ON THE EQUATION $\phi(x^m - y^m) = x^n + y^n$

Florian Luca

Abstract For any positive integer k let $\phi(k)$ be the Euler totient function of k. In this paper we find all positive integer solutions of the diophantine equation $\phi(x^m - y^m) = x^n + y^n$.

For any positive integer k, let $\phi(k)$ be the Euler totient function of k. In [1], we found all solutions of the equation

$$\phi(|x^m + y^m|) = |x^n + y^n|,$$

where x, y are integers, and m, n are positive integers. A problem of a similar nature was suggested by the author in [2]. In this note we study the equation

$$\phi(x^m - y^m) = x^n + y^n, \tag{1}$$

where $x,\ y,\ m,\ n$ are positive integers.

We have the following result.

Theorem *The only positive solutions* $(x,\ y,\ m,\ n)$ *of equation* (1) *are*

$$(x,\ y,\ m,\ n) = (2^l + 1,\ 2^l - 1,\ 2,\ 1)$$

for some positive integer l.

For any positive integer k, let $\mathrm{ord}_2(k)$ be the exponent at which 2 appears in the prime factor decomposition of k.

We begin with the following lemmas.

1991 AMS *Mathematics Subject Classification.* 11A25, 11D61, 11D72.

Lemma 1 *Let $n > 0$ be a positive integer, and let $s \geq 0$ be a real number such that* $\mathrm{ord}_2(\phi(n)) \leq s$. *Then*

$$\frac{\phi(n)}{n} \geq \frac{1}{s+2}.$$

Proof: If n is a power of 2, then

$$\frac{\phi(n)}{n} = \frac{1}{2} \geq \frac{1}{s+2}.$$

Suppose now that

$$n = 2^{\delta} p_1^{\beta_1} \dots p_k^{\beta_k},$$

where $\delta \geq 0$, $k \geq 1$, $\beta_1, \ \dots, \ \beta_k$ are positive, and $p_1 < \dots < p_k$ are odd primes. Then

$$\phi(n) = 2^{\lambda} p_1^{\beta_1 - 1}(p_1 - 1) \dots p_k^{\beta_k - 1}(p_k - 1), \tag{2}$$

where $\lambda = \max(\delta - 1, \ 0)$. Since $\mathrm{ord}_2(\phi(n)) \leq s$, and since $p_1, \ \dots, \ p_k$ are odd primes, it follows that $k \leq s$, and $p_i \geq i + 2$ for $i = 1, \ \dots, \ k$. Hence,

$$\frac{\phi(n)}{n} \geq \frac{1}{2} \prod_{i=1}^{k} \Big(1 - \frac{1}{p_i}\Big) \geq \frac{1}{2} \prod_{i=1}^{k} \Big(1 - \frac{1}{i+2}\Big) = \frac{1}{s+2} \quad \blacksquare.$$

Lemma 2 *Let $x, \ y$ be integers such that $x - y \geq 2$, and let $m, \ n$ be positive integers. If $n - m \geq 2$, then*

$$\frac{x^n - y^n}{x^m + y^m} > 2x.$$

Proof: Since $n \geq m + 2$, it follows that $n \geq 3$. Clearly

$$\frac{x^n - y^n}{x^m + y^m} > \frac{(x - y) \cdot (x^{n-1} + x^{n-2} y)}{x^m + y^m} \geq 2 \cdot \frac{x^{n-1} + x^{n-2} y}{x^m + y^m}.$$

It suffices to show that

$$\frac{x^{n-1}+x^{n-2}y}{x^m+y^m} \geq x$$

or

$$x^{n-2}+x^{n-3}y \geq x^m+y^m.$$

This follows since $x^{n-2} > x^m$, and $x^{n-3}y \geq y^{n-2} \geq y^m$. ■

Lemma 3 *Let* $x,\ y$ *be two nonzero integers such that* $x+y \neq 0$, *and* $\gcd(x,\ y)$ *is odd. Let* n *be a positive integer. Then,*

$$\mathrm{ord}_2(x^n+y^n) \leq \mathrm{ord}_2(x+y).$$

Proof: If $x \not\equiv y \bmod 2$, then both x^n+y^n, and $x+y$ are odd, so the asserted inequality certainly holds. Suppose then that $x \equiv y \bmod 2$). Since $\gcd(x,\ y)$ is odd, it follows that both x, and y are odd. If n is even, then $x^n+y^n \equiv 2 \bmod 4$. Hence,

$$\mathrm{ord}_2(x^n+y^n) = 1 \leq \mathrm{ord}_2(x+y),$$

in this case. If n is odd, then

$$\begin{aligned}\mathrm{ord}_2(x^n+y^n) &= \mathrm{ord}_2(x+y) + \underbrace{\mathrm{ord}_2(x^{n-1}-x^{n-2}y+\ldots+y^{n-1})}_{=0} \\ &= \mathrm{ord}_2(x+y).\end{aligned}$$ ■

Lemma 4 *Let* x, y *be odd integers such that* $x > y$. *Assume that* $\gcd(x,\ y) = 1$. *Let* $n > 0$ *be a positive even integer. Then,*

$$\gcd\bigl(x^{n+1}-y^{n+1},\ x^n+y^n\bigr) = 2.$$

Proof: Let $D = \gcd\bigl(x^{n+1}+y^{n+1},\ x^n+y^n\bigr)$, and let $p \mid D$ be a prime. Since $p\ |x^{n+1}+y^{n+1}$, and $p\ x^n+y^n$, it follows that

$$p \mid (x^{n+1}+y^{n+1}) - y(x^n+y^n) = x^n(x-y).$$

Hence, $p \mid x(x-y)$. If $p \mid x$, then, since $p \mid x^n + y^n$, it follows that $p \mid y^n$. Hence, $p \mid y$. This contradicts the fact that $\gcd(x,\ y) = 1$. Assume that $p \mid x - y$. Since

$$p \mid x^n + y^n = \big((x-y) + y\big)^n + y^n,$$

it follows that $p \mid 2y^n$. Since $p \mid x - y$, and since $\gcd(x,\ y) = 1$, it follows that $p \not| \, y$, therefore $p \mid 2$. Since both x and y are odd, it follows that both $x^{n+1} + y^{n+1}$, and $x^n + y^n$ are even. From the previous argument we conclude that $D = 2^\lambda$. Since one of the two numbers $n,\ n+1$ is even, it follows that one of the two numbers $x^{n+1} + y^{n+1}$, or $x^n + y^n$ is a sum of two odd squares which is $2 \pmod 4$. Hence, $D = 2$. ■

Proof of the Theorem

Notice first of all that $x > y$. Moreover, since

$$x^m - y^m \geq \phi(x^m - y^m) = x^n + y^n,$$

it follows that $m > n$. Let $\alpha = \mathrm{ord}_2\big(\gcd(x,\ y)\big)$. Write $x = 2^\alpha x_1$, and $y = 2^\alpha y_1$. Clearly, at most one of the integers x_1, y_1 is even. We first show that both x_1, and y_1 are odd. Indeed, for if not, assume that $x_1 \not\equiv y_1 \mod 2)$.

Suppose first that $\alpha = 0$. In this case $x = x_1$, and $y = y_1$. It follows that $x^m - y^m$ is an odd number whose Euler indicator is again odd. Hence, $x^m - y^m = 1$, which has no solution $(x,\ y,\ m)$ with $y > 0$, and $m > 1$.

Suppose now that $\alpha \geq 1$. Then

$$\begin{aligned} x^m - y^m &= 2^{m\alpha}(x_1^m - y_1^m), \\ x^n + y^n &= 2^{n\alpha}(x_1^n + y_1^n). \end{aligned} \tag{2}$$

Then

$$\phi(x^m - y^m) = \phi\big(2^{m\alpha}(x_1^m - y_1^m\big) = 2^{m\alpha - 1}\phi(x_1^m - y_1^m). \tag{3}$$

Equation (1) becomes

$$2^{(m-n)\alpha - 1}\phi(x_1^m - y_1^m) = x_1^n + y_1^n.$$

Since $(m-n)\alpha - 1 \geq 0$, it follows that $x_1^m - y_1^m$ is an odd number whose Euler indicator is again odd. Hence, $x_1^m - y_1^m = 1$, which has no solutions $(x_1,\ y_1,\ m)$ such that $y_1 > 0$, and $m > 1$. From the previous analysis we conclude that x_1 and y_1 are both odd.

Since both x_1, and y_1 are odd, it follows easily that $x - y \geq 2$. In particular, $x \geq 3$. Since both $x_1^m - y_1^m$, and $x_1^n + y_1^n$ are even, it follows, by formulae (2) and (3), that

$$\frac{\phi(x^m - y^m)}{x^m - y^m} = \frac{\phi\big(2^{m\alpha}(x_1^m - y_1^m)\big)}{2^{m\alpha}(x_1^m - y_1^m)} = \frac{\phi(x_1^m - y_1^m)}{x_1^m - y_1^m}. \tag{4}$$

By Lemma 3, it follows that

$$\begin{aligned} \mathrm{ord}_2(x_1^n + y_1^n) &\leq \mathrm{ord}_2(x_1 + y_1) \leq \log_2(x_1 + y_1) \\ &< \log_2 2x = 1 + \log_2 x. \end{aligned} \tag{5}$$

From relations (4), (5), and Lemma 1, it follows that

$$\frac{x^n + y^n}{x^m - y^m} = \frac{\phi(x^m - y^m)}{x^m - y^m} = \frac{\phi(x_1^m - y_1^m)}{x_1^m - y_1^m} > \frac{1}{3 + \log_2 x}. \tag{6}$$

Inequality (6) is equivalent to

$$3 + \log_2 x > \frac{x^m - y^m}{x^n + y^n}. \tag{7}$$

We now show that $m = n + 1$. Indeed, if $m - n \geq 2$, then, by Lemma 2 and inequality (7) it follows that

$$3 + \log_2 x > \frac{x^m - y^m}{x^n + y^n} > 2x.$$

The above inequality implies that $x \leq 2$, which contradicts the fact that $x \geq 3$. Hence, $m = n + 1$.

We now show that n is odd. Indeed, assume that n is even. We distinguish two cases.

Case 1. $\alpha = 0$.

Since n is even, it follows that $x^n + y^n \equiv 2 \pmod 4$. Hence, $\mathrm{ord}_2(x^n + y^n) = 1$. Write

$$x^{n+1} - y^{n+1} = 2^\delta p_1^{\beta_1} \ldots p_k^{\beta_k}, \tag{8}$$

where $\delta \geq 1$, $k \geq 0$, $\beta_i \geq 1$ for $i = 1, \ldots, k$, and $p_1 < \ldots < p_k$ are odd primes.

Suppose first that $k = 0$. Then $x^{n+1} - y^{n+1} = 2^\delta$. It follows that

$$\mathrm{ord}_2\big(\phi(x^{n+1} - y^{n+1})\big) = \delta - 1 = 1,$$

or $\delta = 2$. We conclude that

$$4 = x^{n+1} - y^{n+1} > (x - y) \cdot (x^n + y^n) \geq 2 \cdot (3^2 + 1^2) = 20,$$

which is a contradiction.

Hence, $k \geq 1$. Since

$$\phi(x^{n+1} - y^{n+1}) = 2^{\delta-1} p_1^{\beta_1 - 1}(p_1 - 1) \ldots p_k^{\beta_k - 1}(p_k - 1)$$

it follows that

$$\begin{aligned} 1 = \mathrm{ord}_2(x^n + y^n) &= \mathrm{ord}_2\big(\phi(x^{n+1} - y^{n+1})\big) \\ &= (\delta - 1) + \mathrm{ord}_2(p_1 - 1) + \ldots + \mathrm{ord}_2(p_k - 1). \end{aligned}$$

It follows that $\delta = 1$, and $k = 1$. Let $p = p_1$, and $\beta = \beta_1$. Then,

$$\begin{aligned} 2p^\beta &= x^{n+1} - y^{n+1}, \\ (p-1)p^{\beta-1} &= \phi(x^{n+1} - y^{n+1}) = x^n + y^n. \end{aligned} \tag{9}$$

From relations (9) it follows that

$$2p^{\beta-1} = \gcd\big(2p^\beta,\ (p-1)p^{\beta-1}\big) = \gcd\big(x^{n+1} - y^{n+1},\ x^n + y^n\big). \tag{10}$$

We now compute $\gcd\big(x^{n+1} - y^{n+1},\ x^n + y^n\big)$. Let $d = \gcd(x,\ y)$. Write $x = d\overline{x}$, and $y = d\overline{y}$. Then,

$$\gcd\big(x^{n+1} - y^{n+1},\ x^n + y^n\big) = d^n \gcd\big(d(\overline{x}^{n+1} - \overline{y}^{n+1}),\ \overline{x}^n + \overline{y}^n\big). \tag{11}$$

Since $\gcd(\overline{x},\ \overline{y}) = 1$, both $\overline{x}$, $\overline{y}$ are odd, and n is even, it follows, by Lemma 4, that

$$\gcd\bigl(\overline{x}^{n+1} - \overline{y}^{n+1},\ \overline{x}^n + \overline{y}^n\bigr) = 2.$$

Equation (11) becomes

$$\text{(12)}\quad \gcd\bigl(x^{n+1} - y^{n+1},\ x^n + y^n\bigr) = 2d^n \gcd(d,\ \overline{x}^n + \overline{y}^n) = 2d^n d_1,$$

where $d_1 = \gcd(d,\ \overline{x}^n + \overline{y}^n)$. From formulae (10) and (12) it follows that

$$\text{(13)}\qquad 2p^{\beta-1} = 2d^n d_1.$$

From formulae (9) and (13) it follows that

$$\text{(14)}\quad d^{n+1}(\overline{x}^{n+1} - \overline{y}^{n+1}) = x^{n+1} - y^{n+1} = 2p^{\beta} = p(2p^{\beta-1}) = 2pd^n d_1,$$

or

$$\text{(15)}\qquad p = \frac{d}{d_1} \cdot \frac{\overline{x}^{n+1} - \overline{y}^{n+1}}{2}.$$

Since $\overline{x}^{n+1} - \overline{y}^{n+1} > 2$, it follows, from formula (15), that d/d_1 is a proper divisor of p. Hence, $d = d_1$. Formula (15) is then

$$\text{(16)}\qquad p = \frac{\overline{x}^{n+1} - \overline{y}^{n+1}}{2}.$$

From formulae (9) and (13) it follows that

$$\text{(17)}\qquad \begin{aligned} d^n(\overline{x}^n + \overline{y}^n) = x^n + y^n = (p-1)p^{\beta-1} &= \frac{p-1}{2} \cdot (2p^{\beta-1}) \\ &= \frac{p-1}{2} \cdot 2d^n d_1, \end{aligned}$$

or

$$\text{(18)}\quad \overline{x}^n + \overline{y}^n = \frac{p-1}{2} \cdot d_1 = \frac{d_1}{2} \cdot (p-1) = \frac{d_1}{2} \cdot \Bigl(\frac{\overline{x}^{n+1} - \overline{y}^{n+1}}{2} - 1\Bigr).$$

We now show that $d_1 = 1$. Indeed, assume that this is not the case. Since $d_1 \geq 3$ it follows, by equation (18), that

$$\overline{x}^n + \overline{y}^n \geq \frac{3}{2} \cdot \Big(\frac{\overline{x}^{n+1} - \overline{y}^{n+1}}{2} - 1 \Big) > \frac{3}{2} \cdot \Big(\frac{(\overline{x} - \overline{y}) \cdot (\overline{x}^n + \overline{y}^n)}{2} - 1 \Big)$$
$$\geq \frac{3}{2}(\overline{x}^n + \overline{y}^n - 1) > \overline{x}^n + \overline{y}^n,$$

which is a contradiction. Hence, $d_1 = 1$. It follows that $x = \overline{x}$, and $y = \overline{y}$.

From equation (16) it follows easily that $n + 1 = q$ is an odd prime, and that $y = x - 2$. Equation (18) can now be rewritten as

$$x^{q-1} + (x-2)^{q-1} = \frac{1}{2} \cdot \Big(\frac{x^q - (x-2)^q}{2} - 1 \Big),$$

or

$$4x^{q-1} + 4(x-2)^{q-1} + 2 = x^q - (x-2)^q. \tag{19}$$

We now show that equation (19) has no solution $(x,\ q)$ with q an odd prime. We distinguish the following three situations:

(a) $q \not| \, x(x-2)$. In this case, $x^{q-1} \equiv (x-2)^{q-1} \equiv 1 \pmod{q}$. Reducing equation (19) modulo q we obtain

$$4 + 4 + 2 \equiv x - (x-2) \equiv 2 \pmod{q},$$

or $8 \equiv 0 \pmod{q}$, which is a contradiction.

(b) $q \mid x$. In this case $(x-2)^{q-1} \equiv 1 \pmod{q}$. Reducing equation (19) modulo q we obtain

$$4 + 2 \equiv -(x-2) \equiv 2 \pmod{q},$$

or $4 \equiv 0 \pmod{q}$, which is a contradiction.

(c) $q \mid x - 2$. In this case $x^{q-1} \equiv 1 \pmod{q}$. Reducing equation (19) modulo q we obtain

$$4 + 2 \equiv x \equiv (x-2) + 2 \equiv 2 \pmod{q},$$

or $4 \equiv 0 \pmod{q}$, which is again a contradiction.

This disposes of Case 1.

Case 2. $\alpha \neq 0$.

From equations (2) it follows that

$$2^{\alpha}\phi(x_1^{n+1} - y_1^{n+1}) = x_1^n + y_1^n. \tag{20}$$

Equation (20) implies

$$2^{\alpha-1}\phi(x_1^{n+1} - y_1^{n+1}) = \frac{x_1^n + y_1^n}{2}. \tag{21}$$

Since $x_1,\ y_1$ are odd, and since n is even, it follows that

$$\frac{x_1^n + y_1^n}{2} \equiv 1 \pmod{2}.$$

From equation (21) it follows that $\alpha = 1$, and that $x_1^{n+1} - y_1^{n+1}$ is an even number whose Euler function is 1. The only such number 2. The equation $x_1^{n+1} - y_1^{n+1} = 2$ has no solution $(x_1,\ y_1,\ n)$ with $y_1 > 0$, and $n > 1$.

From the previous analysis we conclude that n is odd. In this case

$$(x+y) \mid \gcd\big(x^n + y^n,\ x^{n+1} - y^{n+1}\big).$$

Moreover, since n is odd, it follows that

$$\frac{x^{n+1} - y^{n+1}}{x+y} \equiv 0\ (\bmod (x-y)).$$

In particular, $\frac{x^{n+1}-y^{n+1}}{x+y}$ is even. Now let

$$x + y = 2^{\lambda} p_1^{\gamma_1} ... p_k^{\gamma_k},$$

where $\lambda > 0$, $k \geq 0$, $\gamma_i > 0$ for $i = 1,\ ...,\ k$, and $p_1 < ... < p_k$ are odd primes. Since $\frac{x^{n+1}-y^{n+1}}{x+y}$ is even, it follows that

$$\begin{aligned} 2^{\lambda}\phi\Big(\frac{x^{n+1} - y^{n+1}}{x+y}\Big) \Bigm| \phi(x^{n+1} - y^{n+1}) &= x^n + y^n \\ &= (x+y) \cdot \frac{x^n + y^n}{x+y}, \end{aligned}$$

or

$$\phi\Big(\frac{x^{n+1} - y^{n+1}}{x + y}\Big) \;\Big|\; \frac{x + y}{2^{\lambda}} \cdot \frac{x^n + y^n}{x + y}.$$

Hence, $\phi\Big(\frac{x^{n+1} - y^{n+1}}{x+y}\Big)$is odd. Since the only even number whose Euler function is odd is 2, it follows that

$$\frac{x^{n+1} - y^{n+1}}{x + y} = 2.$$

This implies that $n = 1$, and $y = x - 2$. Equation 1 becomes

$$\phi(4(x - 1)) = 2(x - 1). \tag{22}$$

Assume that

$$x - 1 = 2^l q_1^{\mu_1} ... q_t^{\mu_t},$$

where $l \geq 1$, $t \geq 0$, $\mu_i > 0$ for $i = 1, \ ..., \ t$, and $q_1 < ... < q_t$ are odd primes. We show that $t = 0$. Indeed, assume that this is not the case. Since $t \geq 1$, it follows that the power at which q_t appears in the right hand side of equation (22) is μ_t, but the power at which q_t appears in the left hand side of equation (22) is only $\mu_t - 1$. This contradiction shows that $t = 0$. Hence, $x = 2^l + 1$, and the solution has the asserted form.

The theorem is therefore completely proved. ■

References

[1] F. Luca, *On the equation* $\phi(|x^m + y^m|) = |x^n + y^n|$, submitted.

[2] F. Luca, *Problem 10626*, Amer. Math. Monthly **104** (1997), 871.

Florian Luca
Department of Mathematics,
Syracuse University,
215 Carnegie Hall,
Syracuse, New York 13244-1150.
e-mail: fgluca@syr.edu