SOME THEOREMS ON THE EULER ϕ-FUNCTION

N. G. GUNDERSON

The Euler ϕ-function, $\phi(m)$, denotes the number of positive integers not greater than m which are relatively prime to m.[1] It was noted by U. Scarpis[2] that $n|\phi(p^n-1)$. Generalizations of this result are obtained in Theorems 9 and 10.

The first five theorems are either well known or self-evident.[3]

THEOREM 1. *If $p_1, \cdots, p_k$ are the distinct prime factors of m, then*

$$\phi(m) = m(p_1 - 1)(p_2 - 1) \cdots (p_k - 1)/p_1p_2 \cdots p_k.$$

THEOREM 2. *If $a_1, \cdots, a_k$ are relatively prime in pairs, then*

$$\phi(a_1 \cdots a_k) = \phi(a_1)\cdot\phi(a_2) \cdots \phi(a_k).$$

THEOREM 3. *If w is the product of the distinct prime factors common to m and n, then*

$$\phi(mn) = w\cdot\phi(m)\cdot\phi(n)/\phi(w).$$

THEOREM 4. *If $a|b$, then $\phi(a)|\phi(b)$.*

THEOREM 5. *If $q|a$ and $q\equiv 1 \pmod{p^\alpha}$, then $p^\alpha|\phi(a)$.*

THEOREM 6. *If p is an odd prime, $a\neq b$, and $\alpha \geqq 1$, then*

$$p^{2\alpha-1} \mid \phi(a^{p^\alpha} + b^{p^\alpha}).$$

The proof is by induction on α. We assume $a>b$. In the notation of Birkhoff and Vandiver,[4] $a^p+b^p=V_{2p}/V_p$. By their Theorems V and I, there is a prime divisor q of a^p+b^p such that $q\equiv 1 \pmod p$ unless $p=3$, $a=2$, $b=1$. Then by Theorem 5, $p|\phi(a^p+b^p)$, and in the exceptional case, $3|\phi(2^3+1^3)$. Thus the theorem holds for $\alpha=1$, starting the induction, so we assume it for all positive integers less than α. We adopt the notation $C=AB$, where

$$C = a^{p^\alpha} + b^{p^\alpha}, \qquad P = p^{\alpha-1}, \qquad A = a^p + b^p,$$

$$B = a^{(p-1)P} - a^{(p-2)P}\cdot b^P + \cdots - a^P\cdot b^{(p-2)P} + b^{(p-1)P}.$$

Received by the editors June 12, 1942.

[1] In this discussion all letters represent positive integers. In particular, p and q represent primes.

[2] Period. Mat. vol. 29 (1913) p. 138.

[3] See, for example, L. E. Dickson, *History of the theory of numbers*, vol. 1, chap. 5.

[4] Ann. of Math. (2) vol. 5 (1903) pp. 173–180.

Case 1. $(a, b)=1$.

Again using the notation of Birkhoff and Vandiver, $B=C/A=(V_{2pP}/V_{pP})(V_P/V_{2P})$, so we see by their Theorems V and I that there is a prime divisor q of B such that $q\equiv 1 \pmod{p^\alpha}$. Hence by Theorem 5 we have that $p^\alpha | \phi(B)$. By the hypothesis of induction we have $p^{2(\alpha-1)-1} | \phi(A)$.

Now, if $(A, B)\neq 1$, let r be a common prime factor of A and B. Then $a^P\equiv -b^P \pmod r$, so that $B\equiv p\cdot a^{(p-1)P}\equiv 0 \pmod r$. If $r|a$, then $r|b$, contrary to $(a, b)=1$, so $r=p$. Then by Theorem 3,

$$\phi(C) = p\cdot\phi(A)\cdot\phi(B)/(p-1),$$

so we have that $p\cdot p^{2(\alpha-1)-1}\cdot p^\alpha | \phi(C)$. But since $\alpha>1$, $3\alpha-2>2\alpha-1$, so $p^{2\alpha-1}|\phi(C)$.

If $(A, B)=1$, then $\phi(C)=\phi(A)\cdot\phi(B)$, and $p^{2(\alpha-1)-1}\cdot p^\alpha|\phi(C)$. Again, since $\alpha>1$, $3\alpha-3\geqq 2\alpha-1$, and $p^{2\alpha-1}|\phi(C)$.

Case 2. $(a, b)\neq 1$.

Let $(a, b)=c$, $a=ca_1$, $b=cb_1$, $(a_1, b_1)=1$. Further, since $a>b$, a_1 and b_1 are not both 1, and so $a_1>b_1$. By Case 1, $p^{2\alpha-1}|\phi(a_1^{p\alpha}+b_1^{p\alpha})$ so by Theorem 4, $p^{2\alpha-1}|\phi(a^{p\alpha}+b^{p\alpha})$.

THEOREM 7. *If* $a\neq b$, *then* $2^{\alpha+1}|\phi(a^{2\alpha}+b^{2\alpha})$.

We note that $a^{2\alpha}+b^{2\alpha}=2^\beta$ would imply $a=b=2$, so $a^{2\alpha}+b^{2\alpha}$ has an odd factor, say q. For $(a, b)=1$, Euler[5] has shown that $q\equiv 1 \pmod{2^{\alpha+1}}$, so by Theorem 5, $2^{\alpha+1}|\phi(a^{2\alpha}+b^{2\alpha})$. For $(a, b)\neq 1$ we proceed as in Case 2 of Theorem 6.

THEOREM 8. *If* $a>b$, *then* $p^{2\alpha-1}|\phi(a^{p\alpha}-b^{p\alpha})$.

The proof of this theorem parallels that of Theorem 6.

THEOREM 9. *If* $a>b$, *and* m *is the product of the distinct prime factors of* n, *then* $(n^2/m)|\phi(a^n-b^n)$.

Let $n=P_1P_2\cdots P_k$ where $P_i=p_i^{\alpha_i}$. Then $a^n-b^n=(a^{n_i})^{P_i}-(b^{n_i})^{P_i}$ where $n_i=P_1\cdots P_{i-1}P_{i+1}\cdots P_k$. Then by Theorem 8, $p_i^{2\alpha_i-1}|\phi(a^n-b^n)$, and the theorem follows immediately.

THEOREM 10. *If* $a\neq b$, *then* $n|\phi(a^n+b^n)$.

This proof parallels that of Theorem 9.

Theorems 9 and 10 can be combined in various ways, for example, we have this theorem:

[5] Commentationes Arithmeticae Collectae, vol. 1, p. 55. See also Amer. Math. Monthly vol. 10 (1903) p. 171, misprint of $2m$ for 2^m.

THEOREM 11. *If* $(a, b) = 1$, *and* m *is the product of the distinct prime factors of* n, *then*

$$(n^3/m) \mid \phi(a^{2n} - b^{2n}).$$

CORNELL UNIVERSITY

APPLICATIONS OF TRANSITIVITIES OF BETWEENNESS IN LATTICE THEORY[1]

M. F. SMILEY AND W. R. TRANSUE

Introduction. This paper solves three characterization problems for lattices[2] [1]. Problem I is to characterize those metric spaces [2] into which lattice operations which are consistent with the given metric [1, p. 41] may be introduced. Problem II is to characterize those members of a rather general class of abstract systems which are modular lattices, while Problem III consists in the characterization of lattices in an even larger class of abstract systems.

Problem I has already been solved by V. Glivenko [3]. He showed that the property: "Among those elements metrically between [4, p. 76; 2] two elements a and b, the element $a \cup b$ is farthest from O," and its dual characterize those metric spaces which are also metric lattices with the same metric and least element O. Our approach to Problem I is through the existence of certain metric singularities [2, p. 47] in every metric lattice. Our solution also involves certain five point transitivities [5, Part I] of metric betweenness. The abstract system involved in Problem II (Problem III) is a wide generalization of the concept of a metric space—so general, in fact, that it also includes the concept of a modular lattice (lattice). We find it not difficult to extend the ideas essential to our solution of Problem I to give analogous solutions of Problems[3] II and III. Briefly, our results consist in characterizing the three important systems: metric

---

Presented to the Society, April 4, 1942; received by the editors June 2, 1942.

[1] This paper is an expansion of our note *Metric lattices as singular metric spaces* which was presented to the Society on December 29, 1941, and which was to appear in Bull. Amer. Math. Soc.

[2] Numbers in square brackets refer to the list of references at the end of the paper.

[3] It would be interesting to characterize metric spaces among our general systems. This problem appears difficult to us, and we make no attempt to solve it.