Settling a Question about Pythagorean Triples

TOM VERHOEFF

Department of Mathematics and Computing Science

Eindhoven University of Technology

P.O. Box 513, 5600 MB Eindhoven, The Netherlands

E-Mail address: mcvax.UUCP!eutrc3!wstomv

February 1988

ABSTRACT

Do there exist two right-angled triangles with integer length sides that have the lengths of exactly two sides in common? We show by elementary means that the answer is: 'No'. The question turns out to be equivalent to a couple of well-known (and solved) problems in Number Theory.

THE PROBLEM

All variables in this note range over the positive integers (that excludes zero). The triple (a, b, c) is called *Pythagorean* when

$$a^2+b^2=c^2. \tag{0}$$

This condition can also be interpreted as expressing that the triangle with sides of lengths a, b, and c has a right angle. The question is:

> Do there exist Pythagorean triples with exactly *two* elements in common, when interpreted as sets?

By examining the following list of Pythagorean triples it is clear that no element in common or a single element in common is quite possible (the latter even in ''many ways'').

(3, 4, 5) (5,12,13) (6, 8,10) (8,15,17)

(9,12,15) (9,40,41) (16,63,65) (33,56,65)

THE ANALYSIS OF PYTHAGOREAN TRIPLES

Before settling the above question in the negative we present the well-known analysis of Pythagorean triples, which gives a parameterized solution of (0). We use the following notations.

$d \mid x$ means d is a positive divisor of x

x **gcd** y is the greatest common divisor of x and y

x **mod** d is the remainder of x divided by d

We recall a couple of important elementary properties:

$$d \mid x \wedge d \mid y \Rightarrow d \mid (x+y) \tag{1}$$

$$d \mid (x \textbf{ gcd } y) \equiv d \mid x \wedge d \mid y$$

$$x \mid y \equiv x \textbf{ gcd } y = x$$

$$x \textbf{ gcd } y = y \textbf{ gcd } x \quad \text{(symmetry)}$$

$$(x \textbf{ gcd } y) \textbf{ gcd } z = x \textbf{ gcd } (y \textbf{ gcd } z) \quad \text{(associativity)}$$

$$x(y \textbf{ gcd } z) = xy \textbf{ gcd } xz \quad \text{(distribution)}$$

$$x \mid x \wedge x \textbf{ gcd } x = x \quad \text{(idempotence)}$$

$$1 \mid x \wedge 1 \textbf{ gcd } x = 1$$

When x **gcd** $y = 1$, we call x and y *coprime*. As instructive examples we derive the following two lemmas.

Lemma 0

If x and y are coprime, then so are x and y **gcd** z for any z.

Proof Assuming x **gcd** $y = 1$ we compute

$$x \textbf{ gcd } (y \textbf{ gcd } z)$$

$=$ { associativity }

$(x \textbf{ gcd } y) \textbf{ gcd } z$

$=$ { assumption }

$1 \textbf{ gcd } z$

$=$ { property }

1

□

Lemma 1

If x and y are coprime and $xy = z^2$, then $x = (x \textbf{ gcd } z)^2$ and $y = (y \textbf{ gcd } z)^2$.

Proof Assuming $x \textbf{ gcd } y = 1$ and $xy = z^2$ we compute

$(x \textbf{ gcd } z)^2$

$=$ { three times distribution }

$(x^2 \textbf{ gcd } zx) \textbf{ gcd } (xz \textbf{ gcd } z^2)$

$=$ { associativity }

$x^2 \textbf{ gcd } ((zx \textbf{ gcd } xz) \textbf{ gcd } z^2)$

$=$ { idempotence, using $zx = xz$ }

$x^2 \textbf{ gcd } (xz \textbf{ gcd } z^2)$

$=$ { assumption $xy = z^2$ }

$x^2 \textbf{ gcd } (xz \textbf{ gcd } xy)$

$=$ { twice distribution }

$x(x \textbf{ gcd } (z \textbf{ gcd } y))$

$=$ { Lemma 0, using symmetry and assumption $x \textbf{ gcd } y = 1$ }

x

Because of the symmetry in the statement we also have $y = (y \textbf{ gcd } z)^2$.

□

Let us now proceed with the analysis of our ''generic'' Pythagorean triple (a,b,c). Obviously, we have $a<c$ and $b<c$. Furthermore, from (0) and the fact that x^2 has an even number of factors 2, follows that $a\neq b$. Hence, the three numbers in a Pythagorean triple are distinct. Observe that (b,a,c) is also Pythagorean. Therefore, a set of three positive integers defines zero or two (essentially equivalent) Pythagorean triples.

A Pythagorean triple is called *primitive* when one is their only common divisor, that is, when their **gcd** equals 1. A common divisor of any two of a, b, and c, however, is by virtue of (0) also a divisor of the third element. So in a primitive triple all pairs are coprime. Observing that (da,db,dc) is also Pythagorean, it appears to be sufficient to study the primitive Pythagorian triples. We now assume that our triple is primitive.

We argue that exactly one of a and b is even (hence, the other odd). For that purpose we use

Lemma 2

If x is even, then $x^2 \textbf{ mod } 4 = x^2 \textbf{ mod } 2 = 0$;

if x is odd, then $x^2 \textbf{ mod } 8 = x^2 \textbf{ mod } 4 = x^2 \textbf{ mod } 2 = 1$.

Proof If $x=2y$ we have

$$x^2=(2y)^2=4y^2,$$

and if $x=2y+1$ we obtain

$$x^2=(2y+1)^2=4y^2+4y+1=4y(y+1)+1,$$

observing that one of y and $y+1$ is even.

□

Not both a and b are even, since they are coprime. If they were both odd, then on account of (0) and Lemma 2 we would have $1+1=c^2 \textbf{ mod } 4$, but this is impossible by Lemma 2. Thus, one of a and b is odd and the other is even and, hence, c is odd. Without loss of generality, assume that b is even, say $b=2k$ (not necessarily $a<b$). Since a and c are now both odd, we can define integers u and v by

$$u=(c+a)/2,$$

$$v=(c-a)/2.$$

Using that a and c are coprime and applying

Lemma 3

If x and y are both odd and $x>y$, then x **gcd** $y = w$ **gcd** z, where $w=(x+y)/2$ and $z=(x-y)/2$.

Proof Use $w+z=x$, $w-z=y$ and (1).

□

we see that u and v are also coprime. Furthermore, we have

$$4k^2=b^2=c^2-a^2=(c+a)(c-a)=4uv.$$

From $k^2=uv$ and u **gcd** $v=1$ follows, by Lemma 1, that both u and v are squares, say $u=m^2$ and $v=n^2$. Thus, every primitive solution of (0) with even b can be written as:

$$\begin{cases} a=u-v=m^2-n^2 \\ b=2\sqrt{uv}=2mn \\ c=u+v=m^2+n^2, \end{cases} \tag{2}$$

where

$$\begin{cases} m=\dfrac{b}{2}\ \textbf{gcd}\ \dfrac{c+a}{2} \\ n=\dfrac{b}{2}\ \textbf{gcd}\ \dfrac{c-a}{2}. \end{cases}$$

By their construction these m and n satisfy

$$\begin{cases} m>n \\ m\ \textbf{gcd}\ n=1 \\ m-n \text{ odd.} \end{cases} \tag{3}$$

Conversely, every pair m and n satisfying (3) yields via (2) a primitive Pythagorean triple with even b. We leave this as an exercise to the reader. As is readily verified, the general solution (with even b) of (0) is now given by

$$\begin{cases} a=d(m^2-n^2) \\ b=2dmn \qquad \text{for } m>n \\ c=d(m^2+n^2). \end{cases} \tag{4}$$

This concludes our analysis of individual Pythagorean triples. Before embarking on the final solution it is useful to include two more lemmas.

Lemma 4

If x and y are coprime and $d \mid xy$, then $d = (d \textbf{ gcd } x)(d \textbf{ gcd } y)$.

Proof Assuming $x \textbf{ gcd } y = 1$ and $d \mid xy$ we compute

$(d \textbf{ gcd } x)(d \textbf{ gcd } y)$

$=$ { three times distribution }

$(d^2 \textbf{ gcd } xd) \textbf{ gcd } (dy \textbf{ gcd } xy)$

$=$ { associativity, and $xd = dx$ }

$(d^2 \textbf{ gcd } (dx \textbf{ gcd } dy)) \textbf{ gcd } xy$

$=$ { twice distribution }

$d(d \textbf{ gcd } (x \textbf{ gcd } y)) \textbf{ gcd } xy$

$=$ { $x \textbf{ gcd } y = 1$ assumed }

$d(d \textbf{ gcd } 1) \textbf{ gcd } xy$

$=$ { property }

$d \textbf{ gcd } xy$

$=$ { property, using assumption $d \mid xy$ }

d

□

Lemma 5

If x and v are coprime, y and u are coprime, and $xy = uv$, then $x = u$ and $y = v$.

Proof Assuming $x \textbf{ gcd } v = 1$ and $xy = uv$ we derive

$1 = y \textbf{ gcd } u$

$\equiv$ { arithmetic ($x \neq 0$ by convention) }

$x = x(y \textbf{ gcd } u)$

$\equiv$ { distribution }

$x = xy \textbf{ gcd } xu$

$\equiv$ { $xy = uv$ assumed }

$x = uv$ **gcd** xu

$\equiv$ { distribution, using $xu = ux$ }

$x = u(v$ **gcd** $x)$

$\equiv$ { x **gcd** $v = 1$ assumed }

$x = u$

$\equiv$ { $xy = uv$ assumed }

$y = v$

□

In a similar vein one can prove results like: x and y are coprime if and only if x^2 and y^2 are coprime. This result is tacitly used below (to keep you alert).

THE SOLUTION

We now address the question stated earlier: Are there Pythagorean triples that have exactly two elements in common? We shall show that no such triples exist by the method of *infinite descent* due to Fermat. This can be translated into a proof by mathematical induction if one prefers so.

First, however, we superficially analyze the relationship between two such desired triples. If they have their smallest two elements in common, then they have equal largest elements as well and, hence, the triples are equal (as sets, that is). If they have the same largest element and one of the others in common, then they are also equal (as sets). Therefore, the only case to be examined further is two triples where the largest of one is among the smallest two of the other. That is, we consider two triples (a, b, c) and (b, c, d) with

$$\begin{cases} a^2+b^2=c^2 \\ b^2+c^2=d^2 \end{cases} \tag{5}$$

(not necessarily $a < b$). Since this relation implies

a **gcd** b **gcd** $c = b$ **gcd** c **gcd** d,

we may assume without loss of generality that both triples are primitive. In that case our preceeding analysis has shown that exactly one of a and b, and exactly one of b and c are even; therefore, b is

even. That is, a pair of primitive candidate triples must have the same even element. We shall construct another pair of primitive Pythagorean triples with exactly two elements in common, but which have a smaller common even element than the original pair. Now recall that the elements are positive. So, according to the principle of infinite descent there do not exist such Pythagorean triples with exactly two elements in common.

Because the Pythagorean triples (a,b,c) and (b,c,d) are primitive, they are generated by pairs m,n and k,l respectively. We have the following relations:

$$\begin{array}{ll} m>n & k>l \\ m \textbf{ gcd } n=1 & k \textbf{ gcd } l=1 \\ m-n \text{ odd} & k-l \text{ odd} \\ a=m^2-n^2 & \\ b=2mn & b=2kl \\ c=m^2+n^2 & c=k^2-l^2 \\ & d=k^2+l^2 \end{array} \tag{6}$$

Eliminating b and c by combining their expressions yields

$$kl=mn \tag{7}$$

$$k^2=l^2+m^2+n^2 \tag{8}$$

We define e, f, g, and h by

$$e=l \textbf{ gcd } m$$

$$f=l \textbf{ gcd } n$$

$$g=k \textbf{ gcd } m$$

$$h=k \textbf{ gcd } n$$

From (6) and Lemma 0 follows that e, f, g, and h are pairwise coprime. From (6) and Lemma 4, using (7), we obtain

$$k=gh$$

$$l=ef$$

$$m=eg$$

$$n=fh$$

Substituting these results in (8) yields

$$(gh)^2=(ef)^2+(eg)^2+(fh)^2$$

or, equivalently,

$$g^2h^2=e^2f^2+e^2g^2+f^2h^2. \tag{9}$$

Taking (8) modulo 8, using Lemma 2 and the restrictions on the parity of k, l, m, and n from (6), tells us that k is odd (since k even would imply $0=1+1+0$ or $0=1+1+4$). Then both g and h are odd and, furthermore, exactly one of e and f is even (l and one of m and n is even). Assume that f is even; the other case is completely analogous. In that case e is odd and, therefore, h^2+e^2 and h^2-e^2 are even. So (9) can be rewritten as

$$g^2\left(\frac{h^2-e^2}{2}\right)=\left(\frac{h^2+e^2}{2}\right)f^2. \tag{10}$$

Recalling that e, f, g, and h are pairwise coprime and observing that $(h^2+e^2)/2$ and $(h^2-e^2)/2$ are coprime on account of Lemma 3, we can apply Lemma 5 to (10) giving

$$g^2=(h^2+e^2)/2,$$

$$f^2=(h^2-e^2)/2.$$

Subtracting and adding these equations yields

$$e^2+f^2=g^2,$$

$$f^2+g^2=h^2.$$

Thus (e,f,g) and (f,g,h) constitute another pair of primitive Pythagorean triples with exactly two elements in common, and for the even element f we have $f < 2efgh=b$.

This concludes the nonexistence proof.

EQUIVALENT PROBLEMS

We mention several equivalent formulations of our problem as expressed in (5). For instance, by isolating b^2, equation system (5) can also be written as

$$c^2-a^2=d^2-c^2=b^2.$$

Put in this way the question is: Can you find three squares (a^2, c^2, and d^2) in *Arithmetic Progression*, under the additional constraint that the common difference (i.e., additive constant) is itself also a square (b^2)? Fermat posed this problem in 1636 (cf. [0], p. 435).

Another formulation directly derived from (5) is

$$\begin{cases} c^2-b^2=a^2 \\ c^2+b^2=d^2. \end{cases} \tag{11}$$

This asks whether it is possible to make the expressions c^2-b^2 and c^2+b^2 both squares (using the same values for b and c in both expressions). Euler called two expressions *concordant forms* if they could be made squares simultaneously (cf. [0], p. 473). So our problem could be stated as: Are c^2-b^2 and c^2+b^2 concordant forms?

The equation system (11) has been generalized. Positive integer k is called a *congruent number* when

$$\begin{cases} c^2-kb^2=a^2 \\ d^2+kb^2=d^2 \end{cases} \tag{12}$$

has non-trivial solutions. Our problem, therefore, translates into: Is 1 a congruent number? Bouwkamp [1] explained to me that congruent numbers are still not completely understood. For instance, he has designed an algorithm that enumerates all congruent numbers, but in a haphazard order. It is not known, in general, how to decide whether a number is congruent.

The transformation

$$\begin{cases} a=x-y \\ b=2z \\ c=x+y \end{cases}$$

gives a one-to-one correspondence between solutions of (12) and

$$\begin{cases} x^2+y^2=c^2 \\ xy/2=kz^2 \end{cases} \tag{13}$$

Therefore, k is a congruent number if and only if there exists an integer right triangle, the area of which is k times a square. Thus, our problem can be paraphrased as: Is the area of an integer right triangle ever a square? Fermat explicitly solved this version of our problem. In fact, it is said to be ‘‘the only instance of a detailed proof left by him’’ (cf. [0], p. 615). The proof is, of course, by infinite descent, and is, for example, presented in [0] (p. 615), [2] (Ch. 8-6), and [3] (Ch. II, §X). According to [3]

(p. 14) this was one of Fermat's major discoveries. We were not aware of the connection with this version of the problem until after our proof was found.

The last restatement that we give of our problem derives from (11) using Lemma 4: Has the equation

$$c^4 - b^4 = x^2$$

non-trivial solutions? That is, can the hypotenuse and another side of an integer right triangle both have square lengths?

We have not been able to locate our version of the problem in the literature.

REFERENCES

[0] L.E. Dickson, *History of the Theory of Numbers*, Vol. II (Diophantine Analysis), New York: Chelsea Publishing Company, 1966.

[1] C.J. Bouwkamp (Eindhoven University of Technology), private communication.

[2] O. Ore, *Number Theory and its History*, New York: McGraw-Hill, 1948.

[3] A. Weil, *Number Theory: An Approach through History; From Hammurapi to Legendre*, Boston: Birkhäuser, 1984.