Smarandache Notions Journal, Vol. 12, No. 1-2-3, Spring 2001, pp. 36-43.

Henry Ibstedt

Abstract: This study originates from questions posed on alternating iterations involving the pseudo-Smarandache function Z(n) and the Euler function $\phi(n)$. An important part of the study is a formal proof of the fact that $Z(n)<n$ for all $n\neq 2^k$ ($k\geq 0$). Interesting questions have been resolved through the surprising involvement of Fermat numbers.

I. The behaviour of the pseudo-Smarandache function

Definition of the Smarandache pseudo function Z(n): Z(n) is the smallest positive integer m such that 1+2+...+m is divisible by n.

Adding up the arithmetical series results in an alternative and more useful formulation: For a given integer n , Z(n) equals the smallest positive integer m such that m(m+1)/2n is an integer. Some properties and values of this function are given in [1], which also contains an effective computer algorithm for calculation of Z(n). The following properties are evident from the definition:

1. $Z(1)=1$
2. $Z(2)=3$
3. For any odd prime p, $Z(p^k)=p^k-1$ for $k\geq 1$
4. For $n=2^k$, $k\geq 1$, $Z(2^k)=2^{k+1}-1$

We note that $Z(n)=n$ for $n=1$ and that $Z(n)>n$ for $n=2^k$ when $k\geq 1$. Are there other values of n for which $Z(n)\geq n$? No, there are none, but to my knowledge no proof has been given. Before presenting the proof it might be useful to see some elementary results and calculations on Z(n). Explicit calculations of $Z(3\cdot 2^k)$ and $Z(5\cdot 2^k)$ have been carried out by Charles Ashbacher [2]. For $k>0$:

$$Z(3\cdot 2^k)=\begin{cases} 2^{k+1}-1 & \text{if } k\equiv 1 \pmod 2 \\ 2^{k+1} & \text{if } k\equiv 0 \pmod 2 \end{cases}$$

$$Z(5\cdot 2^k)=\begin{cases} 2^{k+2} & \text{if } k\equiv 0 \pmod 4 \\ 2^{k+1} & \text{if } k\equiv 1 \pmod 4 \\ 2^{k+2}-1 & \text{if } k\equiv 2 \pmod 4 \\ 2^{k+1}-1 & \text{if } k\equiv 3 \pmod 4 \end{cases}$$

A specific remark is made in each case that $Z(n)<n$.

Before proceeding to the theorem a study of $Z(a\cdot 2^k)$. a odd and $k>0$, we will carry out a specific calculation for $n=7\cdot 2^k$.

We look for the smallest integer m for which $\frac{m(m+1)}{7\cdot 2^{k+1}}$ is integer. We distinguish two cases:

Case 1:	Case 2:
$m=7x$	$m=2^{k+1}y$
$m+1=2^{k+1}y$	$m+1=7x$
Eliminating m results in	
$2^{k+1}y-1=7x$	$2^{k+1}y+1=7x$
$2^{k+1}y\equiv 1 \pmod 7$	$2^{k+1}y\equiv -1 \pmod 7$
Since $2^3\equiv 1$ (mod 3) we have	
If $k\equiv -1$ (mod 3) then	
$y\equiv 1$ (mod 7) ; $m=2^{k+1}-1$	$y\equiv 8$ mod 7); $m=2^{k+1}\cdot 8=2^{k+4}$
If $k\equiv 0$ (mod 3) then	
$2y\equiv 1$ (mod 7), $y=4$; $m=2^{k+1}\cdot 4-1=2^{k+3}-1$	$y\equiv 3$ (mod 7); $m=3\cdot 2^{k+1}$
If $k\equiv 1$ (mod 3) then	
$4y\equiv 1$ (mod 7), $y=2$; $m=2^{k+1}\cdot 2-1=2^{k+2}-1$	$y\equiv 5$ (mod 7); $m=5\cdot 2^{k+1}$

By choosing in each case the smallest m we find:

$$Z(7\cdot 2^k)=\begin{cases} 2^{k+1}-1 & \text{if } k\equiv -1 \pmod 3 \\ 3\cdot 2^{k+1} & \text{if } k\equiv 0 \pmod 3 \\ 2^{k+2}-1 & \text{if } k\equiv 1 \pmod 3 \end{cases}$$

Again we note that $Z(n)<n$.

In a study of alternating iterations [3] it is stated that apart from when $n=2^k$ ($k\geq 0$) $Z(n)$ is <u>at most n</u>. If it ever happened that $Z(n)=n$ for $n>1$ then the iterations of $Z(n)$ would arrive at an invariant, i.e. $Z(\ldots Z(n)\ldots)=n$. This can not happen, therefore it is important to prove the following theorem.

Theorem: $Z(n)<n$ for all $n\neq 2^k$, $k\geq 0$.

Proof: Write n in the form $n=a\cdot 2^k$, where a is odd and $k>0$. Consider the following four cases:

1. $a\cdot 2^{k+1} \mid m$
2. $a\cdot 2^{k+1} \mid (m+1)$
3. $a \mid m$ and $2^{k+1} \mid (m+1)$
4. $2^{k+1} \mid m$ and $a \mid (m+1)$

If a is composite we could list more cases but this is not important as we will achieve our goal by finding m so that $Z(n)\leq m<n$ (where we will have $Z(n)=m$ in case a is prime)

Cases 1 and 2:
Case 1 is excluded in favor of case 2 which would give $m= a\cdot 2^{k+1}-1>n$. We will see that also case 2 be excluded in favor of cases 3 and 4.

Case 3 and 4. In case 3 we write m=ax. We then require $2^{k+1} | (ax+1)$, which means that we are looking for solutions to the congruence

$$ax \equiv -1 \pmod{2^{k+1}} \quad (1)$$

In case 4 we write m+1=ax and require $2^{k+1} | (ax-1)$. This corresponds to the congruence

$$ax \equiv 1 \pmod{2^{k+1}} \quad (2)$$

If $x=x_1$ is a solution to one of the congruencies in the interval $2^k < x < 2^{k+1}$ then $2^{k+1}-x_1$ is a solution to the other congruence which lies in the interval $0 < x < 2^k$. So we have m=ax or m=ax-1 with $0<x<2^k$, i.e. m<n exists so that m(m+1)/2 is divisible by n when a>1 in $n=a\cdot 2^k$. If a is a prime number then we also have Z(n)=m<n. If $a=a_1\cdot a_2$ then Z(n) $\leq$m which is a fortiori less than n..

Let's illustrate the last statement by a numerical example. Take n=70 =5·7·2. An effective algorithm for calculation of Z(n) [1] gives Z(70)=20. Solving our two congruencies results in:

$35x \equiv -1 \pmod 4$ Solution x=1 for which m=35

$35x \equiv 1 \pmod 4$ Solution x=3 for which m=104

From these solutions we chose m=35 which is less than n=70. However, here we arrive at an even smaller solution Z(70)=20 because we do not need to require both a_1 and a_2 to divide one or the other of m and m+1.

II. Iterating the Pseudo-Smarandache Function

The theorem proved in the previous section assures that an iteration of the pseudo-Smarandache function does not result in an invariant, i.e. Z(n)≠n is true for n≠1. On iteration the function will leap to a higher value only when $n=2^k$. It can only go into a loop (or cycle) if after one or more iterations it returns to 2^k. Up to $n=2^{28}$ this does not happen and a statistical view on the results displayed in diagram 1 makes it reasonable to conjecture that it never happens. Each row in diagram 1 corresponds to a sequence of iterations starting on $n=2^k$ finishing on the final value 2. The largest number of iterations required for this was 24 and occurred for $n=2^{14}$ which also had the largest numbers of leaps form 2^j to $2^{j+1}-1$. Leaps are represented by ↑ in the diagram. For $n=2^{11}$ and 2^{12} the iterations are monotonously decreasing.

III. Iterating the Euler ϕ function

The function $\phi(n)$ is defined for n>1 as the number of positive integers less than and prime to n. The analytical expression is given by

$$\phi(n) = n\prod_{p|n}(1-\frac{1}{p})$$

k/j	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2
2																											↑
3																										↑	↑
4																									↑		↑
5																								↑		↑	↑
6																							↑			↑	↑
7																						↑					↑
8																					↑					↑	↑
9																				↑							↑
10																			↑					↑		↑	↑
11																		↑									
12																	↑										
13																↑										↑	↑
14															↑				↑					↑		↑	↑
15														↑													↑
16													↑														↑
17												↑								↑							↑
18											↑																↑
19										↑																↑	↑
20									↑																	↑	↑
21								↑																		↑	↑
22							↑																				↑
23						↑																				↑	↑
24					↑																						↑
25				↑																							↑
26			↑																						↑		↑
27		↑																								↑	↑
28	↑																							↑		↑	↑

Diagram 1.

For n expressed in the form $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_r^{\alpha_r}$ it is often useful to express $\phi(n)$ in the form

$$\phi(n) = p_1^{\alpha_1 - 1}(p_1 - 1) p_2^{\alpha_2 - 1}(p_2 - 1) \cdot \ldots \cdot p_r^{\alpha_r - 1}(p_r - 1)$$

It is obvious from the definition that $\phi(n)<n$ for all $n>1$. Applying the ϕ function to $\phi(n)$ we will have $\phi(\phi(n))< \phi(n)$. After a number of such iterations the end result will of course be 1. It is what this chain of iterations looks like which is interesting and which will be studied here. For convenience we will write $\phi_2(n)$ for $\phi(\phi(n))$. $\phi_k(n)$ stands for the k^{th} iteration. To begin with we will look at the iteration of a few prime powers.

$\phi(2^\alpha)=2^{\alpha-1}$, $\phi_k(2^\alpha)=2^{\alpha-k}$, ... $\phi_\alpha(2^\alpha)=1$.

$\phi(3^\alpha)=3^{\alpha-1}\cdot 2$, $\phi_2(3^\alpha)=3^{\alpha-2}\cdot 2$, ... $\phi_k(3^\alpha)=3^{\alpha-k}\cdot 2$ for $k\leq\alpha$.
In particular $\phi_\alpha(3^\alpha)=2$.

Proceeding in the same way we will write down $\phi_k(p^\alpha)$, $\phi_\alpha(p^\alpha)$ and first first occurrence of an iteration result which consists purely of a power of 2.

$\phi_k(5^\alpha)=5^{\alpha-k}\cdot 2^{k+1},\ k\leq\alpha \qquad \phi_\alpha(5^\alpha)=2^{\alpha+1}$

$\phi_k(7^\alpha)=7^{\alpha-k}\cdot 3\cdot 2^{k},\ k\leq\alpha \qquad \phi_\alpha(7^\alpha)=3\cdot 2^{\alpha}, \qquad \phi_{\alpha+1}(7^\alpha)=2^{\alpha}.$

$\phi_k(11^\alpha)=11^{\alpha-k}\cdot 5\cdot 2^{2k-1},\ k\leq\alpha \qquad \phi_\alpha(11^\alpha)=5\cdot 2^{2\alpha-1} \qquad \phi_{\alpha+1}(11^\alpha)=2^{2\alpha}.$

$\phi_k(13^\alpha)=13^{\alpha-k}\cdot 3\cdot 2^{2k},\ k\leq\alpha \qquad \phi_\alpha(13^\alpha)=3\cdot 2^{2\alpha} \qquad \phi_{\alpha+1}(13^\alpha)=2^{2\alpha}.$

$\phi_k(17^\alpha)=17^{\alpha-k}\cdot 2^{3k+1},\ k\leq\alpha \qquad \phi_\alpha(17^\alpha)=2^{3\alpha+1}.$

$\phi_k(19^\alpha)=19^{\alpha-k}\cdot 3^{k+1}\cdot 2^{k},\ k\leq\alpha \qquad \phi_\alpha(19^\alpha)=3^{\alpha+1}\cdot 2^{\alpha} \qquad \phi_{2\alpha+1}(19^\alpha)=2^{\alpha}.$

$\phi_k(23^\alpha)=23^{\alpha-k}\cdot 11\cdot 5\cdot 2^{3k-4},\ k\leq\alpha \qquad \phi_\alpha(23^\alpha)=11\cdot 5\cdot 2^{3\alpha-4} \qquad \phi_{\alpha+2}(23^\alpha)=2^{3\alpha-1}.$

Table 1. Iteration of p^6. A horizontal line marks where the rest of the iterated values consist of descending powers of 2

#	p=2	p=3	p=5	p=7	p=11	p=13	p=17	p=19	p=23
1	32	486	12500	100842	1610510	4455516	22717712	44569782	141599546
2	16	162	5000	28812	585640	1370928	10690688	14074668	61565020
3	8	54	2000	8232	212960	421824	5030912	4444632	21413920
4	4	18	800	2352	77440	129792	2367488	1403568	7448320
5	2	6	320	672	28160	39936	1114112	443232	2590720
6		2	128	192	10240	12288	524288	139968	901120
7			64	64	4096	4096	262144	46656	327680
8			32	32	2048	2048	131072	15552	131072
9			16	16	1024	1024	65536	5184	65536
10			8	8	512	512	32768	1728	32768
11			4	4	256	256	16384	576	16384
12			2	2	128	128	8192	192	8192
13					64	64	4096	64	4096
14					32	32	2048	32	2048
15					16	16	1024	16	1024
16					8	8	512	8	512
17					4	4	256	4	256
18					2	2	128	2	128
19							64		64
20							32		32
21							16		16
22							8		8
23							4		4
24							2		2

The characteristic tail of descending powers of 2 applies also to the iterations of composite integers and plays an important role in the alternating Z-ϕ iterations which will be subject of the next section.

IV. The alternating iteration of the Euler ϕ function followed by the Smarandache Z function.

Charles Ashbacher [3] found that the alternating iteration $Z(\ldots(\phi(Z(\phi(n)))\ldots)$ ends in 2-cycles of which he found the following four[1]:

2-cycle	First Instance
2 - 3	$3=2^2-1$
8 - 15	$15=2^4-1$
128 - 255	$255=2^8-1$
32768 - 65535	$65535=2^{16}-1$

The following questions were posed:

1) Does the Z-ϕ sequence always reduce to a 2-cycle of the form $2^{2^r-1} \leftrightarrow 2^{2^r}-1$ for $r\geq 1$?

2) Does any additional patterns always appear first for $n=2^{2^r}-1$?

Theorem: The alternating iteration $Z(\ldots(\phi(Z(\phi(n)))\ldots)$ ultimately leads to one of the following five 2-cycles: 2 -3, 8 - 15, 128 - 255, 32768 - 65535, 2147483648 - 4294967295.

Proof:
Since $\phi(n)<n$ for all $n>1$ and $Z(n)<n$ for all $n\neq 2^k$ ($k\geq 0$) any cycle must have a number of the form 2^k at the lower end and $Z(2^k)=2^{k+1}-1$ at the upper end of the cycle. In order to have a 2-cycle we must find a solution to the equation

$$\phi(2^{k+1}-1)=2^k$$

If $2^{k+1}-1$ were a prime $\phi(2^{k+1}-1)$ would be $2^{k+1}-2$ which solves the equation only when $k=1$. A necessary condition is therefore that $2^{k+1}-1$ is composite, $2^{k+1}-1=f_1\cdot f_2\cdot\ldots\cdot f_i\cdot\ldots\cdot f_r$ and that the factors are such that $\phi(f_i)=2^{u_i}$ for $1\leq i\leq r$. But this means that each factor f_i must be a prime number of the form $2^{u_i}+1$. This leads us to consider

$$q(r)=(2-1)(2+1)(2^2+1)(2^4+1)(2^8+1)\ldots(2^{2^{r-1}}+1)$$

or

$$q(r)=(2^{2^r}-1)$$

Numbers of the form $F_r=2^{2^r}+1$ are known as Fermat numbers. The first five of these are prime numbers

$$F_0=3,\ F_1=5,\ F_2=17,\ F_3=257,\ F_4=65537$$

[1] It should be noted that 2, 8, 128 and 32768 can be obtained as iteration results only through iterations of the type $\phi(\ldots(Z(\phi(n)))\ldots)$ whereas the "complete" iterations $Z(\ldots(\phi(Z(\phi(n)))\ldots)$ lead to the invariants 3, 15, 255, 65535. Consequently we note that for example $Z(\phi(8))=7$ not 15, i.e. 8 does not belong to its own cycle.

while F_5=641·6700417 as well as F_6 , F_7 , F_8 , F_9 , F_{10} and F_{11} are all known to be composite.

From this we see that

$$\phi(2^{2^r}-1)=\phi(q(r))=\phi(F_0)\,\phi(F_1)\cdot\ldots\cdot\phi(F_{r-1})=2\cdot 2^2\cdot\ldots\cdot 2^{2^{r-1}}=2^{1+2+2^2+2^3+\ldots+2^{r-1}}=2^{2^r-1} \quad (3)$$

for r=1, 2, 3, 4 5 but breaks down for r=6 (because F_5 is composite) and consequently also for r>6.

Evaluating (3) for r=1,2,3,4,5 gives the complete table of expressions for the five 2-cycles.

Cycle #	2-cycle	Equivalent expression
1	2 ↔ 3	$2 \leftrightarrow 2^2-1$
2	8 ↔ 15	$2^3 \leftrightarrow 2^4-1$
3	128 ↔ 255	$2^7 \leftrightarrow 2^8-1$
4	32768 ↔ 65535	$2^{15} \leftrightarrow 2^{16}-1$
5	2147483648 ↔ 4294967295	$2^{31} \leftrightarrow 2^{32}-1$

The answers to the two questions are implicit in the above theorem.

1) The Z-ϕ sequence always reduces to a 2-cycle of the form $2^{2^r-1} \leftrightarrow 2^{2^r}-1$ for r≥1.

2) Only five patterns exist and they always appear first for $n=2^{2^r}-1$, r=1,2,3,4,5.

A statistical survey of the frequency of the different 2-cycles, displayed in table 2, indicates that the lower cycles are favored when the initiating numbers grow larger. Cycle #4 could have appeared in the third interval but as can be seen it is generally scarcely represented. Prohibitive computer execution times made it impossible to systematically examine an interval were cycle #5 members can be assumed to exist. However, apart from the "founding member" 2147483648 ↔ 4294967295 a few individual members were calculated by solving the equation:

$$Z(\phi(n)=2^{32}-1$$

The result is shown in table 3.

Table 2. The distribution of cycles for a few intervals of length 1000.

Interval	Cycle #1	Cycle #2	Cycle #3	Cycle #4
3 ≤ n ≤ 1002	572	358	70	-
10001 ≤ n ≤ 11000	651	159	190	-
100001 ≤ n ≤ 101000	759	100	141	0
1000001 ≤ n ≤ 1001000	822	75	86	17
10000001 ≤ n ≤ 100001000	831	42	64	63
100000001 ≤ n ≤1000001000	812	52	43	93

Table 3. A few members of the cycle #5 family.

n	$\phi(n)$	$Z(\phi(n))$	$\phi(Z(\phi(n)))$
38655885321	25770196992	4294967295	2147483648
107377459225	85900656640	4294967295	2147483648
966397133025	515403939840	4294967295	2147483648
1241283428641	1168248930304	4294967295	2147483648
11171550857769	7009493581824	4294967295	2147483648
31032085716025	23364978606080	4294967295	2147483648
279288771444225	140189871636480	4294967295	2147483648
283686952174081	282578800082944	4294967295	2147483648
2553182569566729	1695472800497664	4294967295	2147483648
7092173804352025	5651576001658880	4294967295	2147483648
63829564239168225	33909456009953280	4294967295	2147483648
81985529178309409	76861433622560768	4294967295	2147483648
2049638229457735225	1537228672451215360	4294967295	2147483648

References

1. H. Ibstedt, *Surfing on the Ocean of Numbers*, Erhus University Press, 1997.
2. Charles Ashbacher, *Pluckings From the Tree of Smarandache Sequences and Functions*, American Research Press, 1998.
3. Charles Ashbacher, On Iterations That Alternate the Pseudo-Smarandache and Classic Functions of Number Theory, *Smarandache Notions Journal, Vol. 11, No 1-2-3.*

7, Rue du Sergent Blandan
92130 Issy les Moulineaux, France