ON INDEPENDENT PYTHAGOREAN NUMBERS

Konstantine Zelator
(formerly known as Konstantine Spyropoulos)
Department of Mathematics, Carnegie Mellon University, Pittsburgh, PA 15213
(Submitted October 1991)

INTRODUCTION

In a paper of Sypriya Mohanty and S. P. Mohanty (refer to [1]), the notion of an independent Pythagorean number is introduced and discussed. Recall that any Pythagorean triple (x, y, z) may be represented by

$$x = 2uvt,\ \ y = t(u^2 - v^2),\ \ z = t(u^2 + v^2) \tag{1}$$

where u and v are relatively prime natural numbers of opposite parity, that is, $u + v \equiv 1 \pmod 2$, $(u, v) = 1$, $u > v$, and t some natural number.

In the same paper, Definition 1 (p. 31) calls the area of a Pythagorean triangle a "Pythagorean number." And that of a primitive Pythagorean triangle a " primitive Pythagorean number." Thus, a Pythagorean number is a positive integer of the form

$$A = \frac{1}{2}(2uvt)[t(u^2 - v^2)] = t^2uv(u^2 - v^2), \tag{2}$$

where the natural numbers u and v satisfy the above conditions.

When the Pythagorean triangle at hand is primitive, i.e., when $t = 1$, we obtain the general form of a primitive Pythagorean number described by

$$B = uv(u^2 - v^2). \tag{3}$$

The authors define the notion of an independent Pythagorean number and they prove that there exist infinitely many primitive Pythagorean numbers that are not independent (Theorem 10, p. 40). According to that definition (Definition 2, p. 40), a Pythagorean number is called independent if it cannot be obtained from another Pythagorean number by multiplying the latter by t^2, where t is a natural number > 1.

Note that if a Pythagorean number is independent, it must be primitive. The converse, of course, is false, as the authors have proved: there exist (infinitely many) primitive Pythagorean numbers that are not independent.

In this paper, we will address Problem 2 in the author's paper. Namely, find sufficient conditions for an integer B to be an independent Pythagorean number. We will find families of primitive Pythagorean numbers that are independent. First, we will state the two theorems of this paper, then their proofs.

Theorem 1: Let u and v be natural numbers such that $u + v \equiv 1 \pmod 2$, $(u, v) = 1$, and $u > v$. Assume that either

(a) all four numbers $u, v, u - v$, and $u + v$ are squarefree (the case $v = 1$ included), or

(b) the three integers $u - v, u + v$, and $\frac{uv}{4}$ are all squarefree and $\frac{uv}{4}$ odd (the case $v = 1$ included).

Then the primitive Pythagorean number $uv(u^2 - v^2)$ is independent.

Theorem 2: Let $p > 3$ be a prime and $v \geq 1, w \geq 3$ be odd squarefree natural numbers (the case $v = 1$ included) both of whose (distinct) prime divisors are all congruent to 1 mod p. Let n be a positive integer and r an odd prime distinct from p and the prime divisors of w. Assume that $(u, v) = 1$, where $u = 2^n \cdot r \cdot {}^2w$. Furthermore, suppose that $u - v$ is a squarefree integer such that each of its prime divisors is congruent to 1 mod p and that $u + v$ is a squarefree integer containing exactly one prime divisor $q \not\equiv 1 \pmod{p}$, while the rest of its prime divisors, if any, are all congruent to 1 modulo p. Assume that $n = 1$ or $n = 2$.

Then the primitive Pythagorean number $uv(u^2 - v^2)$ is independent.

Proof of Theorem 1: Suppose that

$$uv(u^2 - v^2) = t^2 \cdot b \tag{4}$$

where b is a Pythagorean number and t some positive integer. Since b is a Pythagorean number, according to (2), b must be of the form

$$b = T^2 \cdot U \cdot V(U^2 - V^2), \tag{5}$$

for some positive integers T, U and V where

$$U > V, U + V \equiv 1 \pmod{2} \text{ and } (U, V) = 1. \tag{6}$$

Substituting for b in (4), we obtain

$$\begin{aligned} uv(u^2 - v^2) &= t^2 \cdot T^2 \cdot U \cdot V \cdot (U^2 - V^2) \text{ or} \\ uv(u - v)(u + v) &= t^2 \cdot T^2 \cdot U \cdot V \cdot (U^2 - V^2). \end{aligned} \tag{7}$$

If hypothesis (a) is satisfied, then the product $uv(u - v)(u + v)$ must be a squarefree integer, since each of the numbers $uv, u - v$, and $u + v$ is squarefree, and these three integers are mutually coprime in view of $(u, v) = 1$ and $u + v = 1 \pmod{2}$. Then (7) clearly implies $t^2T^2 = 1 \Rightarrow tT = 1 \Rightarrow t = T = 1$.

If hypothesis (b) is satisfied, 4 must exactly divide the left-hand side of (7). Since $uv \equiv 0$ and $u \pm v \equiv 1 \pmod{2}$, t^2T^2 must be odd and $uv \equiv 0 \pmod{4}$. Dividing (7) by 4, we obtain

$$\frac{uv}{4} \cdot (u - v)(u + v) = t^2T^2 \cdot \frac{UV}{4} \cdot (U^2 - V^2) \tag{8}$$

Since the left-hand side of (8) is an odd squarefree integer, we have $t^2T^2 = 1 \Rightarrow tT = 1 \Rightarrow t = T = 1$. Hence, $uv(u^2 - v^2)$ is an independent Pythagorean number.

Proof of Theorem 2: Evidently, according to the hypothesis, the Pythagorean number $uv(u^2 - v^2)$ must be of the form

$$uv(u^2 - v^2) = uv(u - v)(u + v) = 2^n \cdot q \cdot r^2 \cdot p_1 \cdots p_m,,$$

where all the odd primes $q, r, p_1, \cdots, p_m$ are distinct and $p_1 \equiv \cdots \equiv p_m \equiv 1 \pmod{p}$. Suppose that

$$2^n \cdot q \cdot r^2 \cdot p_1 \cdots p_m = t^2 ab(a-b)(a+b), \tag{9}$$

where the positive integers a and b have opposite parity, $(a,b)=1$, and $a>b$. Assume that a is odd and b even (the case a even and b odd is treated in exactly the same way). We set $b = 2^k \cdot B$, B odd, and $t = 2^\delta T$ in (9) to obtain

$$2^n \cdot q \cdot r^2 \cdot p_1 \cdots p_m = T^2 \cdot 2^{2\delta+k} \cdot a \cdot B(a-2^k \cdot B)(a+2^k \cdot B), \tag{10}$$

which gives

$$q \cdot r^2 \cdot p_1 \cdots p_m = T^2 \cdot a \cdot B(a-2^k \cdot B)(a+2^k \cdot B), \tag{11}$$

since we must have $2\delta + k = n$; with $1 \le k \le n$, $\delta \ge 0$, and T odd.

First, we will prove that (11) cannot be satisfied for T odd and $T > 1$. Let us assume to the contrary that (11) is satisfied for some $T > 1$ and T odd. In view of the fact that the left-hand side of (11) represents the unique factorization of the right-hand side of (11) into powers of distinct primes and because r^2 is the only square of a prime, it is rather obvious that we must have $T = r$; hence, (11) implies

$$q \cdot p_1 \cdots p_m = a \cdot B(a-2^k \cdot B)(a+2^k \cdot B). \tag{12}$$

Since $p_1 \equiv \cdots \equiv p_m \equiv 1 \pmod{p}$, (12) clearly shows that if $q|aB$, then $a - 2^k B \equiv 1$ and $a + 2^k B \equiv 1 \pmod{p}$; so $2a \equiv 2$ and $2^{k+1} B \equiv 0 \pmod{p}$; therefore if $q|aB$,

$$a \equiv 1 \text{ and } B \equiv 0 \pmod{p}, \tag{13}$$

which is a contradiction, since p as a divisor of B would divide the left-hand side of (12), contrary to the fact that p is distinct from q, $p_1, \cdots, p_m$. Next, suppose that $q|(a-2^k \cdot B)$ or that $q|(a+2^k \cdot B)$. Equation (12) clearly implies in such a case, $a \equiv B \equiv 1 \pmod{p}$. Also if $q|a-2^k \cdot B$, we must have $a - 2^k \cdot B \equiv q \pmod{p}$; and since $a \equiv 1 \pmod{p}$, we end up with $2 \equiv q+1 \pmod{p} \Rightarrow q \equiv 1 \pmod{p}$, contradicting the hypothesis again [note that $a - 2^k B \equiv q$ and $a + 2^k B \equiv 1 \pmod{p}$ or vice versa].

Hence, we conclude that (11) is not possible with $T > 1$. Consequently, $T = 1$; thus, from $t = 2^\delta \cdot T$, we obtain $t = 2^\delta$. We will show that $\delta = 0$. According to the hypothesis, $n = 1$ or 2. If $n = 1$, then, from $2\delta + k = n$ and $k \ge 1$, we immediately obtain $\delta = 0$. For $n = 2$, again we must have $\delta = 0$, in view of $2\delta + k = n$ and $k \ge 1$. Therefore, $\delta = 0$, and since we also have $T = 1$, it follows that $t = 2^\delta T \Rightarrow t = 1$. The proof is complete.

REFERENCE

1. Supriya Mohanty & S. P. Mohanty. "Pythagorean Numbers." *Fibonacci Quarterly* **28.1** (1990):31-42.

AMS numbers: 11A99; 11A25; 11D99

❖❖❖