

ON THE SOLUTIONS OF THE CONGRUENCE $n^2 \equiv 1 \pmod{\phi^2(n)}$

FLORIAN LUCA AND MICHAL KRŽIŽEK

(Communicated by David E. Rohrlich)

ABSTRACT. In this note, we show that if n is a positive integer satisfying the congruence $n^2 \equiv 1 \pmod{\phi^2(n)}$, then $n \leq 3$.

For any positive integer n let $\phi(n)$ be the value of the Euler function at n .

Very little is known (see problem **B37** in [2]) about the composite values of n for which $n \equiv 1 \pmod{\phi(n)}$. D. H. Lehmer conjectured there there is no such n and Pomerance (see [5]) showed that the number of composite n less than x satisfying the above congruence is

$$(1) \quad O(x^{1/2}(\log x)^{3/4}(\log \log x)^{-1/2}).$$

In this note, we look at the positive integers n satisfying

$$(2) \quad n^2 \equiv \pm 1 \pmod{\phi^2(n)}.$$

Our result is

Theorem. *If n satisfies congruence (2), then $n \in \{1, 2, 3\}$.*

We begin with the following lemmas.

Lemma 1. *Assume that $d > 1$ is not a square. Then, the smallest positive solution (X_1, Y_1) of the Pell equation*

$$(3) \quad X^2 - dY^2 = 1$$

satisfies

$$(4) \quad \max(X_1, Y_1) < e^{3\sqrt{d} \log d}.$$

Proof. The proof follows immediately from Theorem 13.5 on page 329 in [3]. \square

Lemma 2. *Let $t \geq 2$ be an integer. Let p_y be the y th prime number in the arithmetic progression $(2^t m + 1)_{m \geq 1}$. Then,*

$$(5) \quad p_y \geq 2^{t-2} y \log y + 1 \quad \text{for all } y \geq 2^t.$$

Moreover, inequality (5) holds also when p_y is the y th prime in the arithmetic progression $(2^t m - 1)_{m \geq 1}$.

Received by the editors November 16, 1999.

2000 *Mathematics Subject Classification.* Primary 11A07, 11A25, 11D09.

©2001 American Mathematical Society

Proof. Assume that inequality (5) fails for some $t \geq 2$ and some $y \geq 2^t$. For any positive integers x, k, l such that $x > k > l$ let $\pi(x; k, l)$ denote the number of primes p such that $p \leq x$ and $p \equiv l \pmod{k}$. Then, by a result of Montgomery and Vaughan (see [4]), we know that

$$(6) \quad \pi(x; k, l) < \frac{2x}{\phi(k) \log(x/k)}.$$

We apply inequality (6) for $x = 2^{t-2}y \log y + 1$, $k = 2^t$ and $l = 1$ and get

$$y \leq \pi(x; k, l) < \frac{2 \cdot (2^{t-2}y \log y + 1)}{2^{t-1} \log\left(\frac{y \log y}{4}\right)},$$

or

$$2^{t-1}y \left(\log\left(\frac{y \log y}{4}\right) - \log y \right) < 2,$$

or

$$\log\left(\frac{\log y}{4}\right) < \frac{1}{2^{t-2}y} \leq \frac{1}{4},$$

or

$$\log y < 4e^{1/4},$$

or

$$y \leq 170.$$

Since $2^t \leq y \leq 170$, it follows that $t \leq 7$. We now check that inequality (5) holds for all values of $t \leq 7$ and $2^t \leq y \leq 170$, which gives the final contradiction. \square

Let d be a positive integer which is not a square and let (X_j, Y_j) be the j th positive solution of the Pell equation

$$X^2 - dY^2 = 1.$$

It is well-known that

$$X_j = \frac{(X_1 + \sqrt{d}Y_1)^j + (X_1 - \sqrt{d}Y_1)^j}{2}$$

and

$$Y_j = \frac{(X_1 + \sqrt{d}Y_1)^j - (X_1 - \sqrt{d}Y_1)^j}{2\sqrt{d}}.$$

In particular, $(Y_j)_{j \geq 1}$ is a *Lucas sequence of the first kind* and $(X_j)_{j \geq 1}$ is a *Lucas sequence of the second kind*. It is well-known that the sequence $(Y_j)_{j \geq 0}$ satisfies the property that $(Y_i, Y_j) = Y_{(i,j)}$ for all positive integers i and j . A prime divisor p of Y_j is called *primitive* if $p \nmid Y_k$ for any $k < j$. From results of Carmichael (see [1]), we know that Y_j has a primitive divisor for all $j \geq 1$ except maybe for $j \in \{2, 3, 4, 6, 12\}$. Moreover, every primitive divisor of Y_j is either a divisor of d or is congruent to $\pm 1 \pmod{j}$. We record these observations as

Lemma 3. *If $j \geq 8$ and $j \neq 12$, then Y_j has primitive divisors and all of them are either divisors of d or are congruent to $\pm 1 \pmod{j}$.*

We are now ready to prove the theorem.

Proof. Assume that $n \geq 3$. It is very easy to show that the congruence $n^2 \equiv -1 \pmod{\phi^2(n)}$ cannot occur. Indeed, for $n \geq 3$, the number $\phi(n)$ is even. Now the relation $\phi^2(n) \mid (n^2 + 1)$ is impossible because -1 is not a quadratic residue modulo 4. \square

Assume now that $n^2 \equiv 1 \pmod{\phi^2(n)}$. It follows that there exists an integer $d \geq 1$ such that

$$(7) \quad n^2 - d\phi^2(n) = 1.$$

It is easy to see that d is not a square because the only consecutive squares are 0 and 1 but $n \geq 3$. Let (X_1, Y_1) be the smallest solution of the Pell equation

$$(8) \quad X^2 - dY^2 = 1.$$

Equation (7) implies that $n = X_m$ and $\phi(n) = Y_m$ for some $m \geq 1$. Since n and $\phi(n)$ are coprime, it follows that n is square-free. Write

$$(9) \quad n = p_1 \dots p_l,$$

for some prime numbers $2 \leq p_1 < \dots < p_l$. Notice first that since $\phi(n)$ is even, it follows that $p_1 \geq 3$. Moreover, since

$$Y_m = \phi(n) = (p_1 - 1) \dots (p_l - 1),$$

it follows that

$$(10) \quad \omega(n) = l \leq \text{ord}_2(\phi(n)) = \text{ord}_2(Y_m).$$

Let

$$(11) \quad m = 2^t m_1,$$

where $t \geq 0$ and m_1 is odd. It is well-known that

$$(12) \quad \text{ord}_2(Y_m) = t + \text{ord}_2(Y_1).$$

By inequality (4), it follows that

$$(13) \quad \text{ord}_2(Y_1) \leq \frac{\log Y_1}{\log 2} < \frac{3}{\log 2} \sqrt{d} \log d.$$

Hence,

$$(14) \quad l < t + \frac{3}{\log 2} \sqrt{d} \log d.$$

We now write

$$(15) \quad \sqrt{d} < \frac{X_m}{Y_m} = \prod_{i=1}^l \left(1 + \frac{1}{p_i - 1}\right),$$

or

$$(16) \quad \log(\sqrt{d}) < \sum_{i=1}^l \log\left(1 + \frac{1}{p_i - 1}\right) < \sum_{i=1}^l \frac{1}{p_i - 1}.$$

We now use the fact that $p_i > (i + 1) \log(i + 1) + 1$. Indeed, this follows, for example, from a formula in [6], by noticing that p_i is at least the $i + 1$ st prime number. With this inequality, we conclude that

$$(17) \quad \sum_{i=1}^l \frac{1}{p_i - 1} \leq \frac{1}{3 - 1} + \frac{1}{5 - 1} + \int_3^{l+1} \frac{dx}{x \log x} < \frac{3}{4} + \log \log(l + 1).$$

Combining inequalities (14), (16) and (17), we get

$$(18) \quad \log(\sqrt{d}) < \frac{3}{4} + \log \log \left(t + 1 + \frac{3}{\log 2} \sqrt{d} \log d \right).$$

Assume first that $t \leq 1$. In this case, inequality (18) forces

$$(19) \quad d \leq 136.$$

Assume now that $t \geq 2$. We first show that every prime divisor p_i of X_m is, in fact, a primitive divisor of $Y_{2^{t+1}s}$ for some divisor s of m_1 . Indeed, to see why this is so, assume that p is a prime such that $p \mid X_m$. Since $Y_{2m} = 2X_m Y_m$ and $(X_m, Y_m) = 1$, it follows that $p \mid Y_{2m}$ and $p \nmid Y_m$. Let j be the divisor of $2m$ such that p is a primitive divisor of Y_j . From the above arguments, it follows easily that $\text{ord}_2(j) = \text{ord}_2(2m)$. But this last equality and formula (11) imply that $j = 2^{t+1}s$ for some divisor s of m_1 .

In particular, by Lemma 3, every prime p_i is either a divisor of d or is congruent to $\pm 1 \pmod{2^{t+1}}$. Since, at any rate, $(X_m, d) = 1$, it follows that every prime p_i is congruent to $\pm 1 \pmod{2^{t+1}}$. We now take a closer look at the primes q in the arithmetic progression $(2^{t+1}s - 1)_{s \geq 1}$. We denote these primes by $q_1 < q_2 < \dots < q_j < \dots$. For $j < 2^{t+1}$, we certainly have $q_j \geq 2^{t+1}j - 1$. When $j \geq 2^{t+1}$, it follows, by Lemma 2, that

$$(20) \quad q_j \geq 2^{t-1}j \log j + 1.$$

Hence,

$$\begin{aligned} \sum_{j=1}^l \frac{1}{q_j - 1} &\leq \sum_{j=1}^{2^{t+1}-1} \frac{1}{2^{t+1}j - 2} + \frac{1}{2^{t-1}} \sum_{j=2^{t+1}}^l \frac{1}{j \log j} \\ &< \frac{1}{2^{t+1} - 2} + \int_1^{2^{t+1}-1} \frac{dx}{2^{t+1}x - 2} + \frac{1}{2^{t-1}} \int_{2^{t+1}-1}^l \frac{dx}{x \log x} \\ (21) \quad &< \frac{1}{2^{t+1} - 2} + \frac{\log(2^{t+1} + 1)}{2^{t+1}} + \frac{\log \log l}{2^{t-1}}. \end{aligned}$$

A similar argument for the first l primes r_j from the arithmetic progression $(2^{t+1}s + 1)_{s \geq 1}$ shows that

$$(22) \quad \sum_{j=1}^l \frac{1}{r_j - 1} < \frac{1}{2^{t+1}} + \frac{\log(2^{t+1} - 1)}{2^{t+1}} + \frac{\log \log l}{2^{t-1}}.$$

Hence,

$$(23) \quad \sum_{i=1}^l \frac{1}{p_i - 1} < \sum_{j=1}^l \frac{1}{q_j - 1} + \sum_{j=1}^l \frac{1}{r_j - 1} < \frac{1}{2^{t+1} - 2} + \frac{1}{2^{t+1}} + \frac{(t + 1) \log 2}{2^t} + \frac{\log \log l}{2^{t-2}}.$$

From inequalities (14), (16) and (23), we get

$$(24) \quad \log(\sqrt{d}) < \frac{1}{2^{t+1} - 2} + \frac{1}{2^{t+1}} + \frac{(t + 1) \log 2}{2^t} + \frac{\log \log \left(t + \frac{3}{\log 2} \sqrt{d} \log d \right)}{2^{t-2}}.$$

It is easy to check that the function appearing in the right-hand side of inequality (24) is decreasing for $t \geq 2$ (for all values of $d \geq 2$). Hence, inequality (24) implies, in particular, that

$$\log(\sqrt{d}) < \frac{1}{6} + \frac{1}{8} + \frac{3 \log 2}{4} + \log \log \left(2 + \frac{3}{\log 2} \sqrt{d} \log d \right),$$

which implies that

$$(25) \quad d \leq 161.$$

Hence, inequalities (19) and (25) show that $d < 162$.

We have computed the first solutions of all the Pell equations (3) for all non-square values of $d < 162$ and concluded that $\text{ord}_2(Y_1) < 10$. We now use inequality (24) with the upper bound

$$\frac{3}{\log 2} \sqrt{d} \log d$$

on $\text{ord}_2(Y_1)$ (see formula (13)) replaced by the upper bound 10 to conclude that

$$(26) \quad \frac{1}{2} \log 2 \leq \log(\sqrt{d}) < \frac{1}{2^{t+1}-2} + \frac{1}{2^{t+1}} + \frac{(t+1) \log 2}{2^t} + \frac{\log \log(t+10)}{2^{t-2}}.$$

Inequality (26) leads to $t \leq 4$, therefore, $l \leq 14$. Since now we know that X_m is divisible by at most 14 odd primes, it follows that

$$\sqrt{d} < \frac{X_m}{Y_m} = \prod_{i=1}^l \left(1 + \frac{1}{p_i - 1} \right) \leq \left(1 + \frac{1}{3-1} \right) \left(1 + \frac{1}{5-1} \right) \dots \left(1 + \frac{1}{47-1} \right) < 3.61,$$

therefore $d \leq 13$. Since $\text{ord}_2(Y_1) \leq 2$ for $d \leq 13$, it follows that $l \leq 6$. Moreover, we can now show that $t \leq 1$. Indeed, if $t \geq 2$, then the prime numbers p_i are congruent to $\pm 1 \pmod{8}$. Hence,

$$\begin{aligned} \sqrt{d} &< \left(1 + \frac{1}{7-1} \right) \left(1 + \frac{1}{17-1} \right) \left(1 + \frac{1}{23-1} \right) \left(1 + \frac{1}{31-1} \right) \left(1 + \frac{1}{41-1} \right) \left(1 + \frac{1}{43-1} \right) \\ &< \sqrt{2}, \end{aligned}$$

which is impossible. Hence, $t \leq 1$ and $l \leq t + \text{ord}_2(Y_1) \leq 3$. It follows that

$$\sqrt{d} < \left(1 + \frac{1}{3-1} \right) \left(1 + \frac{1}{5-1} \right) \left(1 + \frac{1}{7-1} \right),$$

or $d \leq 3$. Hence, $d \in \{2, 3\}$. Moreover, notice that $p_1 \in \{3, 5\}$, because otherwise, if $p_1 \geq 7$, then

$$\sqrt{d} < \left(1 + \frac{1}{7-1} \right) \left(1 + \frac{1}{11-1} \right) \left(1 + \frac{1}{13-1} \right) < \sqrt{2},$$

which is impossible.

Assume first that $d = 2$. The case $p_1 = 5$ cannot occur, because the equation

$$X_m^2 - 2Y_m^2 = 1$$

with $5 \mid X_m$ leads to

$$-2Y_m^2 \equiv 1 \pmod{5},$$

which is impossible because -2 is a quadratic non-residue modulo 5.

If $p_1 = 3$, then, since $X_1 = 3$, it follows that m is odd. Hence, $\text{ord}_2(Y_m) = 1$, and therefore X_m is prime. Since $3 \mid X_m$, it follows that $X_m = 3$ and $n = 3$.

Assume now that $d = 3$. The case $p_1 = 3$ cannot occur because the equation

$$X_m^2 - 3Y_m^2 = 1$$

with $3 \mid X_m$ leads to $0 \equiv 1 \pmod{3}$, which is impossible. Finally, the case $p_1 = 5$ cannot occur either because the equation

$$X_m^2 - 3Y_m^2 = 1,$$

together with $5 \mid X_m$, implies

$$-3Y_m^2 \equiv 1 \pmod{5}$$

which is impossible because -3 is a quadratic non-residue modulo 5.

The theorem is therefore proved.

ACKNOWLEDGEMENTS

We would like to thank the referee for suggestions that improved this paper. The referee also suggested that there might be some chance by the methods of our paper to prove that for a fixed nonzero number a the equation $n^2 \equiv a \pmod{\phi(n)^2}$ has only finitely many solutions n . Unfortunately, we got nowhere with this problem.

The first author would like to thank the Mathematical Institute of the Czech Academy of Sciences for their hospitality during the period when this paper was written. This work was supported by grant no. 201/98/1452 of the Grant Agency of the Czech Republic.

REFERENCES

- [1] R.D. Carmichael: On the numerical factors of the arithmetic forms $\alpha^n + \beta^n$, *Ann. of Math.* **2** (15) (1913), 30-70.
- [2] R.K. Guy: Unsolved problems in number theory, Springer-Verlag, 1994. MR **96e**:11002
- [3] L.K. Hua: Introduction to number theory, Springer-Verlag, 1982. MR **83f**:10001
- [4] H.L. Montgomery, R.C. Vaughan: On the large sieve, *Mathematika* **20** (1973), 119-134. MR **51**:10260
- [5] C. Pomerance: On composite n for which $\phi(n) \mid n - 1$, *Acta Arith.* **28** (1976), 387-389; II *Pacific J. Math.* **69** (1977), 177-186. MR **52**:13608; MR **55**:7901
- [6] J.B. Rosser, L. Schoenfeld: Approximate formulas for some functions of prime numbers, *Illinois J. Math.* **6** (1962), 64-94. MR **25**:1139

MATHEMATICAL INSTITUTE, ACADEMY OF SCIENCES, ŽITNÁ 25, 115 67 PRAHA 1, CZECH REPUBLIC

E-mail address: luca@math.cas.cz

Current address: Instituto de Matemáticas de la UNAM, Campus Morelia, Apartado Postal 61-3 (Xangari), CP. 58 089, Morelia, Michoacán, Mexico

E-mail address: fluca@matmor.unam.mx

MATHEMATICAL INSTITUTE, ACADEMY OF SCIENCES, ŽITNÁ 25, 115 67 PRAHA 1, CZECH REPUBLIC

E-mail address: krizek@math.cas.cz