ON A CLASS OF NON-CONGRUENT AND NON-PYTHAGOREAN NUMBERS

Konstantine Dabmian Zelator*
Department of Mathematics, Carnegie Mellon University, Pittsburgh, PA 15213
(*Submitted August 1993*)

In one of his famous results, Fermat showed that there exists no Pythagorean triangle with integer sides whose area is an integer square. His elegant method of proof is one of the first known examples in the history of the theory of numbers where the method of infinite descent is employed. Mohanty [3] has defined a Pythagorean number as the area of a Pythagorean triangle and studied properties of such numbers. Fermat has thus shown that no Pythagorean number can be an integer square.

To extend Fermat's result, one may ask if there exists a Pythagorean triangle whose area is p times a perfect square, p a given prime. It turns out that, for certain primes $p \equiv 1, 5, 7 \pmod 8$, this is the case; for example, the primes $p = 5, 7, 41$ have this property. For $p = 5$, the triangle $(3^4 - 1, 8, 3^4 + 1)$ has area $A = 5(3 \cdot 4)^2$. For $p = 7$, the triangle $(4^4 - 3^4, 2 \cdot 4^2 \cdot 3^2, 4^4 + 3^4)$ has area $A = 7 \cdot (3 \cdot 4 \cdot 5)^2$. For $p = 41$, the triangle $(5^4 - 4^4, 2 \cdot 5^2 \cdot 4^2, 5^4 + 4^4)$ has area $A = 41 \cdot (5 \cdot 4 \cdot 3)^2$. However, as shown below, no Pythagorean number can equal p times an integer square if p is a prime congruent to 3 (mod 8).

A natural question to ask is whether there exists a number $k \equiv 3 \pmod 8$ and a Pythagorean number which equals k times a square. There is no reason to believe that such a number of k does not exist. Furthermore, one may attempt to find infinitely many such numbers k.

In this paper the following result is proven. Let k be an odd squarefree positive integer with $k \equiv 3 \pmod 8$. Assume that k belongs to one of the following families:

Family (a): $k = p_1$, where p_1 is a prime with $p_1 \equiv 3 \pmod 8$.

Family (b): $k = p_1 p_2$, where p_1 and p_2 are primes such that $p_1 \equiv 5 \pmod 8$ and $p_2 \equiv 7 \pmod 8$, with p_1 being a quadratic nonresidue of p_2 (so, by quadratic reciprocity, p_2 is also a nonresidue of p_1).

Family (c): $k = p_1 p_2 \ldots p_n, n \geq 2$, where $p_1 p_2 \ldots p_n$ are distinct primes such that $p_1 \equiv 3 \pmod 8$, $p_2 \equiv \cdots \equiv p_n \equiv 1 \pmod 8$; the primes $p_2, \ldots, p_n$ are all quadratic residues of each other, and they are all quadratic nonresidues of p_1 (so, by quadratic reciprocity, p_1 is a quadratic nonresidue of $p_2, \ldots, p_n$ as well).

Family (d): $k = p_1 p_2 p_3 \cdots p_n$, $n \geq 3$, where $p_1, p_2, p_3, \ldots, p_n$ are distinct primes such that $p_1 \equiv 5 \pmod 8$, $p_2 \equiv 7 \pmod 8$, and $p_3 \equiv \cdots \equiv p_n \equiv 1 \pmod 8$, with p_1 being a quadratic nonresidue of p_2 (so, by quadratic reciprocity, p_2 is a nonresidue of p_1 as well) and $p_3, \ldots, p_n$ being quadratic residues of each other; and **either** with $p_3, \ldots, p_n$ being quadratic residues of p_1 (so, by quadratic reciprocity, p_1 is a quadratic residue of $p_3, \ldots, p_n$) and with $p_3, \ldots, p_n$ being quadratic nonresidues of p_2 (so, by reciprocity, p_2 is a quadratic nonresidue of $p_3, \ldots, p_n$) **or** vice-versa.

---

* Formerly known as Konstantine Spyropoulos.

Theorem: Let k be an odd squarefree positive integer, $k \equiv 3 \pmod 8$ and suppose that k belongs to one of the families (a)-(d) listed above. Then there is no Pythagorean triangle whose area equals k times an integer square.

Proof: Let (A, B, C) be a Pythagorean triple whose area is k times a square, $\frac{1}{2}AB = kD^2$. One easily sees that we may assume $(A, B) = 1$, for if it were otherwise, the problem would reduce to the case of a Pythagorean triple (A_1, B_1, C_1) with $(A_1, B_1) = 1$ and $\frac{1}{2}A_1B_1 = kD_1^2$. By assuming that (A, B, C) is a primitive Pythagorean triple, we may set $A = M^2 - N^2$, $B = 2MN$, $C = M^2 + N^2$, for positive integers M, N with $(M, N) = 1$ and $M + N \equiv 1 \pmod 2$. Thus, from $\frac{1}{2}AB = kD^2$, one obtains

$$(M-N)(M+N)MN = kD^2. \tag{1}$$

Since $(M, N) = 1$ and $M + N \equiv 1 \pmod 2$, we have

$$\begin{aligned}(M,N) &= (M, M+N) = (M, M-N) = (N, M-N)\\ &= (N, M+N) = (M-N, M+N) = 1.\end{aligned} \tag{2}$$

Thus, all the factors $M-N, M+N, M,$ and N on the left-hand side of (1) are pairwise relatively prime. Therefore, since k is squarefree, there are precisely four cases or possibilities and their ramifications.

The first possibility is that precisely one of the factors on the left-hand side of (1) is equal to k times a square, while the rest of them are perfect squares.

The second possibility is that one of $M+N, M-N, M,$ or N equals a times a square, another of the factors equals b times a square, and the other two factors are integer squares with $ab = k$ and $1 < a, b < k$.

The third possibility is that one of the factors equals a times a square, another equals b times a square, a third equals c times a square, and the fourth is just an integer square with $abc = k$ and $1 < a, b, c < k$.

The fourth possibility is that $M = aM_1^2$, $N = bN_1^2$, $M + N = cU^2$, $M - N = dV^2$, with $abcd = k$ and $1 < a, b, c, d < k$.

Case 1. Exactly one of $M+N, M-N, M,$ or N equals k times an integer square, while the remaining three are integer squares.

First, suppose $M = kM_1^2, N = N_1^2, M - N = U^2, M + N = V^2$. Consequently, we obtain

$$kM_1^2 - N_1^2 = U^2, \tag{3}$$
$$kM_1^2 + N_1^2 = V^2. \tag{4}$$

Thus, $2kM_1^2 = U^2 + V^2$ and $(U, V) = 1$ by (2). However, the last equation constitutes a contradiction, since $k \equiv 3 \pmod 4$, and it is well known that no prime congruent to 3 (mod 4) divides the sum of two relatively prime integer squares.

Next, suppose that $N = kN_1^2, M = M_1^2, M - N = U^2, M + N = V^2$. Thus,

$$M_1^2 - kN_1^2 = U^2, \tag{5}$$
$$M_1^2 + kN_1^2 = V^2. \tag{6}$$

Since $M+N \equiv 1 \pmod 2$, we also have $M_1+N_1 \equiv 1 \pmod 2$. But then equation (6) implies, by virtue of $k \equiv 3 \pmod 4$, that $M_1 \equiv 1 \pmod 2$ and $N_1 \equiv 0 \pmod 2$. Moreover, $(M_1, N_1)=1$, so $(N_1, U)=1$ as well. By adding (5) and (6), we obtain

$$2M_1^2 = U^2 + V^2. \tag{7}$$

Clearly, we may assume M_1, U, and V to be positive (recall $M, N \neq 0$), and since (2) implies that $(U, V)=1$, it follows (see [2], p. 427, lines 4 and 5) that

$$M_1 = m^2+n^2,\ U = m^2+2mn-n^2,\ V = n^2+2mn-m^2 \tag{8}$$

for positive integers m, n with $m+n \equiv 1 \pmod 2$ and $(m,n)=1$. Consequently, combining (6) and (8), we have

$$\begin{aligned} kN_1^2 &= V^2 - M_1^2 = (V-M_1)(V+M_1) \\ &= (2mn-2m^2)(2n^2+2mn) = 4mn(n-m)(n+m); \end{aligned}$$

thus,

$$kN_2^2 = (n-m)(n+m)\cdot m \cdot n, \tag{9}$$

where $N_1 = 2N_2$. Therefore, $(n^2-m^2, 2mn, m^2+n^2)$ is a primitive Pythagorean triple whose area equals kN_2^2. But $kN_1^2 = V^2 - M_1^2 \leq V^2 = M+N$. Hence, $0 < n+m < M+N$; thus, an infinite descent with respect to the initial equation (1) is established.

Now suppose that $M = M_1^2, N = N_1^2, M-N = kU^2$, and $M+N = V^2$. Then

$$M_1^2 - N_1^2 = kU^2, \tag{10}$$
$$M_1^2 + N_1^2 = V^2. \tag{11}$$

Adding (10) and (11), we obtain

$$2M_1^2 = kU_1^2 + V^2. \tag{12}$$

Now, since $U \equiv V \equiv 1 \pmod 2$, (12) implies $2M_1^2 \equiv k+1 \pmod 8$; hence, $k \equiv 2M_1^2 - 1 \equiv \pm 1$ (mod 8). But $k \equiv 3 \pmod 8$, so this is a contradiction.

Finally, suppose that $M = M_1^2, N = N_1^2, M-N = U^2$, and $M+N = kV_1^2$. This leads to a contradiction, since $M+N = M_1^2 + N_1^2 = kV_1^2$, $k \equiv 3 \pmod 4$ and $(M_1, N_1)=1$. This concludes the proof of Case 1.

Case 2. One of $M+N, M-N, M$, or N is a times a square, one is b times a square, and the other two are squares, with $ab = k \equiv 3 \pmod 8$ and $1 < a, b < k$. Note that $ab \equiv 3 \pmod 8$ implies that either $a \equiv 3, b \equiv 1 \pmod 8$ or vice versa, or $a \equiv 5, b \equiv 7 \pmod 8$ or vice versa. First, suppose that $a \equiv 1, b \equiv 3 \pmod 8$. Since $ab = k$ with $1 < a, b < k$, it follows that k belongs to Family (c) or Family (d) of the Theorem.

If k belongs to Family (c), then $k = p_1 \cdot p_2 \cdot \cdots \cdot p_n$ with $p_1 \equiv 3 \pmod 8$ and $p_2 \equiv p_3 \equiv \cdots \equiv p_n \equiv 1 \pmod 8$. Also, $a = q_1 \cdot q_2 \cdot \cdots \cdot q_k$ and $b = p_1$ or $b = p_1 q_{k+1} q_{k+2} \cdots q_{n-1}$, where the two sets of q's are disjoint and their union is $\{p_2, p_3, \ldots, p_n\}$. All the various subcases of Case 2 lead to a congruence of the form $b \cdot R^2 \equiv e \cdot L^2 \pmod{q_1}$, with $(bR, q_1) = 1$ and where $e = 1, -1, 2$, or -2; thus, since $q_1 \equiv 1 \pmod 8$, b is a quadratic residue of q_1. On the other hand, according to the hypothesis, p_1 is a quadratic nonresidue and $q_{k+1}, q_{k+2}, \ldots, q_{n-1}$ are all quadratic residues of q_1. Thus, b is a quadratic nonresidue of q_1, a contradiction.

If k belongs to Family (d), then $k = p_1 \cdot p_2 \cdot \cdots \cdot p_n$ with $p_1 \equiv 5$, $p_2 \equiv 7$, and $p_3 \equiv p_4 \equiv \cdots \equiv p_n \equiv 1 \pmod 8$. Thus, as above, $a = q_1 \cdot q_2 \cdot \cdots \cdot q_k$ and $b = p_1 p_2$ or $b = p_1 p_2 q_{k+1} \cdots q_{n-2}$, where the two sets of q's are disjoint and their union is $\{p_3, p_4, \ldots, p_n\}$. Again, as above, b is a quadratic residue of q_1. Also, according to the hypothesis, each of $q_{k+1}, q_{k+2}, \ldots, q_{n-2}$ are quadratic residues of q_1, and **either** p_1 is a quadratic residue of q_1 and p_2 is a quadratic nonresidue of q_1 **or** p_1 is a quadratic nonresidue of q_1 and p_2 is a quadratic residue of q_1. In any event, we see that b must be a quadratic nonresidue of q_1. This contradiction completes the proof of this subcase.

Since the proofs for the remaining subcases and cases are similar to those above, we omit the details, except to note that Legendre's theorem (see [2], p. 422) is used in these proofs.

Recall that a natural number k is a congruent number if there exist natural numbers a, b, and c with $a^2 + b^2 = c^2$ and $2ab = k$. We now have the following corollary.

Corollary: If k is an integer satisfying the hypothesis of the Theorem, then kd^2, for any positive integer d, is a non-congruent number.

Proof: Since an integer kd^2 is congruent if and only if there exist nonzero integers a, b, and c such that $a^2 + b^2 = c^2$ and $2ab = kd^2$, if kd^2 were a congruent number, then we would have $(2a)^2 + (2b)^2 = (2c)^2$ and $\frac{1}{2}(2a)(2b) = k \cdot d^2$, which implies that $(2a, 2b, 2c)$ is a Pythagorean triangle whose area equals k times an integer square, contradicting the Theorem.

REFERENCES

1. W. Sierpinski. *Elementary Theory of Numbers*, p. 64. Warsaw, 1964.
2. L. E. Dickson. *History of the Theory of Numbers* **II**:422. Second ed. New York: Chelsea Publishing Co., 1952.
3. S. Mohanty. "Pythagorean Numbers." *The Fibonacci Quarterly* **28.1** (1988):31-42.

AMS Classification Numbers: 11A99, 11A25, 11D9