ON THE EQUATION $\varphi(|x^m - y^m|) = 2^n$

Florian Luca, Bielefeld

(Received November 2, 1998)

Abstract. In this paper we investigate the solutions of the equation in the title, where φ is the Euler function. We first show that it suffices to find the solutions of the above equation when $m = 4$ and x and y are coprime positive integers. For this last equation, we show that aside from a few small solutions, all the others are in a one-to-one correspondence with the Fermat primes.

Keywords: Euler function, Fermat primes

MSC 2000: 11A25, 11A51, 11A63

1. Introduction

For any positive integer k let $\varphi(k)$ be the Euler function of k. In this note, we find all solutions of the equation

$$\varphi(|x^m - y^m|) = 2^n, \tag{1}$$

where x and y are integers and m and n are positive integers such that $m \geqslant 2$.

Let $k \geqslant 3$ be a positive integer. It is well-known that the regular polygon with k sides can be constructed with the ruler and the compass if and only if $\varphi(k)$ is a power of 2. In particular, knowing all solutions of equation (1) enables one to find all regular polygons which can be constructed with the ruler and the compass for which the number of sides is the difference of equal powers of integers. Some equations of a similar flavour as (1) were treated in [2] and [3]. In [2], we found all regular polygons which can be constructed with the ruler and the compass whose number

Financial support from the Alexander von Humboldt Foundation is gratefully acknowledged.

of sides is either a Fibonacci or a Lucas number, while in [3] we found all regular polygons whose number of sides is a binomial coefficient.

Concerning equation (1), we first prove

Proposition. *In order to find all solutions of equation* (1), *it suffices to find only those for which* $x > y \geqslant 1$, $\gcd(x, y) = 1$ *and* $m = 4$.

Then we prove

Theorem. *Assume that* (x, y, m, n) *is a solution of equation* (1) *satisfying the conditions from Proposition. Then,*

(2)

$$(x,y) = \begin{cases} (2^{2^{l-1}}+1, 2^{2^{l-1}}-1) & \text{where } l \geqslant 1 \text{ and } 2^{2^l}+1 \text{ is a prime number or} \\ (2^{2^l}, 1) & \text{for } l = 0,1,2,3. \end{cases}$$

2. Reduction of the problem

In this section, we supply a proof of Proposition.

Proof. Let $C = \{k;\ \varphi(k) \text{ is a power of } 2\}$. It is well-known that a positive integer k belongs to C if and only if $k = 2^{\alpha} p_1 \dots p_t$ for some $\alpha \geqslant 0$ and $t \geqslant 0$, where $p_i = 2^{2^{\beta_i}} + 1$ are distinct Fermat primes. In particular, it follows that the elements belonging to the set C satisfy the following two properties:

1) If $a \in C$ and $b|a$, then $b \in C$.
2) Assume that $a, b \in C$. Then, $ab \in C$ if and only if $\gcd(a, b)$ is a power of 2.

Assume that (x, y, m) are such that $|x^m - y^m| \in C$. We may assume that $x \geqslant |y| \geqslant 0$. We first show that it suffices to assume that $\gcd(x, y) = 1$. Indeed, let $d = \gcd(x, y)$. Write $x = dx_1$ and $y = dy_1$. Then,

$$|x^m - y^m| = d^m |x_1^m - y_1^m| \in C.$$

Since $m \geqslant 2$, we conclude by 1) and 2) above that $|x_1^m - y_1^m| \in C$ and that d is a power of 2. Conversely, if (x_1, y_1, m) are such that $|x_1^m - y_1^m| \in C$ and if d is a power of 2, it follows by 2) that

$$|x^m - y^m| = d^m |x_1^m - y_1^m| \in C$$

as well. Hence, it suffices to find all solutions of equation (1) for which $\gcd(x, y) = 1$.

Assume first that $xy = 0$. It follows that $y = 0$. Since $\gcd(x, y) = 1$ and $x > 0$, we conclude that $x = 1$.

Assume now that $x = |y|$. Since $\gcd(x, y) = 1$ and φ is not defined at 0, it follows that $x = 1, y = -1$ and m is odd.

From now on, we assume that $x > |y| > 0$. We first show that we may assume $m > 2$. Indeed, suppose that $m = 2$. Since $m = 2$ is even, we may assume that $y > 0$. Since

$$x^2 - y^2 = (x - y)(x + y) \in C,$$

it follows by 1) above that $x - y \in C$ and $x + y \in C$. Let $c_1 = x - y$ and $c_2 = x + y$. Since $x > y > 0$, it follows that $c_2 > c_1 > 0$. Moreover, since $\gcd(x, y) = 1$, we conclude that either both c_1 and c_2 are odd and $\gcd(c_1, c_2) = 1$, or both c_1 and c_2 are even in which case $\gcd(c_1, c_2) = 2$ and one of the numbers c_1 or c_2 is a multiple of 4. Conversely, let $c_2 > c_1$ be any two numbers in C satisfying one of the above two conditions. Then one can easily see that if we denote

$$x = \frac{c_1 + c_2}{2} \quad \text{and} \quad y = \frac{c_1 - c_2}{2},$$

then x and y are positive integers, $x > y$, $\gcd(x, y) = 1$ and $x^2 - y^2 = c_1c_2 \in C$. These arguments show that equation (1) has an infinity of solutions when $m = 2$ and that all such solutions can be parametrized in terms of two parameters c_1 and c_2 belonging to C and satisfying certain restrictions.

From now on, we assume that $m > 2$. We first show that m is a power of 2. Assume that this is not the case and let p be an odd prime such that $p|m$. Replacing $x^{m/p}$ and $y^{m/p}$ respectively by x and y, we may assume that $|x^p - y^p| \in C$. From 1), it follows that

$$u_p = \frac{|x^p - y^p|}{|x - y|} \in C.$$

Since p is odd and $\gcd(x, y) = 1$, it follows that u_p is odd. In particular, u_p is square-free. Let P be a prime dividing u_p. On the one hand, we have $x^p - y^p \equiv 0 (\operatorname{mod} P)$. On the other hand, since $P \not| xy$, it follows, by Fermat's little theorem, that $x^{P-1} - y^{P-1} \equiv 1 - 1 \equiv 0 (\operatorname{mod} P)$. Hence,

$$P|(x^p - y^p, x^{P-1} - y^{P-1}) = x^{(p,P-1)} - y^{(p,P-1)}. \tag{3}$$

Since $P \in C$, it follows that $P - 1$ is a power of 2. Since p is odd, this implies that $(p, P - 1) = 1$. From formula (3), we conclude that $P|x - y$. Hence, $x \equiv y (\operatorname{mod} P)$. It now follows that

$$u_p = \frac{|x^p - y^p|}{|x - y|} \equiv |x^{p-1} + x^{p-2}y + \ldots + y^{p-1}| \equiv px^{p-1} (\operatorname{mod} P).$$

Since $P|u_p$, it follows that $p = P$. Since u_p is square-free, it follows that $u_p = 1$ or p.

On the other hand, the sequence

$$u_k = \frac{|x^k - y^k|}{|x-y|} \quad \text{for } k \geqslant 0$$

is a *Lucas sequence of the first kind*. From [1] we know that u_q is divisible by a prime $Q > q$ for any prime $q > 3$. From the above result it follows that $p = 3$ and that $u_3 = 1$ or 3. This leads to the equations

$$x^2 \pm xy + y^2 = 1 \text{ or } 3.$$

The only solution (x, y) of the above equations such that $x > |y| > 0$ is $(2, -1)$ which does not lead to a solution of equation (1). Hence, m is a power of 2. Since $m > 2$, it follows that m is a multiple of 4. We may now replace x and y by $x^{m/4}$ and $y^{m/4}$ respectively and study equation (1) only for $m = 4$. Clearly, since $m = 4$ is even, we may assume that $y > 0$.

Proposition is therefore proved. $\square$

3. The proof of theorem

Since $x^4 - y^4 = (x-y)(x+y)(x^2+y^2) \in C$, it follows that $x - y \in C$, $x + y \in C$ and $x^2 + y^2 \in C$. We distinguish two cases:

Case 1. $x \equiv y \equiv 1 (\operatorname{mod} 2)$.

In this case, one of the numbers $x - y$ or $x + y$ is divisible by 4 and the other one is 2 modulo 4. Moreover, since both x and y are odd, it follows that $x^2 + y^2$ is 2 modulo 8. It now follows that there exists $\varepsilon \in \{\pm 1\}$ such that

$$\begin{aligned} x - \varepsilon y &\equiv 2 (\operatorname{mod} 4), \\ x + \varepsilon y &\equiv 0 (\operatorname{mod} 4). \end{aligned}$$

Write

$$\begin{aligned} x - \varepsilon y &= 2 \prod_{i=1}^{I} (2^{2^{\alpha_i}} + 1), \\ x + \varepsilon y &= 2^s \prod_{j=1}^{J} (2^{2^{\beta_j}} + 1), \\ x^2 + y^2 &= 2 \prod_{k=1}^{K} (2^{2^{\gamma_k}} + 1), \end{aligned} \tag{4}$$

where $s \geqslant 2$, I, J and K are three non-negative integers (some of them may be zero), $0 \leqslant \alpha_1 < \ldots < \alpha_I$, $0 \leqslant \beta_1 < \ldots < \beta_J$, $0 \leqslant \gamma_1 < \ldots < \gamma_K$ and $2^{2^\delta} + 1$ is a Fermat prime whenever $\delta \in \{\alpha_i\}_{i=1}^I \cup \{\beta_j\}_{j=1}^J \cup \{\gamma_k\}_{k=1}^K$.

Notice first that the three sets $\{\alpha_i\}_{i=1}^I, \{\beta_j\}_{j=1}^J, \{\gamma_k\}_{k=1}^K$ are pairwise disjoint. Indeed, assume for example that $\delta \in \{\alpha_i\}_{i=1}^I \cap \{\beta_j\}_{j=1}^J$. It follows that $2^{2^\delta} + 1 | (x - y, x + y)$, which contradicts the fact that x and y are coprime.

Notice also that $K > 0$ and that $\gamma_1 > 0$. Indeed, if $K = 0$ then $x^2 + y^2 = 2$, which is impossible because $x > y \geqslant 1$. If $\gamma_1 = 0$, it follows that $3 = 2^{2^0} + 1 | x^2 + y^2$, which is impossible because x and y are coprime and -1 is not a quadratic residue modulo 3.

We now use formulae (4) and the identity

$$2(x^2 + y^2) = (x - y)^2 + (x + y)^2 \tag{5}$$

to conclude that

$$4 \prod_{k=1}^{K} (2^{2^{\gamma_k}} + 1) = 4 \prod_{i=1}^{I} (2^{2^{\alpha_i}} + 1)^2 + 2^{2s} \prod_{j=1}^{J} (2^{2^{\beta_j}} + 1)^2$$

or

$$\prod_{k=1}^{K} (2^{2^{\gamma_k}} + 1) = \prod_{i=1}^{I} (2^{2^{\alpha_i}} + 1)^2 + 2^{2(s-1)} \prod_{j=1}^{J} (2^{2^{\beta_j}} + 1)^2. \tag{6}$$

Our main goal is to show that $I = J = 0$.

Suppose that this is not so. In order to achieve a contradiction, we proceed in three steps.

Step 1.I. $0 \in \{\alpha_i\}_{i=1}^I \cup \{\beta_j\}_{j=1}^J$.

Assume that this is not the case.

Suppose first that $I > 0$. Hence, $\alpha_1 \neq 0$. Notice first that

$$\prod_{i=1}^{I} (2^{2^{\alpha_i}} + 1) = \sum_{\mathcal{H} \subseteq \{1,\ldots,I\}} 2^{\sum_{i \in \mathcal{H}} 2^{\alpha_i}} \tag{7}$$

and the sum appearing on the right hand side of identity (7) is precisely the binary expansion of the product appearing on the left hand side (this is because of the fact that all exponents appearing on the right hand side of identity (7) have distinct binary representations, therefore they are all distinct). Since $\alpha_1 > 0$, it follows that

$$\prod_{i=1}^{I} (2^{2^{\alpha_i}} + 1)^2 = 1 + 2^{2^{\alpha_1} + 1} + 2^{2^{\alpha_1 + 1}} + \text{higher powers of } 2, \tag{8}$$

where the higher powers of 2 are missing when $I = 1$. From formula (6), it follows that
(9)

$$1 + 2^{2^{\gamma_1}} + \text{higher powers of } 2 = \prod_{k=1}^{K} (2^{2^{\gamma_k}} + 1)$$
$$= (1 + 2^{2^{\alpha_1}+1} + \text{higher powers of } 2) + 2^{2(s-1)}(1 + \text{higher powers of } 2).$$

Clearly, the numbers $2^{\alpha_1} + 1$ and $2(s-1)$ are distinct because the first is odd and the second is even. On the one hand, from formula (9) and the fact that 2^{γ_1} is even we conclude that $2^{\gamma_1} = 2(s-1)$. On the other hand, since the binary representation of the number given by formula (9) has at least three digits of 1, it follows that $K \geqslant 2$.

If $J = 0$, then formulae (6) and (9) imply

$$\begin{aligned} 1 + 2^{2^{\gamma_1}} + 2^{2^{\gamma_2}} + \text{higher powers of } 2 &= \prod_{k=1}^{K} (2^{2^{\gamma_k}} + 1) \\ &= 1 + 2^{2(s-1)} + 2^{2^{\alpha_1}+1} + \text{higher powers of } 2. \end{aligned} \tag{10}$$

Formula (10) leads to $2^{\gamma_2} = 2^{\alpha_1} + 1$, which is impossible because $\alpha_1 > 0$.

Suppose now that $J > 0$. In this case, $\beta_1 > 0$. Arguments similar to the preceeding ones yield that

$$\begin{aligned} 1 + 2^{2^{\gamma_1}} + 2^{2^{\gamma_2}} + \text{higher powers of } 2 &= \prod_{k=1}^{K} (2^{2^{\gamma_k}} + 1) \\ &= (1 + 2^{2^{\alpha_1}+1} + \text{higher powers of } 2) \\ &\quad + 2^{2(s-1)}(1 + 2^{2^{\beta_1}+1} + \text{higher powers of } 2). \end{aligned} \tag{11}$$

From equation (11) and the fact that $2^{\gamma_1} = 2(s-1)$, it follows that at least one of the following three situations must occur:

1) $2^{\gamma_2} = 2^{\alpha_1} + 1$. This is impossible because $\alpha_1 > 0$.
2) $2^{\gamma_2} = 2(s-1) + 2^{\beta_1} + 1 = 2^{\gamma_1} + 2^{\beta_1} + 1$. This is impossible because both β_1 and γ_1 are positive.
3) $2^{\alpha_1} + 1 = 2(s-1) + 2^{\beta_1} + 1$ or $2^{\alpha_1} = 2(s-1) + 2^{\beta_1} = 2^{\gamma_1} + 2^{\beta_1}$, which is impossible because $\beta_1 \neq \gamma_1$.

This completes the argument in the case $I > 0$.

Assume now that $I = 0$. Hence, $J > 0$ and $\beta_1 > 0$. Arguments similar to the previous ones imply that formula (6) reads

$$\begin{aligned} 1 + 2^{2^{\gamma_1}} + \text{higher powers of } 2 &= \prod_{k=1}^{K} (2^{2^{\gamma_k}} + 1) \\ &= 1 + 2^{2(s-1)}(1 + 2^{2^{\beta_1}+1} + \text{higher powers of } 2). \end{aligned} \tag{12}$$

From equation (12), it again follows that $2^{\gamma_1} = 2(s-1)$ and $K \geqslant 2$. Formula (12) can now be written as

$$(13)\qquad \begin{aligned} 1 + 2^{2^{\gamma_1}} + 2^{2^{\gamma_2}} + \text{higher powers of } 2 &= \prod_{k=1}^{K} (2^{2^{\gamma_k}} + 1) \\ &= 1 + 2^{2(s-1)}(1 + 2^{2^{\beta_1}+1} + \text{higher powers of } 2). \end{aligned}$$

From equation (13), it follows that $2^{\gamma_2} = 2(s-1) + 2^{\beta_1} + 1 = 2^{\gamma_1} + 2^{\beta_1} + 1$, which is impossible because both β_1 and γ_1 are positive.

Step 1.I is therefore proved.

S t e p 1.II. If $I > 0$, then $\alpha_1 \neq 0$.

Suppose that this is not the case. Assume that $I > 0$ but $\alpha_1 = 0$. Let $t \geqslant 1$ be such that $\alpha_i = i - 1$ for $i = 1, \ldots, t$ and either $I = t$ or $\alpha_{t+1} \geqslant t + 1$. Then

$$(14)\qquad \prod_{i=1}^{I} (2^{2^{\alpha_i}} + 1) = \prod_{i=1}^{t} (2^{2^{i-1}} + 1) \prod_{i \geqslant t+1}^{I} (2^{2^{\alpha_i}} + 1) = (2^{2^t} - 1) \prod_{i \geqslant t+1}^{I} (2^{2^{\alpha_i}} + 1).$$

Hence,

$$(15)\qquad \begin{aligned} \prod_{i=1}^{I} (2^{2^{\alpha_i}} + 1)^2 &= (1 + 2^{2^t+1} + \text{higher powers of } 2)(1 + \text{higher powers of } 2) \\ &= 1 + 2^{2^t+1} + \text{higher powers of } 2. \end{aligned}$$

From formulae (6) and (15), it follows that

(16)

$$\begin{aligned} 1 + 2^{2^{\gamma_1}} + \text{higher powers of } 2 &= \prod_{k=1}^{K} (2^{2^{\gamma_k}} + 1) \\ &= (1 + 2^{2^t+1} + \text{higher powers of } 2) + 2^{2(s-1)}(1 + \text{higher powers of } 2). \end{aligned}$$

Clearly, $2^t + 1$ and $2(s-1)$ are distinct because the first number is odd and the other is even. From formula (16), it follows that $2^{\gamma_1} = 2(s-1)$ and that $K \geqslant 2$. Formula (6) now becomes

$$(17)\qquad \begin{aligned} 1 + 2^{2^{\gamma_1}} + 2^{2^{\gamma_2}} + \text{higher powers of } 2 &= \prod_{k=1}^{K} (2^{2^{\gamma_k}} + 1) \\ &= (1 + 2^{2^t+1} + \text{higher powers of } 2) \\ &\quad + 2^{2(s-1)}(1 + \text{higher powers of } 2). \end{aligned}$$

Suppose first that $J = 0$. Then $2^{\gamma_2} = 2^t + 1$, which is false because t is positive.

Suppose now that $J > 0$. Since $\alpha_i = i-1$ for $i = 1, \dots, t$, it follows that $\beta_1 \geqslant t \geqslant 1$. From the arguments employed in Step 1.I, it follows that formula (17) can be written as

$$
\begin{aligned}
1 + 2^{2^{\gamma_1}} + 2^{2^{\gamma_2}} + \text{higher powers of } 2 &= \prod_{k=1}^{K} (2^{2^{\gamma_k}} + 1) \\
&= (1 + 2^{2^t+1} + \text{higher powers of } 2) \\
&\quad + 2^{2(s-1)}(1 + 2^{2^{\beta_1}+1} + \text{higher powers of } 2).
\end{aligned} \tag{18}
$$

From equation (18) and the fact that $2^{\gamma_1} = 2(s-1)$, it follows that one of the following situations must occur:

1) $2^{\gamma_2} = 2^t + 1$. This is impossible because $t > 0$.
2) $2^{\gamma_2} = 2(s-1) + 2^{\beta_1} + 1 = 2^{\gamma_1} + 2^{\beta_1} + 1$. This is impossible because both γ_1 and β_1 are positive.
3) $2^t + 1 = 2(s-1) + 2^{\beta_1} + 1$ or $2^t = 2^{\gamma_1} + 2^{\beta_1}$, which is impossible because $\gamma_1 \neq \beta_1$.

This completes the proof of Step 1.II.

Step 1.III. If $J > 0$, then $\beta_1 \neq 0$.

Notice first that Steps 1.I, 1.II and 1.III contradict each other.

Assume that the claim made in Step 1.III does not hold. Let $J > 0$ and assume that $\beta_1 = 0$. Let $t \geqslant 1$ be such that $\beta_j = j - 1$ for $j = 1, \dots, t$ and either $J = t$ or $J > t$ and $\beta_{t+1} \geqslant t + 1$. We have

$$
\prod_{j=1}^{J} (2^{2^{\beta_j}} + 1) = \prod_{j=1}^{t} (2^{2^{j-1}} + 1) \prod_{j \geqslant t+1}^{J} (2^{2^{\beta_j}} + 1) = (2^{2^t} - 1) \prod_{j \geqslant t+1}^{J} (2^{2^{\beta_j}} + 1). \tag{19}
$$

Hence,

$$
\prod_{j=1}^{J} (2^{2^{\beta_j}} + 1)^2 = (2^{2^t} - 1)^2 \prod_{j \geqslant t+1}^{J} (2^{2^{\beta_j}} + 1)^2 = 1 + 2^{2^t+1} + \text{higher powers of } 2. \tag{20}
$$

From formula (6) it follows that

$$
\begin{aligned}
1 + 2^{2^{\gamma_1}} + \text{higher powers of } 2 &= \prod_{k=1}^{K} (2^{2^{\gamma_k}} + 1) \\
&= (1 + \text{higher powers of } 2) + 2^{2(s-1)}(1 + 2^{2^t+1} + \text{higher powers of } 2).
\end{aligned}
$$

Assume first that $I = 0$. It follows that

$$
\begin{aligned}
(21) \qquad 1 + 2^{2^{\gamma_1}} + \text{higher powers of } 2 &= \prod_{k=1}^{K} (2^{2^{\gamma_k}} + 1) \\
&= 1 + 2^{2(s-1)}(1 + 2^{2^t+1} + \text{higher powers of } 2).
\end{aligned}
$$

From equation (21), it follows that $K \geqslant 2$ and that $2^{\gamma_1} = 2(s-1)$. Formula (21) can now be written as

$$
\begin{aligned}
(22) \qquad 1 + 2^{2^{\gamma_1}} + 2^{2^{\gamma_2}} + \text{higher powers of } 2 &= \prod_{k=1}^{K} (2^{2^{\gamma_k}} + 1) \\
&= 1 + 2^{2(s-1)}(1 + 2^{2^t+1} + \text{higher powers of } 2).
\end{aligned}
$$

From equation (22) and the fact that $2^{\gamma_1} = 2(s-1)$, it follows that $2^{\gamma_2} = 2(s-1) + 2^t + 1 = 2^{\gamma_1} + 2^t + 1$, which is impossible because both γ_1 and t are positive.

Assume now that $I > 0$. In this case, $\alpha_1 \geqslant t \geqslant 1$. From formula (6) and the arguments employed at Step 1.I, it follows that

$$
\begin{aligned}
(23) \qquad 1 + 2^{2^{\gamma_1}} + \text{higher powers of } 2 &= \prod_{k=1}^{K} (2^{2^{\gamma_k}} + 1) \\
&= (1 + 2^{2^{\alpha_1}+1} + \text{higher powers of } 2) \\
&\quad + 2^{2(s-1)}(1 + 2^{2^t+1} + \text{higher powers of } 2).
\end{aligned}
$$

Notice that $2^{\alpha_1} + 1$ and $2(s-1)$ are distinct because the first number is odd and the other is even. From formula (23), it follows that $2^{\gamma_1} = 2(s-1)$ and that $K \geqslant 2$. Formula (23) can now be written as

$$
\begin{aligned}
(24) \qquad 1 + 2^{2^{\gamma_1}} + 2^{2^{\gamma_2}} + \text{higher powers of } 2 &= \prod_{k=1}^{K} (2^{2^{\gamma_k}} + 1) \\
&= (1 + 2^{2^{\alpha_1}+1} + \text{higher powers of } 2) \\
&\quad + 2^{2(s-1)}(1 + 2^{2^t+1} + \text{higher powers of } 2).
\end{aligned}
$$

From equation (24) and the fact that $2^{\gamma_1} = 2(s-1)$, it follows that one of the following situations must occur:

1) $2^{\gamma_2} = 2^{\alpha_1} + 1$. This is impossible because $\alpha_1 > 0$.
2) $2^{\gamma_2} = 2(s-1) + 2^t + 1 = 2^{\gamma_1} + 2^t + 1$. This is impossible because both γ_1 and t are positive.
3) $2^{\alpha_1} + 1 = 2(s-1) + 2^t + 1 = 2^{\gamma_1} + 2^t + 1$. This leads to $\gamma_1 = t$ and $\alpha_1 = t + 1$.

In this last case, it follows that $\alpha_2 \geqslant t+2$ and $\beta_{t+1} \geqslant t+2$, whenever they exist. From formulae (6) and (19) we get

(25)

$$\begin{aligned}
1 + 2^{2^t} + 2^{2^{\gamma_2}} + \text{higher powers of } 2 &= \prod_{k=1}^{K}(2^{2^{\gamma_k}}+1) \\
&= (2^{2^{t+1}}+1)^2 \prod_{i \geqslant 2}^{I}(2^{2^{\alpha_i}}+1)^2 + 2^{2^t}(2^{2^t}-1)^2 \prod_{j \geqslant t+1}^{J}(2^{2^{\beta_j}}+1)^2 \\
&= (2^{2^{t+1}}+1)^2 + 2^{2^t}(2^{2^t}-1)^2 + \text{higher powers of } 2 \\
&= 1 + 2^{2^t} + 2^{2^t+2^{t+1}} + 2^{2^{t+2}} + \text{higher powers of } 2.
\end{aligned}$$

Equation (25) implies $2^{\gamma_2} = 2^t + 2^{t+1}$, which is impossible.

Step 1.III is thus proved.

Steps 1.I, 1.II and 1.III imply that $I = J = 0$. From formula (6), it follows that

$$\prod_{k=1}^{K}(2^{2^{\gamma_k}}+1) = 1 + 2^{2(s-1)}. \tag{26}$$

From equation (26), it follows that $K = 1$ and $2^{\gamma_1} = 2(s-1)$. Solving the first two equations of system (4) for x and y we get

$$x = 2^{2^{\gamma_1-1}}+1 \quad \text{and} \quad y = \varepsilon(2^{2^{\gamma_1-1}}-1), \tag{27}$$

where $2^{2^{\gamma_1}}+1$ is a Fermat prime and $\varepsilon \in \{\pm 1\}$. Since $y > 0$, it follows that $\varepsilon = 1$. This belongs to the first family of solutions claimed by Theorem.

Case 2. $x \not\equiv y (\operatorname{mod} 2)$.

In this case all three numbers $x-y, x+y$ and x^2+y^2 are odd. Assume that

$$\begin{aligned}
x - y &= \prod_{i=1}^{I}(2^{2^{\alpha_i}}+1), \\
x + y &= \prod_{j=1}^{J}(2^{2^{\beta_j}}+1), \\
x^2 + y^2 &= \prod_{k=1}^{K}(2^{2^{\gamma_k}}+1),
\end{aligned} \tag{28}$$

where I, J and K are three non-negative integers (some of them may be zero), $0 \leqslant \alpha_1 < \ldots < \alpha_I$, $0 \leqslant \beta_1 < \ldots < \beta_J$, $0 \leqslant \gamma_1 < \ldots < \gamma_K$ and $2^{2^\delta}+1$ is a Fermat prime whenever $\delta \in \{\alpha_i\}_{i=1}^I \cup \{\beta_j\}_{j=1}^J \cup \{\gamma_k\}_{k=1}^K$.

Notice again that the three sets $\{\alpha_i\}_{i=1}^I, \{\beta_j\}_{j=1}^J, \{\gamma_k\}_{k=1}^K$ are pairwise disjoint, $K > 0$ and $\gamma_1 > 0$. Notice also that $I + J > 0$.

We proceed in four steps.

S t e p 2.I. $K = J$ and $\gamma_k = \beta_k + 1$ for all $k = 1, \ldots, K$.

From formulae (28) and from the arguments immediately below formula (7), it follows that

$$\begin{aligned}\lfloor \log_2(x-y) \rfloor &= \sum_{i=1}^{I} 2^{\alpha_i},\\ \lfloor \log_2(x+y) \rfloor &= \sum_{j=1}^{J} 2^{\beta_j},\\ \lfloor \log_2(x^2+y^2) \rfloor &= \sum_{k=1}^{K} 2^{\gamma_k}.\end{aligned} \tag{29}$$

We now use the following obvious

Lemma.
1) *If z is a positive number, then*

$$\lfloor \log_2 z^2 \rfloor \in \{2\lfloor \log_2 z \rfloor, 2\lfloor \log_2 z \rfloor + 1\}. \tag{30}$$

2) *If $a > b$ are positive numbers, then*

$$\lfloor \log_2(a+b) \rfloor \in \{\lfloor \log_2 a \rfloor, \lfloor \log_2 a \rfloor + 1\}. \tag{31}$$

From identity (5) and the above Lemma, it follows that

$$\begin{aligned}1 + \lfloor \log_2(x^2+y^2) \rfloor &= \lfloor \log_2(2(x^2+y^2)) \rfloor\\ &= \lfloor \log_2((x+y)^2 + (x-y)^2)) \rfloor\\ &\in \{2\lfloor \log_2(x+y) \rfloor + u | u = 0, 1, 2\}.\end{aligned} \tag{32}$$

From formulae (29) and (32), it follows that

$$1 + \sum_{k=1}^{K} 2^{\gamma_k} = u + \sum_{j=1}^{J} 2^{\beta_j+1} \qquad \text{for some } u \in \{0, 1, 2\}. \tag{33}$$

Since $\gamma_1 > 0$, it follows that the number appearing on the left hand side of equation (33) is odd. Hence, $u = 1$, $K = J$ and $\gamma_k = \beta_k + 1$ for all $k = 1, \ldots, K$.

Step 2.I is thus proved.

S t e p 2.II. $0 \in \{\alpha_i\}_{i=1}^{I} \cup \{\beta_j\}_{j=1}^{J}$.

Assume that this is not the case. By Step 2.I, we know that $J > 0$. In particular, $\beta_1 > 0$.

We use formulae (28) and identity (5) to conclude that

$$2\prod_{k=1}^{K}(2^{2^{\gamma_k}}+1) = \prod_{i=1}^{I}(2^{2^{\alpha_i}}+1)^2 + \prod_{j=1}^{J}(2^{2^{\beta_j}}+1)^2. \tag{34}$$

By the arguments employed in Step 1.I, it follows that

$$\begin{aligned} 2 + 2^{2^{\gamma_1}+1} + \text{higher powers of } 2 &= 2\prod_{k=1}^{K}(2^{2^{\gamma_k}}+1) \\ &= \prod_{i=1}^{I}(2^{2^{\alpha_i}}+1)^2 + (1 + 2^{2^{\beta_1}+1} + \text{higher powers of } 2). \end{aligned} \tag{35}$$

If $I = 0$, then formula (35) becomes

$$\begin{aligned} 2 + 2^{2^{\gamma_1}+1} + \text{higher powers of } 2 &= 2\prod_{k=1}^{K}(2^{2^{\gamma_k}}+1) \\ &= 1 + (1 + 2^{2^{\beta_1}+1} + \text{higher powers of } 2). \end{aligned} \tag{36}$$

From formula (36), it follows that $2^{\gamma_1}+1 = 2^{\beta_1}+1$ or $\gamma_1 = \beta_1$, which is impossible.

Suppose now that $I > 0$. In this case, $\alpha_1 > 0$. By the arguments employed in Step 1.I, it follows that

$$\begin{aligned} 2 + 2^{2^{\gamma_1}+1} + \text{higher powers of } 2 &= 2\prod_{k=1}^{K}(2^{2^{\gamma_k}}+1) \\ &= (1 + 2^{2^{\alpha_1}+1} + \text{higher powers of } 2) \\ &\quad + (1 + 2^{2^{\beta_1}+1} + \text{higher powers of } 2). \end{aligned} \tag{37}$$

From equation (37), it follows that one of the following situations must occur:

1) $2^{\gamma_1}+1 = 2^{\alpha_1}+1$. This implies $\gamma_1 = \alpha_1$, which is impossible.
2) $2^{\gamma_1}+1 = 2^{\beta_1}+1$. This implies $\gamma_1 = \beta_1$, which is impossible.
3) $2^{\alpha_1}+1 = 2^{\beta_1}+1$. This implies $\alpha_1 = \beta_1$, which is impossible.

Step 2.II is thus proved.

S t e p 2.III. If either $I = 0$ or $\alpha_1 \neq 0$, then $x = 2$ and $y = 1$.

Suppose that either $I=0$ or $\alpha_1 \neq 0$. By Steps 2.I and 2.II above, it follows that $\beta_1 = 0$ and $\gamma_1 = 1$. We now show that $I = 0$ and $J = 1$. Suppose that this is not the case. Then at least one of the numbers α_1 or β_2 exists. From formula (34) and the fact that $\beta_1 = 0$ and $\gamma_1 = 1$, it follows that

$$\begin{aligned} 2 + 2^3 + \text{higher powers of } 2 &= 2\prod_{k=1}^{K}(2^{2^{\gamma_k}}+1) \\ &= \prod_{i=1}^{I}(2^{2^{\alpha_i}}+1)^2 + 3^2\prod_{j\geqslant 2}^{J}(2^{2^{\beta_j}}+1)^2 \\ &= \prod_{i=1}^{I}(2^{2^{\alpha_i}}+1)^2 + (1+2^3)\prod_{j\geqslant 2}^{J}(2^{2^{\beta_j}}+1)^2. \end{aligned} \tag{38}$$

It follows that $K \geqslant 2$. Since $J = K$, it follows that $J \geqslant 2$ as well. Suppose, for example, that $I = 0$. From formula (38), it follows that

$$\begin{aligned} 2 + 2^3 + 2^{2^{\gamma_2}+1} + \text{higher powers of } 2 &= 2\prod_{k=1}^{K}(2^{2^{\gamma_k}}+1) \\ &= 1 + (1+2^3)(1+2^{2^{\beta_2}+1} + \text{higher powers of } 2). \end{aligned} \tag{39}$$

From equation (39), it follows that $2^{\gamma_2}+1 = 2^{\beta_2}+1$, which is impossible because $\gamma_2 \neq \beta_2$.

Assume now that $I > 0$. From formula (38), it follows that

$$\begin{aligned} 2 + 2^3 + 2^{2^{\gamma_2}+1} + \text{higher powers of } 2 &= 2\prod_{k=1}^{K}(2^{2^{\gamma_k}}+1) \\ &= (1 + 2^{2^{\alpha_1}+1} + \text{higher powers of } 2) \\ &\quad + (1+2^3)(1+2^{2^{\beta_2}+1} + \text{higher powers of } 2). \end{aligned} \tag{40}$$

From equation (40), it follows that one of the following must occur:

1) $2^{\gamma_2}+1 = 2^{\alpha_1}+1$. This is impossible because $\gamma_2 \neq \alpha_1$.
2) $2^{\gamma_2}+1 = 2^{\beta_2}+1$. This is impossible because $\gamma_2 \neq \beta_2$.
3) $2^{\alpha_1}+1 = 2^{\beta_2}+1$. This is impossible because $\alpha_1 \neq \beta_2$.

Hence, $I = 0$, $J = K = 1$, $\beta_1 = 0$ and $\gamma_1 = 1$. It follows that $x - y = 1$ and $x + y = 3$. Hence, $(x, y) = (2, 1) = (2^{2^0}, 1)$ which is one of the solutions claimed by Theorem.

Step 2.III is thus proved.

Assume now that $(x, y) \neq (2, 1)$. By Steps 2.I, 2.II and 2.III, it follows that $I > 0$ and $\alpha_1 = 0$. The proof of Theorem will be completed once we show

S t e p 2.IV. If $\alpha_1 = 0$, then $(x, y) = (2^{2^l}, 1)$ for some $l = 1, 2, 3$.

Let $t \geqslant 1$ be such that $\alpha_i = i - 1$ for $i = 1, \ldots, t$ and either $I = t$ or $I > t$ and $\alpha_{t+1} \geqslant t + 1$. It now follows that

$$\prod_{i=1}^{I}(2^{2^{\alpha_i}} + 1) = \prod_{i=1}^{t}(2^{2^{i-1}} + 1) \prod_{i \geqslant t+1}^{I} (2^{2^{\alpha_i}} + 1) = (2^{2^t} - 1) \prod_{i \geqslant t+1}^{I} (2^{2^{\alpha_i}} + 1). \tag{41}$$

Hence,

$$\prod_{i=1}^{I}(2^{2^{\alpha_i}} + 1)^2 = 1 + 2^{2^t+1} + \text{higher powers of } 2. \tag{42}$$

From equation (34), it follows that

$$\begin{aligned} 2 + 2^{2^{\gamma_1}+1} + \text{higher powers of } 2 &= 2\prod_{k=1}^{K}(2^{2^{\gamma_k}} + 1) \\ &= (1 + 2^{2^t+1} + \text{higher powers of } 2) \\ &\quad + (1 + 2^{2^{\beta_1}+1} + \text{higher powers of } 2). \end{aligned} \tag{43}$$

From equation (43) and the fact that $\gamma_1 = \beta_1 + 1 > \beta_1$, it follows that $2^t + 1 = 2^{\beta_1} + 1$ or $\beta_1 = t$. Hence, $\gamma_1 = t + 1$. Equation (34) now becomes

$$\begin{aligned} 2 + 2^{2^{t+1}+1} + \text{higher powers of } 2 &= 2\prod_{k=1}^{K}(2^{2^{\gamma_k}} + 1) \\ &= (2^{2^t} - 1)^2 \prod_{i \geqslant t+1}^{I} (2^{2^{\alpha_i}} + 1)^2 + (2^{2^t} + 1)^2 \prod_{j \geqslant 2}^{J}(2^{2^{\beta_j}} + 1)^2. \end{aligned} \tag{44}$$

We now show that $I = t$ and $J = 1$.

Suppose, for example, that $I > t$ and $J = 1$. Then, from formula (44), it follows that $K > 1$, which contradicts the fact that $K = J$.

Suppose now that $I = t$ and $J > 1$. Then $K = J > 1$. Since $\beta_2 \geqslant t + 2$, it follows, by formula (44), that

$$\begin{aligned} 2 + 2^{2^{t+1}+1} + 2^{2^{\gamma_2}+1} + \text{higher powers of } 2 &= 2\prod_{k=1}^{K}(2^{2^{\gamma_k}} + 1) \\ &= (2^{2^t} - 1)^2 + (2^{2^t} + 1)^2 + 2^{2^{\beta_2}+1} + \text{higher powers of } 2 \\ &= 2 + 2^{2^{t+1}+1} + 2^{2^{\beta_2}+1} + \text{higher powers of } 2. \end{aligned} \tag{45}$$

Equation (45) implies that $\gamma_2 = \beta_2$ which is impossible.

Finally, suppose that $I > t$ and $J > 1$. Since $\beta_2 \geqslant t + 2$ and $\alpha_{t+1} \geqslant t + 2$, it follows, by formula (44), that

(46)

$$\begin{aligned} 2 + 2^{2^{t+1}+1} + 2^{2^{\gamma_2}+1} + \text{higher powers of } 2 &= 2\prod_{k=1}^{K}(2^{2^{\gamma_k}} + 1) \\ &= ((2^{2^t} - 1)^2 + 2^{2^{\alpha_{t+1}}+1} + \text{higher powers of } 2) \\ &\quad + ((2^{2^t} + 1)^2 + 2^{2^{\beta_2}+1} + \text{higher powers of } 2) \\ &= 2 + 2^{2^{t+1}+1} + 2^{2^{\alpha_{t+1}}+1} + 2^{2^{\beta_2}+1} + \text{higher powers of } 2. \end{aligned}$$

Equation (46) implies that one of the following three situations must occur:

1) $2^{\gamma_2} + 1 = 2^{\alpha_{t+1}} + 1$. This implies $\gamma_2 = \alpha_{t+1}$, which is impossible.
2) $2^{\gamma_2} + 1 = 2^{\beta_2} + 1$. This implies $\gamma_2 = \beta_2$, which is impossible.
3) $2^{\alpha_{t+1}} + 1 = 2^{\beta_2} + 1$. This implies $\alpha_{t+1} = \beta_2$, which is impossible.

The above arguments show that $I = t$, $J = K = 1$, $\alpha_i = i - 1$ for $i = 1, \ldots, t$, $\beta_1 = t$ and $\gamma_1 = t + 1$. It now follows that

$$x - y = 2^{2^t} - 1 \quad \text{and} \quad x + y = 2^{2^t} + 1. \tag{47}$$

This implies $x = 2^{2^t}$ and $y = 1$. It remains to show that $t \leqslant 3$. But this comes from the fact that if $t \geqslant 4$, then $x^4 - y^4 = 2^{2^{t+2}} - 1$ is divisible by $2^{2^5} + 1$ which is not a Fermat prime (in fact, $\varphi(2^{2^5} + 1)$ is not a power of 2).

Theorem is thus completely proved.

A c k n o w l e d g e m e n t s. The author would like to thank an annonymous referee for suggestions that greatly improved the quality of this paper. He would also like to thank professor Andreas Dress and his research group in Bielefeld for their hospitality during the period when this paper was written.

References

[1] *R. D. Charmichael*: On the numerical factors of arithmetic forms $\alpha^n \pm \beta^n$. Ann. Math. *15* (1913–1914), 30–70.
[2] *F. Luca*: Equations involving arithmetic functions of Fibonacci and Lucas numbers. Preprint. To appear in Fibo. Quart.
[3] *F. Luca*: Pascal's triangle and constructible polygons. Preprint.

Author's address: *Florian Luca*, FSP/Mathematik, Universität Bielefeld, Postfach 10 01 31, 33501 Bielefeld, Germany, e-mail: `fluca@Mathematik.Uni-Bielefeld.de`.