ON THE NUMBERS $\phi(a^n \pm b^n)$

A. ROTKIEWICZ

The Euler $\phi$-function, $\phi(m)$, denotes the number of positive integers not greater than $m$ which are relatively prime to $m$. N. G. Guderson (see [1]) generalizing the result of U. Scarpis (see [2]), that $n \mid \phi(p^n - 1)$, shows that, if $a > b$, and $m = \text{the product of the distinct prime factors of } n$, then

$$\frac{n^2}{m} \mid \phi(a^n - b^n), \text{ also } n \mid \phi(a^n + b^n).$$

We shall prove an even more general theorem as follows:

**Theorem 1.** If $a, b, n$, are natural numbers, $a > b$, $n \geq 1$, and $\theta(n)$ denotes the number of divisors of $n$, then

$$n^{\theta(n)/2} \mid \phi(a^n - b^n).$$

We give here a proof of Theorem 1 based on the following theorem (see [3]).

**Theorem T.** If $a, b, n$ are natural numbers, $a > b$, $(a, b) = 1$, $n > 2$, then $a^n - b^n$ is divisible by at least one prime $p_n$ (so called “primitive divisor”) of the form $nk + 1$, such that $p_n$ does not divide any of the integers $a^r - b^r$ ($r = 1, 2, \cdots, n - 1$); the case $a = 2, b = 1, n = 6$ provides the sole exception.

**Proof of Theorem 1.** Let $(a, b) = d > 1, a > b$, then $a = ad_1, b = bd_1, (a_1, b_1) = 1$ and $a_1 > b_1$. Since if $a \mid b$, then $\phi(a) \mid \phi(b)$, and $a^n_1 - b^n_1 \mid a^n - b^n$ it follows that $\phi(a_1^n - b_1^n) \mid \phi(a^n - b^n)$. Therefore we can suppose that $a, b$ are relatively prime.

1. Let $(a, b) = 1, a > b, 2 \nmid n$.

By Theorem T for each $1 < i \mid n, 2 \nmid n$ the number $a^i - b^i$ has a primitive divisor $p_i$ of the form $ik + 1$ such that $p_i$ does not divide $a^r - b^r$ for $0 < r < i$. It follows that $(p_i, p_j) = 1$ for $i > j$.

Because $(p_i, p_j) = (p_j, p_i)$, therefore $(p_i, p_j) = 1$ for $i \neq j$. So since $a^i - b^i \mid a^n - b^n$ for $i \mid n$, we obtain

$$\prod_{1 < i \mid n} p_i \mid a^n - b^n, \text{ where } (p_i, p_j) = 1 \text{ if } i \neq j.$$  

By Theorem T, $p_i$ for $i > 2, 2 \nmid n$ has the form $ik + 1$, hence $i \mid \phi(p_i)$ and $\prod_{1 < i \mid n} \phi(p_i) = \phi\left( \prod_{1 < i \mid n} p_i \right)$, since if $a_1, a_2, \cdots, a_k$ are relatively

Received by the editors May 11, 1960.

419
prime in pairs then \( \phi(a_1 \cdot a_2 \cdots a_k) = \phi(a_1) \cdot \phi(a_2) \cdots \phi(a_k) \). The product of all divisors of \( n \) is \( n^{\theta(n)/2} \), where \( \theta(n) \) denotes the number of divisors of \( n \) (see [4]).

From these remarks it follows that

\[
(3) \quad n^{\theta(n)/2} = \prod_{1 \leq i < n} i \left| \prod_{1 < i \leq n} \phi(p_i) = \phi \left( \prod_{1 < i \leq n} p_i \right) \right| \phi(a^n - b^n)
\]

and Theorem 1 holds.

2. Suppose that \( 2 \mid n \) and that \( p_6 \) does not exist. Then by Theorem T, \( a = 2, b = 1, 6 \mid n \), hence

\[
(4) \quad \prod_{6 \mid n} p_i \mid 2^n - 1
\]

where \( p_i \) denotes the primitive divisor of the number \( 2^i - 1 \). Since for \( 6 \mid n \), we have \( 2^6 - 1 \mid 2^n - 1 \), also \( (2^6 - 1, p_i) = 1 \) for \( i > 6 \), therefore from (4) it follows that

\[
\prod_{6 \mid n} p_i \mid 2^n - 1
\]

3. If \( 2 \mid n \) and if \( p_0 \) exists, then

\[
(5) \quad n^{\theta(n)/2} = 2 \cdot \prod_{2 \mid n} i \left| \phi(a^2 - b^2) \cdot \phi \left( \prod_{2 < i \leq n} p_i \right) \right| \phi(a^n - b^n)
\]

because \( 2 \mid \phi(n) \) for \( n > 2 \), \( a^2 - b^2 \geq a + b \geq 2 + 1 = 3 \). Theorem 1 is thus completely proved.

**EXAMPLE.** By Guderson's Theorem, we have \( (240^3/30) \phi(a^{240} - b^{240}) \)

for \( a > b \), by Theorem 1,

\[
1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 8 \cdot 10 \cdot 12 \cdot 15 \cdot 16 \cdot 20 \cdot 24 \cdot 30 \cdot 40 \cdot 48 \cdot 60 \cdot 80 \cdot 120 \cdot 240
\]

\[
= 240^{10} \phi(a^{240} - b^{240})
\]

By \( T \) a number \( a^{2n} - b^{2n} \) for \( n > 1 \), \( (a, b) = 1, a > b \), has a primitive divisor \( p_{2n} \) of the form \( 2nk + 1 \), except when \( a = 2, b = 1, n = 3 \).

Since \( p_{2n} \mid a^{2n} - b^{2n} = (a^n - b^n)(a^n + b^n) \) also \( p_{2n} \mid a^x - b^x \) for \( 0 < x < 2n \), therefore \( p_{2n} \mid a^n + b^n \). If \( p_{2n} \mid a^x + b^x \) for \( 0 < x < n \), then \( p_{2n} \mid a^{2x} - b^{2x} \) for \( 0 < x < 2n \), which is impossible, because by hypothesis \( p_{2n} \) is a primitive divisor of \( a^{2n} - b^{2n} \). Therefore,
THEOREM T'. If $a$, $b$, $n$ are natural numbers, $a>b$, $(a, b) = 1$, $n>1$, then $a^n+b^n$ is divisible by at least one prime $p$ of the form $2nk+1$, such that $p$ does not divide any of the integers $a^r+b^r$ ($r=1, 2, \ldots, n-1$); the case $a=2$, $b=1$, $n=3$ provides the only exception.

THEOREM 2. If $a$, $b$, $n$ are natural numbers, $a>b$, $n=2^a\cdot n_1$, where $(2, n_1)=1$, $a\geq 0$, then

(4) $\left(2^{a+2} \cdot n\right)^{\Phi(n_1)/2} \mid \phi(a^n + b^n)$ for $n \neq 3 \cdot (2k + 1)$,

(5) $\frac{1}{2} \left(2^{a+2} \cdot n\right)^{\Phi(n)/2} \mid \phi(a^n + b^n)$ for $n = 3 \cdot (2k + 1)$, ($k = 1, 2, \ldots$).

This theorem follows from Theorem T' in the same manner that Theorem 1 follows from Theorem T.

REFERENCES


INSTITUTE OF MATHEMATICS, WARSAW UNIVERSITY, POLAND