A RATIO ASSOCIATED WITH $\phi(x) = n$

KENNETH B. STOLARSKY* and STEVEN GREENBAUM
University of Illinois, Urbana, IL 61801

(Submitted March 1984)

1. INTRODUCTION

Let $\phi(x)$ be Euler's totient function. The literature on solving the equation $\phi(x) = n$ (see [1, pp. 221-223], [2-5], [6, pp. 50-55, problems B36-B42], [7-11], [12, pp. 228-256], and the references therein) can be viewed as a collection of open problems. For $n = 2^\alpha$, we essentially have the problem of factoring the Fermat numbers. Another notorious example is Carmichael's conjecture [3, 7] that if a solution exists it is not unique. Some results (e.g., Example 15 of [12, pp. 238-239]) can be established on the basis of Schinzel's Conjecture H [12, p. 128] of which the twin prime conjecture is a very special case. See also [10, 11].

Here we define a new ratio $R(n)$ that is associated with this equation in a very natural way. Our main result, Theorem 3 of §3, is that $R(n)$ can be arbitrarily large. This can be read independently of §2, where the highest power of 2 dividing $R(n)$ is studied.

To define $R(n)$, let L_n be the least common multiple of all solutions of $\phi(x) = n$. Then, let G_n be the greatest common divisor of all numbers $a^n - 1$, where a is in the reduced residue system modulo L_n given by

$$1 \leqslant a \leqslant L_n, \qquad (a, L_n) = 1, \tag{1.1}$$

Since

$$a^n - 1 = a^{\phi(x)} - 1 \equiv 0 \bmod x \tag{1.2}$$

for any solution x, we have

$$a^n - 1 \equiv 0 \bmod L_n. \tag{1.3}$$

Hence, the ratio $R(n)$ defined by

$$R(n) = G_n / L_n \tag{1.4}$$

is an integer. For example, if $n = 2$, then x is 3, 4, or 6, so

$$L_2 = 12,\ G_2 = (1^2 - 1, 5^2 - 1, 7^2 - 1, 11^2 - 1) = 24, \tag{1.5}$$

and hence $R(2) = 2$.

Our L_n, G_n resemble Carmichael's L and M on pp. 221-222 of [1]. In fact, Carmichael very briefly alludes to the ratio M/L on p. 222. However, his table on p. 222 shows that his $M = M_n$ is often astronomical in comparison to our G_n, and that M_n/G_n need not be an integer.

We write $(m)_p$ for the highest power of the prime p in m, and $(m)_{\text{odd}}$ for $m/(m)_2$. Thus, $(m)_2 = 2^e$ is equivalent to $2^e \| m$. Theorem 3 of §3 asserts that,

*This work was partially supported by the National Science Foundation under grant MCS-8031615.

for every prime p and every $M > 0$, there is an $n = n(p, M)$ such that

$(R(n))_p > M$.

2. RESULTS ON PARITY

By means of induction, the binomial theorem, and the identity

$z^2 - 1 = (z - 1)(z + 1)$,

it is easy to prove the following lemma.

Lemma 1: If $\alpha \geqslant 1$ is an integer, then

$$2^{\alpha+2} \| 11^{2^\alpha} - 1, \tag{2.1}$$

$$2^{\alpha+2} \| (8m + 5)^{2^\alpha} - 1, \tag{2.2}$$

and

$$2^{\alpha+2} | (2k + 1)^{2^\alpha} - 1. \tag{2.3}$$

Propositions 1-3 and Theorems 1 and 2 are consequences of this Lemma. We give the details of the proof for Theorem 2 only; the others are similar.

Write Φ for the set of all n such that $\phi(x) = n$ has a solution, and Φ' for the complement of this set.

Proposition 1: If $n \geqslant 2$, then $2 | L_n$. If $n = 2n'$, where $n \in \Phi$ and $n' \in \Phi'$, then $2 \| L_n$.

It is harder to show that infinitely often *every* solution is even; this is proved in [12, p. 238, Example 14].

Proposition 2: If $n \geqslant 2$, then $(R(n))_2 \geqslant 2$.

Proposition 3: If $(n)_2 = 2^\alpha$, then $(R(n))_2 \leqslant 2^{\alpha+1}$.

In the case of $n = 136 = 8 \cdot 17$, for example, the bound of Proposition 3 is exact.

Theorem 1: Let $s \geqslant 1$ be a fixed integer. If $t \geqslant 0$ is minimal, such that

$$n = 2^t(2s + 1) \in \Phi, \tag{2.4}$$

then

$$(R(n))_2 = 2^{t+1}. \tag{2.5}$$

We observe that again $n = 136 = 8 \cdot 17$ illustrates this result, since 17, 34, and 68 all belong to Φ'. Theorem 1 is proved with the aid of Proposition 3 which, in turn, is proved with the assistance of (2.2) of Lemma 1.

Corollary 1: If $s \geqslant 1$ is an integer and $n = 2(2s + 1) \in \Phi$, then $(R(n))_2 = 4$.

Proof: Clearly, $2s + 1 \in \Phi'$.

Corollary 2: Infinitely often $(R(n))_2 = 4$.

Proof: If p is any prime of the form $4s + 3$, then

$$4s + 2 = p - 1 = \phi(p). \tag{2.6}$$

We may vary s so that p runs over the primes of the form

$$p = 2^{t+1}s + 2^t + 1; \tag{2.7}$$

this implies that

$$\phi(p) = 2^t(2s + 1) \in \Phi. \tag{2.8}$$

However, it does *not* follow directly from crude density considerations and the prime number theorem for arithmetic progressions that the $2^h(2s + 1)$ for $1 \leqslant h < t$ will sometimes all lie in Φ'. In fact, Erdös [4] has proved that, for any $M > 0$, the number of elements of Φ not exceeding x is

$$\gg \frac{x}{\log x}(\log \log x)^M. \tag{2.9}$$

Corollary 3: Schinzel's Conjecture H [12, p. 128] implies that, for any fixed $t \geqslant 0$, the equality $(R(n))_2 = 2^{t+1}$ holds infinitely often.

Proof: For $t = 0, 1$, this follows unconditionally from Theorem 2 and Theorem 1, Corollary 2. For $t \geqslant 3$, we first show that there are infinitely many s for which the two polynomials

$$2s + 1, \quad 2^{t+1}s + 2^t + 1 \tag{2.10}$$

are simultaneously prime, whereas the $t - 1$ polynomials

$$2(2s + 1), \quad 2^2(2s + 1), \ \ldots, \ 2^{t-1}(2s + 1) + 1 \tag{2.11}$$

are all composite. In fact, for $(A, B) = 1$ and $A > 0$, the greatest common divisor of the infinite set

$$(2x + 1)[2A(2x + 1) + B], \qquad x = 1, 2, 3, \ldots, \tag{2.12}$$

is unity (a trivial exercise in [12, p. 130]). Hence, "condition S" of Conjecture H is satisfied for the first two polynomials, and the above assertion follows from [10] (use statement C_{13}, p. 1). Now write $p = 2^{t+1}s + 2^t + 1$ so

$$\phi(p) = 2^t(2s + 1) \in \Phi. \tag{2.13}$$

If

$$\phi(x) = 2^h(2s + 1), \qquad 0 \leqslant h < t, \tag{2.14}$$

then x must be divisible by a non-Fermat prime q such that

$$\phi(q) \mid 2^h(2s + 1). \tag{2.15}$$

Hence,

$$q - 1 = 2^g(2s + 1), \qquad 0 \leqslant g \leqslant h, \tag{2.16}$$

a contradiction. Hence, t satisfies the hypothesis of Theorem 1, and the result follows. C. Pomerance's proof does not use H.

Theorem 2: If $\alpha \geqslant 1$ and $n = 2^\alpha$, then $(R(n))_2 = 2$.

Proof: Since $\phi(2^{\alpha+1}) = n$, we have $2^{\alpha+1} \mid L_n$. Since for any odd m,

$$\phi(2^{\alpha+2}m) \geqslant 2^{\alpha+1} > 2^\alpha, \tag{2.17}$$

we have $2^{\alpha+1} \| L_n$.

For any integer s, we have $10 | \phi(11s)$, so $\phi(11s) \neq 2^\alpha$. Hence (since $L_n \geqslant 12$ is true for $n \leqslant 12$, and is obvious for $n > 12$), the number 11 is in the reduced residue system. Thus,

$$G_n | 11^{2^\alpha} - 1 \tag{2.18}$$

and, by (2.1) of Lemma 1,

$$(G_n)_2 \leqslant 2^{\alpha+2}. \tag{2.19}$$

Because every element of the reduced residue system is odd, (2.3) of Lemma 1 yields $2^{\alpha+2} | (G_n)_2$. Hence, $(G_n)_2 = 2^{\alpha+2}$ and the result follows.

Remark: We know of no other cases in which $(R(n))_2 = 2$. For $\ell(\alpha) = [\log_2 \alpha] \leqslant 4$, numerical calculations suggest, for $n = 2^\alpha$, that

$$L_n = 2n \prod_{m=0}^{\ell(\alpha)} F_m \quad \text{and} \quad G_n = 2L_n, \tag{2.20}$$

where F_m is the Fermat number

$$F_m = 2^{2^m} + 1. \tag{2.21}$$

However, this simply reflects the fact that the Fermat numbers F_m are prime for $m \leqslant 4$, and (2.20) must fail for $\ell(\alpha) \geqslant 5$; see [12, pp. 237-238, Example 13]. It is possible that $(R(n))_{\text{odd}} > 1$ for infinitely many $n = 2^\alpha$. C. Pomerance has proved the converse of Theorem 2.

3. ARBITRARILY LARGE $R(n)$

Observe that

$$\phi(x) = 2 \iff x = 3,\ 4,\ \text{or}\ 6, \tag{3.1}$$

and

$$\phi(x) = 44 \iff x = 3 \cdot 23,\ 4 \cdot 23,\ \text{or}\ 6 \cdot 23. \tag{3.2}$$

We say that 23 is a *prime replicator* of 2.

Definition: The prime p is a *prime replicator* of m if all solutions of

$$\phi(x) = m(p - 1) \tag{3.3}$$

are given by $b_1 p, \ldots, b_r p$, where $b_1, \ldots, b_r$ are all solutions of

$$\phi(x) = m. \tag{3.4}$$

Theorem E: Given $m \geqslant 2$, all but $o(x/\log x)$ of the primes are prime replicators of m.

Proof: This is a result of Erdős [5, pp. 15-16]. His proof [5, pp. 15-18] uses Brun's method.

It follows by the prime number theorem for arithmetic progressions that every arithmetic progression containing infinitely many primes has infinitely many prime replicators of m.

Theorem 3: Let q be any prime, and $e \geqslant 1$ an integer. Then, for some n,

$$(R(n))_q \geqslant q^e. \tag{3.5}$$

<u>Proof</u>: Set $m = \phi(q^e)$. Let $b_1, \ldots, b_r$ be all solutions of $\phi(x) = m$. Set

$$B = [b_1, \ldots, b_r] \quad \text{and} \quad q^f = (B)_q. \tag{3.6}$$

Clearly, $f \geqslant e$. By Theorem E, we can choose k so that

$$p = q^f\phi(q^{2f})k + 1 > B \tag{3.7}$$

is a prime replicator of m. Then all solutions to

$$\phi(x) = n = m(p - 1) = q^f\phi(q^{2f})mk \tag{3.8}$$

are $b_1p, \ldots, b_rp$, so

$$L_n = [b_1, \ldots, b_r]p = Bp. \tag{3.9}$$

If a is in the reduced residue system, then

$$a = q^fh + t, \quad 0 \leqslant t < q^f, \quad (t, q) = 1. \tag{3.10}$$

Hence, for $Q = q^{2f}$, we have

$$\begin{aligned} a^n - 1 = (t + q^fh)^n - 1 &= t^n + nt^{n-1}q^fh + \cdots - 1 \\ &\equiv t^n - 1 \bmod Q \equiv s^{\phi(Q)} - 1 \bmod Q, \end{aligned} \tag{3.11}$$

where $(s, Q) = 1$. By Euler's generalization of Fermat's simple theorem, the above is congruent to zero, and hence

$$(G_n/L_n) = (G_n)_q/q^f \geqslant q^{2f}/q^f \geqslant q^e. \tag{3.12}$$

REFERENCES

1. R. D. Carmichael. "Notes on the Simplex Theory of Numbers." *Bull. Amer. Math. Soc. 15* (1909):217-223.
2. R. D. Carmichael. "Note of a New Number Theory Function." *Bull. Amer. Math. Soc. 16* (1910):232-238.
3. R. D. Carmichael. "Note on Euler's ϕ-Function." *Bull. Amer. Math. Soc. 28* (1922):109-110.
4. P. Erdös. "Some Remarks on Euler's Function and Some Related Problems." *Bull. Amer. Math. Soc. 51* (1945):540-544.
5. P. Erdös. "Some Remarks on Euler's ϕ Function." *Acta Arith. 4* (1958):10-19.
6. Richard K. Guy. *Unsolved Problems in Number Theory*. New York: Springer-Verlag, 1980.
7. V. L. Klee, Jr. "On a Conjecture of Carmichael." *Bull. Amer. Math. Soc. 53* (1947):1183-1186.
8. V. L. Klee, Jr. "On the Equation $\phi(x) = 2m$." *American Math. Monthly 53* (1946):327-328.
9. A. Schinzel. "Sur l'equation $\phi(x) = m$." *Elem. Math. 11* (1956):75-78.
10. A. Schinzel. Remarks on the paper "Sur certaines hypothèses concernant les nombres premiers." *Acta Arith. 7* (1961):1-8.
11. A. Schinzel & W. Sierpinski. "Sur certaines hypothèses concernant les nombres premiers." *Acta Arith. 4* (1958):185-208; Corrigendum, *Acta Arith. 5* (1960):259.
12. W. Sierpinski. *Theory of Numbers*. Trans. by A. Hulanicki. Warsaw: Polish Academy of Science, 1964.

◆◇◆◇◆