SOME CONGRUENCE PROPERTIES OF THE ϕ-FUNCTION

By P. Kesava Menon
(*Madras Christian College, Tambaram*)

Received August 6, 1946
(Communicated by Prof. B. S. Madhava Rao)

Let $\phi(n)$ denote the number of numbers not greater than and prime to n. Then the following lemma can easily be proved:

Lemma 1.—If a and b are prime to n and m is the least positive integer for which

$$a^m \equiv b^m \bmod n,$$

then every integer N such that

$$a^N \equiv b^N \bmod n$$

is a multiple of m; in particular $\phi(n)$ is a multiple of m.

We now proceed to prove the following:

Theorem 1.—If a is greater than and prime to b, then

$$\phi(a^n - b^n) \equiv 0 \bmod n.$$

For, obviously

$$a^n \equiv b^n \bmod (a^n - b^n);$$

and if $r < n$, then $a^r - b^r < a^n - b^n$, so that

$$a^r \not\equiv b^r \bmod (a^n - b^n).$$

It follows from lemma 1 that n is a divisor of $\phi(a^n - b^n)$.

Theorem 2.—If a is prime* to b and $n \geqslant 2$, then

$$\phi\{a^{m(n-1)} + a^{m(n-2)} b^m + a^{m(n-3)} b^{2m} + \ldots + b^{m(n-1)}\} \equiv 0 \bmod mn.$$

Proof.—It is clear that

$$a^{mn} - b^{mn} \equiv 0 \bmod \{a^{m(n-1)} + a^{m(n-2)} b^m + \ldots + b^{m(n-1)}\} \qquad (1)$$

If N is the least positive integer such that

$$a^N - b^N \equiv 0 \bmod \{a^{m(n-1)} + a^{m(n-2)} b^m + \ldots + b^{m(n-1)}\} \qquad (2)$$

then, by lemma 1, N is a divisor of mn. Also, for $N \leqslant m(n-1)$,

$$|a^N - b^N| < a^{m(n-1)} + a^{m(n-2)} b^m + \ldots + b^{m(n-1)}$$

* Here, as well as in what follows we shall exclude the case $a = b = 1$.

Therefore

$$mn \geqslant N \geqslant m(n-1). \qquad (3)$$

Let g be the g.c.d. of m and N and let

$$m = gm_1, \ N = gN_1.$$

Writing $a^g = \alpha$ and $b^g = \beta$ we see from (2) that N_1 is the least positive integer such that

$$\alpha^{N_1} \equiv \beta^{N_1} \bmod \{\alpha^{m_1(n-1)} + \alpha^{m_1(n-2)}\beta^{m_1} + \ldots + \beta^{m_1(n-1)}\}.$$

It follows that N_1 is a divisor of $m_1 n$, and since N_1 is prime to m_1, that N_1 is a divisor of n. But from (3) we see that

$$N_1 \geqslant m_1(n-1) \geqslant (n-1).$$

Hence $N_1 = n$, $m_1 = 1$, and so $m = g$, $N = mn$.

Therefore, by lemma 1, mn is a divisor of

$$\phi\{a^{m(n-1)} + a^{m(n-2)}b^m + \ldots + b^{m(n-1)}\}.$$

2. Let $n = p^\alpha n_1$, where p is prime and n_1 is prime to p. Then if we write

$$f(m, n) = a^{m(n-1)} + a^{m(n-2)}b^m + \ldots + b^{m(n-1)}$$

we have

Lemma 2.—$a^n - b^n = (a^{n_1} - b^{n_1}) \prod_{i=1}^{\alpha} f(n/p^i, p).$

Let us further suppose that a is prime to b. Then we have

Lemma 3.—The g.c.d. of any two of the numbers

$$a^{n_1} - b^{n_1}, \ f(n/p^i, p) \ (i = 1, 2, \ldots, \alpha)$$

is either p or 1.

For, if d is a common divisor of

$$f(n/p^j, p) \text{ and } f(n/p^i, p) \ (i < j),$$

then

$$0 \equiv f(n/p^j, p)\,(a^{n/p^j} - b^{n/p^j})$$
$$\equiv a^{n/p^{j-1}} - b^{n/p^{j-1}} \bmod d;$$

and so

$$0 \equiv f(n/p^i, p) \equiv pa^{n(p-1)/p^i} \bmod d$$

so that, since d is prime to a,

$$d = p \text{ or } 1.$$

Similarly we can show that the g.c.d. of

$$a^{n/p^\alpha} - b^{n/p^\alpha} \text{ and } f(n/p^i, p)$$

is either p or 1.

Lemma 4. $f(n/p^i, p) \equiv f(n/p^\alpha, p) \bmod p \;\; (i = 1, 2, \ldots, \alpha)$.

This follows immediately from

$$a^{n/p^i} = a^{p^{\alpha-i}\, n/p^\alpha} \equiv a^{n/p^\alpha} \bmod p.$$

Lemma 5. If $f(m, p) \equiv 0 \bmod p$, then

$$a^m \equiv b^m \bmod p.$$

For,

$$0 \equiv f(m, p)\,(a^m - b^m) = a^{mp} - b^{mp} \bmod p,$$

and

$$a^{mp} \equiv a^m \bmod p$$

$$b^{mp} \equiv b^m \bmod p$$

so that

$$0 \equiv a^{mp} - b^{mp} \equiv a^m - b^m \bmod p.$$

Conversely, we have

Lemma 6. If $a^m \equiv b^m \bmod p$, then

$$f(m, p) \equiv 0 \bmod p.$$

From lemmas 2 to 6 we get

Lemma 7. If any one of

$$a^{n_1} - b^{n_1},\ f(n/p^i, p) \qquad (i = 1, 2, \ldots, \alpha)$$

is prime to p, then they are all prime to each other, and

$$\phi(a^n - b^n) = \phi(a^{n_1} - b^{n_1}) \prod_{i=1}^{\alpha} \phi\{f(n/p^i, p)\}$$

Similarly we get

Lemma 8. If any one of $a^{n_1} - b^{n_1}, f(n/p^i, p)$ $(i = 1, 2, \ldots, \alpha)$ is divisible by p, then so are all of them and

$$(a^{n_1} - b^{n_1})/p,\ f(n/p^i, p)/p \quad (i = 1, 2, \ldots, \alpha)$$

are prime to each other; further, $a^n - b^n$ is divisible by $p^{\alpha+1}$ and

$$\phi\{(a^n - b^n)/p^{\alpha+1}\} = \phi\{(a^{n_1} - b^{n_1})/p\} \prod_{i=1}^{\alpha} \phi\{f(n/p^i, p)/p\}.$$

Lemma 9. None of

$$f(n/p^i, p) \quad (i = 1, 2, \ldots, \alpha - 1)$$

is divisible by a higher power of p than the first.

If one of a, b is a multiple of p, then the other is not, and so $f(n/p^i, p)$ is clearly prime to p. Therefore we may assume that a and b are both prime to p. Then

$$a^{\frac{n}{p^i}\left(1-\frac{1}{p}\right)} \equiv 1 \bmod p^2,\ \alpha > i+1$$

i.e.,

$$a^{n/p^i} \equiv a^{n/p^{i+1}} \bmod p^2,\ \alpha > i+1,$$

and so

$$f(n/p^i, p) \equiv f(n/p^{i+1}, p) \bmod p^2,\ i < \alpha - 1.$$

It follows that if any one of $f(n/p^i, p)$ $(i = 1, 2, \ldots, \alpha - 1)$ is divisible by p^2, then so are all the others; but this cannot be the case because of lemma 3.

We are now in a position to prove

THEOREM 3.—If $n = p^\alpha n_1$ where p is the smallest prime factor of n, and n_1 is prime to p, and a is greater than and prime to b, then

$$\phi(a^n - b^n)$$

is divisible by

$$\phi(a^{n_1} - b^{n_1})\, n^\alpha / p^{\alpha(\alpha-1)/2} \text{ if } a^n - b^n \text{ is prime to } p,$$

and by

$$\phi(a^{n_1} - b^{n_1})\,(pn)^\alpha / p^{\alpha(\alpha-1)/2} \text{ if } p \text{ is a divisor of } a^n - b^n.$$

Proof.—If any one of $a^{n_1} - b^{n_1}$, $f(n/p^i, p)$ $(i = 1, 2, \ldots, \alpha)$ is prime then by lemma 7 we have

$$\phi(a^n - b^n) = \phi(a^{n_1} - b^{n_1}) \prod_{i=1}^{\alpha} \phi\{f(n/p^i, p)\}.$$

But, by theorem 2,

$$\phi\{f(n/p^i, p)\} \equiv 0 \bmod n/p^{i-1},$$

and so

$$\phi(a^n - b^n) \equiv 0 \bmod \phi(a^{n_1} - b^{n_1}) \prod_{i=1}^{\alpha} n/p^{i-1}.$$

If, on the other hand, $a^{n_1} - b^{n_1}$, $f(n/p^i, p)$ are all divisible by p, then by lemma 8

$$\phi\{(a^{n} - b^{n})/p^{\alpha+1}\} = \phi\{(a^{n_1} - b^{n_1})/p\} \prod_{i=1}^{\alpha} \phi\{f(n/p^i, p)/p\}.$$

But $f(n/p^i, p)/p$ being prime to p for $i < \alpha$, (by lemma 9)

$$\phi\{f(n/p^i, p)\} = \phi\{f(n/p^i, p)/p\}\,\phi(p),$$

and so, by theorem 2

$$\phi\{f(n/p^i, p)/p\} \equiv 0 \bmod n/p^{i-1},\ i < \alpha,$$

since every prime factor of n/p^{i-1} is greater than $\phi(p) = p - 1$. Further, if the greatest power of p dividing $a^n - b^n$ be $p^{\alpha+1+r}$ $(r \geqslant 0)$, then either

$a^{n_1} - b^{n_1}$ or $f(n_1, p)$ is divisible by p^{r+1} and

$$\phi(a^n - b^n) = \phi(p^{\alpha+1+r})\, \phi[(a^n - b^n)/p^{\alpha+1+r}]$$

$$= \begin{cases} p^{\alpha+1} \phi[(a^n - b^n)/p^{\alpha+1}] \text{ if } r \geqslant 1 \\ p^{\alpha}(p-1)\, \phi[(a^n - b^n)/p^{\alpha+1}] \text{ if } r = 0; \end{cases}$$

and

$$\phi(a^{n_1} - b^{n_1}) = \phi(p^{r+1})\, \phi[(a^{n_1} - b^{n_1})/p^{r+1}]$$

$$= \begin{cases} p\, \phi[(a^{n_1} - b^{n_1})/p] \text{ if } r \geqslant 1, \\ (p-1)\, \phi[(a^{n_1} - b^{n_1})/p \text{ if } r = 0. \end{cases}$$

It follows that

$$\phi(a^n - b^n) = p^{\alpha} \phi(a^{n_1} - b^{n_1}) \cdot \frac{\phi[(a^n - b^n)/p^{\alpha+1}]}{\phi[(a^{n_1} - b^{n_1})/p]}$$

$$= p^{\alpha} \phi(a^{n_1} - b^{n_1}) \prod_{i=1}^{\alpha} \phi\{f(n/p^i, p)/p\}$$

$$\equiv 0 \bmod p^{\alpha} \phi(a^{n_1} - b^{n_1}) \prod_{i=1}^{\alpha} n/p^{i-1},$$

since $\phi\{f(n_1, p)/p\}$ is certainly divisible by $n_1 p$ by Theorem 2 whether $f(n_1, p)$ is divisible by a higher power of p than the first ore not, from the fact that n_1 is prime to $\phi(p)$. This completes the proof of the theorem.

From theorem 3 we get the following refinement of theorem 1.

THEOREM 4.—If $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$, where $p_1 > p_2 > \ldots > p_r$ are the distinct prime factors of n, and a is greater than and prime to b, then

$$\phi(a^n - b^n) \equiv 0 \bmod \prod_{i=1}^{r} p_i^{\alpha_i(\alpha_1 + \alpha_2 + \cdots + \alpha_{i-1}) + \frac{\alpha_i(\alpha_i+1)}{2}}$$

Proof.—From theorem 3 we have

$$\phi(a^n - b^n) \equiv 0 \bmod \phi(a^{n/p_1^{\alpha_1}} - b^{n/p_1^{\alpha_1}}) \times n^{\alpha_1}/p_1^{\alpha_1(\alpha_1-1)/2}.$$

Since p_2 is the least prime factor of $n/p_1^{\alpha_1}$ we have similarly

$$\phi(a^{n/p_1^{\alpha_1}} - b^{n/p_1^{\alpha_1}}) \equiv 0 \bmod \phi(a^{n/p_1^{\alpha_1} p_2^{\alpha_2}} - b^{n/p_1^{\alpha_1} p_2^{\alpha_2}})$$

$$\times \left(\frac{n}{p_1^{\alpha_1}}\right)^{\alpha_2} \Big/ p_2^{\alpha_2(\alpha_2-1)\,2}$$

and so on. Thus

$$\phi(a^n - b^n) \equiv 0 \bmod \prod_{i=1}^{r} \left(\frac{n}{p_1^{\alpha_1} \ldots p_{i-1}^{\alpha_{i-1}}}\right)^{\alpha_i} \Big/ p_i^{\alpha_i(\alpha_{i-1})}$$

which is easily seen to be theorem 4.