BULLETIN OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 79, Number 2, March 1973

CONTRIBUTION TO THE THEORY OF EULER'S FUNCTION $\varphi(x)$[1]

BY EMIL GROSSWALD

Communicated by Dock S. Rim, August 21, 1972

1. **Introduction.** The last few years have witnessed a renewed interest in the study of the number $N(n)$ of solutions of the equation

$$\varphi(x) = n, \tag{1}$$

where $\varphi(x)$ is Euler's totient function.

The purpose of the present paper is to give a sharpened (and corrected) version of a theorem of Carmichael (Theorem 1; see [**1**, Theorem II]) and the proof of a weak form of the

CONJECTURE. For all natural integers n, $N(n) \neq 1$.

Lower case letters (with or without subscripts, or superscripts) stand, in general, for natural integers, p and q, in particular, for odd rational primes.

2. **Main results.**

DEFINITION. The natural integer k is said to be *admissible*, if its (unique) representation as a sum of distinct powers of 2,

$$k = 2^{s_1} + 2^{s_2} + \cdots + 2^{s_r}, \qquad s_1 > s_2 > \cdots > s_r \geqq 0,$$

is such that $2^{2^{s_j}} + 1$ is a (Fermat) prime for each $j = 1, 2, \ldots, r$. The set of admissible integers is denoted by K.

REMARK. For $r = 0$ it is convenient to consider the corresponding $k = 0$ as an admissible integer; one observes that formally one has $2^0 + 1 = 2$, a prime.

THEOREM 1. *Let $\chi(k)$ be the characteristic function of the set K ($\chi(k) = 1$ if $k \in K$, $\chi(k) = 0$ if $k \notin K$) and set $g(m) = \sum_{0 \leqq k \leqq m} \chi(k)$; then, if $n = 2^m$, equation* (1) *has*

$$N(n) = g(m) + \chi(m) \tag{I}$$

solutions.

COROLLARY 1. *For $n = 2^m$*, $N(2^m) = \min(m + 2, 32)$.

AMS(MOS) subject classifications (1970). Primary 10A20; Secondary 10B15, 10B99, 10-01.

[1] This paper was written with partial support from the National Science Foundation, through the grant GP 23170.

It is trivial, but useful, to observe that if (1) has the odd solution x_0, then it also has the even solution $2x_0$ and conversely. Hence, if (1) has exactly one solution, then $4|x_0$, as observed already by Carmichael (see [**1**]; see also Donnelly [**2**]).

In the study of (1) for general n, it is convenient to consider residue classes modulo $M = 2^c \cdot 3$. Also, the following easily proven Lemma and its Corollary are useful.

LEMMA. *The equation* $p^a(p-1) = q^b(q-1)$ *cannot have solutions in primes* p, q, *with* $p > q$, *unless* $a = 0$ *and* $p = q^b(q-1)$.

COROLLARY 2. *The equations* (2), (2′), (3), (4), (4′), (5), *and* (5′) *have at most* 2 *solutions* (*i.e.*, $\delta = 0, 1$, *or* 2).

THEOREM 2. *For* $n = 2$, *equation* (1) *has the three solutions* $x = 3, 4$, *and* 6. *For* $2 \neq n \equiv 2 \pmod{12}$, (1) *has, in general, no solution. Let* $\delta(n)$ *be the number of solutions of*

$$n = p^{2m-1}(p-1), \qquad p \equiv -1 \pmod{12}; \tag{2}$$

then

$$N(n) = 2\delta(n) \tag{II}$$

and to a solution p *of* (2) *correspond the solutions* p^{2m} *and* $2p^{2m}$ *of* (1).

THEOREM 2. *For* $n \equiv -2 \pmod{12}$, *let* $\delta(n)$ *be the number of solutions of*

$$n = p^{2m}(p-1), \qquad p \equiv -1 \pmod{12}; \tag{2′}$$

then

$$N(n) = 2\delta(n), \tag{II′}$$

and to a solution p *of* (2′) *correspond the two solutions* p^{2m+1} *and* $2p^{2m+1}$ *of* (1).

THEOREM 3. *Let* $n \equiv 6 \pmod{12}$; *if* $\delta(n)$ *stands for the number of solutions of*

$$n = p^{c-1}(p-1), \qquad p = 3 \text{ or } p \equiv 7 \pmod{12}, \tag{3}$$

then

$$N(n) = 2\delta(n), \tag{II″}$$

and to a solution p *of* (3) *correspond the two solutions* p^c *and* $2p^c$ *of* (1).

REMARK. All possible cases actually occur. The smallest values of $n \equiv 6 \pmod{12}$, for which (1) has 0, 2, or 4 solutions are $n = 90$, $n = 30$, and $n = 6$, respectively.

Theorems 2, 2′, and 3, together with the trivial remark that, for $1 < n \equiv 1 \pmod 2$, $N(n) = 0$, settle the problem for all residue classes $n \not\equiv 0 \pmod 4$. A partial solution of the problem of determining $N(n)$ for $n \equiv 0 \pmod 4$ is obtained by considering the modulus $M = 24 = 2^3 \cdot 3$.

THEOREM 4. *Let* $n \equiv 4 \pmod{24}$ *and denote by* δ_1 *the number of solutions of*

$$n/2 = p^{2m-1}(p-1), \qquad p \equiv -1 \pmod{12}; \tag{4}$$

by δ_2 *the number of solutions of*

$$n = p^{2m}(p-1), \qquad p \equiv 5 \pmod{12}; \tag{4$'$}$$

and by δ_3 *the number of solutions of*

$$n = p_1^{c_1-1} p_2^{c_2-1} (p_1 - 1)(p_2 - 1), \qquad \begin{aligned} &p_1 \equiv p_2 \equiv -1 \pmod{12}, \\ &c_1 \equiv c_2 \pmod 2; \end{aligned} \tag{4$''$}$$

then

$$N(n) = 3\delta_1 + 2\delta_2 + 2\delta_3. \tag{III}$$

REMARKS. In Theorem 4, $\delta_1 = 0$ or 1; $\delta_2 = 0, 1$, or 2, while δ_3 may be any nonnegative integer. If $\delta_1 = 1$, then $x_0 = p^{2m}$ is the unique odd solution of $\varphi(x_0) = n/2$ and to it correspond the three solutions $3p^{2m}$, $4p^{2m}$, and $6p^{2m}$ of (1). To each solution p of (4′) correspond the two solutions p^{2m+1} and $2p^{2m+1}$ of (1), and to each solution p_1, p_2 of (4″), correspond the two solutions $p^{c_1}p^{c_2}$ and $2p^{c_1}p^{c_2}$ of (1).

If $n \equiv -4 \pmod{24}$, then $N(n)$ is still given formally by (III), where $\delta_1, \delta_2, \delta_3$ are now the numbers of solutions of equations very similar to (but not identical with) (4), (4′), (4″), and $\delta_1 = 0, 1$, or 2; $\delta_2 = 0$ or 1; and $\delta_3 = 0, 1, 2, \ldots$; the exact statement of the corresponding Theorem 4′ may be omitted.

THEOREM 5. *Let* $n \equiv 12 \pmod{24}$ *and set* $n = 12 \cdot 3^{b-1}f$, $(f, 6) = 1$. *If* $f > 1$, *denote by* δ_1' $(=0, 1$, *or* $2)$ *the number of solutions of*

$$2 \cdot 3^b f = p^{c-1}(p-1), \qquad p \equiv 7 \pmod{12}; \tag{5}$$

by δ_2' $(=0, 1$, *or* $2)$ *the number of solutions of*

$$4 \cdot 3^b f = p^{c-1}(p-1), \qquad p \equiv 13 \pmod{24}; \tag{5$'$}$$

and by δ_3' $(=0, 1, \ldots)$ *the number of solutions of*

$$4 \cdot 3^b f = p_1^{c_1-1} p_2^{c_2-1}(p_1 - 1)(p_2 - 1), \qquad \begin{aligned} &p_1 \equiv p_2 \equiv 3 \pmod 4, \\ &3 \nmid p_1 p_2; \end{aligned} \tag{5$''$}$$

then

(III′) $$N(n) = 3\delta_1' + 2(\delta_2' + \delta_3').$$

If $f = 1$, *then*

(III″) $$N(n) = 3 + \delta_0 + 2(\delta_0' + J + R),$$

where $\delta_0 = 1$ *if* $2 \cdot 3^b + 1$ *is a prime*, $\delta_0 = 0$ *otherwise*; $\delta_0' = 1$ *if* $4 \cdot 3^b + 1$ *is a prime*, $\delta_0' = 0$ *otherwise*; J *is the number of integers* a_j, $1 \leqq a_j < b$, *such that* $2 \cdot 3^{b-a_j+1}$ *is a prime*; *and* R *is the number of partitions of* b *into two positive summands*, $b = b_r' + b_r''$, $b_r' \neq b_r''$, $1 \leqq r \leqq R$, *such that* $2 \cdot 3^{b'} + 1$ *and* $2 \cdot 3^{b''} + 1$ *should both be primes.*

REMARKS. To each solution p of (5) correspond the three solutions $3p^c$, $4p^c$, and $6p^c$ of (1); to each solution p of (5′) correspond the two solutions p^c and $2p^c$ of (1); and to each solution p_1, p_2 of (5″) correspond the two solutions $p_1^{c_1} p_2^{c_2}$ and $2p_1^{c_1} p_2^{c_2}$ of (1). It may be shown that the prime solutions of (5′) must in fact be of the form $p = 1 + 4 \cdot 3^b \pmod{8 \cdot 3^b}$. In case $f = 1$, (1) always has the three solutions $4 \cdot 3^{b+1}$, $7 \cdot 3^b$, and $2 \cdot 7 \cdot 3^b$.

Theorems 2 to 5 and the remark that $1 < n \equiv 1 \pmod 2 \Rightarrow N(n) = 0$ give the exact number of solutions of (1) for $n \not\equiv 0 \pmod 8$. If we use the modulus $M = 48$, we are able to settle the case of the residue classes $0 \not\equiv n \equiv 8 \pmod{16}$; and by using the modulus $M = 96$, also the classes $0 \not\equiv n \equiv 16 \pmod{32}$. In all cases, formulae like (II), or (III) show that the *Conjecture* holds for all residue classes considered. Nevertheless, the attempt to settle the *Conjecture* by an induction from the modulus $M = 2^c \cdot 3$ to the modulus $2M = 2^{c+1} \cdot 3$ fails. We can, therefore, state only

REMARKS 6. *The Conjecture holds, except, possibly, for integers* $n \equiv 0 \pmod{2^c}$, *with* $c \geqq 5$.

This is only slightly stronger than the first statement of the following theorem, essentially due to Donnelly [**2**].

THEOREM A. *The Conjecture holds, except, possibly for integers* $n \equiv 0 \pmod{2^c}$, *with* $c \geqq 4$, *and if* x_0 *is the smallest integer for which* $N(x_0) = 1$, *then* $n\,(=\varphi(x_0)) \equiv 0 \pmod{2^{14}}$.

3. **Sketches of proofs.** Only the proofs of Theorem 1 (with Corollary) and Theorem 2 will be sketched; the other proofs, while more complicated, run along similar lines.

PROOF OF THEOREM 1. Let $x = 2^b f$, f odd, be a solution of (1) with $n = 2^m$. Then, by the multiplicativity of the φ-function, $\varphi(x) = 2^{b-1} \varphi(f) = 2^m$, $\varphi(f) = 2^k$, $k = m - b + 1$. If $p^c | f$, then $p^{c-1} | 2^k$, so that $c = 1$ and f is square-free, $f = p_1 p_2 \dots p_r$, say, $p_i \neq p_j$ if $i \neq j$. Then $\varphi(f) = \prod_{p|f}(p - 1) = 2^k$, so that $p - 1 = 2^e$. As is well known, this is possible only for $e = 2^s$; hence, $p|f \Rightarrow p = 1 + 2^{2^s}$, $\varphi(f) = \prod_{j=1}^r 2^{2^{s_j}} = 2^k$, $k = \sum_{j=1}^r 2^{s_j}$. It follows that a solution of (1) of the form $x = 2^b f$ is possible only if b is such, that $k = m - b + 1$ is admissible, i.e., if k has a diadic representation $k = \sum_{j=1}^r 2^{s_j}$ with all $2^{2^{s_j}} + 1$ primes. To each such b there exists a unique solution $x = 2^b f$, except for $b = 1$, i.e., for $k = m$, when besides $x = 2f$, there is also the added solution $x = f$. This essentially finishes the proof of Theorem 1.

PROOF OF COROLLARY 1. The Corollary follows from the remark that all integers up to $2^5 - 1$ are admissible, while 2^5 is not. For $m \leqq 31$, $N(2^m) = 1 + \sum_{0 \leqq k \leqq m} 1 = m + 2$; in particular, $N(2^{31}) = 33$. For $m = 32$, one has the 32 solutions $x = 2^b f$ with $2 \leqq b \leqq 33$ (but not with $b = 1$; $n = 2^{32}$ still (see [**1**]) seems to be the smallest known integer such that (1) has no odd solution); more generally, for $m > 32$ at least the 32 solutions $x = 2^b f$ with $b = m - k + 1$, $0 \leqq k \leqq 31$, always exist, as claimed.

PROOF OF THEOREM 2. For $n = 2$ the result follows from Theorem 1. Otherwise, $n = \varphi(x) = 2(6k + 1) \equiv 2 \pmod 4$, $k > 0$, so that x is divisible by at most one single odd prime p (otherwise $4|n$). If $x = p^c$ is a solution of (1), also $2p^c$ is one. Finally, if $x = 4y$, $y \neq 1$, then $4|n$, a contradiction. Hence, either $x = 4$ (and this is excluded by $n > 2$), or else $2^e|x \Rightarrow e = 0$, or $e = 1$, i.e., $x = p^c$, or $x = 2p^c$. As seen, each of these two is a solution of (1) if, and only if, the other one is and if $\delta(n)$ is the number of odd solutions $x = p^c$ of (1), then $N(n) = 2\delta(n)$. If $x = p^c$, then $\varphi(x) = p^{c-1}(p - 1) = 2(6k + 1)$. If $p = 3$, then $3^{c-1} = 6k + 1 \equiv 1 \pmod 3$, $c = 1$, $n = 2$, excluded. If $p \equiv 1, 5, \text{ or } 7 \pmod{12}$, then $(p - 1)/2 \equiv 0, 2, \text{ or } 3 \pmod 6$, a contradiction. It follows that $p \equiv -1 \pmod{12}$. Taking congruences modulo 12, $n = \varphi(x) = (p - 1)p^{c-1} \equiv (-2)(-1)^{c-1} \equiv 2(-1)^c \pmod{12}$ and $n \equiv 2 \pmod{12}$ imply that c is even, $c = 2m$ and Theorem 2 is proved. The proofs of the other theorems are similar and will be suppressed.

BIBLIOGRAPHY

1. R. D. Carmichael, *On Euler's ϕ-function*, Bull. Amer. Math. Soc. **13** (1907), 241–243.
2. H. Donnelly, *On a problem concerning Euler's Phi-function* (to appear).

DEPARTMENT OF MATHEMATICS, TEMPLE UNIVERSITY, PHILADELPHIA, PENNSYLVANIA 19122 (Current address after July 1, 1973.)

Current address (until June 30, 1973): Department of Mathematics, The Technion, Haifa, Israel