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

A. ROTKIEWICZ

The Euler ϕ-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 $m=$ the product of the distinct prime factors of n, then

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

We shall prove an even more general theorem as follows:

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

$$n^{\theta(n)/2} \mid \phi(a^n - b^n). \tag{1}$$

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 $a=a_1 d$, $b=b_1 d$, $(a_1, b_1)=1$ and $a_1>b_1$. Since if $a \mid b$, then $\phi(a) \mid \phi(b)$, and $a_1^n-b_1^n \mid a^n-b^n = d^n(a_1^n-b_1^n)$ 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

$$\prod_{1<i \mid n} p_i \mid a^n - b^n, \quad \text{where} \quad (p_i, p_j) = 1 \text{ if } i \neq j. \tag{2}$$

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

Received by the editors May 11, 1960.

prime in pairs then $\phi(a_1 \cdot a_2 \cdot \cdots \cdot a_k) = \phi(a_1) \cdot \phi(a_2) \cdot \cdots \cdot \phi(a_k)$. 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

$$(3) \qquad n^{\theta(n)/2} = \prod_{1<i|n} i \Big| \prod_{1<i|n} \phi(p_i) = \phi\Big(\prod_{1<i|n} p_i\Big) \Big| \phi(a^n - b^n)$$

and Theorem 1 holds.

2. Suppose that $2|n$ and that p_6 does not exist. Then by Theorem T, $a=2$, $b=1$, $6|n$, hence

$$(4) \qquad \prod_{6<i|n} p_i \mid 2^n - 1$$

where p_i denotes the primitive divisor of the number 2^i-1. Since for $6|n$, 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

$$n^{\theta(n)/2} = \prod_{i|n} i = 36 \prod_{6<i|n} i \Big| \phi(2^6 - 1) \cdot \phi\Big(\prod_{6<i|n} p_i\Big)$$

$$= \phi\Big[(2^6 - 1) \cdot \prod_{6<i|n} p_i\Big] \Big| \phi(2^n - 1).$$

3. If $2|n$ and if p_6 exists, then

$$n^{\theta(n)/2} = 2 \cdot \prod_{2<i|n} i \Big| \phi(a^2 - b^2) \cdot \phi\Big(\prod_{2<i|n} p_i\Big)$$

$$= \phi\Big[(a^2 - b^2) \cdot \prod_{2<i|n} p_i\Big] \Big| \phi(a^n - b^n)$$

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

EXAMPLE. By Guderson's Theorem, we have $(240^2/30) \mid \phi(a^{240}-b^{240})$ for $a>b$, by Theorem 1,

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

$$= 240^{10} \mid \phi(a^{240} - b^{240})$$

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 $p_{2n} \nmid a^x-b^x$ 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 $(r=1, 2, \cdots, n-1)$; the case $a=2$, $b=1$, $n=3$ provides the only exception.*

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

$$(4) \quad (2^{\alpha+2} \cdot n)^{\phi(n_1)/2} \mid \phi(a^n + b^n) \qquad \text{for } n \neq 3 \cdot (2k+1),$$

$$(5) \quad \frac{1}{2}(2^{\alpha+2} \cdot n)^{\phi(n)/2} \mid \phi(a^n + b^n) \quad \text{for } n = 3 \cdot (2k+1), (k = 1, 2, \cdots).$$

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

REFERENCES

1. N. G. Guderson, *Some theorems of Euler ϕ-function*, Bull. Amer. Math. Soc. vol. 49 (1943) pp. 278–280.

2. U. Scarpis, Period. Mat. vol. 29 (1913) p. 138.

3. G. D. Birkhoff and H. S. Vandiver, *On integral divisors of a^n-b^n*, Ann. of Math. (2) vol. 5 (1904) pp. 173–180.

4. J. V. Uspensky and M. A. Heaslet, *Elementary number theory*, New York and London, McGraw-Hill, 1939, p. 83, exercise 8.

INSTITUTE OF MATHEMATICS, WARSAW UNIVERSITY, POLAND