Pythagorean Quadruples

Robert Hochberg
Department of Computer Science
East Carolina University
Greenville, NC 27858-4353
email: hochberg@cs.ecu.edu

and

Glenn Hurlbert[*]
Department of Mathematics and Statistics
Arizona State University
Tempe, Arizona 85287-1804
email: hurlbert@asu.edu

April 30, 2002

[*]Partially supported by National Security Agency grant #TKA6169.

Abstract

Pythagorean triples are triples of positive integers (a, b, c) satisfying $a^2 + b^2 = c^2$, i.e., triples of integers which can be the side lengths of a triangle inscribed in a circle with one side as the diameter. This paper considers a *geometric* generalization of these triples: What quadruples of integers can be the side lengths of a convex quadrilateral inscribed in a circle with one side as the diameter? Our investigation leads to interesting recursive constructions, Diophantine equations, and a partial characterization. Along the way we also provide a new proof of Ptolemy's Theorem.

1991 AMS Subject Classification: 11B37, 11D25, 51M04

Key words: Pythagorean triples, quadruples, Ptolemy

1 Introduction

The Pythagorean Theorem says that if a and b are the leg lengths of a right triangle with hypotenuse c, then $a^2 + b^2 = c^2$. The infinitely many integral solutions are well classified, and numerous generalizations have been thoroughly studied. Lagrange [5] proved that every positive integer was the sum of 4 squares of integers. Waring [8] conjectured and Hilbert [4] proved that for every positive integer n there was a constant $c(n)$ such that every positive integer was the sum of $c(n)$ non-negative nth powers. Fermat, Euler, Gauss and Jacobi studied the number of solutions to $a^2 + b^2 = n$ for fixed n (see eg. [3]). Lucas [6] challenged his readers to find all solutions n and c to $\Sigma_{i=1}^{n} i^2 = c^2$, (for a nice solution see [1]) and Pell's equation $a^2 - kb^2 = \pm 1$ for fixed k occupied the attention of many mathematicians. And finally there is the problem posed by Fermat of representing nth powers of integers as the sum of two smaller nth powers for $n > 2$, which was recently solved by Wiles [9].

The above generalizations are all algebraic in nature. Here we offer a *geometric* generalization of Pythagorean triples. It too has a nice associated Diophantine equation, (see equation (5)) and its solution leads to some interesting number theoretic questions. We ask: What 4-tuples of integers (A, B, C, D) are there such that a convex quadrilateral with these side lengths can be inscribed in a circle with diameter D? Since all triples of integers (A, B, C) which satisfy the property that a triangle with side lengths A, B

and C can be inscribed in a circle of diameter C are precisely the Pythagorean triples (such a triangle is necessarily right), we call our solutions *Pythagorean quadruples.* We look for *primitive* Pythagorean quadruples, i.e., those for which $\gcd(A,B,C,D)=1$, for example, (1,1,1,2), the top half of a regular hexagon of side length 1. The reader might enjoy finding a Pythagorean quadruple on his or her own before proceeding.

The formulas which generate all primitive Pythagorean triples ($A = u^2 - v^2, B = 2uv, C = u^2 + v^2$) require only that the generators u and v be relatively prime and of different parity. We are able to find equally simple formulas (Theorem 3) only in the case that some two sides are equal. We include in Section 3 our derivation in this special case, with our primary emphasis on the recursive nature of the family of all such primitive solutions. In contrast to the recursion involved with Pell's equation, our solutions split into several recursive families. In Section 4 we prove two theorems about impossible diameters of Pythagorean triples whose sides are distinct. Section 5 is devoted to questions and conjectures regarding future directions of research.

2 Preliminaries

We begin by labelling the diameter D, its opposite side A, the remaining sides B and C, and the diagonals M and N as in Figure 1.

The smallest distinct-side Pythagorean quadruple is (2,7,11,14). How does one verify that this is indeed a Pythagorean quadruple? Since the

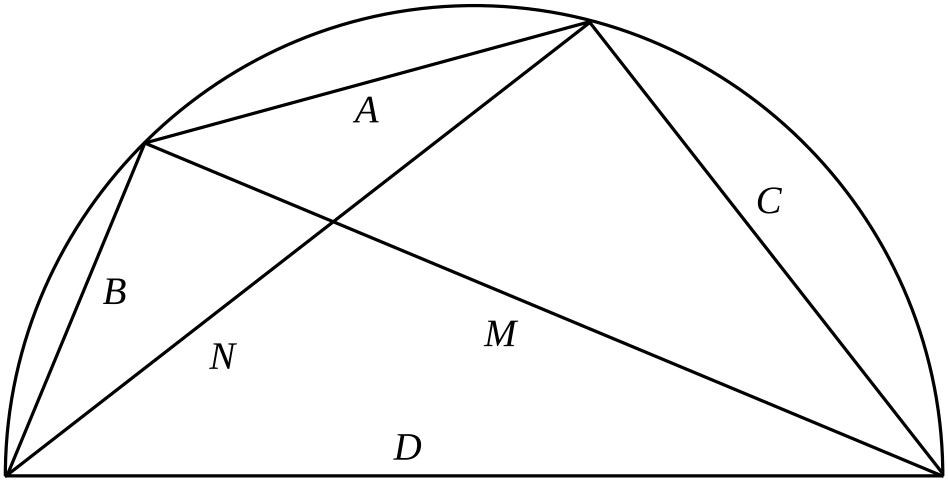

Figure 1.

triangles with sides B, M, D and C, N, D are both right, we find that $M = 7\sqrt{3}$ and $N = 5\sqrt{3}$. Now we use

Proposition 1 (Ptolemy's theorem) *Let a convex quadrilateral have side lengths A, C, D and B (in clockwise order) and let its diagonals have lengths M and N. If this quadrilateral can be inscribed in a circle, then*

$$AD + BC = MN. \tag{1}$$

The converse of Ptolemy's theorem (see [7]) is not true in general (eg. $(A, C, D, B, M, N) = (3, 1, 1, 1, \sqrt{2}, 2\sqrt{2})$), but is true whenever (2) holds below – equation (2) inscribes the right triangles (B, M, D) and (C, N, D) and (1) insures that $A > 0$ so that M and N are the diagonals. Thus, we can now check our example to see that (2,7,11,14) is indeed a Pythagorean quadruple.

Glancing at the right triangles in Figure 1, we see that

$$M^2 + B^2 = D^2 = N^2 + C^2, \tag{2}$$

so that M and N are both square roots of integers. Equation (1) tells us that the product MN is an integer, and thus we can write $M = S\sqrt{k}$ and $N = T\sqrt{k}$ for some integers S, T, and square-free k, which we call the *surd* of our Pythagorean quadruple. Substituting into (1) we get

$$AD + BC = STk. \tag{3}$$

A more useful equation is obtained by substituting for M and N as follows:

$$AD + BC = \sqrt{(D^2 - B^2)(D^2 - C^2)}, \tag{4}$$

which becomes, as a polynomial in D,

$$D^3 - (A^2 + B^2 + C^2)D - 2ABC = 0. \tag{5}$$

This is our generalization of the Pythagorean equation $C^2 - A^2 - B^2 = 0$ for right triangles. Geometrically, it is clear that given positive real numbers A, B, and C, there is a unique positive D (not necessarily integral or rational) so that its corresponding quadrilateral inscribes in a circle of diameter D. Algebraically, (5) describes the same information: the derivative (in D) of the lefthand side is strictly positive so its real root is unique. It is of course positive.

We end this section with a quick new proof of Ptolemy's theorem.

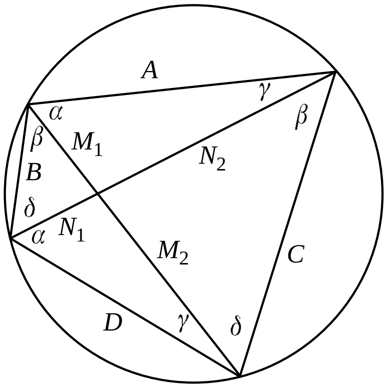

Figure 2a.

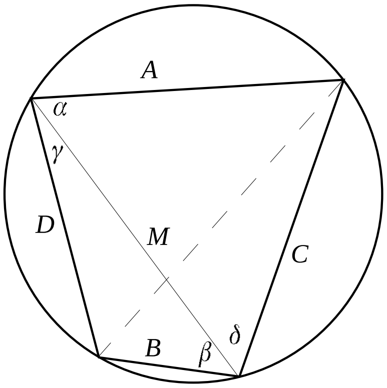

Figure 2b.

Proof of Proposition 1. Let the diagonals cut one another into lengths M_1, M_2, N_1, and N_2 so that $M = M_1 + M_2$ and $N = N_1 + N_2$ (see Figure 2a). We calcuate the area H of the quadrilateral in 2 ways. First we sum the areas of the four triangles, getting

$$\begin{aligned} H &= \tfrac{1}{2}M_1N_1\sin(\pi-\alpha-\gamma) + \tfrac{1}{2}M_1N_2\sin(\pi-\beta-\delta) \\ &\quad + \tfrac{1}{2}M_2N_1\sin(\pi-\beta-\delta) + \tfrac{1}{2}M_2N_2\sin(\pi-\alpha-\gamma) \\ &= \tfrac{1}{2}(M_1N_1 + M_1N_2 + M_2N_1 + M_2N_2)\sin(\alpha+\gamma) \\ &= \tfrac{1}{2}MN\sin(\alpha+\gamma). \end{aligned}$$

Second, if we flip the triangle with sides MBD (see Figure 2b), we calculate this same area to be

$$\begin{aligned} H &= \tfrac{1}{2}AD\sin(\alpha+\gamma) + \tfrac{1}{2}BC\sin(\beta+\delta) \\ &= \tfrac{1}{2}(AD+BC)\sin(\alpha+\gamma). \end{aligned}$$

Hence, $AD + BC = MN$. □

3 Equal Sides

Of course, (1,1,1,2) is the unique primitive Pythagorean quadruple with $A = B = C$, so let us consider the situation in which exactly 2 sides are equal. If the equal sides are not B and C, but rather, say, A and B, then we may flip the triangle with sides A, B and N along the side N (as we did in the proof of Ptolemy's theorem) to make the equal sides opposite one another. So without loss of generality, we assume $A \neq B = C$. But $B = C$ implies $M = N$, so (1) becomes

$$AD + B^2 = M^2,$$

and then

$$AD + 2B^2 = D^2.$$

With $a = A/B$, $d = D/B$, and $m = D/A = d/a$, we obtain

$$ad + 2 = d^2,$$

$$ma^2 + 2 = m^2a^2.$$

and

$$a^2 = 2/(m^2 - m) = 1/\binom{m}{2}. \tag{6}$$

Thus we conclude

Lemma 2 *There exists a Pythagorean quadruple with two equal sides if and only if $\binom{m}{2}$ is the square of a rational number for some rational $m > 1$.* □

Such solutions, with $m = p/q$, become $(q, q\sqrt{\binom{m}{2}}, q\sqrt{\binom{m}{2}}, p)$. With $m = 32/7$, for example, we have the solution $(7, 20, 20, 32)$.

As in the case of Pythagorean triples, we have simple formulas to generate all Pythagorean quadruples with 2 equal sides. Lemma 2 yields

Theorem 3 *All primitive Pythagorean quadruples with equal sides are of the form* $(|2s^2 - r^2|, sr, sr, max\{2s^2, r^2\})$*, where* s *and* r *are any relatively prime natural numbers with* r *odd.*

Proof. Write $m = p/q$ in lowest terms. Then $\binom{m}{2} = p(p-q)/2q^2$ so that

$$\sqrt{\binom{m}{2}} = \frac{1}{q}\sqrt{\frac{p(p-q)}{2}}. \tag{7}$$

Now, $gcd(p, q) = 1$, so $gcd(p, p-q) = 1$ and $\sqrt{p(p-q)/2} \in \mathbf{Z}$ if and only if both $p/2$ and $(p-q)$ are squares, or both p and $(p-q)/2$ are squares, depending upon whether p is even or odd (q is necessarily odd since $p(p-q)$ must be even in (7)). If p is even then let $p/2 = s^2$ and $(p-q) = r^2$, and if p is odd then let $(p-q)/2 = s^2$ and $p = r^2$. In either case, r is odd and (7) becomes

$$\sqrt{\binom{m}{2}} = sr/q, \tag{8}$$

so $a = q/sr$ and $d = p/sr$. With p even we obtain $q = 2s^2 - r^2$, and with p odd we have $q = r^2 - 2s^2$. □

The problem becomes interesting if we fix an odd q and consider how many solutions (q-*solutions*) there are of the form $A = q$, $B = C$, and $D = p$. We already know that q is odd, but since $r^2 \equiv 1 \bmod 8$ and $2s^2 \equiv 0$ or $2 \bmod 8$, we have that $q \equiv \pm 1 \bmod 8$. In fact, since $q = |2s^2 - r^2|$, $(r/s)^2 \equiv 2 \bmod q'$ for each prime q' dividing q. Thus 2 is a quadratic residue of q', so by Gauss' Lemma, $q' \equiv \pm 1 \bmod 8$. Let us call an integer q *admissible* if each of its prime divisors is congruent to $\pm 1 \bmod 8$. Then it so happens that we can recursively generate infinitely many primitive q-solutions (in fact, all of them) whenever q is admissible.

Before plunging into the recursive algorithm, let us first describe its inverse. The idea is to show how all q-solutions are derived from "smaller" q-solutions until a "smallest" (we call *seed*) is found, in somewhat the same fashion as solutions to Pell's equation are constructed. To this end, suppose we have the q-solution $(q, rs, rs, p) = (q, r_n s_n, r_n s_n, p_n)$.

First assume that p_n is even. Then $p_n = 2s_n^2$ and $q = 2s_n^2 - r_n^2$ for some $r_n, s_n > 0$. If $r_n \leq s_n$ then we will stop, so let us suppose that $s_n < r_n$. We let $s_{n-1} = r_n - s_n$ and $r_{n-1} = \sqrt{2s_{n-1}^2 + q}$, so that $q = r_{n-1}^2 - 2s_{n-1}^2$. Then $(s_{n-1} + s_n)^2 = r_n^2 = 2s_n^2 - q$, and the quadratic formula shows that $s_n = s_{n-1} \pm r_{n-1}$. But since $r_{n-1} > s_{n-1}$ we actually have $s_n = s_{n-1} + r_{n-1}$. Finally, one checks that if $(q, r_n s_n, r_n s_n, p_n)$ is a Pythagorean quadruple, then so is $(q, r_{n-1}s_{n-1}, r_{n-1}s_{n-1}, p_{n-1})$, where $p_{n-1} = r_{n-1}^2$. Call this algorithm EVEN.

Next assume that p_n is odd. Then $p_n = r_n^2$ and $q = r_n^2 - 2s_n^2$ for some $r_n, s_n > 0$, and here we suppose not only that $s_n < r_n$, but $s_n > 2r_n/3$ as well. Similarly, let $s_{n-1} = r_n - s_n$ and $r_{n-1} = \sqrt{2s_{n-1}^2 - q}$, so that $q =$

$2s_{n-1}^2 - r_{n-1}^2$. Then $(s_{n-1}+s_n)^2 = 2s_n^2+q$ and $s_n = s_{n-1} \pm r_{n-1}$. But the extra condition $r_n > 3s_n/2$ (which maintains the condition $r_{n-1} > s_{n-1}$) implies that $r_{n-1} > s_{n-1}$, so $s_n = s_{n-1} + r_{n-1}$. And now with $p_{n-1} = 2s_{n-1}^2$ we know that $(q, r_{n-1}s_{n-1}, r_{n-1}s_{n-1}, p_{n-1})$ is Pythagorean if $(q, r_n s_n, r_n s_n, p_n)$ is. Call this algorithm ODD.

Finally we describe algorithm ODD*. Its only deviance from ODD is the condition $r_n \leq 3s_n/2$, and now $s_n = s_{n-1} \pm r_{n-1}$ since $r_{n-1} \leq s_{n-1}$.

The inverse of our recursive algorithm is the combination of EVEN, ODD, and ODD*, since exactly one of the initial conditions will be satisfied. The key observations to make are that EVEN will always be followed by ODD or ODD*, ODD will always be followed by EVEN, and ODD* is the terminating algorithm. Also, we always have $s_{n-1} < s_n$ in EVEN and ODD, so no q-solutions are repeated and thus the algorithm does halt. Because of the ± in ODD*, the inverse algorithm can be pictured as in Figure 3.

The only exception to Figure 3 occurs when equality holds in ODD*. In this case $r_1 = 3$ and $s_1 = 2$ and ODD* produces the trivial hexagonal solution. Here we have only one infinite string of q-solutions, rather than the two pictured.

The value s_0 will be called a *seed* of q, and r_0 its *root*. From the above discussion one sees that all roots are even. One can also see that s_0 is a seed of q if and only if it satisfies

$$\begin{array}{rl} \textit{(i)} & gcd(s_0, q) = 1, \\ \textit{(ii)} & s_0 \leq \sqrt{q}, \text{ and} \\ \textit{(iii)} & 2s_0^2 - q = r_0^2 \text{ for some integer } r_0. \end{array} \tag{9}$$

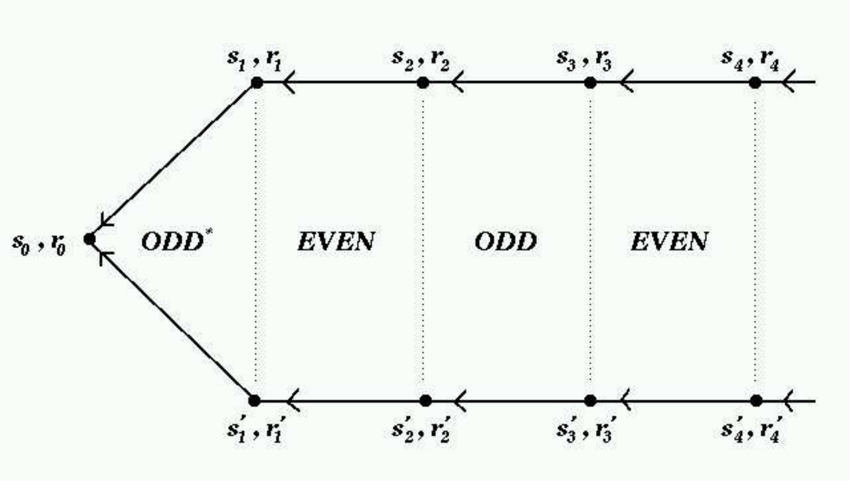

Figure 3.

So to find all primitive q-solutions, we find all seeds of q and for each seed s_0 let $r_0 = \sqrt{2s_0^2 - q}$,

$$s_1 = s_0 - r_0, \qquad s_1' = s_0 + r_0,$$

and

$$r_1 = s_1 + s_0, \qquad r_1' = s_1' + s_0.$$

Then let

$$s_n = s_{n-1} + r_{n-1}, \qquad s_n' = s_{n-1}' + r_{n-1}',$$

and

$$r_n = s_{n-1} + s_n, \qquad r_n' = s_{n-1}' + s_n'.$$

We then obtain solutions $A_n = q$, $B_n = C_n = s_n r_n$, and $D_n = r_n^2$ for odd n, $2s_n^2$ for even n (likewise for A_n', B_n', C_n', D_n'). Table 4 gives an example with $q = 7$, the only seed of which is $s_0 = 2$.

n	s_n	r_n	B_n	D_n	s'_n	r'_n	B'_n	D'_n
0	2	1	2	8				
1	1	3	3	9	3	5	15	25
2	4	5	20	32	8	11	88	128
3	9	13	117	169	19	27	513	729
4	22	31	682	968	46	65	2990	4132
5	53	75	3975	5625	111	157	17427	24649
6	128	181	23168	32768	268	379	101572	143648
.	.		.		.		.	
.	.		.		.		.	
.	.		.		.		.	

Table 4.

q	seeds
7^5	92
17^4	205
$7^2 \cdot 17^2$	89, 101
$17 \cdot 31 \cdot 79$	151, 173, 177, 191
$7^2 \cdot 17^2 \cdot 23$	404, 426, 486, 558
$17 \cdot 23 \cdot 47 \cdot 103$	976, 984, 1004, 1026, 1130, 1166, 1194, 1246

Table 5.

As $n \to \infty$, $D_n \to \infty$, so that geometrically our quadrilaterals tend to approximate an isosceles right triangle (remember $A = q$ is fixed.) Thus, it should be the case that $D_n/B_n \to \sqrt{2}$, and likewise for D'_n/B'_n. Algebraically, we have $D_n/B_n = r_n/s_n = \sqrt{2 \pm q/s_n^2} \to 2$.

One natural question that arises is, just how many seeds does a fixed admissible q have? The keen observer of Table 5 might quess the correct answer. Let π be the number of distinct prime divisors of q.

Theorem 4 *The number of seeds for fixed admissible q is $2^{\pi-1}$.*

As an obvious corollary, we have

Corollary 5 *(A, B, B, D) is a Pythagorean quadruple for some B and D if and only if A is admissible.* □

We will prove Theorem 4 using the following two claims.

Claim 6 *For prime q there is at least one seed.*

Claim 7 *For prime q there is at most one seed.*

Proof of Claim 6. Choose some $\delta \in \{0, 1, \ldots, q-1\}$ so that $\delta^2 \equiv 2 \bmod q$, and for $i = 0, 1, \ldots, \lfloor\sqrt{q}\rfloor$ define $a_i \in \{0, 1, \ldots q-1\}$ by $a_i = i\delta \bmod q$ (notice that $\delta > \lfloor\sqrt{q}\rfloor$). Of the $\lceil\sqrt{q}\rceil$ distinct a_i, some two have difference less than $\sqrt{q} \bmod q$, say a_i and a_j, with $i < j$. But then $0 = a_0$ and a_{j-i} are also less than $\sqrt{q}$ apart, so we may assume that $i = 0$. Moreover, by considering δ versus $-\delta$, we may also ensure that $0 < a_j < \sqrt{q}$.

Now since $2j^2 \equiv (j\delta)^2 \equiv a_j^2 \bmod q$, we know that $2j^2 - a_j^2 = mq$ for some nonzero integer m (since 2 is not square). But $2j^2 - a_j^2 > 0 - q$ implies that $m \geq 0$, while $2j^2 - a_j^2 < 2q$ implies that $m < 2$. Hence $m = 1$ and, by (9), j is a seed. ◇

Proof of Claim 7. Suppose we have two seeds $t_1 > t_2$ and let $\tau_i^2 = 2t_i^2 - q$. Then $2(t_1^2 - t_2^2) = (\tau_1^2 - \tau_2^2)$. If we let $f = (t_1 + t_2)$, $g = (t_1 - t_2)$, $h = (\tau_1 + \tau_2)$, and $l = (\tau_1 - \tau_2)$, then this equation becomes $2fg = hl$. Since

$$q = 2t_1^2 - \tau_1^2 = 2\left(\frac{f+g}{2}\right)^2 - \left(\frac{h+l}{2}\right)^2$$

	$h/2$	l
f	u	v
g	x	y

Figure 6. $fg = uvxy = hl/2$.

we have

$$4q = 2(f+g)^2 - (h+l)^2.$$

Let us make some substitutions (see Figure 6). We let $f = uv$ and $g = xy$ so that $h = 2ux$ and $l = vy$ (h is even since τ_1 and τ_2 are both odd). Then

$$4q = (2u^2 - y^2)(v^2 - 2x^2).$$

Notice that $uv = f > g = xy$ and $2ux = h > l = vy$, so that $(uv)(2ux) > (xy)(vy)$ and $2u^2 > y^2$. Thus also $v^2 > 2x^2$. Now suppose on the contrary that $q|(v^2 - 2x^2)$ (the case that $q|(2u^2 - y^2)$ would be handled similarly). Then $(v^2 - 2x^2) \geq q$ so $v^2 > q$ and $v > \sqrt{q}$. But $uv = f = t_1 + t_2 \leq 2\sqrt{q}$ so that $u \leq 2\sqrt{q}/v < 2$. Hence $u = 1$, $(2u^2 - y^2) = (2 - y^2) > 0$ and $y = 1$. Thus, $(2u^2 - y^2) = 1$ and $(v^2 - 2x^2) = 4q$. But $v = f \leq 2\sqrt{q}$, so $v^2 - 2x^2 < v^2 \leq 4q$, a contradiction. $\diamond$

Proof of Theorem 4. The number of seeds found in the proof of Claim 6 depended on the number of square roots δ of 2. For admissible prime q (and admissible prime powers), the number of square roots is two, δ and $-\delta$, one of which yields the seed. For non-prime admissible q, each distinct prime power factor q_j has two square roots of 2 modq_j, so the Chinese Remainder Theorem guarantees exactly $2^{\pi(q)}$ square roots of 2 mod q occuring, of course, in pairs $\pm\delta_j$. Each pair yields a distinct seed, and thus there are exactly $2^{\pi-1}$ seeds. □

4 Distinct Sides

It is perhaps surprising to note that a diameter of a Pythagorean quadruple cannot be an odd prime. Suppose D is some odd prime, p, and rewrite (5) as $p(p^2 - A^2 - B^2 - C^2) = 2ABC$ to see that p divides the quantity $2ABC$. But $p = D > 2, A, B, C$, a contradiction. This is summarized below.

Theorem 8 *The only Pythagorean quadruple with prime diameter is the trivial (1,1,1,2).* □

Assume that $B \neq C$ in a Pythagorean quadruple of surd k. Then we have two distinct integral solutions (x, y) to the equation $D^2 = x^2 + ky^2$, these being (B, S) and (C, T) (from equation 2), and A is then given by Ptolemy's theorem, $A = (kST - BC)/D$, and must be integral. When D is prime, the above theorem says this is all impossible. Why? It turns out that asking for two distinct solutions to $D^2 = x^2 + ky^2$ is too much when D is prime, as the following theorem shows.

Theorem 9 *For prime p and square-free k, the diophantine equation $p^2 = x^2 + ky^2$ has at most one solution (x, y).*

Proof. Assume $p > 2$, and suppose

$$\begin{aligned} u^2 + kv^2 &= p^2 \qquad (10) \\ w^2 + kz^2 &= p^2. \end{aligned}$$

We will show that $u = w$. Moving u^2 and w^2 to the other sides and multiplying, we find

$$k^2v^2z^2 = (p^2 - u^2)(p^2 - w^2), \tag{11}$$

which can be arranged as

$$(kvz - uw)(kvz + uw) = p^2(p^2 - u^2 - w^2). \tag{12}$$

Thus p^2 must divide the left side of (12). If p divided each factor, then p would divide the difference, $2uw$. But glancing at (10), we see that $p > u, w$, whence p can't divide $2uw$, and so p^2 must divide one of the factors. Taking the square root of both sides of (11) one sees that $kvz < p^2$, so p^2 certainly cannot divide $(kvz - uw)$ and hence must divide $(kvz + uw)$. But $u, w < p$ and $kvz < p^2$ imply $(kvz + uw) < 2p^2$. Hence $(kvz + uw) = p^2$, and substitution into (12) yields

$$(kvz - uw)p^2 = p^2(p^2 - u^2 - w^2),$$

$$kvz - uw = p^2 - u^2 - w^2,$$

and

$$p^2 = u^2 - uw + w^2 + kvz = (u - w)^2 + uw + kvz.$$

But since we know that $p^2 = uw + kvz$, we have $p^2 = (u - w)^2 + p^2$ and thus $u = w$. □

We can say more about the diameter of a Pythagorean quadruple:

Theorem 10 *A diameter of a distinct-side Pythagorean quadruple cannot be the square of a prime.*

Proof. We will show this by proving that $D = p^2$, for p an odd prime, implies that some two sides must be the same. If p is even, then $D = 4$, and A, B, C must be $1, 2, 3$, which doesn't satisfy equation (5). So we take p to be odd. From (5) we have

$$p^2(p^4 - A^2 - B^2 - C^2) = 2ABC. \tag{13}$$

Thus $p^2|2ABC$, while $p \not| 2$ and $p^2 \not| A, B, C$. Hence p must divide two of the sides, say, A and B. If p also divided C, then we could divide all sides by p obtaining an integral solution to (5) with prime diameter, contradicting Theorem 8. So $p \not| C$.

Let $A = p\alpha$ and $B = p\beta$ so that (13) becomes

$$p^2(p^4 - p^2\alpha^2 - p^2\beta^2 - C^2) = 2p^2\alpha\beta C. \tag{14}$$

Dividing by p^2, moving C^2, and factoring again, we obtain

$$p^2(p^2 - \alpha^2 - \beta^2) = C(2\alpha\beta + C), \tag{15}$$

so $p \not| C$ implies $p^2|(2\alpha\beta + C)$. But $A, B < p^2$ implies that $\alpha, \beta < p$, which implies that $2\alpha\beta < 2p^2$. Furthermore, since $C < D = p^2$, we have $2\alpha\beta + C < 3p^2$. Thus, either

$$I: \quad 2\alpha\beta + C = p^2, \tag{16}$$

or

$$II: \quad 2\alpha\beta + C = 2p^2. \tag{17}$$

Case I: We substitute (16) into (15) and divide by p^2 to obtain $p^2 = C + \alpha^2 + \beta^2$. Solving (16) for C and substituting, we get $p^2 = p^2 - 2\alpha\beta + \alpha^2 + \beta^2 = p^2 + (\alpha - \beta)^2$, implying $\alpha = \beta$ and $A = B$.

Case II: We make similar substitutions. Combining (17) and (15) we get $p^2 = 2C + \alpha^2 + \beta^2 = 2(2p^2 - 2\alpha\beta) + \alpha^2 + \beta^2 = 4p^2 + (\alpha - \beta)^2 - 2\alpha\beta$, which implies $2\alpha\beta = 3p^2 + (\alpha - \beta)^2 > 3p^2$. However this contradicts $2\alpha\beta = 2p^2 - C < 2p^2$, from (17). Therefore this case is impossible and Theorem 10 is proven. □

We note that Theorem 10 cannot be improved to the cube of a prime, since (18,161,294,343) is Pythagorean.

5 Remarks

Aside from asking for a complete classification of primitive Pythagorean quadruples, several other questions arise from this work, the most obvious being whether one can find Pythagorean quintuples, and so on.

Conjecture 11 *For every $n \geq 3$ there are infinitely many primitive Pythagorean n-tuples.*

We say that a Pythagorean n-gon (and its corresponding n-tuple of side lengths) has *k parameters* if its set of side lengths takes on exactly k values. Primitive Pythagorean triples have three parameters and are completely characterized. Primitive Pythagorean quadruples with two sides equal have three parameters and are completely characterized in Section 3.

Problem 12 *Characterize primitive Pythagorean n-tuples having three parameters.*

The interesting thing about the quintuple (169,520,561,425,1105) is that the three chords closest to the diameter geometrically are integral, meaning that it contains as a subfigure the Pythagorean quadruple (169,943,425,1105) of surd 1 (its diagonals are 1020 and 1092). Likewise, this quadruple contains two Pythagorean triples. Such quintuples (in general, n-tuples) are called *nested.*

Question 13 *Are there infinitely many n for which there exists a nested Pythagorean n-tuple?*

Notice that this question doesn't require primitivity. The following related question does, however.

Question 14 *Is there some n for which there exist infinitely many nested primitive Pythagorean n-tuples?*

It is also possible to prove that all 5 chords interior to a Pythagorean pentagon are rational. This raises the following natural problem.

Problem 15 *Classify all primitive Pythagorean quadruples of surd 1 (i.e., nested primitive quadruples).*

Fässler [2] considers questions about Pythagorean triples such as how many there are with a common hypotenuse, perimeter, area, etc. One can ask the same questions regarding quadruples. In particular, can one characterize those integers P which are perimeters of primitive Pythagorean quadruples? And for such P, how many distinct quadruples are there? Also, can one classify all integers r which are the root of some admissible q? More questions abound.

Acknowledgement

The authors wish to thank Lucille and David Oakstreet for some of the inspiration which led to this work.

References

[1] W. S. Anglin, The square pyramid puzzle, Amer. Math. Monthly, 97 (1990), 120–124.

[2] A. Fässler, Multiple pythagorean number triples, Amer. Math. Monthly, 98 (1991), 505–517.

[3] Emil Grosswald, *Representations of Integers as Sums of Squares.* New York, Springer-Verlag, 1985.

[4] D. Hilbert, in *Math. Annelen*, 67, 1909 pp. 61–75.

[5] Lagrange, Nouv. Mém. Acad. Roy. Sc. de Berlin, Année 1770, Berlin, 1772 pp. 123–133.

[6] Edouard Lucas, Question 1180, Nouvelles Annales de Mathématiques, ser. 2, 14 (1875) 336.

[7] H.S.M Coxeter and S.L. Greitzer, *Geometry Revisited.* New York, Random House, 1967.

[8] E. Waring, *Meditationes Algebraicae*, Cambridge, 1770, 204–205.

[9] Andrew Wiles, Modular elliptic curves and Fermat's Last Theorem, Annals of Math. **142** (1995), 443–551.