Journal of Integer Sequences, Vol. 11 (2008),
Article 08.1.2

Primes in Classes of the Iterated Totient Function

Tony D. Noe
14025 NW Harvest Lane
Portland, OR 97229
USA
noe@sspectra.com

Abstract

As shown by Shapiro, the iterated totient function separates integers into classes having three sections. After summarizing some previous results about the iterated totient function, we prove five theorems about primes p in a class and the factorization of $p-1$. An application of one theorem is the calculation of the smallest number in classes up to 1000.

1 Introduction

Let $\phi(x)$ denote Euler's totient function. Defining $\phi^0(x) = x$, the iterated totient function is defined recursively for $n > 0$ by $\phi^n(x) = \phi(\phi^{n-1}(x))$. For $x > 1$, $\phi(x) < x$. Hence, for some n we will have $\phi^n(x) = 2$. That x is said to be in class n, and we define the function $C(x) = n$. We define $C(1) = 0$. Table 1, which is sequence A058812 in Sloane [5], shows the numbers in classes 0 to 5. A thorough treatment of the iterated totient function is given by Shapiro [4]. The normal behavior of this function is treated by Erdos et al. [2]. We summarize key results of Shapiro's paper here.

2 Properties of the C function

Shapiro establishes the following properties of the C function:

1. For x or y odd, $C(xy) = C(x) + C(y)$.
2. For x and y both even, $C(xy) = C(x) + C(y) + 1$.

Class	Numbers in this Class
0	1, 2,
1	3, 4, 6,
2	5, 7, 8, 9, 10, 12, 14, 18,
3	11, 13, 15, 16, 19, 20, 21, 22, 24, 26, 27, 28, 30, 36, 38, 42, 54,
4	17, 23, 25, 29, 31, 32, 33, 34, 35, 37, 39, 40, 43, 44, 45, 46, 48, 49, 50, 52, 56, 57, 58, 60, 62, 63, 66, 70, 72, 74, 76, 78, 81, 84, 86, 90, 98, 108, 114, 126, 162,
5	41, 47, 51, 53, 55, 59, 61, 64, 65, 67, 68, 69, 71, 73, 75, 77, 79, 80, 82, 87, 88, 91, 92, 93, 94, 95, 96, 99, 100, 102, 104, 105, 106, 109, 110, 111, 112, 116, 117, 118, 120, 122, 124, 127, 129, 130, 132, 133, 134, 135, 138, 140, 142, 144, 146, 147, 148, 150, 152, 154, 156, 158, 163, 168, 171, 172, 174, 180, 182, 186, 189, 190, 196, 198, 210, 216, 218, 222, 228, 234, 243, 252, 254, 258, 266, 270, 294, 324, 326, 342, 378, 486,

Table 1: Numbers in Classes 0 to 5

3. The largest odd number in class n is 3^n; i.e., for odd x, $x < 3^{C(x)}$.
4. The largest even number in class n is $2 \cdot 3^n$; i.e., for even x, $x < 2 \cdot 3^{C(x)}$.
5. The smallest even number in class n is 2^{n+1}; i.e., for even x, $x \geq 2^{C(x)+1}$.
6. The smallest odd number in class n is greater than 2^n; i.e., for odd x, $x > 2^{C(x)}$.
7. For any integer x, $2^{C(x)} < x \leq 2 \cdot 3^{C(x)}$.

Thus, Shapiro proves that numbers x in class $n > 1$ fall into three sections:

$$2^n < x < 2^{n+1}, \qquad 2^{n+1} \leq x \leq 3^n, \qquad 3^n < x \leq 2 \cdot 3^n.$$

Table 2 shows numbers separated into the three sections. Shapiro establishes the following properties of these classes:

8. Numbers in section I are odd.
9. Numbers in section II are even or odd.
10. Numbers in section III are even.
11. If integer x is in section I, then every divisor of x is in section I of its class.

This last property [4, Theorem 15] is most interesting. For example, it tells us that the factors 5 and 11 of 55 must both be in section I because 55 is in section I. Table 3 shows Section I numbers (sequence A005239); each composite number, shown in bold, has all its factors in section I.

Class	Section I	Section II	Section III
0	1,	2,	
1	3,	4,	6,
2	5, 7,	8, 9,	10, 12, 14, 18,
3	11, 13, 15,	16, 19, 20, 21, 22, 24, 26, 27,	28, 30, 36, 38, 42, 54,
4	17, 23, 25, 29, 31,	32, 33, 34, 35, 37, 39, 40, 43, 44, 45, 46, 48, 49, 50, 52, 56, 57, 58, 60, 62, 63, 66, 70, 72, 74, 76, 78, 81,	84, 86, 90, 98, 108, 114, 126, 162,
5	41, 47, 51, 53, 55, 59, 61,	64, 65, 67, 68, 69, 71, 73, 75, 77, 79, 80, 82, 87, 88, 91, 92, 93, 94, 95, 96, 99, 100, 102, 104, 105, 106, 109, 110, 111, 112, 116, 117, 118, 120, 122, 124, 127, 129, 130, 132, 133, 134, 135, 138, 140, 142, 144, 146, 147, 148, 150, 152, 154, 156, 158, 163, 168, 171, 172, 174, 180, 182, 186, 189, 190, 196, 198, 210, 216, 218, 222, 228, 234, 243,	252, 254, 258, 266, 270, 294, 324, 326, 342, 378, 486,

Table 2: Numbers in Classes 0 to 5 Organized by Section

Class	Numbers in Section I
0	1,
1	3,
2	5, 7,
3	11, 13, **15**,
4	17, 23, **25**, 29, 31,
5	41, 47, **51**, 53, **55**, 59, 61,
6	83, **85**, 89, 97, 101, 103, 107, 113, **115**, **119**, **121**, **123**, **125**,
7	137, 167, 179, **187**, 193, **205**, **221**, 227, 233, **235**, 239, 241, **249**, 251, **253**, **255**,
8	257, **289**, 353, 359, 389, **391**, 401, 409, **411**, **415**, **425**, 443, **445**, 449, **451**, 461, 467, 479,...
9	641, **685**, **697**, 719, 769, **771**, 773, **799**, 809, 821, 823, **835**, 857, **867**, 881, 887, **895**, **901**,...
10	1097, 1283, **1285**, 1361, 1409, **1411**, 1433, 1439, **1445**, **1507**, **1513**, 1543, 1553, 1601,...
11	**2329**, 2657, 2741, 2789, 2819, **2827**, **2839**, 2879, **3043**, 3089, **3151**, **3179**, 3203, **3205**,...
12	**4369**, **4913**, 5441, 5483, **5485**, **5617**, 5639, **5911**, **6001**, 6029, 6053, **6103**, 6173, 6257,...

Table 3: Numbers in Section I of Classes 0 to 12

Shapiro, observing that the smallest number in each of the classes 1 through 8 is prime, conjectured that the smallest number is prime for all classes. However, Mills [3] found counterexamples. Later, Catlin [1, Theorem 1] proved that if the smallest number in a class is odd, then it can be factored into the product of other such numbers. For example, the smallest numbers in classes 11 and 12 factor as $2329 = 17 \cdot 137$ and $4369 = 17 \cdot 257$; note that 17, 137, and 257 are the smallest numbers in classes 4, 7, and 8, respectively.

3 Theorems about primes in classes

Although Shapiro and Catlin give a nice characterization of the composite section I numbers, their papers say little about the prime numbers in sections I and II. We prove five theorems about those primes.

Theorem 1. *Suppose p is an odd prime and $p = 1 + 2^k m$, with $k > 0$ and m odd. Then p is in section I of its class if and only if m is in section I of its class.*

Proof. Observe that for prime p, $\phi(p) = p - 1$, and hence, $C(p - 1) = C(p) - 1$. From Shapiro's properties of the C function, we have $C(p - 1) = k - 1 + C(m)$. Therefore, $C(p) = C(m) + k$. For a prime p in section I, we have the inequality

$$2^{C(p)} < p < 2^{C(p)+1}.$$

Substituting $p = 1 + 2^k m$, we obtain

$$2^{C(m)+k} < 1 + 2^k m < 2^{C(m)+k+1}.$$

Dividing by 2^k produces the inequality

$$2^{C(m)} < m < 2^{C(m)+1},$$

showing that m is a number in section I of its class, which is $C(p) - k$. The proof in the other direction is just as easy. For a number m in section I, we have the inequality

$$2^{C(m)} < m < 2^{C(m)+1}.$$

Multiplying by 2^k produces the inequality

$$2^{C(m)+k} < 2^k m < 2^{C(m)+k+1}.$$

Adding 1 to $2^k m$ does not change the inequality because there is always an odd number between two evens. Hence, we obtain

$$2^{C(m)+k} < 1 + 2^k m < 2^{C(m)+k+1}.$$

But, for integers, this inequality is the same as

$$2^{C(p)} < p < 2^{C(p)+1},$$

which means p is in section I of its class, which is $C(m) + k$. □

Theorem 2. *Suppose p is an odd prime and $p = 1 + 2^k m$, with $k > 0$ and m odd. Then p is in section II of its class if and only if m is in section II of its class.*

Proof. Negating Theorem 1, we have that p is not in Section I if and only if m is not in section I. Because section III consists of only even numbers greater than 2, a prime (and an odd number) not in section I must be in section II. Hence, the theorem follows. □

Theorem 3. *If prime p is in section I of a class, then the factors of $p-1$ are 2 and primes in section I of their class.*

Proof. Factor $p-1$ into the product of an even number and an odd number: $p-1 = 2^k m$, where m is an odd number and $k > 0$. By Theorem 1, m is a number in section I of its class. Using Shapiro's Property 11, we conclude that the prime factors of m are all in section I of their class. Clearly, 2 is also a factor of $p-1$, proving the theorem. □

Theorem 4. *If the smallest number in a class is odd prime p, then the prime factors of $p-1$ are 2 and primes that are the smallest numbers in their class.*

Proof. From properties of the C function, we know that the smallest number in class n is either 2^{n+1} or a number in section I of the class. By assumption, the smallest number is prime. Hence, the prime p must be in section I. By Theorem 1, if p is a prime in section I and $p = 1 + 2^k m$, with $k > 0$ and m odd, then m is a number in section I of its class. Let q be a prime factor of m. Then we can write $m = q\,s$ and

$$p = 1 + 2^k\; q\,s$$

$$C(p) = k + C(q) + C(s).$$

Because m is in section I, by Property 11, q is also. The prime q must be the least number in its class, otherwise if there is a smaller number, p would be smaller (but in the same class), which would contradict the assumption that p is the smallest number in its class. It is obvious that 2 is a prime factor of $p-1$. □

Combining this result with Catlin's theorem, the next theorem gives us a more complete description of the smallest number in a class.

Theorem 5. *Suppose that the smallest number x in a class is odd. If x is composite, then its prime factors are the smallest numbers in their respective classes. If x is prime, then the prime factors of $x-1$ are 2 and primes that are the smallest numbers in their respective classes.*

Proof. The composite case is implied by Catlin's theorem. The prime case is Theorem 4. □

4 A multiplicative function

For more insight into the odd numbers in sections I and II, it is useful to introduce the function

$$D(x) = \frac{x}{2^{C(x)}}$$

for odd integers x. (Here, D could mean "depth"; we want low values of D.) Using Property 1, it is easy to show that D is completely multiplicative; that is, for odd integers x and y,

$$D(xy) = D(x)D(y).$$

Observe that $D(x) < 2$ if and only if x is in section I of its class. If we write a prime number $p = 1 + 2^k m$ with m odd, then it is easy to show that

$$D(p) = 2^{-C(p)} + D(m).$$

Hence, if $D(m)$ is very small, then $D(p)$ will be small. Clearly $D(1) = 1$ is the smallest value of the D function. If $F_5 = 2^{16} + 1 = 65537$ is the largest Fermat prime, then $D(F_5)$ is the second-lowest value of the D function. This value is so low that the first $45426 = \lfloor (\log 2)/(\log D(F_5)) \rfloor$ powers of F_5 are also section I numbers!

5 Computing the least number in a class

Let c_n be the least number in class n. For $n = 1, 2, 3, \ldots, 16$, c_n is

$$3, 5, 11, 17, 41, 83, 137, 257, 641, 1097, 2329, 4369, 10537, 17477, 35209, 65537,$$

which is sequence A007755. When computing c_n, there are two cases to consider: whether c_n is composite or prime. As mentioned above, Catlin proves that when c_n is composite, its factors are among the c_k for $k < n$. For instance,

$$2329 = c_{11} = c_4\ c_7 \quad \text{and} \quad 4369 = c_{12} = c_4\ c_8.$$

When c_n is prime, we know from Theorem 4 that factors of $c_n - 1$ are 2 and prime c_k for $k < n$. For instance,

$$1097 = c_{10} = 1 + 2^3\ c_7 \quad \text{and} \quad 17477 = c_{14} = 1 + 2^2\ c_4\ c_8.$$

For composite c_n, it follows from Property 1 that the sum of the subscripts (with repetition) in the product must be n. For prime c_n, it follows from Property 1 applied to $c_n - 1$ that the sum of the exponent of 2 and subscripts (with repetition) in the product must be n. See Tables 4 and 5 for more examples of these formulas.

Hence, Catlin's theorem and Theorem 4 give us the tools for finding the least number in a class. We start with $c_1 = 3$. If the c_k are known for $k < n$, we can compute c_n using the following procedure: First define the set of possible subscripts

$$K_n = \{k < n : c_k \text{ is prime}\}.$$

Second, define the sets of restricted products of c_k

$$P_r = \left\{ \prod c_{k_i} : k_i \in K_n,\ r = \sum k_i \right\}, \quad r = 1, 2, 3, \ldots, n,$$

that is, all products of prime c_k such that the sum of the subscripts is r. Of course, $P_0 = \{1\}$. Third, define the set

$$Q_n = \bigcup_{k=1}^{n} \left(1 + 2^k P_{n-k}\right).$$

Here, the notation $1 + 2^k P_{n-k}$ means that each element of the set P_{n-k} is multiplied by 2^k and then incremented by 1. Finally, c_n is the smallest of the three quantities: 2^{n+1}, the least number in P_n, and the least prime number in Q_n.

We have used the procedure described above, with some optimizations, to compute c_n for $n \le 1000$. For all these n, we found $c_n < 2^{n+1}$, which supports the conjecture that all c_n are odd. The 280 values of $n \le 1000$ for which c_n is a provable prime are in sequence A136040. Tables 4 and 5 show c_n numerically and symbolically for n up to 100.

We found that the first 22 powers (and only those powers) of Fermat prime F_5 are the least numbers in their class, which extends the result of Mills, who found that the first 15 powers of F_5 are the least numbers in their class. Moreover, as shown in the figure below, it appears that this 22nd power may be an upper bound: we found $D(c_n) < D(F_5^{22}) \approx 1.00034$ for $352 < n \le 1000$. The change at $n = 352$ can be explained by there finally being enough primes p having low $D(p)$ values so that for $n \ge 352$ the set K_n is large enough to ensure that the P_n and Q_n sets have numbers very close to 2^n; that is, very low D values.

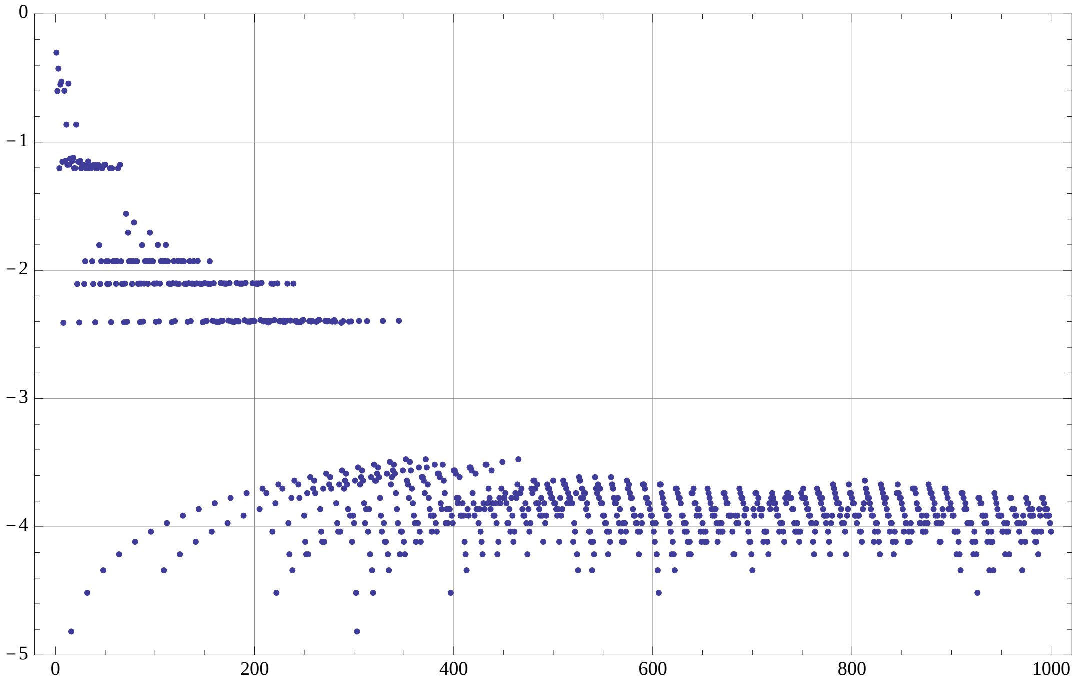

Figure 1: n versus $\log(D(c_n) - 1)$

n	c_n	c_n symbolically
1	3	$1+2$
2	5	$1+2^2$
3	11	$1+2\ c_2$
4	17	$1+2^4$
5	41	$1+2^3\ c_2$
6	83	$1+2\ c_5$
7	137	$1+2^3\ c_4$
8	257	$1+2^8$
9	641	$1+2^7\ c_2$
10	1097	$1+2^3\ c_7$
11	2329	$c_4\ c_7$
12	4369	$c_4\ c_8$
13	10537	$c_5\ c_8$
14	17477	$1+2^2\ c_4\ c_8$
15	35209	$c_7\ c_8$
16	65537	$1+2^{16}$
17	140417	$1+2^7\ c_{10}$
18	281929	$c_8\ c_{10}$
19	557057	$1+2^{15}\ c_4$
20	1114129	$c_4\ c_{16}$
21	2384897	$1+2^{10}\ c_4\ c_7$
22	4227137	$1+2^6\ c_8^2$
23	8978569	$c_7\ c_{16}$
24	16843009	$c_8\ c_{16}$
25	35946497	$1+2^{15}\ c_{10}$
26	71304257	$1+2^6\ c_4\ c_{16}$
27	143163649	$c_8\ c_{19}$
28	286331153	$c_4\ c_8\ c_{16}$
29	541073537	$1+2^7\ c_{22}$
30	1086374209	$c_8\ c_{22}$
31	2281701377	$1+2^{27}\ c_4$
32	4295098369	c_{16}^2
33	9198250129	$c_4\ c_{29}$
34	18325194049	$c_8\ c_{26}$
35	36507844609	$c_{16}\ c_{19}$
36	73016672273	$c_4\ c_{16}^2$
37	139055899009	$c_8\ c_{29}$
38	277033877569	$c_{16}\ c_{22}$
39	586397253889	$c_8\ c_{31}$
40	1103840280833	$c_8\ c_{16}^2$
41	2336533512737	$1+2^5\ c_4\ c_{16}^2$
42	4673067091009	$c_{16}\ c_{26}$
43	9382516064513	$c_8\ c_{16}\ c_{19}$
44	17868687216769	c_{22}^2
45	35460336394369	$c_{16}\ c_{29}$
46	71197706535233	$c_8\ c_{16}\ c_{22}$
47	149535863144449	$c_{16}\ c_{31}$
48	281487861809153	c_{16}^3
49	600470787982337	$1+2^{10}\ c_8\ c_{31}$
50	1200978242389313	$c_8\ c_{16}\ c_{26}$

Table 4: Least Number in Classes 1 to 50

n	c_n	c_n symbolically
51	2278291849363457	$1 + 2^{14}\ c_8\ c_{29}$
52	4538923050090497	$1 + 2^{14}\ c_{16}\ c_{22}$
53	9113306453352833	$c_8\ c_{16}\ c_{29}$
54	18155969234239553	$c_{16}^2\ c_{22}$
55	38280596832649217	$1 + 2^{51}\ c_4$
56	72342380484952321	$c_8\ c_{16}^3$
57	153129396824244769	$c_{16}\ c_{41}$
58	291621356718522497	$1 + 2^7\ c_{51}$
59	583242713437044737	$1 + 2^{22}\ c_8\ c_{29}$
60	1166485424718217217	$1 + 2^{30}\ c_8\ c_{22}$
61	2323964066277761153	$c_{16}^2\ c_{29}$
62	4666084093199565121	$c_8\ c_{16}^2\ c_{22}$
63	9800131862897754113	$c_{16}^2\ c_{31}$
64	18447869999386460161	c_{16}^4
65	39352453561210372097	$1 + 2^{26}\ c_8\ c_{31}$
66	74656206327888494657	$1 + 2^6\ c_8\ c_{52}$
67	148731430780247474177	$1 + 2^{22}\ c_{16}\ c_{29}$
68	297467399933780901889	$c_{16}\ c_{52}$
69	592619738273148829697	$1 + 2^{29}\ c_8\ c_{16}^2$
70	1189887755704357584961	$c_{16}^3\ c_{22}$
71	2426509543591652400137	$1 + 2^3\ c_8^3\ c_{22}^2$
72	4741102589842320261377	$c_8\ c_{16}^4$
73	9630651773242695532609	$c_{22}\ c_{51}$
74	19111988855261800431617	$1 + 2^{21}\ c_8\ c_{16}\ c_{29}$
75	38223977710523600863489	$c_8\ c_{67}$
76	76447955279757801750529	$c_{16}\ c_{60}$
77	152300948808147367100417	$1 + 2^{45}\ c_8^2\ c_{16}$
78	305801153216019899334977	$c_8\ c_{16}^3\ c_{22}$
79	618769376430842916376577	$1 + 2^{12}\ c_8^2\ c_{22}\ c_{29}$
80	1209018056149790439571457	c_{16}^5
81	2446371901576743388450817	$1 + 2^{12}\ c_8\ c_{16}^2\ c_{29}$
82	4892594491879703116251137	$1 + 2^{31}\ c_{51}$
83	9747411779045078715138049	$c_{16}\ c_{67}$
84	19495120989460198967099393	$c_{16}^2\ c_{52}$
85	38838519787207354851852289	$c_{16}\ c_{69}$
86	77981673845596483045589057	$c_{16}^4\ c_{22}$
87	157179431859730823152143377	$1 + 2^4\ c_{16}^2\ c_{22}\ c_{29}$
88	310717640430496142969864449	$c_8\ c_{16}^5$
89	623843871662726366947180577	$1 + 2^5\ c_{16}^2\ c_{52}$
90	1252542413607292614886883329	$c_{16}\ c_{74}$
91	2505084822584743524518887489	$c_{22}\ c_{69}$
92	5010169645169487053324419073	$c_{16}^2\ c_{60}$
93	9981347282039553997660028929	$c_{16}\ c_{77}$
94	20041290178318296142716387649	$c_8\ c_{16}^4\ c_{22}$
95	40394497616832409545668591809	$c_{29}\ c_{66}$
96	79235416345888816038194577409	c_{16}^6
97	160327875017320676305425408289	$c_8\ c_{89}$
98	320645965214320103129750765569	$c_{16}\ c_{82}$
99	638816125763277323754002317313	$c_{16}^2\ c_{67}$
100	1277651744286253059706792919041	$c_{16}^3\ c_{52}$

Table 5: Least Number in Classes 51 to 100

References

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

[2] P. Erdos, A. Granville, C. Pomerance, and C. Spiro, On the normal behavior of the iterates of some arithmetic functions, in: *Analytic Number Theory, Proceedings of a Conference in Honor of P. T. Bateman*, Birkhauser, Boston, 1990, 165-204.

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

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

[5] N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences*, published electronically at www.research.att.com/∼njas/sequences.

2000 *Mathematics Subject Classification*: Primary 11A25.
Keywords: Euler function, iteration, class number.

(Concerned with sequences A005239, A007755, A058811, A058812, A092878, and A136040.)

Received December 14 2007; revised version received January 7 2008. Published in *Journal of Integer Sequences*, January 13 2008.

Return to Journal of Integer Sequences home page.