Points at Rational Distance from the Vertices of a Square

A thesis submitted in partial fulfillment of the requirements for the degree of Master of Science at George Mason University

By

Joseph G. Sadeq
Bachelor of Science
George Mason University, 2008

Director: Dr. Walter Morris, Professor
Department of Mathematical Sciences

Spring Semester 2015
George Mason University
Fairfax, VA

Dedication

For my family.

Acknowledgments

Special thanks to Walter Morris for his enthusiasm, patience, and time; to Jim Lawrence and Geir Agnarsson for their interest and participation; to my parents and A for their endless support; and to Arwyn for her inspiration.

Table of Contents

Abstract

POINTS AT RATIONAL DISTANCE FROM THE VERTICES OF A SQUARE

Joseph G. Sadeq, M.S.

George Mason University, 2015

Thesis Director: Dr. Walter Morris

Guy asks if there exists a point in the plane at rational distance to the corners of the unit square. Also known as the four-distance problem, we establish the equivalence of the problem to the existence of nontrivial solutions to a particular Pythagorean triple, from which we derive known conditions and establish new results. We then provide a generalization given by Barbara of the four-distance problem to regular polygons of unit side, in which a negative answer is almost always obtained.

Chapter 1: Introduction

Diophantine equations, polynomial equations in at least two variables such that only integral solutions are studied, are notorious for being simple to state, yet elusive to solve. One class of Diophantine equations specifically deals with finding points at rational distance from a given set in the plane (under the usual metric). More precisely, given a set S in the plane, a point p is said to be at *rational distance* from S provided $d(p, s_i) \in \mathbb{Q}$ for all $s_i \in S$. Moreover, a set S is said to be a rational distance set provided that all pairwise distances are rational. Although these configurations can easily be viewed geometrically, there are significant gaps in our knowledge of their structures. Several decades ago, Ulam asked if there was a set at rational distance that was dense in the plane [1], a question which not only remains unsolved, but also has had very little progress. Perhaps the only significant result related to Ulam's problem is due to Solymosi and de Zeeuw, in which they showed that no irreducible curve other than a line or a circle contains an infinite rational set [2]. In sharp contrast to Ulam's question, it is unknown if there exists even a set of 8 points in the plane in general position[1] that is at rational distance. The case of 7 points was only solved relatively recently, by Kreisel and Kurz [3].

In this paper, we focus on the following open problem posed by Guy [4]: does there exist a point in the plane at rational distance from the corners of the unit square? We will often refer to this as the *four-distance problem*. One of our main objectives is to establish the equivalence between the four-distance problem and the existence of nontrivial solutions to a particular Pythagorean triple. Guy lists some necessary conditions without proof; we derive his conditions, as well establish some new results. Using a variety of techniques, along with some of our results, we establish several cases where such a point cannot exist.

[1] A set of points is said to be in general position provided no three are collinear and no four are concyclic.

Finally, we examine a generalization given by Barbara [5] of the four-distance problem to regular polygons of unit side, in which a negative answer is obtained in almost all cases.

Chapter 2: Main Results

2.1 Representation as a Pythagorean Triple

Suppose there exists a point in the plane at rational distance from the corners of the unit square. Since scaling the configuration preserves rationality, it suffices to consider only the existence of a point at integral distance from the corners of a square with integer side length. We begin by showing that the integral distance formulation is equivalent to finding nontrivial solutions to a certain Pythagorean triple, which will provide the foundation of our analysis.

Lemma 2.1.1. *The existence of a point at integral distance from the corners of a square with side length n is equivalent to finding nontrivial integer solutions to the Pythagorean triple*

$$(a^2 - b^2 - n^2)^2 + (a^2 - c^2 - n^2)^2 = (2rn)^2$$

where $r^2 = -a^2 + b^2 + c^2$.

Proof. Let n be a positive integer. There exists a point in the plane at integral distance from the corners of a square of side length n if, and only if, there exists $(x, y) \in \mathbb{R}^2$ such that $(x-u_i)^2+(y-v_i)^2 = d_i^2$, where $(u_1, v_1) = (0, 0), (u_2, v_2) = (n, n), (u_3, v_3) = (n, 0), (u_4, v_4) = (0, n)$ and $d_i \in \mathbb{Z}$ for $1 \leq i \leq 4$.

Let $x = r\cos\theta$, $y = r\sin\theta$. Then $(r\cos\theta - u_i)^2 + (r\sin\theta - v_i)^2 = r^2\cos^2\theta - 2u_i r\cos\theta +$

$u_i^2 + r^2 \sin^2\theta - 2v_i r \sin\theta + v_i^2 = d_i^2$ determines the equations

$$r^2 = d_1^2 \tag{2.1}$$

$$-2rn\cos\theta - 2rn\sin\theta = d_2^2 - r^2 - 2n^2 \tag{2.2}$$

$$-2rn\cos\theta = d_3^2 - r^2 - n^2 \tag{2.3}$$

$$-2rn\sin\theta = d_4^2 - r^2 - n^2 \tag{2.4}$$

Moreover,

$$\begin{aligned}(2rn)^2 &= 4r^2n^2 \\ &= 4r^2n^2(\cos^2\theta + \sin^2\theta) \\ &= 4r^2n^2\cos^2\theta + 4r^2n^2\sin^2\theta = \\ &= (-2rn\cos\theta)^2 + (-2rn\sin\theta)^2 = \\ &= (d_3^2 - r^2 - n^2)^2 + (d_4^2 - r^2 - n^2)^2\end{aligned}$$

With equations (2.3) and (2.4) into (2.2) and by changing variables ($d_2 \mapsto a, d_3 \mapsto b, d_4 \mapsto c$) we have the Pythagorean triple

$$(a^2 - b^2 - n^2)^2 + (a^2 - c^2 - n^2)^2 = (2rn)^2 \tag{2.5}$$

where

$$r^2 + a^2 = b^2 + c^2 \tag{2.6}$$

□

A Pythagorean triple (or simply, *triple*) $X^2 + Y^2 = Z^2$ is said to be *primitive* provided $gcd(X, Y, Z) = 1$. Euclid showed [6] that every primitive triple is expressed as $X = u^2 - v^2, Y = 2uv, Z = u^2 + v^2$, where u and v are positive integers with $u > v$. The triple given by Euclid's formula is primitive if and only if u and v are coprime and are of opposite parity. Moreover, every primitive triple arises from a unique pair of such integers u and v.

Euclid's formula does not produce all triples; however, by adding an additional parameter k, all Pythagorean triples $X^2 + Y^2 = Z^2$ can be generated uniquely by

$$X = k(u^2 - v^2), Y = k(2uv), Z = k(u^2 + v^2) \tag{2.7}$$

where u, v and k are positive integers with $u > v$, $u - v$ odd, and gcd(u, v)=1. We shall refer to (2.7) as the parametrized form of a triple.

2.2 Preliminaries

The *three-distance problem*, that is, the existence of a point (excluding those on the lines containing the square's boundary) at rational distance to three corners of the square, is equivalent to finding nontrivial integer solutions to just (2.5). Although previously thought to not be possible, Conway and Guy [7] found an infinite number of solutions. Additionally, Berry gives some parametric families of solutions [8]. For the fourth distance to be an integer, condition (2.6) is required; this arises from incorporating equations (2.3) and (2.4) into (2.2). For the purposes of this paper, any reference to a (nontrivial) solution to the four-distance problem is one such that (2.5) and (2.6) are both satisfied.

Since the existence of a point $(x, y) \in \mathbb{R}^2$ at rational distance to the corners of the unit square is equivalent to the existence of a solution $(n, a, b, c, r) \in \mathbb{Z}^5$ to (2.5) and (2.6), we are free to employ either form as being a representation of the same solution.

Henceforth, in our attempt to characterize the set of solutions, we assume that there is no common factor of n, a, b, c, r in equations (2.5) and (2.6); by translation, we may assume

the square lies in the first quadrant; and by symmetry of the square, we may consider only the solutions that arise from (x, y) lying in the first quadrant of the plane.

2.3 Basic Properties

Having transformed the problem into a more algebraic representation, we begin our analysis by describing the parities of the solution set.

Theorem 2.3.1. *n is even, and all of a, b, c, r are odd (assuming that there is no common factor).*

Proof. From (2.5), denote $A = (a^2 - b^2 - n^2)$, $B = (a^2 - c^2 - n^2)$, $C = (2rn)$. We first note that since C is even, A and B are either both odd or both even. More specifically, as $C^2 \equiv 0 \pmod 4$, A and B are both even, otherwise $A^2 + B^2 \equiv 2 \pmod 4$. Since A and B are both even, k is a multiple of 2, where k is as found in the parametrized form of $A^2 + B^2 = C^2$ by (2.7). Without loss of generality, we may further suppose $A = k(u^2 - v^2)$. Thus, $C - A = k(u^2 + v^2) - k(u^2 - v^2) = k2v^2$, and therefore $4|(C - A)$.

Suppose n is odd. Then either a is even with b and c odd, or a is odd with b and c even. Let a be even. Then $a = 2k, b = 2f + 1, c = 2j + 1, n = 2h + 1$, where $k, f, j, h \in \mathbb{Z}$. Write $C - A = 2rn - (a^2 - b^2 - n^2) = 2rn - a^2 + b^2 + n^2 = 2rn - 4k^2 + 4f^2 + 4f + 1 + 4h^2 + 4h + 1$. Therefore $4|(2rn + 2) = 2(rn + 1)$, and so rn is odd. But a even with b and c odd implies r^2 is even, by (2.6), and so rn is even. Contradiction.

Next, suppose a is odd. Then $a = 2k + 1, b = 2f, c = 2j, n = 2h + 1$. Again, write $C - A = 2rn - 4k^2 - 4k - 1 + 4f^2 + 4h^2 + 4h + 1$. Therefore $4|2rn$, thus rn is even. But a odd with b, c even implies r^2 is odd, and so rn is odd. Contradiction.

Therefore n is even. Moreover, a, b, c all have the same parity, therefore a, b, c (and thus r) are all odd, since otherwise all five would have a common factor. The result follows.

□

Theorem 2.3.2. *n is divisible by 4.*

Proof. Since $A = a^2 - b^2 - n^2$ and $B = a^2 - c^2 - n^2$ are multiples of 4, and $a^2 - b^2$ and $a^2 - c^2$ are multiples of 8, it follows that $\frac{A}{4}$ and $\frac{B}{4}$ are of the same parity. This implies that $\frac{C}{4}$ is even, which means that n is a multiple of 4 since r is odd.

□

Proposition 2.3.1. *For any Pythagorean triple $x^2+y^2 = z^2$, at least one of x, y is divisible by 3.*

Proof. Note that squares modulo 3 are equal to either 0 or 1. Suppose neither x nor y is divisible by 3. Then $x^2 + y^2 \equiv 2 \pmod 3$. But $z^2 \equiv 0$ or $1 \pmod 3$. Contradiction. □

Proposition 2.3.2. *If n is not a multiple of 3, then exactly two of a, b, c, r are divisible by 3.*

Proof. Suppose n is not a multiple of 3. First, suppose all four of a, b, c, r are divisible by 3. By Proposition 2.3.1, $3|(a^2 - b^2 - n^2)$ or $3|(a^2 - c^2 - n^2)$. In either case, $3|n$. Next, by (2.6), any three that are divisible by 3 implies the fourth must be too. If only one is divisible by 3, then (2.6) yields $1 \equiv 2 \pmod 3$. Finally, suppose none of a, b, c, r are divisible by 3. Without loss of generality, suppose $3|(a^2 - b^2 - n^2)$. Then $a^2 - b^2 - n^2 \equiv 1 - 1 - n^2 \equiv 0 \pmod 3$, which implies $3|n$. Since each case yields a contradiction, exactly two of a, b, c, r are divisible by 3. □

Proposition 2.3.3. *For any Pythagorean triple $x^2 + y^2 = z^2$, at least one of x, y, z is divisible by 5.*

Proof. Note that squares modulo 5 are equal to 0, 1, or 4. Suppose none of x, y, z is divisible by 5. Then $x^2 + y^2 = z^2$ becomes $\{1, 4\} + \{1, 4\} \equiv \{1, 4\} \pmod 5$, where the $\{1, 4\}$ denotes that a 1 or a 4 may be taken. A quick check shows that this equation is not solvable.

□

The following proposition is analogous to Proposition 2.3.2.

Proposition 2.3.4. *If n is not a multiple of 5, then exactly two of a, b, c, r are divisible by 5.*

Proof. Suppose n is not a multiple of 5. If none of a, b, c, r are divisible by 5, then $5|(a^2 - b^2 - n^2)$ or $5|(a^2 - c^2 - n^2)$, by Proposition 2.3.3. In either case, $\{1, 4\} - \{1, 4\} \not\equiv \{1, 4\} \pmod 5$.

Suppose only one of a, b, c, r is divisible by 5. Then looking at $r^2 + a^2 = b^2 + c^2$ modulo 5, we have $\{1, 4\} + \{1, 4\} \equiv \{1, 4\} \pmod 5$, which is not possible.

Suppose 5 divides three of a, b, c, r. Then by $r^2 + a^2 = b^2 + c^2$, 5 must divide all four. Contradiction.

Finally, suppose 5 divides all of a, b, c, r. Then both $(a^2 - b^2 - n^2)^2$ and $(a^2 - c^2 - n^2)^2$ are congruent to 1 modulo 5. Therefore $1 + 1 \equiv 0 \pmod 5$. Contradiction.

□

2.4 Sums of Squares

Before continuing, we introduce some algebraic properties of integers that can be expressed as the sum of two squares. Recall that the ring of Gaussian integers $\mathbb{Z}[i]$ is a generalization of the integers in which the property of unique prime factorization still holds. $\mathbb{Z}[i]$ is particularly useful here as it allows us to factor a sum of two integer squares into linear factors. We make use of only some elementary properties of the Gaussian integers. For more information about the Gaussian integers, we invite the reader to refer to a text on abstract algebra such as [9].

Definition 2.4.1. *For $z = a + bi \in \mathbb{Z}[i]$, the conjugate of z is $\bar{z} = a - bi$, and the norm is*

$$N(z) = |z|^2 = z\bar{z} = a^2 + b^2.$$

Moreover, the norm is multiplicative; that is, $N(wz) = N(w)N(z)$, for all $w, z \in \mathbb{Z}[i]$.

Definition 2.4.2. *An element $z = a + bi \in \mathbb{Z}[i]$ is called a unit if there is some $w \in \mathbb{Z}[i]$ such that $zw = wz = 1$.*

An element z is a unit in $\mathbb{Z}[i]$ if and only if $N(z) = \pm 1$.

Definition 2.4.3. *Suppose $z = a + bi \in \mathbb{Z}[i]$ is nonzero and is not a unit. Then z is called irreducible if whenever $z = xy$ with $x, y \in \mathbb{Z}[i]$, at least one of x or y must be a unit in $\mathbb{Z}[i]$. Otherwise z is said to be reducible.*

Definition 2.4.4. *A nonzero element $z = a + bi \in \mathbb{Z}[i]$ is said to be prime if and only if it is irreducible.*

Lemma 2.4.1. *Let n be an integer. If $n \equiv 3 \pmod 4$, then n is not the sum of two squares.*

Proof. Suppose $n = a^2 + b^2$. Note that squares modulo 4 are equal to either 0 or 1. Then $n \equiv 0$, 1, or 2 $\pmod 4$. □

Lemma 2.4.2. *Let p be a prime in $\mathbb{Z}$ of the form $4k + 3$. Then p is prime in $\mathbb{Z}[i]$.*

Proof. Suppose $p \equiv 3 \pmod 4$ is a prime. Then $N(p) = p\bar{p} = p^2$. If p were not irreducible, then there exists a factor $a + bi$ such that $N(a + bi) = a^2 + b^2 = p$. But by the previous lemma, p cannot be the sum of two squares. □

Lemma 2.4.3. *Let p be a prime factor of $a^2 + b^2$. If $p \equiv 3 \pmod 4$, then $p|a$ and $p|b$.*

Proof. Let p be a prime factor of $a^2 + b^2 = (a + bi)(a - bi)$. By Lemma 2.4.2, p is prime in $\mathbb{Z}[i]$, and so $p|(a + bi)$ or $p|(a - bi)$. Assume $p|(a + bi)$. Then $a + bi = p(c + di)$ for some $c, d \in \mathbb{Z}$, that is, $a = pc$ and $b = pd$. Therefore, $p|a$ and $p|b$. □

2.5 Prime Divisors

Lemma 2.4.3 plays an important role in further characterizing solutions to (2.5) and (2.6). In particular, we can now generalize the divisibility by certain prime divisors.

Theorem 2.5.1. *Let p be a prime of form $4k+3$. If $p|n$, then none of a, b, c, r are divisible by p. Similarly, if $q|r$, where q is a prime of form $4j+3$, then none of a, b, c, n are divisible by q.*

Proof. If $p|n$ or $p|r$, then $p|(2rn)^2$, so by Lemma 2.4.3, $p|(\mathrm{a}^2 - b^2 - n^2)$ and $p|(\mathrm{a}^2 - c^2 - n^2)$.

Suppose $p|n$. If $p|a$, then p divides both b and c, which implies p divides r, contradicting there being no common factor to a, b, c, r, n. The cases in which $p|b$ and $p|c$ are analogous. The case in which $p|r$ is handled similarly, noting that $(a^2 - b^2 - n^2)$ and $(a^2 - c^2 - n^2)$ can be expressed as $(c^2 - r^2 - n^2)$ and $(b^2 - r^2 - n^2)$, respectively.

Next, suppose $q|r$. Again, express $(a^2 - b^2 - n^2) = (c^2 - r^2 - n^2)$ and $(a^2 - c^2 - n^2) = (b^2 - r^2 - n^2)$. If $q|n$, then by Lemma 2.4.3, $q|b$ and $q|c$, and therefore $q|a$. Contradiction. The cases in which q divides b or c are handled similarly. If $q|a$, then $q|(b^2 + n^2)$, since $q|(a^2 - b^2 - n^2)$. Also, since $q|(b^2 + r^2 - n^2)$, it follows that $q|(b^2 - n^2)$; therefore $q|((b^2 + n^2) + (b^2 - n^2)) = 2b^2$, that is, $q|b$. Then $q|n$, which implies $q|a$. Contradiction. □

In [4], Guy notes that if n is not a multiple of 3, then exactly two of a, b, c, r are divisible by 3; indeed, this fact was proved in Proposition 2.3.2. We now show that n is necessarily a multiple of 3, thereby allowing our first application of Theorem 2.5.1.

Theorem 2.5.2. *n is a multiple of 3, and none of a, b, c, r are divisible by 3.*

Proof. Suppose n is not a multiple of 3. By Proposition 2.3.2, two of a, b, c, r are divisible by 3. The only possible pairs divisible by 3 are $(a, b), (a, c), (r, b), (r, c)$; any other pair would lead to all a, b, c, r being divisible by 3. Also, $3|(a^2 - b^2 - n^2)$ or $3|(a^2 - c^2 - n^2)$, by Proposition 2.3.1.

If $3|a$ and $3|b$, then $3 \nmid (a^2 - b^2 - n^2)$, since otherwise $3|n$. Therefore by Proposition 2.3.1 $3|(a^2 - c^2 - n^2)$. But $a^2 - c^2 - n^2 \equiv 0 - 1 - 1 \equiv 1 \pmod 3$. Similarly, if $3|a$ and $3|c$, then $3|(a^2 - b^2 - n^2)$. But $a^2 - b^2 - n^2 \equiv 1 \pmod 3$.

If $3|r$ and $3|b$, then $3|(b^2 - r^2) = (a^2 - c^2)$. Also, $3|(2rn)^2$; therefore by Lemma 2.4.3, $3|(a^2 - c^2 - n^2)$. Thus $3|n$. A similar argument is used if $3|r$ and $3|c$.

As each of the four cases lead to a contradiction, 3 divides n. By Theorem 2.5.1, it follows that 3 divides none of a, b, c, r.

□

Despite the similarity between Proposition 2.3.2 and Proposition 2.3.4, a statement analogous to Theorem 2.5.2 cannot be made for the case in which n is a multiple of 5, at least not by using the same method. Since only primes of $\mathbb{Z}$ of the form $4k + 3$ are irreducible in $\mathbb{Z}[i]$, the results of Section 2.5 cannot be used when dealing with primes of the form 4k+1.

Relatively straightforward applications of Theorem 2.5.1 appear to be rather limited to the case of $p = 3$, in part due to the very general property that for every triple $X^2+Y^2 = Z^2$, at least one of X, Y is divisible by 3. Furthermore, under modulo 3, squares are easily described, being equal to either 0 or 1. Considering just the next smallest prime of the form 4k+3 introduces a fair amount of complexity; modulo 7, squares are 0, 1, 2, or 4. While still a small set, the greater number of possible combinations becomes prohibitive to check directly, and given the lack of a general statement of the divisibility by 7 for any triple, is likely not a fruitful approach.

It is interesting to note the similarity between Theorem 2.3.1 and Theorem 2.5.2. There appears to be a marked restriction on the values of distances a, b, c, r with respect to the square's length n, which possibly suggests the unlikelihood of such an arrangement to exist.

Being able to apply the methods used in the proof of Theorem 2.5.2 to other primes of the form 4k+3, such as 7, could perhaps provide further insight. Indeed, if it can be shown that infinitely many primes of the form 4k+3 must divide n, then the four-distance problem would be answered in the negative.

2.6 Representations of Sums of Squares

Thus far, condition (2.6) has played an essential role in describing possible solutions to the four-square problem; indeed, its inclusion was necessary for us to establish even basic

properties. Using the results from the previous section, we can characterize (2.6) slightly further.

Definition 2.6.1. *A positive integer x is said to be representable as a sum of two squares provided $x = y^2 + z^2$, where y, z are integers. Furthermore, x is said to be properly representable provided there exist integers y_1, z_1 such that $x = y_1^2 + z_1^2$ with $gcd(y_1, z_1) = 1$.*

Perhaps the first fundamental result regarding the previous is Fermat's result (though first proven by Euler) that an odd prime p is expressible as the sum of two squares (of integers) if and only if $p \equiv 1 \pmod 4$. The following result is of particular interest; for a proof, see [10].

Theorem 2.6.1. *A positive integer n is properly representable as a sum of two squares if and only if the prime factors of n are all of the form $4k + 1$, except for the prime 2, which may occur to at most the first power.*

If a prime $p = 4k + 3$ were a factor of $r^2 + a^2$, and therefore a factor of $b^2 + c^2$, then p would divide all of a, b, c, r, contradicting Theorem 2.5.1. Thus, the prime factors (other than 2) of $r^2 + a^2$ and $b^2 + c^2$ must be of the form 4k+1. By Theorem 2.6.1, it follows that both $r^2 + a^2$ and $b^2 + c^2$ are *properly* representable as a sum of two squares.

There are several interesting results on representations of sums of squares (and more generally, on representations of quadratic forms); however, there is no immediate indication as to how useful they may lend themselves to further describe the four-distance problem.

Chapter 3: Additional Results

Let $P = (x, y) \in \mathbb{R}^2$ be at integral distance to the corners of the square with side length n, and let $(a, b, c, r, n) \in \mathbb{Z}^5$ be the associated solution to (2.5) and (2.6). In this chapter we establish several theorems as to where P cannot lie. It has been shown that P cannot be on the boundary of the square; Barbara gives a proof by the method of infinite descent [11].

Theorem 3.0.1. *P cannot lie on a line coinciding with one of the square's diagonals.*

Proof. Without loss of generality, let ℓ denote the line coinciding with the square's diagonal passing through vertices $(0, 0)$ and (n, n). Note that for the four distances a, b, c, r to the square's vertices, c corresponds to vertex $(0, n)$, a corresponds to (n, n), b corresponds to $(n, 0)$, and r corresponds to $(0, 0)$. Therefore $c = b$.

If $P \in \ell$, we can express (2.5) as $2(a^2 - b^2 - n^2)^2 = (2rn)^2$. But by taking the square root of both sides, we have that $\sqrt{2}$ is integral. Contradiction.

□

Theorem 3.0.2. *P cannot lie on a circle circumscribing the square.*

Proof. Let A, B, C, D be the vertices of the square inscribed within the circle, and suppose such a point P exists on the circle. Then by Ptolemy's theorem, $AC \cdot PD = AP \cdot CD + AD \cdot CP$. But all edges except for AC are rational. Contradiction. □

The preceding theorem actually establishes the stronger result of no point on a circle circumscribing the square satisifying the three-distance problem.

Theorem 3.0.3. *P cannot lie on a circle inscribed in the square.*

Proof. Let A, B, C, D be the vertices of the square, and P a point on the circle inscribed in the square. We may rescale the square such that its side has length 2, and then translate the

square such that $A = (1,1), B = (1,-1), C = (-1,-1), D = (-1,1)$. Then $AP^2 + CP^2 = (x-1)^2 + (y-1)^2 + (x+1)^2 + (y+1)^2 = 2x^2 + 2y^2 + 4 = 2(x^2+y^2) + 4 = 6$. But 6 is not the sum of 2 rational squares To see this, we show that the more general form $a^2 + b^2 = 6c^2$, with $c \neq 0$, has no nontrivial solutions over the integers. Suppose otherwise. Then viewing under modulo 3, we have that $a \equiv b \equiv c \equiv 0 \pmod 3$. Therefore a, b, c are infinitely divisible by 3. Contradiction. □

Theorem 3.0.3 also provides a stronger result, namely, of there not being any point on the inscribed circle being at rational distance from *two* vertices of the square.

We now prove a much stronger statement using results from Chapter 2, in which both Theorem 3.0.2 and Theorem 3.0.3 are special cases.

Theorem 3.0.4. *Let $C = (\frac{n}{2}, \frac{n}{2})$, and let $R = \frac{nL}{M}$, where L^2 is a positive integer, and M^2 is a positive integer not divisible by 3. Then P cannot lie on a circle with center C and radius R.*

Proof. We may suppose that P does not lie on the boundary of the square. Note that the circle on which P lies is defined by the equation $\left(x - \frac{n}{2}\right)^2 + (y - \frac{n}{2})^2 = (\frac{nL}{M})^2$.

Then

$$\begin{aligned} \frac{n^2L^2}{M^2} &= \left(x - \frac{n}{2}\right)^2 + \left(y - \frac{n}{2}\right)^2 \\ &= x^2 + y^2 - 2\frac{xn}{2} - 2\frac{yn}{2} + 2\frac{n^2}{4} \\ &= r^2 - n\left(x + y - \frac{n}{2}\right) \end{aligned} \tag{3.1}$$

By equation (2.3), and taking into account that $x, y > 0$, we can write

$$-2rn\cos\theta = -2xn = b^2 - r^2 - n^2$$

and therefore

$$x = \frac{-b^2 + r^2 + n^2}{2n} \tag{3.2}$$

Likewise, by (2.4), we have

$$y = \frac{-c^2 + r^2 + n^2}{2n} \tag{3.3}$$

Substituting (3.2) and (3.3) into (3.1), we have

$$\begin{aligned}
\frac{n^2L^2}{M^2} &= r^2 - n\left(x + y - \frac{n}{2}\right) \\
&= r^2 - n\left[\left(\frac{-b^2 + r^2 + n^2}{2n}\right) + \left(\frac{-c^2 + r^2 + n^2}{2n}\right) - \frac{n}{2}\right] \\
&= r^2 - n\left[\frac{2r^2 - b^2 - c^2 + 2n^2 - n^2}{2n}\right] \\
&= r^2 - \left[\frac{2r^2 - b^2 - c^2 + n^2}{2}\right]
\end{aligned} \tag{3.4}$$

By (3.4),

$$2r^2 - (2r^2 - b^2 - c^2 + n^2) = b^2 + c^2 - n^2 = \frac{2n^2L^2}{M^2} \tag{3.5}$$

Thus,

$$b^2 + c^2 = n^2 + \frac{2n^2L^2}{M^2} \tag{3.6}$$

We know that $\frac{2n^2L^2}{M^2}$ is an integer; moreover, it is divisible by 3, by Theorem 2.5.2.

Therefore $3|(b^2 + c^2)$, and so $3|b$ and $3|c$, contradicting Theorem 2.5.1.

□

We remark that Theorem 3.0.4 is likely able to be strengthened further by considering circles whose centers differ from $(\frac{n}{2}, \frac{n}{2})$, which would allow for more freedom in characterizing sets of points that cannot satisfy the four-distance problem. Additionally, if any prime p of the form $4k + 3$ (other than 3) can be shown to be a divisor of n, then the theorem can be extended to account for all M such that M^2 is an integer not divisible by p. If it can be shown that *any* point in the plane must lie on a circle satisfying Theorem 3.0.4 (or a possible generalization of the theorem), then the four-distance problem would be answered in the negative. We don't necessarily expect this to be the case, and even so it likely would be more difficult to show, but an investigation is warranted.

Chapter 4: Generalization to Regular Polygons

We now introduce a generalization of the four-distance problem given by Barbara [5]. We provide a summary of his results which uses concepts from field theory; the reader may decide if it is of interest.

For $n \geq 3$, denote P_n to be the *unit n-gon*; that is, the regular n-gon with unit side. Is there a point in the plane of P_n at rational distance from the vertices of P_n? Barbara establishes the very interesting result: the statement is false for $n = 5$, true for $n = 6$, and false for all $n \geq 7$, except for possibly when $n \in \{8, 12, 24\}$. While his results do not resolve the four-distance problem, Barbara establishes the exceptional rarity of an arbitrary n-gon having the rational distance property.

Let $n = 3$, where T the resulting unit equilateral triangle. By a well-known theorem of Berry [12], there exists a point in the plane of T at rational distance from the vertices of T; in fact, the set of such points is dense in the plane of T. The case of the unit square ($n = 4$), of course, is simply the four-distance problem.

For the case of $n = 6$, consider the centroid of the unit hexagon; then the distance from the centroid to each vertex is of unit length.

For the cases of $n = 5$ and $n \geq 7$, we provide some preliminary statements (for proofs, see Barbara's paper).

Definition 4.0.1. *A 2-group is a group such that every element has order 1 or 2.*

Definition 4.0.2. *A real field F is said to be flat if for every subfield E of F, the Galois group $G(E : \mathbb{Q})$ is a 2-group.*

Proposition 4.0.1. *Let $r_1, r_2, \ldots, r_n$ be nonnegative rational numbers. Then*

$\mathbb{Q}(\sqrt{r_1} \pm \sqrt{r_2} \pm \cdots \pm \sqrt{r_n})$ is a flat field.

Proposition 4.0.2. *Let $n \geq 5, n \neq 6$, and set $\Omega = \mathbb{Q}(\cot \frac{\pi}{n})$. If Ω is a flat field, then $n \in 8, 12, 24$.*

As a corollary to the preceding two propositions, we have the following result.

Corollary 4.0.1. *Let $n = 5$ or $n \geq 7$, with $n \neq 8, 12, 24$. Then the identity*

$$\frac{n}{4} \cot \frac{\pi}{n} = \sqrt{r_1} \pm \sqrt{r_2} \pm \cdots \pm \sqrt{r_n},$$

where each r_i is a nonnegative rational numbers, is impossible.

Proof. Suppose not. Then $\mathbb{Q}(\sqrt{r_1} \pm \sqrt{r_2} \pm \cdots \pm \sqrt{r_n}) = \mathbb{Q}(\frac{n}{4} \cot \frac{\pi}{n}) = \mathbb{Q}(\cot \frac{\pi}{n})$. But by Proposition 4.0.1, $\mathbb{Q}(\sqrt{r_1} \pm \sqrt{r_2} \pm \cdots \pm \sqrt{r_n})$ is a flat field, whereas by Proposition 4.0.2, $\mathbb{Q}(\cot \frac{\pi}{n})$ is not a flat field. Contradiction. □

Theorem 4.0.5. *For $n = 5$ or $n \geq 7$, there is no point in the plane of P_n at rational distance from the vertices of P_n.*

Proof. Suppose not. Let P be a point in the plane of P_n at rational distance from the vertices $A_1, A_2, \cdots, A_n$ of P_n, written in cyclic order, and set $A_{n+1} = A_1$. Let $T_i = PA_iA_{i+1}$, $i = 1, \cdots, n$ be the set of triangles lying in the plane of P_n. Then

$$\text{area}(P_n) = \text{area}(T_1) + \text{area}(T_2) + \cdots + \text{area}(T_n)$$

Since each triangle T_i has rational sides, by Heron's formula we have that the area of each T_i is of the form $\sqrt{r_i}$, where r_i is a nonnegative rational. Thus, it follows that $\text{area}(P_n) = \sqrt{r_1} \pm \sqrt{r_2} \pm \cdots \pm \sqrt{r_n}$. Moreover, $\text{area}(P_n) = \cot \frac{\pi}{n}$. Finally, we obtain $\frac{n}{4} \cot \frac{\pi}{n} = \sqrt{r_1} \pm \sqrt{r_2} \pm \cdots \pm \sqrt{r_n}$. By Corollary 4.0.1, we have a contradiction. □

Bibliography

[1] N. H. Anning and P. Erdős, "Integral distances," *Bulletin of the American Mathematical Society*, vol. 51, pp. 598–600, 1945.

[2] J. Solymosi and F. de Zeeuw, "On a question of Erdős and Ulam," *Discrete and Computational Geometry*, vol. 43, pp. 393–401, 2010.

[3] T. Kreisel and S. Kurz, "There are integral heptagons, no three points on a line, no four on a circle," *Discrete and Computational Geometry*, vol. 39, pp. 786–790, 2006.

[4] R. K. Guy, *Unsolved Problems in Number Theory.* Springer-Verlag, 2004.

[5] R. Barbara, "Points at rational distance from the vertices of a unit polygon," *Bulletin of the Iranian Mathematical Society*, vol. 35, pp. 209–215, 2009.

[6] *Euclid's Elements: Book X, Proposition XXIX.*

[7] R. A. Mollin, *Number Theory and Applications.* Kluwer Academic, 1989.

[8] T. G. Berry, "Points at rational distance from the corners of a unit square," *Ann. Scuola Norm. Sup. Pisa Cl. Sci.*, vol. 17, pp. 505–529, 1990.

[9] D. S. Dummit and R. M. Foote, *Abstract Algebra.* Prentice Hall, 1999.

[10] I. Niven, H. S. Zuckerman, and H. L. Montgomery, *Introduction to Number Theory.* John Wiley and Sons, 1991.

[11] R. Barbara, "The rational distance problem," *The Mathematical Gazette*, vol. 95, pp. 59–61, 2011.

[12] T. G. Berry, "Points at rational distance from the vertices of a triangle," *Acta Arithmetica*, vol. 62, pp. 391–398, 1992.

Biography

Joseph G. Sadeq received his Bachelor of Science in Mathematics from George Mason University in 2008. Since then, he has worked as a research and data analyst. He went on to receive his Master of Science in Mathematics from George Mason University in 2015.