A conjecture about Euler’s totient function and primes

Redoane D.*

E-mail: *red.daoudi@laposte.net

Abstract

Here I present a conjecture about Euler’s totient function and primes.

Keywords: Prime numbers, conjecture, Euler’s totient function

Conjecture

\( \phi \) denotes the Euler’s totient function, \( a \) denotes a natural number > 1 and \( n \) denotes a natural number such that \( n = 4k \) (\( k \) an integer \( \geq 1 \)). If \( \phi(a^n - 2) + 1 \equiv n - 1 \pmod{n} \) then \( \phi(a^n - 2) + 1 \) is always a prime number.

Example with \( a = 119 \) and \( n = 20 \): \( \phi(119^{20} - 2) + 1 \equiv 19 \pmod{20} \) then \( \phi(119^{20} - 2) + 1 \) is prime.

Investigations

Max Alekseyev studied this conjecture but no proof has been found [1].

A counterexample would have to satisfy the equation:

\[ a^n - 2 = c \cdot p^k \]
with $c \in \{1, 2\}$, a prime $p \equiv 3 \pmod{4}$, and an integer $k > 1$. Below I will show that $k$
cannot be even and also cannot be a multiple of 3, implying that $k \geq 5$ is coprime to 6.

Denoting $x := a^{n/4}$, we rewrite the two equations as

$$x^4 - 2 = c \cdot p^k.$$ 

If $k$ is even, then introducing $y := p^{k/2}$, we obtain the quartic equation

$$x^4 - 2 = c \cdot y^2.$$ 

In the case $c = 1$, it is easy to establish absence of meaningful solutions via factoring $x^4 - y^2 = (x^2 - y)(x^2 + y)$, while in the case $c = 2$ we can solve it with Magma’s `IntegralQuarticPoints` function, showing that there are no solutions in this case either.

If $3 \mid k$, then the equation is reduced to two elliptic curves (indexed by $c$):

$$Y^2 = cX^3 + 2,$$

where $Y := a^{n/2}$ and $X := p^{k/3}$. They have the only integral points (easily computed in Magma or Sage) $(X, Y) = (-1, 1)$ for $c = 1$ and $(X, Y) \in \{(-1, 0), (1, 2), (23, 156)\}$ for $c = 2$, neither of which gives us a solution to the original equation.

Hence, we have $\gcd(k, 6) = 1$ and thus $k \geq 5$.

—

PS. We may also notice that for $c = 2$, $x$ must be even the equation takes form

$$8 \left(\frac{x}{2}\right)^4 - p^k = 1,$$

while for $c = 1$ it can be written as

$$x^4 - p^k = 2.$$
That is, $p^k$ if it exists would be the smallest of two powerful numbers that differ in 1 ([OEIS A060355](https://oeis.org/A060355)) or 2 ([OEIS A076445](https://oeis.org/A076445)).

**Reference**