#A42 INTEGERS 10 (2010), 497-515

ON THE ITERATION OF A FUNCTION RELATED TO EULER'S ϕ-FUNCTION

Joshua Harrington
Department of Mathematics, University of South Carolina, Columbia, SC 29208
jh3293@yahoo.com

Lenny Jones
Department of Mathematics, Shippensburg University, Shippensburg, PA 17257
lkjone@ship.edu

Received: 2/23/09, Revised: 3/29/10, Accepted: 5/12/10, Published: 9/23/10

Abstract

A unit x in a commutative ring R with identity is called *exceptional* if $1-x$ is also a unit in R. For any integer $n \geq 2$, define $\phi_e(n)$ to be the number of exceptional units in the ring of integers modulo n. Following work of Shapiro, Mills, Catlin and Noe on iterations of Euler's ϕ-function, we develop analogous results on iterations of the function ϕ_e, when restricted to a particular subset of the positive integers.

1. Introduction

The classical ϕ-function of Euler is defined for any integer $x \geq 1$ as

$$\phi(x) = \begin{cases} 1 & \text{if } x = 1 \\ \displaystyle\prod_{i=1}^{k} p^{a_i - 1}(p_i - 1) & \text{if } x > 1, \end{cases}$$

where $\prod_{i=1}^{k} p_i^{a_i}$ is the canonical factorization of $x > 1$ into distinct prime powers. It is easy to see that for any integer $x \geq 3$, there exists a positive integer n such that $\phi^n(x) = 2$, where $\phi^n(x)$ denotes the n-th iterate of ϕ. Thus, the set of integers $x \geq 3$ can be partitioned into finite subsets, called *classes*, indexed by positive integers n, where x is a member of class n if $\phi^n(x) = 2$. This observation gives rise to a function C defined on the integers $x \geq 3$ by $C(x) = n$, where the class of x is n. This function can be extended to all positive integers by defining $C(1) = C(2) = 0$. Shapiro [8] proved that for any two positive integers x and y,

$$C(xy) = \begin{cases} C(x) + C(y) & \text{if either } x \text{ or } y \text{ is odd} \\ C(x) + C(y) + 1 & \text{if both } x \text{ and } y \text{ are even,} \end{cases} \tag{1}$$

and he used these formulas to study the structure of the classes. Subsequent papers by Mills [4], Catlin [1] and Noe [6] have further investigated the structure of these classes.

In this article, we conduct similar investigations based on a new arithmetic function ϕ_e, defined below, which is closely related to Euler's ϕ-function.

Definition 1. Let R be a commutative ring with identity. A unit $u \in R$ is called *exceptional* if $1-u$ is also a unit in R. (Note that $1-u$ is a unit if and only if $u-1$ is a unit.)

Exceptional units were first introduced in 1969 by Nagell [5]. Since then, they have been useful in solving Diophantine equations and investigating the structure of certain number fields. Most recently, Houriet [3] has used exceptional units to find 42 new Euclidean number fields in degrees 8, 9, 10, 11 and 12. Here we focus on these units in a finite setting, and we do not attempt to exploit any particular properties of exceptional units, aside from the combinatorial implications as indicated below.

Definition 2. Let $n \geq 2$ be an integer.

1. Let $\phi_e(n)$ denote the number of exceptional units in the ring $\mathbb{Z}_n$.
2. For any integer $k \geq 0$, define the k-th iterate of ϕ_e as
$$\phi_e^k(n) := \underbrace{(\phi_e \circ \phi_e \circ \cdots \circ \phi_e)}_{k}(n),$$
so that $\phi_e^0(n) = n$.

2. Preliminaries

In this section, we prove some basic facts about the function ϕ_e needed in the sequel.

Theorem 3. *Let $x, y \geq 2$ be integers, and suppose that $y = \prod_{i=1}^k p_i^{a_i}$, where the p_i are distinct primes, and $a_i \geq 1$. Then we have the following:*

(i) *If $\gcd(x,y) = 1$, then $\phi_e(xy) = \phi_e(x)\phi_e(y)$.*

(ii) $\phi_e(y) = \prod_{i=1}^k p_i^{a_i-1}(p_i - 2)$.

(iii) *If x is a multiple of y, then $\phi_e(xy) = y\phi_e(x)$.*

Proof. Part (i). follows immediately from the Chinese Remainder Theorem.

For the proof of (ii), first suppose that $y = p^a$, for some prime p and some positive integer a. To count the number of exceptional units in $\mathbb{Z}_{p^a}$, we count the total number of units and subtract the number of units that are not exceptional. We know that the total number of units in $\mathbb{Z}_{p^a}$ is given by

$$\phi(p^a) = p^{a-1}(p-1),$$

where ϕ is Euler's function. Since a unit $u \in \mathbb{Z}_{p^a}$ is not exceptional if and only if $u-1$ is not a unit, which is true if and only if p divides $u-1$, we see that the exact number of non-exceptional units in $\mathbb{Z}_{p^a}$ is the same as the exact number of multiples of p in the set $\{0, 1, 2, \ldots, p^a - 1\}$. There are exactly p^{a-1} multiples of p in this set, namely $\big\{0, p, 2p, \ldots, (p^{a-1}-1)p\big\}$. Thus,

$$\phi_e(p^a) = \phi(p^a) - p^{a-1} = p^{a-1}(p-1) - p^{a-1} = p^{a-1}(p-2).$$

Therefore, (ii) follows from (i).

To prove (iii), since x is a multiple of y, we can write $x = \prod_{i=1}^{k} p_i^{a_i+b_i} \prod_{i=k+1}^{t} p_i^{c_i}$, where the p_i are distinct primes, and $b_i \geq 0$, $c_i \geq 1$ for $1 \leq i \leq k$. Then

$$xy = \prod_{i=1}^{k} p_i^{2a_i+b_i} \prod_{i=k+1}^{t} p_i^{c_i}.$$

Hence, using (i) and applying (ii) to xy, gives

$$\begin{aligned}\phi_e(xy) &= \prod_{i=1}^{k} p_i^{2a_i+b_i-1}(p_i-2) \prod_{i=k+1}^{t} p_i^{c_i-1}(p_i-2)\\ &= \prod_{i=1}^{k} p_i^{a_i} \prod_{i=1}^{k} p_i^{a_i+b_i-1}(p_i-2) \prod_{i=k+1}^{t} p_i^{c_i-1}(p_i-2)\\ &= y\phi_e(x),\end{aligned}$$

and the proof of the theorem is complete. □

Remark 4. Since $1-u$ is a unit if and only if $u-1$ is a unit, we can view the function ϕ_e as counting the number of pairs of consecutive units in $\mathbb{Z}_n$. For any integer $k \geq 3$, this function can be generalized to count the number of $k-$tuples of consecutive units in $\mathbb{Z}_n$ by replacing $p_i - 2$ in Theorem 3, part (ii), with $p_i - k$ for any prime $p_i \geq k$, and zero otherwise. However, we are not concerned with such generalizations in this paper.

The following is immediate from Theorem 3.

Corollary 5.

(i) $\phi_e(x) = 0$ *if* x *is even.*

(ii) *For any odd integer* $x \geq 3$*, there exists an integer* $m \geq 0$ *such that* $\phi_e^m(x) = 3$*.*

Definition 6. We define a function C, called the *class function*, on the odd positive integers $x \geq 3$ by $C(x) = m$, where $\phi_e^m(x) = 3$. For the sake of convenience we also define $\phi_e(1) := 1$ and $C(1) := 0$.

Remark 7. Since we never make use of Shapiro's original class function, we use the same symbol C to denote the class function for iterations of ϕ_e in this paper.

Remark 8. In light of Corollary 5, part (i), the domain of C has been restricted to the odd positive integers in Definition 6.

3. Properties of the Class Function

In this section we develop properties of the class function C for iterations of the function ϕ_e defined in the previous section. In particular, we wish to establish simple formulas that relate $C(xy)$, $C(x)$ and $C(y)$, similar to those found by Shapiro in the case of Euler's ϕ-function. However, to achieve this goal, we must further restrict the domain of C, since more complicated formulas are required to describe the situation for arbitrary odd integers x and y (see Example 45). Thus, we are motivated to make the following definition.

Definition 9. We define the domain D of the class function C to consist precisely of all odd positive integers x, such that none of the integers

$$x, \quad \phi_e(x), \quad \phi_e^2(x), \quad \ldots \quad , \phi_e^m(x)$$

has a prime factor $p \equiv 1 \pmod 3$, where $m = C(x)$. For a given integer $m \geq 0$, we define $\{x \in D | \phi_e^m(x) = 3\}$ to be the *m-th class*, and we say that $x \in D$ is in class m if $\phi_e^m(x) = 3$.

For $m \geq 1$, it is straightforward to check that $C(3^{m+1}) = m$ (see Corollary 15), so that each class is nonempty. And although, for small values of m, it is easy to see that the m-th class is finite, it may not be apparent at first glance that all classes are finite. This fact is established in Theorem 22 where the largest element in each class is determined. Table 1 below gives a list of the first seven classes of the elements of D.

Class	Numbers in the Class
0	1, 3
1	5, 9, 15
2	11, 17, 25, 27, 33, 45, 51, 75
3	29, 47, 53, 55, 81, 85, 87, 99, 125, 135, 141, 153, 159, 165, 225, 255, 375
4	83, 89, 101, 121, 137, 145, 167, 187, 227, 235, 243, 249, 257, 261, 265, 267, 275, 289, 297, 303, 363, 405, 411, 423, 425, 435, 459, 477, 495, 501, 561, 625, 675, 681, 705, 765, 771, 795, 825, 867, 1125, 1275, 1875
5	251, 263, 269, 319, 415, 445, 461, 479, 493, 503, 505, 517, 563, 583, 605, 677, 683, 685, 725, 729, 747, 753, 773, 783, 789, 797, 799, 801, 807, 827, 835, 891, 901, 909, 935, 957, 1089, 1135, 1175, 1215, 1233, 1245, 1269, 1277, 1285, 1305, 1325, 1335, 1375, 1377, 1383, 1431, 1437, 1445, 1479, 1485, 1503, 1509, 1515, 1551, 1683, 1689, 1749, 1815, 1877, 2025, 2031, 2043, 2049, 2055, 2115, 2125, 2175, 2295, 2313, 2319, 2385, 2391, 2397, 2475, 2481, 2505, 2601, 2703, 2805, 3125, 3375, 3405, 3525, 3825, 3831, 3855, 3975, 4125, 4335, 5625, 5631, 6375, 9375
6	809, 841, 911, 913, 979, 1091, 1111, 1217, 1255, 1307, 1315, 1331, 1345, 1363, 1411, 1433, 1439, 1481, 1487, 1507, 1511, 1513, 1537, 1553, 1595, 1717, 1837, 2027, 2057, 2075, 2187, 2209, 2225, 2241, 2259, 2297, 2305, 2329, 2349, 2367, 2393, 2395, 2399, 2403, 2421, 2427, 2465, 2477, 2491, 2497, 2515, 2523, 2525, 2585, 2673, 2727, 2733, 2739, 2809, 2815, 2827, 2839, 2871, 2915, 2937, 3025, 3179, 3267, 3273, 3333, 3385, 3407, 3415, 3425, 3527, 3625, 3645, 3651, 3699, 3735, 3765, 3807, 3833, 3859, 3865, 3915, 3921, 3945, 3985, 3993, 3995, 4005, 4035, 4089, 4127, 4131, 4135, 4149, 4175, 4233, 4293, 4299, 4311, 4317, 4337, 4369, 4437, 4443, 4455, 4461, 4505, 4509, 4521, 4527, 4533, 4539, 4545, 4611, 4653, 4659, 4675, 4785, 4913, 5049, 5067, 5151, 5247, 5445, 5511, 5675, 5875, 6075, 6081, 6093, 6129, 6147, 6165, 6171, 6225, 6345, 6385, 6425, 6525, 6625, 6627, 6675, 6875, 6885, 6891, 6915, 6939, 6957, 6987, 7155, 7173, 7179, 7185, 7191, 7197, 7225, 7395, 7425, 7431, 7443, 7473, 7491, 7515, 7545, 7575, 7755, 7803, 8109, 8415, 8427, 8445, 8481, 8517, 8745, 9075, 9377, 9385, 9537, 10125, 10155, 10215, 10221, 10245, 10275, 10575, 10581, 10625, 10875, 11475, 11493, 11499, 11565, 11577, 11595, 11925, 11955, 11985, 12375, 12381, 12405, 12525, 13005, 13011, 13107, 13515, 14025, 14739, 15625, 16875, 16893, 17025, 17625, 19125, 19155, 19275, 19875, 20625, 21675, 28125, 28131, 28155, 31875, 46875

Table 1: Classes 0 Through 6

Lemma 10, Lemma 11 and Lemma 12 are stated without proof since they are immediate consequences of Theorem 3 and Definition 9.

Lemma 10. *Let $x \in D$ with $x \geq 5$. Then $\phi_e^k(x) \equiv 0 \pmod 3$ for all integers $1 \leq k \leq C(x)$.*

Lemma 11. *If $x, y \in D$, then $xy \in D$.*

Lemma 12. *If $xy \in D$, with $x, y > 1$, then $x \in D$ and $y \in D$.*

Lemma 13. *If $x \in D$ and $x \not\equiv 0 \pmod 3$, then $C(3x) = C(x)$.*

Proof. By Theorem 3, part (i), we have $\phi_e(3x) = \phi_e(3)\phi_e(x) = \phi_e(x)$. Thus, $\phi_e^k(3x) = \phi_e^k(x)$ for all integers $k \leq C(x)$. Let $m = C(x)$. Then $\phi_e^m(3x) = \phi_e^m(x) = 3$, and therefore $C(3x) = m = C(x)$, as desired. □

Lemma 14. *If $x \in D$ and $x \equiv 0 \pmod 3$, then $C(3x) = C(x) + 1$.*

Proof. By Theorem 3, part (iii), we have $\phi_e(3x) = 3\phi_e(x)$. Then, by Lemma 10, it follows that $\phi_e^k(3x) = 3\phi_e^k(x)$ for all integers $k \leq C(x)$. Let $m = C(x)$. Then

$$\phi_e^m(3x) = 3\phi_e^m(x) = 9,$$

and since $\phi_e(9) = 3$, we have that $C(3x) = C(x) + 1$. □

Corollary 15. *For any integer $a \geq 1$, we have $C(3^{a+1}) = C(3^a) + 1 = a$.*

Proof. By Theorem 3, part (ii), we have that $\phi_e(3^{a+1}) = 3^a$. Thus, $C(3^{a+1}) = C(3^a) + 1$. Then $C(3^{a+1}) = a$ follows by induction on a. □

Corollary 16. *Suppose that $x \in D$ and $x \equiv 0 \pmod 3$. Then, for any integer $a \geq 1$, we have $C(3^a x) = C(3^a) + C(x) + 1$.*

Proof. Corollary 15 is the case when $x = 3$. Suppose that $x > 3$. Then, since $\phi_e(x) \equiv 0 \pmod 3$ by Lemma 10, it follows from repeated applications of Theorem 3, part (iii), that $\phi_e^k(3^a x) = 3^a\phi_e^k(x)$ for all integers $1 \leq k \leq C(x)$. Let $m = C(x)$. Then

$$\phi_e^m(3^a x) = 3^a\phi_e^m(x) = 3^{a+1},$$

and from Corollary 15 we have that

$$C(3^a x) = a + C(x) = (a-1) + C(x) + 1 = C(3^a) + C(x) + 1,$$

which completes the proof. □

Corollary 17. *If $x \in D$ and $x \not\equiv 0 \pmod 3$, then $C(3^a x) = C(3^a) + C(x)$, for any integer $a \geq 1$.*

Proof. When $a = 1$, the result is just Lemma 13. So assume that $a \geq 2$. Then, by Theorem 3,

$$\phi_e(3^a x) = \phi_e(3^a)\phi_e(x) = 3^{a-1}\phi_e(x).$$

By Lemma 10 and Corollary 16, we have that

$$C(3^{a-1}\phi_e(x)) = C(3^{a-1}) + C(\phi_e(x)) + 1.$$

Thus,

$$C(3^a x) = C(3^{a-1}\phi_e(x)) + 1 = C(3^{a-1}) + 1 + C(\phi_e(x)) + 1 = C(3^a) + C(x).$$

□

Lemma 18. *If $x \in D$, then $C(5x) = C(5) + C(x)$.*

Proof. First note that $5x \in D$ by Lemma 11. Then, from Theorem 3, it follows that

$$\phi_e(5x) = \begin{cases} 5\phi_e(x) & \text{if } x \equiv 0 \pmod 5 \\ 3\phi_e(x) & \text{if } x \not\equiv 0 \pmod 5. \end{cases}$$

Therefore, for any $1 \leq m \leq C(x)$, we have

$$\phi_e^m(5x) = 5\phi_e^m(x) \quad \text{or} \quad \phi_e^m(5x) = 3\phi_e^m(x).$$

Thus,

$$\phi_e^{C(x)}(5x) = 5\phi_e^{C(x)}(x) = 5 \cdot 3 = 15 \quad \text{or} \quad \phi_e^{C(x)}(5x) = 3\phi_e^{C(x)}(x) = 3 \cdot 3 = 9.$$

Since $\phi_e(15) = 3 = \phi_e(9)$, we conclude that $C(5x) = 1 + C(x) = C(5) + C(x)$, which completes the proof of the lemma. □

Lemma 19. *Let $x, p \in D$ with $p \geq 5$ prime. Then $C(px) = C(p) + C(x)$.*

Proof. The lemma has been established for $p = 5$, so assume the lemma holds for the first $k-1$ primes in D. Let p be the k-th prime in D. Note that $px \in D$ by Lemma 11. Then, from Theorem 3, we have that

$$\phi_e(px) = p\phi_e(x) \quad \text{or} \quad \phi_e(px) = (p-2)\phi_e(x).$$

Suppose first that $\phi_e(px) = (p-2)\phi_e(x)$. Then $p-2 = 3^a \prod q_i^{a_i}$, where each q_i is a prime less than p, and so each p_i is among the first $k-1$ primes contained in D. Therefore, by Theorem 3, Lemma 10, Corollary 16 and our assumption, we have that

$$C\left((p-2)\phi_e(x)\right) = C(p-2) + C(\phi_e(x)) + 1.$$

Thus,

$$C(px) = C\left((p-2)\phi_e(x)\right) + 1 = C(p-2) + 1 + C(\phi_e(x)) + 1 = C(p) + C(x),$$

which completes the proof in this case.

Now suppose that $\phi_e(px) = p\phi_e(x)$. Then

$$\phi_e^2(px) = p\phi_e^2(x) \quad \text{or} \quad \phi_e^2(px) = (p-2)\phi_e^2(x).$$

If $\phi_e^2(px) = (p-2)\phi_e^2(x)$, then the result is established by an argument similar to the previous case. So, suppose that $\phi_e^2(px) = p\phi_e^2(x)$. Continuing the iteration, we see that at each step, the only unresolved case is $\phi_e^m(px) = p\phi_e^m(x)$. Thus $\phi_e^{C(x)}(px) = p\phi_e^{C(x)}(x) = 3p$, and hence

$$C(px) = C(p) + C(x),$$

which completes the proof of the lemma. □

We state now the main result of this section, which follows directly from the previous lemmas and corollaries.

Theorem 20. *Let $x, y \in D$. Then*

$$C(xy) = \begin{cases} C(x) + C(y) & \text{if either } 3 \nmid x \text{ or } 3 \nmid y \\ C(x) + C(y) + 1 & \text{if } 3 \mid x \text{ and } 3 \mid y. \end{cases}$$

Remark 21. The two cases in the formulas (1) found by Shapiro [8] are distinguished by divisibility by 2, and here the two cases are distinguished by divisibility by 3.

4. Bounds for $C(x)$

Theorem 22. *The largest number in class m is $3 \cdot 5^m$. The largest number not divisible by 3 in class m is 5^m.*

Proof. From Table 1, we see that the theorem is true for $m \leq 6$. We assume the theorem is true for all classes $m' < m$, and we proceed by induction.

First, for any prime $p > 3$ in class m we have $C(p-2) = m - 1 < m$, and therefore, by our assumption, $p - 2 \leq 3 \cdot 5^{m-1}$. Then $p \leq 3 \cdot 5^{m-1} + 2 \leq 5^m$.

Next, for any prime $p > 3$, if p^a, with $a > 1$, is in class m, we have that $C(p^a) = aC(p) = m$, and so $C(p) = m/a < m$. Thus, by our assumption, $p \leq 5^{m/a}$ and $p^a \leq 5^m$.

Now, if $x = 3^a \prod_{i=1}^{k} p_i^{a_i} \in D$, with $p_i > 3$, is such that $C(x) = m$, then we know from Theorem 20 that

$$C(x) = \begin{cases} \displaystyle\sum_{i=1}^{k} C(p_i^{a_i}) & \text{if } a = 0 \\ \displaystyle\sum_{i=1}^{k} C(p_i^{a_i}) + a - 1 & \text{if } a \geq 1. \end{cases}$$

Thus, since $p_i^{a_i} \leq 5^{C(p_i^{a_i})}$, or equivalently $C(p_i^{a_i}) \geq \frac{\log(p_i^{a_i})}{\log(5)}$, for each p_i, we get

$$C(x) \geq \begin{cases} \displaystyle\sum_{i=1}^{k} \frac{\log(p_i^{a_i})}{\log(5)} = \frac{\log(x)}{\log(5)} & \text{if } a = 0 \\ \displaystyle\sum_{i=1}^{k} \frac{\log(p_i^{a_i})}{\log(5)} + a - 1 \geq \frac{\log(x/3)}{\log(5)} & \text{if } a \geq 1 \end{cases}$$

Therefore

$$x \leq \begin{cases} 5^{C(x)} & \text{if } x \equiv 1, 2 \pmod 3 \\ 3 \cdot 5^{C(x)} & \text{if } x \equiv 0 \pmod 3 \end{cases}$$

which completes the induction and the proof of the theorem. □

Corollary 23. *The maximum value of x for which $C(x) = m$ is $3 \cdot 5^m$. In other words, $x \leq 3 \cdot 5^{C(x)}$.*

Lemma 24. *The smallest number of class m that is divisible by 3 is 3^{m+1}.*

Proof. From Table 1, we see that the theorem is true for $m \leq 6$. Assume that it is true for all classes $m' < m$. Also, suppose that $s \in D$ with $C(s) = m \geq 7$, where $s = 3^a r$, with $r \not\equiv 0 \pmod 3$.

If $a > 1$, then by Lemma 13, Lemma 14 and Corollary 17, we have

$$m = \begin{cases} C(3r) + 1 & \text{if } a = 2 \\ C(3^{a-1}r) + 1 & \text{if } a > 2. \end{cases}$$

Thus, in any case, $C(3^{a-1}r) = m - 1$. Then $3^{a-1}r \geq 3^m$, by our assumption, and hence $s = 3^a r \geq 3^{m+1}$.

Consider now the case when $a = 1$. We need to show that $s = 3r \geq 3^{m+1}$. Suppose that $3r < 3^{m+1}$. Then $\phi_e(r) < r < 3^m$, and $C(r) = m$ by Lemma 13. But $C(\phi_e(r)) = m - 1$, and since $\phi_e(r) \equiv 0 \pmod 3$, we have by our assumption that $\phi_e(r) \geq 3^m$. From this contradiction it follows that $3r \geq 3^{m+1}$, and the proof is complete. □

Lemma 25. *The smallest number of class m that is not divisible by 3 is greater than 3^m.*

Proof. Let s be the smallest number of class m that is not divisible by 3. By Corollary 17, we have that $C(3s) = C(s)$. Then, by Lemma 24, we have $3s > 3^{m+1}$, so that $s > 3^m$. □

The next corollary is a direct consequence of Lemma 24 and Lemma 25.

Corollary 26. *The smallest number in class m is greater than 3^m. In other words, $x > 3^{C(x)}$.*

Combining Corollary 26 and Corollary 23 gives the following main result of this section.

Theorem 27. *For any $x \in D$, we have that*

$$3^{C(x)} < x \leq 3 \cdot 5^{C(x)}.$$

Or equivalently,

$$\frac{\log(x/3)}{\log 5} \leq C(x) < \frac{\log x}{\log 3}.$$

The following corollary is a direct analog of a result found by Pillai [7] for Euler's totient function. We denote the least integer greater than or equal to x as $\lceil x \rceil$.

Corollary 28. *We have*

$$\lceil \log x / \log 5 \rceil \leq C(x) + 1 \leq \lceil \log x / \log 3 \rceil.$$

5. The Structure of a Class

In this section we analyze the elements of a class more closely to determine the nature of the elements in the class. We first note from the work in Section 4 that the numbers 3^{m+1}, 5^m and $3 \cdot 5^m$ are all contained in class m. As Shapiro [8] did for the classes of the iterates of Euler's ϕ-function, we divide the elements of class $m \geq 3$ here into three sections (I, II, and III) and then analyze the elements in each of these sections. Pictorially, for $m \geq 3$, we have:

$$\text{Class } m\text{:} \qquad 3^m < \underbrace{s, \ldots,}_{\text{I}} \underbrace{3^{m+1}, \ldots, 5^m,}_{\text{II}} \underbrace{\ldots, 3 \cdot 5^m}_{\text{III}}.$$

From the theorems of Section 4, we know that no number in section I is divisible by 3, while all the numbers in section III are divisible by 3. In addition, section II contains both numbers that are divisible by 3 and numbers that are not divisible by 3.

Proposition 29. *For any integer x in section III of its class, we have that $x \equiv 0 \pmod 3$, but $x \not\equiv 0 \pmod{81}$.*

Proof. Let $x = 3^a s$, where $s > 1$, $s \not\equiv 0 \pmod 3$, $a \geq 1$ and $C(x) = m$. Then

$$C(3^a s) = C(3^a) + C(s) = a - 1 + C(s) = m,$$

by Corollary 17. Since $s > 3^{C(s)}$ by Corollary 26, it follows that

$$3^a s > 3^{a+C(s)} = 3^{m+1}. \tag{2}$$

Also, since $s \not\equiv 0 \pmod 3$, we have that s must be in section I or II of its class, and so $s \leq 5^{C(s)}$. Consequently, if $a \geq 4$, we see that

$$3^a s \leq 3^a 5^{C(s)} < 5^{a-1} 5^{C(s)} = 5^{a-1+C(s)} = 5^m. \tag{3}$$

Hence, from (2) and (3), $3^a s$ is in section II of its class if $a \geq 4$, which completes the proof of the proposition. □

The following corollary is immediate from Proposition 29.

Corollary 30. *If $\log x / \log 5 > C(x)$, then $x \equiv 0 \pmod 3$, but $x \not\equiv 0 \pmod{81}$.*

While Proposition 29 provides some information about the numbers in section III, more precise information about section III can be gleaned from an analysis of the numbers that appear in section II.

Proposition 31. *If x is an integer in class $m \geq 2$ such that*

$$5^{m-2} \cdot 17 < x < 5^m, \tag{4}$$

then $x \equiv 0 \pmod 3$.

Proof. Using Table 1, the proposition is easily verified for $m = 2, \ldots, 6$. Proceed by induction and assume the proposition is true for all classes $m' < m$ with $m \geq 7$. Suppose that $x \in D$ with $x \not\equiv 0 \pmod 3$, $C(x) = m$ and that x satisfies (4). If x is prime, then $C(x-2) = m-1$ and $x - 2 \leq 3 \cdot 5^{m-1}$. But

$$x - 2 > 5^{m-2} \cdot 17 - 2 > 3 \cdot 5^{m-1},$$

for $m \geq 5$. Thus, x is not prime. Also, x is not of the form 5^a since $5^{m-1} < 5^{m-2} \cdot 17$. Thus, we can write $x = st$, where $1 < s < 5^{C(s)}$ and $1 < t \leq 5^{C(t)}$. Then, from (4) and Theorem 20, we have

$$5^{C(s)} > s > \frac{5^{C(s)+C(t)-2} \cdot 17}{t} \geq 5^{C(s)-2} \cdot 17. \tag{5}$$

But $C(s) < m$ and $s \not\equiv 0 \pmod 3$, so that (5) contradicts our original assumption, and the theorem is proved. □

Proposition 32. *If x is an integer in class $m \geq 5$ such that*

$$5^{m-5} \cdot 1877 < x < 5^{m-2} \cdot 17,$$

then $x \equiv 0 \pmod 3$.

We omit the proof of Proposition 32 since it is similar to the proof of Proposition 31. The following corollary follows from Theorem 22 and the previous work in this section.

Corollary 33. *The three largest numbers (from smallest to largest) in class $m \geq 5$ that are not divisible by 3 are:*

$$5^{m-5} \cdot 1877, \quad 5^{m-2} \cdot 17 \quad \textit{and} \quad 5^m.$$

We can now give a complete description of the numbers in section III of class $m \geq 5$.

Theorem 34. *The numbers in section III of class $m \geq 5$ are exactly the numbers of the form $3^t s$, where all of the following conditions hold:*

$$\begin{aligned} &1 \leq t \leq 3, \\ &s \not\equiv 0 \pmod 3, \\ &5^m/3^t < s \leq 5^{m-t+1}, \\ &s \in D \textit{ with } C(s) = m - t + 1. \end{aligned} \tag{6}$$

Proof. Suppose first that $x = 3^t s$ satisfies conditions (6). Then $x \in D$ by Lemma 11, and

$$C(x) = C(3^t s) = C(3^t) + C(s) = t - 1 + C(s) = m,$$

by Lemma 17. Since $x = 3^t s > 5^m$, we have that x is in section III.

Conversely, let x be an element in section III of class $m \geq 5$. By Proposition 29, we know that we can write $x = 3^t s$, where $1 \leq t \leq 3$ and $s \not\equiv 0 \pmod 3$. Then, since x is in section III of class m, we know that $x = 3^t s > 5^m$. Thus, $s > 5^m/3^t$. By Lemma 12, $s \in D$, and by Corollary 17, we have

$$m = C(x) = C(3^t) + C(s) = t - 1 + C(s),$$

so that $C(s) = m - t + 1$. Finally, $s \leq 5^{m-t+1}$ by Theorem 22, and the proof is complete. □

Remark 35. The upper bound of 5^{m-t+1} on s in Theorem 34 is somewhat misleading since by Corollary 33, there are exactly two values of s which are greater than $5^{m-t-4} \cdot 1877$ when $m - t + 1 \geq 5$, namely $5^{m-t-1} \cdot 17$ and 5^{m-t+1}.

While the number of elements in section III of the form $3^t s$, with $s \not\equiv 0 \pmod 3$ and $t \in \{1, 2\}$, increases as m increases, it turns out that there is exactly one number of the form $27s$ in section III of class m. More precisely, we have:

Corollary 36. *The number $27 \cdot 5^{m-2}$ is the only number of the form $27s$, where $s \not\equiv 0 \pmod 3$, in section III of class $m \geq 5$.*

Proof. The corollary is easily verified by inspection of Table 1 for classes 5 and 6. Now suppose that $m \geq 7$, and let $x = 27s$ be an element of section III of class m. From Theorem 34, we have that $s \not\equiv 0 \pmod 3$ with $s > 5^m/27$ and $C(s) = m - 2$. Since $5^m/27 > 5^{m-4} \cdot 17$ and $m \geq 7$, it follows from Corollary 33 that there is exactly one value for s satisfying conditions (6), namely $s = 5^{m-2}$. □

6. Primes in D

Proposition 37 and Proposition 38 address the nature of certain primes contained in D. We omit the proof of Proposition 37 since it is similar to the proof of Proposition 38.

Proposition 37. *A prime number $p \in D$, $p \neq 11, 53$ satisfies the inequality $p > 257 \cdot 5^{C(p)-4}$ if and only if $p = 3 \cdot 5^{C(p)-1} + 2$.*

Proposition 38. *A prime number $p \in D$, $p \neq 47, 257$ satisfies the inequalities*

$$257 \cdot 5^{C(p)-4} > p > 5633 \cdot 5^{C(p)-6}$$

if and only if $p = 3 \cdot 17 \cdot 5^{C(p)-3} + 2$.

Proof. If $p = 3 \cdot 17 \cdot 5^{C(p)-3} + 2$ then p clearly satisfies the inequalities. So, suppose that $257 \cdot 5^{C(p)-4} > p > 5633 \cdot 5^{C(p)-6}$. By inspection of Table 1, we see that the theorem holds for the first seven classes, so assume that $C(p) \geq 7$. Since $5633 \cdot 5^{C(p)-6} > 5631 \cdot 5^{C(p)-6} + 2$, it follows that

$$p - 2 > 5631 \cdot 5^{C(p)-6} > 5^5 \cdot 5^{C(p)-6} = 5^{C(p)-1} = 5^{C(p-2)},$$

so that $p-2$ must be in section III of its class. Therefore, $p - 2 = 3^t s$ where t and s satisfy the conditions of Theorem 34 with $C(p) = C(p-2) + 1 = C(s) + t$.

First assume that $p - 2 = 3^3 s$. Then

$$s = \frac{p-2}{27} > \frac{5631 \cdot 5^{C(p)-6}}{27} = \frac{5631 \cdot 5^{C(p)-3}}{27 \cdot 125} > 5^{C(p)-3} = 5^{C(s)}$$

Hence, s is in section III of its class, which is a contradiction since $s \not\equiv 0 \pmod 3$.

Next, assume that $p - 2 = 3^2 s$. Then

$$s = \frac{p-2}{9} > \frac{5631 \cdot 5^{C(p)-6}}{9} = \frac{5631 \cdot 5^{C(p)-2}}{9 \cdot 625} > 5^{C(p)-2} = 5^{C(s)}$$

Again, this puts s in section III of its class, which is impossible.

Finally, assume that $p - 2 = 3s$. Then

$$s = \frac{p-2}{3} > \frac{5631 \cdot 5^{C(p)-6}}{3} = 1877 \cdot 5^{C(p)-6} = 1877 \cdot 5^{C(s)-5}$$

Since $s > 1877 \cdot 5^{C(s)-5}$, Proposition 32 states that $s \geq 5^{C(s)-2} \cdot 17$. If $s > 5^{C(s)-2} \cdot 17$, then $s \geq 5^{C(s)}$ by Proposition 31. But, since $p < 257 \cdot 5^{C(p)-4}$, we have that

$$s = \frac{p-2}{3} < \frac{257 \cdot 5^{C(p)-4} - 2}{3} < \frac{\frac{5^4}{2} \cdot 5^{C(p)-4}}{3} = \frac{5^{C(p)}}{6} = 5^{C(s)} \cdot \frac{5}{6} < 5^{C(s)}.$$

Therefore, $s = 5^{C(s)-2} \cdot 17$, and so $p = 3 \cdot 17 \cdot 5^{C(p)-3} + 2$. □

Proposition 39. *If an integer x is in section I of its class then every divisor of x is in section I of its class.*

Proof. The theorem is obviously true for any x that is prime, so suppose x is composite and write $x = ds$. Since x is in section I of its class, we know that $x \not\equiv 0 \pmod 3$, and we can assume that $3 < d < x$. Thus,

$$3^{C(ds)} < ds < 3^{C(ds)+1} = 3^{C(d)+C(s)+1}.$$

If d is not in section I of its class, then $d > 3^{C(d)+1}$. But then, since $s > 3^{C(s)}$, we have that $ds > 3^{C(d)+C(s)+1}$, which is a contradiction. □

Proposition 40. *Let $p = 3^k m + 2$ be a prime where $k > 0$ and $m \not\equiv 0 \pmod 3$. Then p is in section I of its class if and only if m is in section I of its class.*

Proof. Let $p = 3^k m + 2$ be a prime. Then $C(p) = C(m) + k$. Thus, p is in section I of its class if and only if

$$3^{C(p)} = 3^{C(m)+k} < 3^k m + 2 < 3^{C(m)+k+1} = 3^{C(p)+1}. \tag{7}$$

The inequalities in (7) hold if and only if

$$3^{C(m)} < m < 3^{C(m)+1}, \tag{8}$$

and the inequalities in (8) hold if and only if m is in section I of its class. □

Corollary 41. *Let $p = 3^k m + 2$ be prime with $k > 0$ and $m \not\equiv 0 \pmod 3$. Then p is in section II of its class if and only if m is in section II of its class.*

Proof. The result follows from the negation of Proposition 40 and the fact that all numbers in section III are divisible by 3. □

Theorem 42. *Let $p \in D$ be a prime in section I of its class, and let $q > 3$ be a prime factor of $p - 2$. Then q is in section I of its class.*

Proof. Write $p - 2 = 3^k m$, where $k > 0$ and $m \not\equiv 0 \pmod 3$. By Proposition 40, m is a number in section I of its class. Also, by Proposition 39, we conclude that the prime factors of m are all in section I of their respective classes. □

Class	Prime Factorization of the Smallest Element in the Class
1	5
2	11
3	29
4	83
5	251
6	809
7	2243
8	6563
9	20333
10	59051
11	177209
12	531623
13	1594871
14	4782971
15	14348909
16	6563^2

Table 2: Prime Factorization of the Smallest Element in a Class

7. The Smallest Element of a Class

Shapiro [8] produced a table similar to Table 1 for the classes of the iterations of ϕ. He observed that the smallest element in each of the classes 1 through 8 is prime. Shapiro conjectured that the smallest element in class $m \geq 1$ is always prime. This conjecture was shown to be false by Mills [4], who gave several counterexamples. Recently, Noe [6] has given additional counterexamples. From Table 1, one might be tempted to make a similar conjecture in the situation of this paper. However, we see from Table 2, which gives the prime factorization of the smallest element in each class $1 \leq m \leq 16$, that the smallest element of each class $m \geq 1$ need not be prime. At this time, we have no way of determining which classes have a smallest element which is composite.

The following proposition is an adaptation of a result due to Catlin [1] to the situation here.

Proposition 43. *If x is the smallest element in its class and $x \not\equiv 0 \pmod 3$, then the prime divisors of x are the smallest elements in their respective classes.*

Proof. If x is prime, then the proposition is obvious. So, assume that x is composite, and write $x = ps$, where p is a prime. If there is some number $t < p$ with $C(t) = C(p)$, then, since $x \not\equiv 0 \pmod{3}$, we have by Theorem 20 that

$$C(x) = C(p) + C(s) = C(t) + C(s) = C(ts). \tag{9}$$

Since $ts < ps = x$, (9) contradicts the assumption that x is the smallest element in its class. □

Proposition 44. *If $x = 3^s + 2$ is prime, then x is the smallest element in its class.*

Proof. If $x = 3^s + 2$ is prime, then $C(x) = s$. Since $3^s + 1 \notin D$, and since every element y in class s is such that $y > 3^s$ by Theorem 27, the result follows. □

8. Final Remarks and a Conjecture

To obtain the result in Theorem 20, and all subsequent results contained in this paper, it is necessary to restrict the domain of the class function C. The following example shows that the simple formulas in Theorem 20 for the class of a product xy in terms of the sum of the classes of x and y fail to hold in a more general setting.

Example 45. Let $x = 10391$ and $y = 3463$. Note that y is a prime factor of $x - 2$, and since $y \equiv 1 \pmod{3}$, it follows that neither x nor y is an element of D. It is straightforward to show that $C(xy) = 13$, $C(x) = 10$ and $C(y) = 9$. Thus,

$$C(xy) = C(x) + C(y) - 6,$$

which illustrates that the formulas which appear in Theorem 20 do not hold in this case.

Although it is possible to extend the class function to a slightly larger domain, the formulas analogous to the formulas found in Theorem 20 become more complicated. Further extensions proved unmanageable. In light of Example 45 and additional numerical evidence, we make the following conjecture.

Conjecture 46. *Given any positive integer n, there exist positive integers x and y such that $C(x) + C(y) - C(xy) > n$.*

Based on data generated by computer, the existence of the integers x and y in Conjecture 46 seems to be related to the existence of infinitely many twin primes.

This apparent connection, if true, could render the proof of Conjecture 46 intractable. On the other hand, the truth of Conjecture 46 might conceivably help in establishing the Twin Prime Conjecture. We have examined examples of prime values of x and y satisfying $C(x) + C(y) - C(xy) = n$ where $2 \leq n \leq 7$, and we have observed in these examples that twin primes divide many of the iterations of $\phi_e(x)$ and $\phi_e(y)$. One possible explanation for this phenomenon is simply the formula (Theorem 3 part (ii)) for ϕ_e itself. That is, the presence of factors of the form $p_i - 2$ might account for the abundance of twin primes in the iteration process. This heuristic suggests that there might also be a connection between the generalization of ϕ_e described in Remark 4 and the famous Conjecture B of Hardy and Littlewood [2]:

Conjecture 47. (Hardy and Littlewood)*Let $k \geq 2$ be a fixed even integer. Then there are infinitely many primes p such that $p + k$ is also prime.*

Of course, the above discussion is little more than speculation, and we have not pursued it beyond this point.

Finally, in an attempt to prove Conjecture 46, we searched for primes p such that the sequence of iterations of p is the following:

$$p, \quad \phi_e(p) = 3p_1, \quad \phi_e^2(p) = p_2, \quad \phi_e^3(p) = 3p_3, \quad \ldots \quad , \phi_e^t(p) = p_t,$$

$$\text{and} \quad \phi_e^{t+1}(p) = 3^k,$$

for some positive integer k, and where each p_i is a prime. The existence of such a prime p for arbitrarily large t would then provide a proof of Conjecture 46. Unfortunately, a covering argument shows that such sequences do not exist for $t > 4$.

Acknowledgements The authors thank the anonymous referee for the valuable suggestions.

References

[1] P. A. Catlin, Concerning the iterated ϕ function, *Amer. Math. Monthly*, **77**, (1970), 60–61.

[2] G. H. Hardy and J. E. Littlewood, Some problems of 'Partitio numerorum'; III: On the expression of a number as a sum of primes, *Acta Math.*, **44**, no. 1, (1923), 1–70.

[3] Julien Houriet, Exceptional units and Euclidean number fields, *Arch. Math. (Basel)*, **88**, (2007), 425–433.

[4] W. H. Mills, Iteration of the ϕ function, *Amer. Math. Monthly*, **50**, (1943), 547–549.

[5] Trygve Nagell, Sur un type particulier d'unités algébriques (French), *Ark. Mat.*, **8**, (1969), 163–184.

[6] Tony D. Noe, Primes in classes of the iterated totient function, **11**, Article 08.1.2, (2008).

[7] S. S. Pillai, On a function connected with $\phi(n)$, *Bull A.M.S.*, **35**, (1929), 837–841.

[8] Harold Shapiro, An arithmetic function arising from the ϕ function, *Amer. Math. Monthly*, **50**, (1943), 18–30.