{a=0}^{h-1} \sigma_a^{h-1}(x_1, \ldots, x_{h-1}) x_{h+1} \cdot \ldots \cdot x_k.$$

Now σ_a^{h-1} is the sum of all products of a distinct unknowns selected from the $h-1$ unknowns. So

$$\sigma_a^{h-1}(x_1, \ldots, x_{h-1}) x_{h+1} \cdot \ldots \cdot x_k$$

consists of $\binom{h-1}{a}$ terms, each of the form

$$x_{i_1} \cdot \ldots \cdot x_{i_a} \cdot x_{h+1} \cdot \ldots \cdot x_k. \tag{32}$$

Let $\{j_1, \ldots, j_b\}$ denote the complement of $\{i_1, \ldots, i_a\}$ in $\{1, 2, \ldots, h-1\}$, where $a+b = h-1$. Then, we may rewrite expression (32) as

$$\frac{x_1 \cdot \ldots \cdot x_{h-1} \cdot x_{h+1} \cdot \ldots \cdot x_k}{x_{j_1} \cdot \ldots \cdot x_{j_b}}. \tag{33}$$

Since each $x_i \geq 1$, the expression in (33) is $\leq \phi(\mathbf{x})$. Therefore,

$$\begin{aligned} |\pi(x_i) - \pi(y_i)| &\leq \sum_{h=1}^{k} \sum_{a=0}^{h-1} \binom{h-1}{a} \phi(\mathbf{x}) \\ &= \phi(\mathbf{x}) \left(\sum_{h=1}^{k} 2^{h-1} \right) \\ &= (2^k - 1)\phi(\mathbf{x}). \end{aligned}$$

This immediately implies Lemma 5.1 and, with it, completes the proof of Theorem 5.2.

6. Bounds on the numerators and denominators of the density estimate

6.1. **Estimating the cardinality of $B_K(R)$.**

Recall that $B_K(R)$ consists of all relatively prime integer $(k+1)$-tuples $(a_1, \ldots, a_k, b)$ such that each $|a_i| \leq R$ and $0 < b \leq R$. In this section, we obtain the following estimate:

$$|B_K(R)| = \frac{2^k R^{k+1}}{\zeta(k+1)} + \mathcal{O}(f_{k+1}(R)). \tag{34}$$

Since

$$\lim_{R\to\infty} \frac{f_{k+1}(R)}{R^{k+1}} = 0,$$

it follows that (cf. the last paragraph in §4.2)

$$|B_K(R)| \sim \frac{2^k R^{k+1}}{\zeta(k+1)}. \tag{35}$$

Our derivation of the estimate (34) is based on Theorem 5.2. However, that theorem refers only to tuples whose entries are positive integers. So, we must see how to include zero and negative entries into our count. To do this we first introduce some extra notation.

Let I and J be disjoint subsets of $\{1, \ldots, k\}$.

Define

$$B_K(R; I, J; k) = \left\{ (a_1, \ldots, a_k, b) \in B_K(R) : \begin{array}{lcl} a_i < 0 & \Leftrightarrow & i \in I \\ a_i = 0 & \Leftrightarrow & i \in J \\ a_i > 0 & \Leftrightarrow & \text{otherwise.} \end{array} \right\}. \tag{36}$$

In the notation of §5,

$$B_K(R; \emptyset, \emptyset; k) = Q(k+1, \mathbf{R}),$$

where $\mathbf{R}$ is the $(k+1)$-tuple $(R, \ldots, R)$.

Therefore, according to Theorem 5.2,

$$|B_K(R; \emptyset, \emptyset; k)| = \frac{R^{k+1}}{\zeta(k+1)} + \mathcal{O}(f_{k+1}(\mathbf{R})), \tag{37}$$

where

$$f_{k+1}(\mathbf{R}) = \left\{ \begin{array}{ll} R\ln(R), & k = 1 \\ R^k, & k > 1. \end{array} \right. \tag{38}$$

For each subset I, the set $B_K(R; I, \emptyset; k)$ consists entirely of relatively prime $(k+1)$-tuples $(a_1, \ldots, a_k, b)$ for which all the entries are non-zero. Since changing the sign of one or more of the a_i's does not affect their absolute values or divisibility properties, such sign changes can be used to define a bijection between any two of the $B_K(R; I, \emptyset; k)$'s. Of course, they are all pairwise disjoint. So, using equation (37), we obtain

$$|\bigsqcup_I B_K(R; I, \emptyset; k)| = \frac{2^k R^{k+1}}{\zeta(k+1)} + \mathcal{O}(f_{k+1}(\mathbf{R}), \tag{39}$$

where $\bigsqcup$ denotes the disjoint sum.

The remaining $(k+1)$-tuples in $B_K(R)$ consist of those for which some a_i's are zero. These all sit in "lower dimensional" cubes, and so their contribution gets absorbed by the big $\mathcal{O}$ notation. We make this precise as follows.

Suppose first that $k > 1$, $0 < m < k$, and J is a subset of $\{1, \ldots, k\}$ of cardinality m. Then delete the elements of J from $\{1, \ldots, k\}$, and renumber the remaining numbers, in order, using $\{1, \ldots, k-m\}$. Given any I disjoint from J as before, renumber it using the renumbering just obtained. This produces a subset I' of $\{1, \ldots, k-m\}$. These operations on indices determine a bijection between $B_K(R; I, J; k)$ and $B_K(R; I', \emptyset; k-m)$. Therefore, for any fixed, non-empty J of cardinality m, equation (39) implies that

$$|\bigsqcup_I B_K(R; I, J; k)| = \frac{2^{k-m} R^{k-m+1}}{\zeta(k-m+1)} + \mathcal{O}(f_{k-m+1}(\mathbf{R}). \tag{40}$$

If J^* is any <u>other</u> non-empty subset of $\{1, \ldots, k\}$, then $\bigsqcup_I B_K(R; I, J; k)$ and $\bigsqcup_{I^*} B_K(R; I^*, J^*; k)$ are disjoint. They have the same cardinality when $|J| = |J^*|$. Therefore, letting J range over all non-empty *proper* subsets of $\{1, \ldots, k\}$, we have

$$|\bigsqcup_{J \neq \emptyset} \bigsqcup_I B_K(R; I, J; k)| = \sum_{|J|=m=1}^{k-1} \left(\binom{k}{m} \frac{2^{k-m} R^{k-m+1}}{\zeta(k-m+1)} + \mathcal{O}(f_{k-m+1}(\mathbf{R}) \right). \tag{41}$$

We leave to the reader the check that the expression on the right is $\mathcal{O}(f_{k+1}(\mathbf{R}))$.

Now consider the case $m = k$. Then $J = \{1, \ldots, k\}$, and the only possible set I is the empty set. In this case the left-hand side of equation (40) reduces to $|B_K(R; \emptyset, J)|$. But the cube $B_K(R; \emptyset, J)$ is just the singleton set consisting of $(0, \ldots, 0, 1)$, and so, allowing the case $J = \{1, \ldots, k\}$ in the expression on the left-hand side of (41), we still get that its cardinality is $\mathcal{O}(f_{k+1}(\mathbf{R}))$

A similar special argument applies to the case $k = 1$, which we leave to the reader.

We can now conclude: Since $B_K(R)$ is precisely the disjoint union of $\bigsqcup_I B_K(R; I, \emptyset; k)$ and $\bigsqcup_{J \neq \emptyset} \bigsqcup_I B_K(R; I, J; k)$, estimate (34) follows immediately.

6.2. **Defining Q(R) and estimating its cardinality.** We recall from Section 4 that the definition of density as well as all the related concepts and computations began with a choice of basis $\mathcal{V} = \{v_1, \ldots, v_k\}$ of the field K over $\mathbb{Q}$. We made no assumptions about $\mathcal{V}$. It will now be convenient, for notational and computational simplicity, to make the assumption that each real number v_i is ≥ 1 (cf. Appendix B). Set $||\mathcal{V}|| = \pi(v_i)$ $(= v_1 \cdot \ldots \cdot v_k)$.

Define $\mathbf{m}$ and $\mathbf{n}$ in $\mathbb{R}^{k+1}$ as follows:

$$\begin{aligned} m_i = n_i &= \frac{2R}{(k+1)v_i}, \quad i = 1, \ldots, k \\ m_{k+1} &= \frac{k}{k+1}R, \\ n_{k+1} &= R. \end{aligned}$$

Then the set $Q(R)$ is defined to be the set difference

$$Q(R) = Q(k+1, \mathbf{n}) \setminus Q(k+1, \mathbf{m}), \tag{42}$$

where we use the "cubes" defined in Section 5. Since $Q(k+1, \mathbf{m}) \subseteq Q(k+1, \mathbf{n})$, we have

$$|Q(R)| = |Q(k+1, \mathbf{n})| - |Q(k+1, \mathbf{m})|. \tag{43}$$

According to Theorem 5.2 and the definition of $Q(k+1, \mathbf{n})$,

$$|Q(k+1, \mathbf{n})| = \frac{2^k R^{k+1}}{(k+1)^k ||\mathcal{V}|| \zeta(k+1))} + \mathcal{O}(f_{k+1}(\mathbf{n})). \tag{44}$$

Applying Theorem 5.2 to $|Q(k, \mathbf{m})|$, and using the fact that $f_{k+1}(\mathbf{m}) \leq f_{k+1}(\mathbf{n})$, we get, similarly, that

$$|Q(k+1, \mathbf{m})| = \frac{k 2^k R^{k+1}}{(k+1)^{k+1} ||\mathcal{V}|| \zeta(k+1)} + \mathcal{O}(f_{k+1})(\mathbf{n}), \tag{45}$$

where we think of $\mathbf{n}$ as a function of $\mathbf{m}$.

Therefore, combining (44) and (45),

$$\begin{aligned} |Q(R)| &= \frac{2^k R^{k+1}}{(k+1)^k ||\mathcal{V}|| \zeta(k+1)} - \frac{k 2^k R^{k+1}}{(k+1)^{k+1} ||\mathcal{V}|| \zeta(k+1)} + \mathcal{O}(f_{k+1}(\mathbf{n})) \\ &= \frac{2^k R^{k+1}}{(k+1)^{k+1} ||\mathcal{V}|| \zeta(k+1)} + \mathcal{O}(f_{k+1}(\mathbf{n})). \end{aligned}$$

An easy computation shows that the geometric mean $\gamma(\mathbf{n})$ is given by

$$\gamma(\mathbf{n}) = R \cdot \left(\frac{2^k}{(k+1)^k ||\mathcal{V}||} \right)^{\frac{1}{k+1}},$$

so that, setting D equal to the coefficient of R in this expression, we get

$$f_{k+1}(\mathbf{n}) = \begin{cases} DR \ln(DR), & k = 1 \\ D^k R^k, & k > 1. \end{cases}$$

Therefore, we obtain

$$|Q(R)| = \frac{2^k R^{k+1}}{(k+1)^{k+1}||\mathcal{V}||\zeta(k+1)} + \mathcal{O}(F_{k+1}(R)), \tag{46}$$

where, here, $F_{k+1}(R)$ is obtained from $f_{k+1}(\mathbf{n})$ above by deleting all reference to the constant factor D.

Again, as before, we obtain from the above big $\mathcal{O}$ relation the corresponding asymptotic relation

$$|Q(R)| \sim \frac{2^k R^{k+1}}{(k+1)^{k+1}||\mathcal{V}||\zeta(k+1)}. \tag{47}$$

6.3. Using $|Q(R)|$ as a lower bound for $|B_K(R) \cap [-2,2]|$.

Lemma 6.1. *$Q(R) \subseteq B_K(R) \cap [-2,2]$. Hence, $|Q(R)| \leq |B_K(R) \cap [-2,2]|$*

Proof. Referring to the defining equation for $Q(R)$ (equation (42)), we note that since $Q(k+1,\mathbf{n})$ is a subset of $B_K(R)$, by construction, we need only check that $(a_1,\ldots,a_k,b)$ in $Q(R)$ satisfies

$$-2 \leq \frac{a_1 v_1 + \ldots + a_k v_k}{b} \leq 2.$$

Moreover, since all the terms in the middle expression are positive, it remains only to verify the right-hand inequality.

Choose any $(a_1,\ldots,a_k,b)$ in $Q(R)$. Then, by construction,

$$0 < a_i \leq \frac{2R}{(k+1)v_i}, \quad i = 1,\ldots,k$$

and

$$\frac{k}{k+1}R < b \leq R.$$

Therefore,

$$0 < \frac{a_1 v_1 + \ldots + a_k v_k}{b} \leq \frac{\frac{2k}{k+1}R}{\frac{k}{k+1}R} = 2,$$

as desired. □

We may now use Lemma 6.1, together with the asymptotic estimate (47), to get a lower bound for $|B_K(R) \cap [-2,2]|$. In particular, choose any $\epsilon \in (0,1)$. Then,

$$|B_K(R) \cap [-2,2]| \geq \frac{2^{k-\epsilon} R^{k+1}}{(k+1)^{k+1}||\mathcal{V}||\zeta(k+1)},$$

for R sufficiently large. This is clearly a vast underestimate in general, but it will do for our purposes.

7. Proof of Theorem 4.1

Recall that Theorem 4.1 asserts that

$$\delta_K(R) \quad \text{is} \quad \mathcal{O}(R^{-\frac{2}{3}(k+1)})$$

when K is a real field of degree $k \leq 2$. As shown in Section 4, in the presence of the estimates in the preceding section, this follows from the existence of a function

$$S : (0, \infty) \to (0, \infty),$$

such that

(a) S is $\mathcal{O}(R^{\frac{1}{3}})$, and
(b) $f(K) \cap B_K(R) \subseteq f(B_K(S))$.

Recall that f here is the polynomial function given by $f(x) = x^3 - 3x$.

In this section we construct such a function S. In general, S will depend on K, although the basic form and idea of the construction will be the same for each K.

Note that a typical element in the left-hand set in b) above is of the form $f(\alpha)$ such that the height $h_K(f(\alpha))$ is $\leq R$. In order to gain usable information from this fact, we must be able to compute this height or some bound on the height in terms of the data supplied by α. The problem we initially face is that, for any $\beta \in K$, $h_K(\beta)$ is defined in terms of a canonical representation of β in terms of the selected basis $\mathcal{V}$ of K (cf. (2)). The $k+1$ integers appearing in this representation are assumed to be relatively prime. However, although this is what we may assume for the integers appearing in the representation of α, when we apply f to this representation and expand to get the result into the appropriate form, the integer coefficients we get need not be relatively prime. Our first task, therefore, is to obtain a bound on the greatest common divisor of these coefficients.

7.1. **Bounding the greatest common divisor.** When $K = \mathbb{Q}$, there is no problem. For if we choose $a/b \in \mathbb{Q}$, where a and b are relatively prime integers and $b > 0$, then $f(a/b) = (a^3 - 3b^2a)/b^3$, and it is easy to check that numerator and denominator are relatively prime. So we now turn to real fields of degree 2.

Real quadratic fields are known to be of the form $\mathbb{Q}(\sqrt{d})$, where d is any positive, square-free integer. In this case, we choose the basis $\mathcal{V}$ to be the set $\{1, \sqrt{d}\}$. $\mathcal{V}$ consists of integral elements of K, but we do not use this fact. Every α in K may be written uniquely as

$$\alpha = \frac{a_1 + a_2\sqrt{d}}{b}, \tag{48}$$

where a_1, a_2, b are relatively prime integers and $b > 0$ (cf. (2)). Now apply f to (48) to obtain

$$f(\alpha) = \alpha^3 - 3\alpha = \frac{(a_1^3 + 3da_1a_2^2 - 3a_1b^2) + (3a_1^2a_2 + da_2^3 - 3a_2b^2)\sqrt{d}}{b^3}. \tag{49}$$

In this subsection, we write the long expression as

$$\frac{A_1 + A_2\sqrt{d}}{B}$$

to simplify notation. Often, we shall use the triple (A_1, A_2, B) instead of this fraction. Let G denote the greatest common divisor (g.c.d.) of A_1, A_2, B.

Using this notation, we can express the height $h_K(f(\alpha))$ as follows:

$$h_K(f(\alpha)) = \frac{\max(|A_1|, |A_2|, B)}{G}. \tag{50}$$

Lemma 7.1. $G|8d$

Proof. Let p be a prime dividing G, and suppose that $p|a_1$. Since $p|B$, we know that $p|b$, and so we cannot also have $p|a_2$. Therefore, using $p|A_2$, we have $p|3a_1^2 + da_2^2 - 3b^2$. This implies $p|d$.

Next, suppose that $p^2|G$ and also $p|a_1$. Then, since p^2 divides $3a_1^2a_2 - 3a_2b^2$ as well as A_2, we have $p^2|da_2^3$. We still cannot have $p|a_2$ from the above argument, so $p^2|d$, which contradicts the fact that d is squarefree.

Therefore, any common prime factor p of G and a_1 must be a factor of d and occurs only to the first power in G.

Now suppose that a prime p divides G but p does not divide a_1. In this case, p divides $A_1/a_1 = a_1^2 + 3da_2^2 - 3b^2$ and also b, so p cannot divide a_2. This implies that p divides $A_2/a_2 = 3a_1^2 + da_2^2 - 3b^2$. Hence p divides both

$$a_1^2 + 3da_2^2$$

and

$$3a_1^2 + da_2^2,$$

which implies that $p|8a_1^2$, hence $p|8$. Therefore, in this case $p = 2$.

Still sticking to the case $p|G$ and $p \not| a_1$ (so $p = 2$), suppose that $2^4|G$. Since a_1 and a_2 are both odd in this case, and odd numbers represent invertible elements in the ring of integers $\mod 16$, we may divide A_1 by a_1 and A_2 by a_2 in that ring to obtain congruences

$$\begin{aligned} a_1^2 + 3da_2^2 - 3b^2 &\equiv 0 \mod 16 \\ 3a_1^2 + da_2^2 - 3b^2 &\equiv 0 \mod 16. \end{aligned}$$

By our assumption on G, we have $16|B = b^3$, which implies that $4|b$, hence $b^2 \equiv 0 \mod 16$. Therefore, the above equations become

$$\begin{aligned} a_1^2 + 3da_2^2 &\equiv 0 \mod 16 \\ 3a_1^2 + da_2^2 &\equiv 0 \mod 16. \end{aligned}$$

Subtracting the first of these from three times the second, we get

$$8a_1^2 \equiv 0 \mod 16,$$

a contradiction since a_1 is odd.

Therefore, the highest power of 2 dividing G is $\leq 2^3$.

The result is now immediate. □

Applying the lemma to equation (50), we get

Corollary 7.1.

$$h_K(f(\alpha)) \geq \frac{\max(|A_1|, |A_2|, B)}{8d}.$$

7.2. **A certain cubic curve.** The estimates that we want to make to conclude the proof of Theorem 4.1 all involve features of a certain cubic function:

$$\Phi_{D,E}(x) = D(x^3 - 3E^2x),$$

where D and E are positive real parameters.

Lemma 7.2. *Choose any real $T > 0$ and suppose that $E \leq T^{1/3}$. If $x \geq T^{1/3} + E$, then $\Phi_{D,E}(x) > DT$.*

Therefore, making use of the contrapositive, $\Phi_{D,E}(x) \leq DT \quad \Rightarrow \quad x \leq 2T^{1/3}$.

The proof is an exercise in elementary calculus and so will be omitted.

Note that since $\Phi_{D,E}$ is an odd function of x, Lemma 7.2 implies that for T and E as in the lemma,

$$\Phi_{D,E}(x) \geq -DT \quad \Rightarrow \quad x \geq -2T^{1/3}.$$

7.3. **Constructing S.** We continue with the notation of Section 7.1

7.3.1. *The case K=$\mathbb{Q}$.* . Recall that, for $a/b \in \mathbb{Q}$, a, b relatively prime and $b > 0$, we have

$$f(a/b) = \frac{a^3 - 3b^2a}{b^3} = \Phi_{1,b}(a)/b^3.$$

Therefore, applying Lemma 7.2(c), with $T = R$, $D = 1$, and $E = B$, we may conclude that if $\Phi_{1,b}(a) \leq R$ and $b \leq R^{1/3}$, then $a \leq 2R^{1/3}$. Similarly, by the remark following the lemma, if $\Phi_{1,b}(a) \geq -R$ and $b \leq R^{1/3}$, then $a \geq -2R^{1/3}$. Using the fact that the numerator and denominator in the above expression for $f(a/b)$ are relatively prime, we may interpret the foregoing as saying that

$$f(a/b) \in B_K(R) \Rightarrow a/b \in B_K(2R^{1/3}).$$

Now apply f to the right hand side of this implication to conclude that

$$f(K) \cap B_K(R) \subseteq f(B_K(2R^{1/3})).$$

This argument shows that we may define the desired function S by

$$S(R) = 2R^{1/3},$$

thus concluding the proof of Theorem 4.1 in the case $K = \mathbb{Q}$.

7.3.2. *The case of real quadratic fields.* We refer to Section 7.1 and particularly to expression (49) to point to the notation that we shall be using here.

(a) We assume throughout this part that $B \leq 8dR$ so that $b = B^{1/3} \leq (8dR)^{1/3}$, where R is an arbitrary positive real as before. (Here $8dR$ will correspond to the real number T appearing in Lemma 7.2 and b will correspond to the parameter E.)

Suppose now that $a_1 \geq (8dR)^{1/3} + b$. In particular, a_1 is positive, so we have inequality

$$A_1 = a_1^3 + 3da_1a_2^2 - 3a_1b^2 \geq a_1^3 - 3b^2a_1 = \Phi_{1,b}(a_1).$$

Using Lemma 7.2, we get the further inequality

$$\Phi_{1,b}(a_1) > 8dR.$$

Therefore, (always assuming $B \leq 8dR$), we get the implication

$$a_1 \geq (8dR)^{1/3} + b \quad \Rightarrow \quad A_1 > 8dR.$$

Using the contrapositive version of this, we conclude that we have the implication

$$A_1 = a_1^3 + 3da_1a_2^2 - 3a_1b^2 \leq 8dR \quad \Rightarrow \quad a_1 \leq (8dR)^{1/3} + b \leq 2(8dR)^{1/3}. \tag{51}$$

Similarly, using the fact that $\Phi_{1,b}(X)$ is an odd function of x, as mentioned after Lemma 7.2, we may also conclude that when $b \leq (8dR)^{1/3}$, we have the implication

$$A_1 = a_1^3 + 3da_1a_2^2 - 3a_1b^2 \geq -8dR \quad \Rightarrow \quad a_1 \geq -2(8dR)^{1/3}. \tag{52}$$

Consolidating these, we get

$$\left.\begin{array}{rcl} B & \leq & 8dR \\ |A_1| & \leq & 8dR \end{array}\right\} \quad \Rightarrow \quad |a_1| \leq 2(8dR)^{1/3}.$$

(b) We now apply a similar argument to

$$A_2 = 3a_1^2 + da_2^3 - 3a_2b^2.$$

We assume throughout this part that $B \leq 8R$. (Here $8R$ will correspond to the real number T appearing in Lemma 7.2 and $c = b/\sqrt{d}$ will correspond to the parameter E.)

Suppose that $a_2 \geq (8R)^{1/3} + c$. Of course a_2 is positive, so that we get the inequality

$$A_2 = 3a_1^2 + da_2^3 - 3a_2b^2 > da_2^3 - 3a_2b^2 = d(a_2^3 - 3c^2a_2) = \Phi_{d,c}(a_2),$$

We can now apply Lemma 7.2 again to get the further inequality

$$\Phi_{d,c}(a_2) > 8dR.$$

Thus, as above, we get an implication

$$a_2 \geq (8R)^{1/3} + c \quad \Rightarrow \quad A_2 > 8dR.$$

A similar argument yields, in the presence of the assumption $B \leq 8dR$,

$$a_2 \leq -(8R)^{1/3} - c \quad \Rightarrow \quad A_2 < -8dR.$$

Combining these two implications and passing to contrapositives, we get

$$\left.\begin{array}{rcl} B & \leq & 8dR \\ |A_2| & \leq & 8dR \end{array}\right\} \quad \Rightarrow \quad |a_2| \leq 2(8R)^{1/3} < 2(8dR)^{1/3}.$$

(c) We now wrap things up and finish the proof of Theorem 4.1.

Suppose that $f(\alpha) \in B_K(R)$. That is, $h_K(f(\alpha)) \leq R$. By equation (50) and Corollary 7.1, we get

$$\frac{\max(|A_1|, |A_2|, B)}{8d} \leq \frac{\max(|A_1|, |A_2|, B)}{G} = h_K(f(\alpha)) \leq R,$$

so that

$$\max(|A_1|, |A_2|, B) \leq 8dR.$$

The conclusions in (a) and (b) above imply that $h_K(\alpha) = \max(|a_1|, |a_2|, b) \leq 2(8dR)^{1/3}$. Therefore, $\alpha \in B_K(2(8dR)^{1/3})$, implying that $f(\alpha) \in f(B_K(2(8dR)^{1/3}))$, i.e., $f(K) \cap B_K(R) \subseteq f(B_K(2(8dR)^{1/3}))$.

The desired conclusion now follows by defining the function $S = S(R)$ by

$$S(R) = 2(8dR)^{1/3}.$$

This completes the proof of Theorem 4.1.

8. Some further comments

Several further directions are possible for the inquiry begun by this paper.

For example, one could attempt to prove Conjecture 1 for other real number fields K or for all of them. And one could attempt to prove the sharper Conjecture 2 for fields of low degree. There is also the global question, presumably substantially harder, of obtaining the density of Tri in $\mathbb{A} \cap \mathbb{R}$.

Another kind of problem would be to improve the estimates given in this paper, even for fields K of small degree. If one follows the arguments given here, it seems that what is required is further information on the "geometric" distribution of relatively prime k-tuples of integers. For example, I do not know whether the distribution is uniform throughout $\mathbb{R}^k$. Perhaps analytic number theorists have looked at this, but I do not know of any such results.

Along another line, we mentioned briefly that the set of angles that are both constructible and trisectable forms a countable subgroup of the circle group. It would be interesting to obtain further information about this group.

Finally, one might attempt to solve similar estimation problems for p-sectability, either for various specific primes p or for primes p in general. (See Appendix A below for some preliminary results in this direction.) Since the key trigonometric equations are much more complicated for $p \geq 3$, other techniques are probably required.

Appendix A. n-sectability of angles

Let n be any positive integer. The reader may naturally wonder what n-fold subdivisions are achievable for all angles via Euclidean ruler and compass construction. Of course, when n has the form 2^k, such subdivisions are always possible via iterated bisection. The case $n = 3$ was settled by P-L. Wantzel, as we have discussed in the main body of this paper. The case of general n is settled by the following theorem:

Theorem A.1. *Suppose n is a positive integer such that, for any angle α, there exists a Euclidean construction that starts with α and produces α/n, i.e., suppose that every α is n-sectable. Then, n has the form 2^k, for some non-negative integer k.*

Proof. **Case 1:** Assume that n is an odd prime. We write $n = p$.

The standard identity $(\exp(ip\theta) = \exp(i\theta)^p$ yields the following trigonometric formula:

$$cos(p\theta) = \sum_{k=0}^{q}\sum_{\ell=0}^{k}(-1)^{k+\ell}\binom{p}{2k}\binom{k}{\ell}\cos(\theta)^{p-2k+2\ell},$$

where $q = \frac{1}{2}(p-1)$. Set $a = \cos(p\theta)$ and $x = \cos(\theta)$. Then, we have an equation

$$P(x,a) = \sum_{k=0}^{q}\sum_{\ell=0}^{k}(-1)^{k+\ell}\binom{p}{2k}\binom{k}{\ell}x^{p-2k+2\ell} \; - \; a = 0. \tag{53}$$

We regard $P(x,a)$ as a polynomial in x with parameter the constant term a, analogous to the polynomial $p(x,a)$ defined in §1.2. Indeed, the explicit relationship between $P(x,a)$ and $p(x,a)$ when $n = 3$ is given by $2P(x,a) = p(2x,2a)$. We now obtain information about the coefficients of $P(x,a)$ in equation (53).

a) The top-degree monomial in $P(x,a)$ is $2^{p-1}x^p$.

To see this, we consider the summands on the right hand side of equation (53), and, holding k-fixed, we see that the maximum exponent obtainable occurs when $\ell = k$, yielding x^p. This is independent of k, so x^p is the maximum power of x occurring in the formula. This would imply that the degree of $P(x,a)$ is p, provided that the coefficients in the formula satisfying $\ell = k$ do not sum to zero.

The terms with $\ell = k$ have coefficient sum $\sum_{k=0}^{q}(-1)^{2k}\binom{p}{2k} = \sum_{k=0}^{q}\binom{p}{2k}$, which is clearly not zero. The symmetry properties of the terms $\binom{p}{2k}$ allow us to compute the sum. For consider the terms $\binom{p}{m}, m = 0,1,2,\ldots,p$. These pair off as equals $\binom{p}{m} \leftrightarrow \binom{p}{p-m}$, with m even if and only if $p-m$ is odd. It follows that $\sum_{k=0}^{q}\binom{p}{2k} = \frac{1}{2}\sum_{m=0}^{p}\binom{p}{m} = 2^{p-1}$.

This verifies that $P(x,a)$ has degree p with leading coefficient 2^{p-1}.

b) Except for the leading coefficient and the parameter a, every coefficient in $P(x,a)$ is divisible by p. Indeed the coefficient of the first-degree term is $(-1)^q p$.

The coefficient $(-1)^{k+\ell}\binom{p}{2k}\binom{k}{\ell}$ is clearly divisible by the prime p as long as $k \neq 0$. This implies the first statement. For the second statement, set $p - 2k + 2\ell = 1$. Then

it follows that $0 \leq \ell = k - \frac{1}{2}(p-1) = k - q \leq 0$. Therefore $\ell = 0$ and $k = q$, which implies that the coefficient of x in $P(x, a)$ is as stated.

We now can apply the Eisenstein criterion [Wae] to the polynomial $P(x, a)$ for appropriate choice of the parameter a. In particular, choose any integer c that is divisible by p but not by p^2, and let d be any positive integer prime to c such that that $-1 \leq c/d \leq 1$. Then $d^p P(x, c/d)$ is a polynomial in $\mathbb{Z}[x]$ whose top coefficient is not divisible by p, whose remaining coefficients are divisible by p, but whose constant term is not divisible by p^2. These are precisely the conditions under which the Eisenstein criterion implies that $d^p P(x, c/d)$ is irreducible in $\mathbb{Z}[x]$, except possibly for constant factors. It follows immediately from Gauss's Lemma that $P(x, c/d)$ is irreducible in $\mathbb{Q}[x]$.

The argument now is almost identical to the case $n = 3$ argued before. Choose α such that $\cos(\alpha) = c/d$. Then $\cos(\alpha/p)$ is a zero of $P(x, c/d)$, by equation (53) and the preceding trigonometric formula. Suppose $\cos(\alpha/p)$ were constructible over $\{(0,0), (1,0), \alpha\}$, and let f be its minimal polynomial. Then the degree of f over $\mathbb{Q}(\cos(\alpha)) = \mathbb{Q}(c/d) = \mathbb{Q}$ is divisible by a power of 2 and f is a factor of $P(x, c/d)$ in $\mathbb{Q}[x]$, contradicting the irreducibility of $P(x, c/d)$. Therefore, α/p is not constructible, concluding Case 1.

Case 2: General n. We begin with a simple general observation.

Lemma A.1. *Suppose that k is a factor of n. If α is n-sectable, then it is k-sectable.*

Proof. Write $n = k\ell$. Since α/n is constructible over $\{(1,0), (0,1), \alpha\}$, so is the multiple $\alpha/k = \ell\alpha/n$. □

Now suppose that n is not a power of 2. Then it has an odd prime factor p. Let α be an angle that is not p-sectable, which exists by Case 1. Then, by Lemma A.1, α is not n-sectable. This proves the theorem. □

Remarks: (a) The above argument can be slightly elaborated to imply that if r is a rational number strictly between 0 and 1, and if, for any given angle α, there is a Euclidean construction that starts with α and produces the angle $r\alpha$, then r must have the form $k/2^\ell$, for some integers k and ℓ, where $\ell \geq 0$. Of course, when r does have that form and any α is given, the angle $r\alpha$ can be constructed.

(b) Let α be any angle, and set $a = \cos(\alpha)$ as before. Choose any positive integer n. Then, as we have seen above $\cos(\alpha/n)$ is algebraic over $\mathbb{Q}(a)$. In particular, $\cos(\alpha/n)$ is an algebraic number whenever a is. It follows that the non-n-sectable angles α produced in the proof of Theorem A.1 have algebraic cosines.

Proposition A.1. *If n is a positive integer such that $2\pi/n$ can be constructed (i.e., the regular polygon of n sides can be constructed), then there exists a countable dense subset of S^1 consisting of n-sectable angles.*

Proof. This follows from the construction of Yates described earlier in §3.1. Namely, let m be any positive integer prime to n, and choose integers a and b such that $an + bm = 1$. Multiply this equation by the quantity $2\pi/mn$ Then, $(1/n)(2\pi/m) = a(2\pi/m) + b(2\pi/n)$, showing that $2\pi/m$ is n-sectable. The set of such angles $2\pi/m$ is clearly countable and dense in S^1. □

As is well known, Gauss showed that a necessary and sufficient condition for $2\pi/n$ to be constructible is that $\phi(n)$ be a power of 2, where ϕ is the Euler function. Examples of odd n for which this is true are: $n = 3, 5, 17, 257, 65537$.

Proposition A.2. *If n is a positive odd integer such that $2\pi/n$ can be constructed , then there exists a countable dense subset of S^1 consisting of non-n-sectable angles.*

Proof. To see this, suppose that n is an odd number such that $2\pi/n$ is constructible, and suppose that β is a non-n-sectable angle. By the argument for Proposition A.1, every integer multiple of $\pi/2^k$ is n-sectable, for any $k \geq 0$. *We claim that $\gamma = \beta + c\pi/2^k$ is not n-sectable, for every integer c and every $k \geq 0$.* The argument is essentially that given in §1.2. We give it here for the reader's convenience: Suppose γ were n-sectable. Then, starting with β we could construct γ and then γ/n. Construct $c\pi/n2^k$ and subtract this from γ/n, obtaining β/n. This would provide a Euclidean $n-$*section* of β, which is impossible. The set of all these non-n-sectable γ's is clearly countable and dense in S^1. □

If $\cos(\beta)$ above is an algebraic number—and such β exist for every n that is not a power of 2, by Remark (b) above—then it is easy to see that $\cos(\gamma)$ is algebraic. Therefore, the foregoing gives a countable dense set of non-n-sectable angles with algebraic cosines. The case of transcendental cosines is handled by the next result, which extends Corollaries 3.1 and 3.2.

Theorem A.2. *Suppose that $cos(\alpha)$ is transcendental and that n is a positive integer that is not a power of 2. Then α is not n-sectable. Therefore, the set of all non-n-sectable angles is uncountable, and the set of all n-sectable angles is countable.*

Proof. We use the notation introduced above. In particular, we use the polynomial $P(x, a)$ in (53), where $a = \cos(\alpha)$. Let $P(x, t) \in \mathbb{Q}[t]$ be the polynomial obtained from $P(x, a)$ by replacing a by the indeterminate t.

Assume first that n is an odd prime p. We claim that $P(x, t)$ is irreducible in $\mathbb{Q}[t]$. To see this, choose c/d as in Case 1 of the proof of Theorem A.1. Let χ be the $\mathbb{Q}$-algebra homomorphism that sends t to c/d, so that $\chi(P(x, t)) = P(x, c/d)$. Since $P(x, c/d)$ is irreducible, by Case 1 of the proof of Theorem A.1, $P(x, t)$ must be irreducible, as claimed.

It follows immediately that $P(x, a)$ is irreducible, because $\mathbb{Q}[t] \cong \mathbb{Q}[a]$ when a is transcendental.

We now argue as we did earlier. Since n is not a power of 2, it has an odd prime factor p. If $\cos(\alpha/p)$ is constructible over $\mathbb{Q}(a)$, then its minimal polynomial over

$\mathbb{Q}(a)$, say f, has degree a power of 2. In particular, the degree does not equal 0 or p. But $\cos(\alpha/p)$ is a zero of $P(x, a)$, so f divides $P(x, a)$, contradicting the irreducibility of $P(x, a)$.

Therefore, α is not p-sectable. Applying Lemma A.1, we conclude that α is not n-sectable.

The last two statements of the theorem simply use the standard facts about transcendental numbers and algebraic numbers. □

Appendix B. Change of basis

Let $\mathcal{V}_1 = \{v_1, \ldots, v_k\}$ and $\mathcal{V}_2 = \{w_1, \ldots, w_k\}$ be $\mathbb{Q}$-vector space bases of the real number field K, and let h_1 and h_2 be the corresponding height functions, as defined in §7.1. We show first that h_1 and h_2 are commensurate. More precisely, we show that there is a positive integer d such that

$$\frac{1}{d} h_2 \leq h_1 \leq d h_2. \tag{54}$$

Let $T = [t_{ij}]$ be the $k \times k$ matrix of rational numbers given by

$$w_j = \sum_{i=1}^{k} t_{ij} v_i, \quad j = 1, \ldots, k.$$

We say that T is *elementary* if one of the following is true: (a) T represents a permutation of the basis $\mathcal{V}_1$. (b) T represents the addition (resp., subtraction) of one basis vector of $\mathcal{V}_1$ to (resp., from) another. (c) T represents the multiplication of one basis vector of $\mathcal{V}_1$ by a non-zero rational number while fixing the others.

Of course, every product of elementary matrices is invertible. Elementary row-reduction would imply the converse, except row reduction allows a slightly richer class of elementary matrices of type (b). However, it is easy to see that these can be obtained by multiplying suitable elementary matrices of the above type. So, every invertible matrix is a product of ones that are elementary in the above sense.

Lemma B.1. *If T is an elementary matrix, then (54) holds.*

Corollary B.1. *Let h_1 and h_2 be height functions corresponding to two choices of rational bases of K. Then, there exists a positive integer d satisfying the inequalities (54).*

Proof. Let T be the change of basis matrix, factor it into a product of elementary matrices, and apply the lemma successively to these. □

It remains to prove the lemma.

Proof. (a) When T is a permutation matrix, the representations of a field element α in terms of the two bases differ only by a permutation of the coefficients. But the definition of the height function shows that it is invariant under permutation of coefficients, so that $h_1 = h_2$ in this case: i.e., the inequalities are satisfied for $d = 1$.

(b) Without loss of generality, let us assume that the basis change involves adding (resp., subtracting) v_2 to (resp. from) v_1 and fixing the other vectors. Then, writing

$$\alpha = (a_1v_1 + \ldots + a_kv_k)/b, \tag{55}$$

as in §7.1, we have

$$\alpha = (a_1w_1 + (a_2 \mp a_1)w_2 + a_3w_3 + \ldots + a_kw_k)/b.$$

It is easy to see that $a_1, \ldots, a_k, b$ are relatively prime if and only if $a_1, (a_2 \mp a_1), a_3, \ldots, a_k, b$ are relatively prime. Therefore, assuming the former,we get

$$h_2(\alpha) = \max\{|a_1|, |a_2 \mp a_1|, |a_3|, \ldots, |a_k|, b\} \leq 2\max\{|a_1|, \ldots, |a_k|, b\} = 2h_1(\alpha).$$

A symmetric argument proves the same inequality with h_1 and h_2 exchanged. Therefore (54) holds in this case with $d = 2$.

(c) Here we do not lose generality by assuming that $t_{ij} = \delta_{ij}$ (the Kronecker delta) when $(i, j) \neq (1, 1)$, and $t_{11} = t$, where t is a rational number, which can be written "in lowest terms" as $t = r/s$. Then, with α as above in (55), we may write

$$\alpha = (a_1/t)w_1 + a_2w_2 + \ldots a_kw_k)/b = ((sa_1)w_1 + (ra_2)w_2 + \ldots + (ra_k)w_k)/rb.$$

Notice that in this last representation of α, the integers $sa_1, ra_2, \ldots, ra_k, rb$ may not be relatively prime. So, we cannot apply the usual formula for the height function to these. However, if we divide all these integers by their greatest common divisor, G, then the resulting integers are relatively prime, and they do result from a representation of α. It follows that

$$h_2(\alpha) = \max\{sa_1, ra_2, \ldots, ra_k, rb\}/G. \tag{56}$$

To proceed further, we need some sort of upper bound for G. This is provided by the following claim: *G divides rs.* To see this, suppose that p is a prime dividing G and that p^m is the highest power of p dividing G. If p^m fails to divide r *and* p^m fails to divide s, then p must divide $a_1, \ldots, a_k$ and b, a contradiction. Therefore, p^m divides r, or it divides s. Hence it divides rs. It follows that $G|rs$.

We now apply this to equation (56).

$$\begin{aligned} h_2(\alpha) &\geq \max\{sa_1, ra_2, \ldots, ra_k, rb\}/|rs| \\ &\geq \min\{|r|, |s|\}\max\{|a_1|, \ldots, |a_k|, b\}/|rs| \\ &= h_1(\alpha)/\max\{|r|, |s|\}. \end{aligned}$$

Thus, the right-hand inequality in (54) holds in this last case as well, with $d = \max\{|r|, |s|\}$. A symmetric argument produces the left-hand inequality. □

Next we use Corollary B.1 to show that our conjectures and results concerning density do not depend on the choice of the basis.

If h_1 and h_2 are height functions satisfying (54), and if

$$B_i(R) = h_i^{-1}[0, R), \tag{57}$$

then Corollary B.1 implies that

$$B_1(R/d) \subseteq B_2(R) \subseteq B_1(dR). \tag{58}$$

We recall the definition of density, with respect to each height function:

$$\delta_i(R) = \frac{|Tri \cap B_i(R)|}{|[-2,2] \cap B_i(R)|}, \tag{59}$$

for $i = 1, 2$, (cf. §7.1). We shall show that $\delta_1(R)$ is $\mathcal{O}(R^{-\frac{2}{3}(k+1)}) \Leftrightarrow \delta_2(R)$ is $\mathcal{O}(R^{-\frac{2}{3}(k+1)})$.

Of course, by symmetry we need only prove one implication, say $\Rightarrow$.

Using (59) for $i = 2$, together with (58), we have

$$\delta_2(R) \leq \frac{|Tri \cap B_1(dR)|}{[-2,2] \cap B_2(R)|}.$$

Using (58) again, we get

$$\delta_2(R) \leq \frac{|Tri \cap B_1(dR)|}{[-2,2] \cap B_1(R/d)|} = \delta_1(dR) \cdot \frac{|[-2,2] \cap B_1(dR)|}{|[-2,2] \cap B_1(R/d)|}.$$

We now use the "box" $Q_1(R/d)$ constructed exactly as $Q(R)$ is constructed in §6.2, equation (41). The inclusion $Q_1(R/d) \subseteq [-2,2] \cap B_1(R/d)$ follows exactly as in Lemma 6.1, so we get

$$\delta_2(R) \leq \delta_1(dR) \cdot \frac{|B_1(dR)|}{|Q_1(R/d)|}.$$

Just as in §6, one shows that both $|B_1(dR)|$ and $|Q_1(R/d)|$ are $\mathcal{O}(R^{k+1})$. It follows that their quotient is bounded, say by M.

Thus, we have shown that $\delta_2(R) \leq M\delta_1(dR)$. From this, the desired implication is immediate.

Appendix C. Constructible non-trisection numbers of arbitrarily high degree

Since the standard examples of non-trisectable angles—namely, $\pi/3 + \pi/2^n$— are constructible, it may be of some interest to obtain information about how complicated they are to construct, by which we mean the minimal number of Euclidean ruler and compass steps it would take to construct them. This problem is certainly not well-posed, but even without going into a lengthy analysis, we can probably agree that the $\log_2$ of the algebraic degree of $\cos(\pi/3 + \pi/2^n)$ (or, $2\cos(\pi/3 + \pi/2^n)$) gives a weak lower bound. It ignores all the "rational" constructions required, but it does count the "quadratic" ones.

In this appendix we prove the following:

Proposition C.1. *The degree of* $2\cos(\pi/3 + \pi/2^n)$ *is* 2^n.

The proof is an extended exercise that uses standard trigonometric identities and well-known facts about field extensions.

C.1. **Basic identities and computations.** Define the numbers a_n, b_n, c_n, d_n as follows, for all $n \geq 0$:

$$a_n = 2\cos(\pi/2^n) \tag{60}$$

$$b_n = 2\sin(\pi/2^n) \tag{61}$$

$$c_n = 2\cos((\pi/3) + (\pi/2^n)) \tag{62}$$

$$d_n = 2\cos((\pi/3) - (\pi/2^n)) \tag{63}$$

It is easy to prove, say inductively, that these numbers are all algebraic. In fact, since the angles in question are all obviously constructible, so are their sines and cosines (and also the doubles of these). Therefore, their degrees must be powers of 2. Our task is to show that these powers are not lower than expected.

Next, we display certain standard trigonometric identities in terms of the numbers a_n, b_n, c_n, d_n. These will be used in our arguments. We also give a table of values of these numbers for $n \leq 2$.

$$a_{n-1} = a_n^2 - 2. \tag{64}$$

$$a_{n-1} = 2 - b_n^2. \tag{65}$$

$$b_{n-1} = a_n b_n. \tag{66}$$

$$c_n = \frac{1}{2}a_n - \frac{\sqrt{3}}{2}b_n. \tag{67}$$

$$d_n = \frac{1}{2}a_n + \frac{\sqrt{3}}{2}b_n. \tag{68}$$

$$d_{n-1} = 2 - c_n^2. \tag{69}$$

$$a_{n-1} = c_n d_n + 1. \tag{70}$$

$$c_{n-1} = 2 - d_n^2. \tag{71}$$

n	a_n	b_n	c_n	d_n
0	-2	0	-1	-1
1	0	2	$-\sqrt{3}$	$\sqrt{3}$
2	$\sqrt{2}$	$\sqrt{2}$	$\frac{1-\sqrt{3}}{\sqrt{2}}$	$\frac{1+\sqrt{3}}{\sqrt{2}}$

C.2. **The degrees of a_n and b_n.** In addition to $\mathbb{Q}$, it will be convenient to work with the field $K = \mathbb{Q}(\sqrt{3})$. This has class number 1. That is, its ring of integers $\mathcal{O}_K$ is a UFD. So, every irreducible in $\mathcal{O}_K$ is a prime. Eisenstein's Theorem applies to $\mathcal{O}_K$.

We define polynomials $p_n(x) \in \mathbb{Z}[x], \quad n \geq 1$:

$$\begin{aligned} p_1(x) &= x^2 - 2 \\ p_n(x) &= p_1(p_{n-1}(x)). \end{aligned}$$

Lemma C.1. *For all* $1 \leq k \leq n$,

$$\begin{aligned} p_k(a_n) &= a_{n-k} \\ p_k(b_n) &= \begin{cases} -a_{n-1}, & k = 1 \\ a_{n-k}, & k \geq 2. \end{cases} \end{aligned}$$

We omit the easy induction proof.

Lemma C.2. $p_n(x)$ *is irreducible over* $\mathbb{Q}$ *and over* K.

Proof. We show first that $p_n(x)$ has the form $x^{2^n} + 2xq(x) \pm 2$, for some $q(x) \in \mathbb{Z}[x]$. When $n = 1$ this is immediate from the definition. Assume the result for $n - 1 \geq 1$ and compute

$$p_n(x) = p_{n-1}(x)^2 - 2 = x^{2^n} + 2x(2q(x)x^{2^{n-1}} \pm 2x^{2^{n-1}-1} + 2xq(x)^2 \pm 4q(x)) + 2,$$

which has the desired form.

Now consider first the case of $\mathbb{Q}$. We use the prime $2 \in \mathbb{Z}$, and we apply Eisenstein's criterion to $p_n(x)$, which clearly satisfies it. Thus $p_n(x)$ is irreducible over $\mathbb{Q}$.

For the case $K = \mathbb{Q}(\sqrt{3})$, we use the prime $1 + \sqrt{3} \in \mathcal{O}_K$. (To see that $1 + \sqrt{3}$ is irreducible in $\mathcal{O}_K$, compute the norm $N(1 + \sqrt{3}) = (1 + \sqrt{3})(1 - \sqrt{3}) = -2$, which is prime in $\mathbb{Z}$. Since $\mathcal{O}_K$ is a UFD, $1 + \sqrt{3}$ is prime.) Again, Eisenstein's criterion is seen to be satisfied. So $p_n(x)$ is irreducible over K. □

By Lemma C.1, $p_{n-1}(a_n) = p_{n-1}(b_n) = a_1 = 0$, for $n \geq 2$. Therefore, using a direct calculation to take care of the case $n = 1$, we have:

Corollary C.1. $deg_{\mathbb{Q}}(a_n) = deg_{\mathbb{Q}}(b_n) = deg_K(a_n) = deg_K(b_n) = 2^{n-1}$, *for* $n \geq 1$.

C.3. **The fields** $F(a_n), F(b_n), F(c_n), F(d_n)$**, for** $F = \mathbb{Q}, K$**.** From identity (64), we may conclude that

$$F(a_n) < F(a_{n+1}), \tag{72}$$

for all $n \geq 0$ and $F = \mathbb{Q}$ or K. Identity (66), together with $F(a_0) = F(a_1) = F$ and Corollary C.1, allows one to prove inductively that $F(a_n) = F(b_n)$, for all n. We leave this to the reader. Using this and (72), we get

$$F(b_n) < F(b_{n+1}), \tag{73}$$

for all $n \geq 0$. Each of the extensions in (72) and (73) has degree 2, for $n \geq 1$, by Corollary C.1.

Equations (69) and (71) yield two infinite towers of field extensions

$$K = K(d_1) < K(c_2) < K(d_3) < \dots$$

and

$$K = K(c_1) < K(d_2) < K(c_3) < \dots,$$

where each extension has degree ≤ 2.

Lemma C.3. *For all $n \geq 0$, $K(c_n) = K(d_n) = K(a_n) = K(b_n)$.*

Proof. We already have the last equality. The proof of the remaining equalities is by induction on n. The cases $n = 0, 1$ are obvious, using the chart of computed values. Assume the result for $n-1$. Since, $K(a_n) = K(b_n)$, equations (67) and (68) imply that $c_n, d_n \in K(a_n)$. Thus, we have

$$K(a_{n-1}) = K(c_{n-1}) = K(d_{n-1}) < K(c_n), K(d_n) < K(a_n).$$

Therefore, since $[K(a_n) : K(a_{n-1})] = 2$, it suffices to show that $c_n, d_n \notin K(a_{n-1})$. But, if $c_n \in K(a_{n-1})$, then equation (70) would show that $d_n \in K(a_{n-1})$. So, adding identities (67) and (68), we could conclude that $a_n \in K(a_{n-1})$, which is not possible. Therefore, $c_n \notin K(a_{n-1})$. Similarly, $d_n \notin K(a_{n-1})$. This concludes the induction. □

Combining this with Corollary C.1, we get

Corollary C.2. *$deg_K(c_n) = deg_K(d_n) = 2^{n-1}$, for all $n \geq 1$.*

It remains to obtain a similar result for the field $\mathbb{Q}$.

Similarly to what we deduced above from equations (69) and (71), we have $\mathbb{Q}(c_{n-1}) < \mathbb{Q}(d_n)$ and $\mathbb{Q}(d_{n-1}) < \mathbb{Q}(c_n)$, for all $n \geq 2$. We now compute:

$$\mathbb{Q}(c_1) = \mathbb{Q}(\sqrt{3}) = K = K(c_1),$$

and, similarly, $\mathbb{Q}(d_1) = K(d_1)$. Now, assume inductively that $\mathbb{Q}(c_{n-1}) = K(c_{n-1})$ and $\mathbb{Q}(d_{n-1}) = K(d_{n-1})$. Then, we have

$$\mathbb{Q}(d_n) = \mathbb{Q}(c_{n-1})(d_n) = K(c_{n-1})(d_n) = K(d_n)$$

and

$$\mathbb{Q}(c_n) = \mathbb{Q}(d_{n-1})(c_n) = K(d_{n-1})(c_n) = K(c_n).$$

Therefore,

$$\begin{aligned} deg_{\mathbb{Q}}(c_n) &= [\mathbb{Q}(c_n) : \mathbb{Q}] \\ &= [K(c_n) : \mathbb{Q}] \\ &= [K(a_n) : \mathbb{Q}] \\ &= [K(a_n) : K][K : \mathbb{Q}] \\ &= 2^n. \end{aligned}$$

Similarly for $deg_{\mathbb{Q}}(d_n)$.

This completes the proof of Proposition 5

References

[Bor] E. Bortolotti. *La trisezione dell'angolo.* Rendiconti delle sessioni dell'Accademia delle scienze dell'Istituto di Bologna. Vol. 27. (1923) 125 -138.

[Cou] Richard Courant and Herbert Robbins. "What is Mathematics?" Thirteenth Printing. Oxford University Press. New York, London, Toronto (1967).

[Dud] Underwood Dudley. "The Trisectors." The Mathematical Association of America, Springer-Verlag (1987).

[Gui] Ivor Grattan-Guiness. "The Rainbow of Mathematics." W.W. Norton & Company, New York (1997).

[Har] Robin Hartshorne. "Geomtery: Euclid and Beyond." Springer-Verlag, New York (2000).

[Hen] David Henderson and Daina Taimina. "Experiencing Geometry," Third Edition, Pearson Prentice Hall (2005).

[Hog] J.P. Hogendijk. *Pure mathematics in Islamic Culture.* "History and Philosophy of the Mathematical Sciences, " ed. I. Grattan-Guiness. The Johns Hopkins University Press, Baltimore and London (1994) 70-84.

[Hus] Dale Husemoller. "Elliptic Curves." Springer-Verlag, New York (1986).

[Lan] Serge Lang. "Fundamentals of Diophantine Geometry." Springer-Verlag, New York (1983).

[Sit] Brian D. Sittinger. *The probability that random algebraic integers are relatively r-prime.* J. Number Theory 130 (2010) 164-171.

[Wae] B. L. van der Waerden. "Modern Algebra," Volume 1. Frederick Ungar Publishing, New York (1953).

[Wan] Pierre-Laurent 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.

[Yat] Robert C. Yates. "The Trisection Problem." The Franklin Press, Inc., Baton Rouge, La. (1942).