Scan A6872
A260020
A33631
A33632
A260021

Golomb

Equality among ...

7 pages

add to several

tqk

A6872

apparently unpublished

A260020

A33631

A33632

A260021

Equality Among Number–Theoretic Functions

—Solomon W. Golomb

1 INTRODUCTION

The functions $\phi(n)$ and $\sigma(n)$ of elementary number theory may be defined by $\phi(1) = \sigma(1) = 1$ and for

$$n = \Pi_{i=1}^{\nu(n)} p_i^{a_i}$$

with $n > 1$,

$$\phi(n) = \Pi_{i=1}^{\nu(n)} p_i^{a_i - 1}(p_i - 1)$$

while

$$\sigma(n) = \Pi_{i=1}^{\nu(n)} (p_i^{a_i+1} - 1)/(p_i - 1).$$

We will be interested in values of $n > 1$ for which two (or more) of the following five functions are equal:

n, $\phi(n)$, $\sigma(n)$, $\phi(\sigma(n))$ and $\sigma(\phi(n))$.

(At $n = 1$, each of these has the value "1".)

For all $n > 1$ we know that $\phi(n) < n < \sigma(n)$. Hence also for $n > 1$, $\phi(\sigma(n)) < \sigma(n)$; and for $n > 2$, $\phi(n) < \sigma(\phi(n))$.

The equations of interest are therefore:

1. $\phi(\sigma(n)) = n$
2. $\sigma(\phi(n)) = n$
3. $\phi(n) = \phi(\sigma(n))$
4. $\sigma(n) = \sigma(\phi(n))$
5. $\phi(\sigma(n)) = \sigma(\phi(n))$

all of which have solutions with $n > 1$.

2 The Equations $\phi(\sigma(n)) = n$ and $\sigma(\phi(n)) = n$.

There is a natural one-to-one correspondence between the solutions of $\phi(\sigma(n)) = n$ and those of $\sigma(\phi(n)) = n$, as a consequence of an extremely general theorem:

Theorem 1. Let S and T be any two non–empty sets. Let $f : S \to T$ and $g : T \to S$ be any functions from S into T and from T into S, respectively.

$$\begin{array}{rcl} \text{Let } X & = & \{x \in S \mid g(f(x)) = x\} \\ \text{and let } Y & = & \{y \in T \mid f(g(y)) = y\}. \end{array}$$

(Thus $X \subset S$ and $Y \subset T$.) Then there is a one-to-one onto mapping $h : X \leftrightarrow Y$ given by

$h : X \to Y$ by $h : x \to f(x) = y$,
$h^{-1} : Y \to X$ by $h^{-1} : y \to g(y) = x$.

Proof. Suppose x_0 is a solution of $g(f(x_0)) = x_0$. Then, setting $f(x_0) = y_0$, we have $f(g(y_0)) = f(g(f(x_0))) = f(x_0) = y_0$. That is, whenever x_0 is left fixed by gf, we find that $y_0 = f(x_0)$ is left fixed by fg.

Conversely, suppose y_1 is a solution of $f(g(y_1)) = y_1$. Then, setting $g(y_1) = x_1$, we have $g(f(x_1)) = g(f(g(y_1))) = g(y_1) = x_1$. That is, whenever y_1 is left fixed by fg, then $x_1 = g(y_1)$ is left fixed by gf. ■

Examples:

i) From $\phi(\sigma(1)) = \phi(1) = 1$, we have $\sigma(\phi(1)) = \sigma(1) = 1$.
ii) From $\phi(\sigma(8)) = \phi(15) = 8$, we have $\sigma(\phi(15)) = \sigma(8) = 15$.
iii) From $\phi(\sigma(12)) = \phi(28) = 12$, we have $\sigma(\phi(28)) = \sigma(12) = 28$.

In view of Theorem 1, each of these examples involves a pair of integers a, b, such that $\phi(a) = b, \sigma(b) = a$. This is necessary and sufficient for $\sigma(\phi(a)) = a, \phi(\sigma(b)) = b$.

Theorem 2. Let k be any member of the set $\{1,2,4,8,16,32\}$. Then the pair of integers $a_k = 2^k - 1, b_k = 2^{k-1}$, satisfies the relations $\phi(a_k) = b_k, \sigma(b_k) = a_k$. Hence, for these numbers, $\phi(\sigma(b_k)) = b_k, \sigma(\phi(a_k)) = a_k$.

Proof. For *any* exponent $m, \sigma(2^m) = 2^{m+1} - 1$. Hence, with $b_k = 2^{k-1}$, we have $\sigma(b_k) = 2^k - 1 = a_k$.

With $a_k = 2^k - 1$ where $k \in \{1,2,4,8,16,32\}$, we see that a_k factors into distinct consecutive Fermat primes:

$$
\begin{array}{lllll}
a_1 & = & 2^1 - 1 & = & 1 \text{ (the empty product)} \\
a_2 & = & 2^2 - 1 & = & 3 \qquad = F_1 \\
a_4 & = & 2^4 - 1 & = & 3 \cdot 5 \qquad = F_1 \cdot F_2 \\
a_8 & = & 2^8 - 1 & = & 3 \cdot 5 \cdot 17 \qquad = F_1 \cdot F_2 \cdot F_3 \\
a_{16} & = & 2^{16} - 1 & = & 3 \cdot 5 \cdot 17 \cdot 257 \qquad = F_1 \cdot F_2 \cdot F_3 \cdot F_4 \\
a_{32} & = & 2^{32} - 1 & = & 3 \cdot 5 \cdot 17 \cdot 257 \cdot 65537 \qquad = F_1 \cdot F_2 \cdot F_3 \cdot F_4 \cdot F_5.
\end{array}
$$

Thus we see that $\phi(a_k) = \phi(2^k - 1) = 2^{k-1}$ for these six values of k. ■

Notes.

1. Since $F_6 = 2^{32} + 1 = 641 \cdot 6700417$ is composite, there are no further examples of this type.
2. The example $\phi(28) = 12, \sigma(12) = 28$, mentioned earlier, shows that there are instances of $\phi(a) = b, \sigma(b) = a$, in addition to those given by Theorem 2.

3 The Equations $\phi(n) = \phi(\sigma(n))$ and $\sigma(n) = \sigma(\phi(n))$.

Since $\sigma(n) > n$ for all $n > 1$, it may seem surprising that $\phi(n) = \phi(\sigma(n))$ has many solutions. Specifically, each member of the sequence. A6872
(*) 1,3,15,26,39,45,74,104,111,117,122,146,183,195, ...
is a solution of $\phi(n) = \phi(\sigma(n))$.

Many of the members of this sequence can be obtained from the following theorem.

Theorem 3. Suppose $q > 3$ and $p = 2q - 1$ are both prime. Then $n = 2p, n = 3p, n = 8p, n = 9p$, and $n = 15p$ all satisfy $\phi(n) = \phi(\sigma(n))$.

Proof. If $n = 2p$ then $\phi(n) = p - 1 = 2(q-1)$, while
$\phi(\sigma(n)) = \phi(3 \cdot 2 \cdot q) = 2(q-1)$.

If $n = 3p$ then $\phi(n) = 2(p-1) = 4(q-1)$, while
$\phi(\sigma(n)) = \phi(4 \cdot 2 \cdot q) = 4(q-1)$.

If $n = 8p$ then $\phi(n) = 4(p-1) = 8(q-1)$, while
$\phi(\sigma(n)) = \phi(15 \cdot 2 \cdot q) = 8(q-1)$.

If $n = 9p$ then $\phi(n) = 6(p-1) = 12(q-1)$, while
$\phi(\sigma(n)) = \phi(13 \cdot 2 \cdot q) = 12(q-1)$.

If $n = 15p$ then $\phi(n) = 8(p-1) = 16(q-1)$, while
$\phi(\sigma(n)) = \phi(24 \cdot 2 \cdot q) = 16(q-1)$. ■

Notes.

3. The case $q = 3, p = 2q - 1 = 5$ gives valid examples with $n = 3p$ and $n = 9p$,but fails at $n = 2p$ and at $n = 8p$.

4. The sequence of solutions of $\phi(n) = \phi(\sigma(n))$ listed above, as far as it extends, can be obtained from Theorem 3 and Note 3) above.

A more generalized result than Theorem 3 is the following.

Theorem 4. Let m be any positive integer which satisfies $2\phi(m) = \phi(2\sigma(m))$. (The sequence of values of m with this property begins 2,3,8,9,15,26,39,45,74, ...and coincides with the sequence (*) except where a term in either sequence is a square or twice a square, i.e. except for terms m for which $\sigma(m)$ is *odd*, since otherwise $\phi(m) = \phi(\sigma(m))$ holds if and only if $\phi(2\sigma(m)) = 2\phi(\sigma(m))$.) Let q and $p = 2q - 1$ be odd primes. If $p \nmid m$ and $(q, \sigma(m)) = 1$, then $n = mp$ satisfies $\phi(n) = \phi(\sigma(n))$. A260020

Proof. Suppose $n = mp$ as in the statement above. Since $p \nmid m$, we have $\phi(mp) = \phi(m)\phi(p) = \phi(m) \cdot 2(q-1)$, and $\sigma(mp) = \sigma(m) \cdot 2q$. Since $(q, \sigma(m)) = 1$, we have $\phi(\sigma(mp)) = \phi(2\sigma(m)q) = \phi(2\sigma(m))\phi(q) = 2\phi(m) \cdot (q-1) = \phi(mp)$. ■

All currently known examples of $n > 1$ which satisfy $\phi(n) = \phi(\sigma(n))$ are instances of Theorem 4. It is conceivable that this is in fact the general solution.

The solutions of $\sigma(n) = \sigma(\phi(n))$ seem to be far less numerous than the solutions of $\phi(n) = \phi(\sigma(n))$. In particular, for $n \leq 200$, the only solutions are $n = 1$ and $n = 87$. It is likely that the example $n = 87$ is part of a larger family of solutions.

4 The Equation $\phi(\sigma(n)) = \sigma(\phi(n))$.

Theorem 5. The expression $\sigma(\phi(n)) - \phi(\sigma(n))$ is both positive and negative infinitely often.

"Proof."
1) If there are infinitely many Mersenne primes: suppose $2^k - 1$ is prime, and let $n = 2^{k-1}$. Then $\sigma(\phi(n)) = \sigma(2^{k-2}) = 2^{k-1} - 1$, while $\phi(\sigma(n)) = \phi(2^k - 1) = 2^k - 2 = 2\sigma(\phi(n))$.

2) Suppose p, q, and r are all odd primes, where $p+1 = 2q$ and $p-1 = 12r$. Let $n = p$. Then $\phi(\sigma(n)) = \phi(p+1) = \phi(2q) = q - 1 = \frac{p-1}{2}$, while $\sigma(\phi(n)) = \sigma(p-1) = \sigma(12r) = 28(r+1) = 28(p+11)/12 = \frac{7}{3}(p+11)$. ■

Notes.

5. Statistically, $\sigma(\phi(n)) - \phi(\sigma(n))$ appears to be positive far more often than negative. It would be interesting to determine the asymptotic distribution of the set of n's for which this difference is positive.

6. For $n \leq 200$, the only instances of $\phi(\sigma(n)) = \sigma(\phi(n))$ occur at $n = 1$ and at $n = 9$. Are there other examples?

A6872

√ fq4 Sent email to rshar

Equality Among Number–Theoretic Functions

SECOND UPDATE: December 29, 1992

—*Solomon W. Golomb*

Oscar Moreno has provided computer search data on solutions to the equations **1.** to **5.** as follows.

For equations **1.** $\phi(\sigma(n)) = \mathbf{n}$ and **2.** $\sigma(\phi(n)) = \mathbf{n}$, which have paired solutions by Theorem 1, and the specific solution pairs $n = 2^{k-1}$ for **1.** and $n = 2^k - 1$ for **2.**, for each $k \in \{1, 2, 4, 8, 16, 32\}$, there are the following additional solutions to **1.** with $n \leq 2^{15}$: $n = 12; 240; 720; 6912$. (The corresponding solutions to **2.** are $n = 28; 744; 2418; 20440$.)

The solutions to **4.** $\sigma(\phi(n)) = \sigma(n)$ for $n \leq 20,000$ are: $\{1, 87, 362, 1257, 1798, 5002, 9374.\}$ Each of these values for $n > 1$ is either 2 or 3 times one or two larger primes, but no predictable pattern has yet emerged. A33631

The solutions to **5.** $\phi(\sigma(n)) = \sigma(\phi(n))$ for $n \leq 20,000$ are $\{1, 9, 225, 242, 516, 729, 3872, 13932, 14406, 17672, 18225\}$. We had observed in Theorem 6 that $n = 3^{p-1}$ is a solution whenever $(3^p - 1)/2$ is prime, which accounts for $\{9, 729, 531441, 3^{70}, 3^{102}\}$. The numerical data suggested: A33632

Theorem 7. Whenever $(3^p - 1)/2$ is prime, $n = 25 \cdot 3^{p-1}$ satisfies **5.**
Proof: $\phi(25 \cdot 3^{p-1}) = 40 \cdot 3^{p-2}$ and $\sigma(\phi(25 \cdot 3^{p-1})) = 15(3^p - 3)$.
$\sigma(25 \cdot 3^{p-1}) = 31 \cdot (3^p - 1)/2$ and $\phi(\sigma(25 \cdot 3^{p-1})) = 15(3^p - 3)$. ■

More generally,

Theorem 8. If a satisfies $\sigma(2\phi(a)) = 3\phi(\sigma(a))$ with $(a\phi(a), 3) = 1$, then $n = a \cdot 3^{p-1}$ satisfies **5.** for all p for which $(3^p - 1)/2$ is prime.

Several of the other solutions to **5.** found by Moreno are twice perfect squares: $242 = 2 \cdot 11^2$; $3872 = 2 \cdot 44^2 = 16 \cdot 242$; $17672 = 2 \cdot 94^2$. A relation may also exist between the solutions $516 = 12 \cdot 43$ and $13932 = 18^2 \cdot 43 = 27 \cdot 516$. Finally, $14406 = 6 \cdot 7^4$.

For equation **3.** $\phi(n) = \phi(\sigma(n))$, Moreno found the following solutions $n \leq 6000$ which are *not* given by Theorem 3: $\{3, 15, 45, 175, 357, 585, 608, 646, 962, 1071, 1292, 1443, 1508, 1586, 1664, 1665, 1898, 2275, 2295, 2379, 2745, 2847,$ A260021

$3285, 3848, 4082, 4329, 4514, 4641, 4736, 4845, 5018, 5402\}$. Most, *but not all*, of these are in fact given by Theorem 4. The value $n = 175$ is new, and by Theorem 4 accounts also for $n = 175 \times 13 = 2275$.

In addition to the "multipliers" 2, 3, 8, 9, and 15 of Theorem 3, we get a much longer list from Theorem 4, which also includes 26, 39, 45, 74, 104, 111, 117, 122, 146, 183, 195, etc. Two additions to this list are 175 (any solution of **3.** which is neither a square nor twice a square will be a multiplier); and 128, which *is* twice a square and is seen to satisfy the condition $2\phi(m) = \phi(2\sigma(m))$ of Theorem 4, although it is not itself a solution of **3.** Note that both $128 \cdot 13 = 1664$ and $128 \cdot 37 = 4736$ are entries in Moreno's list.

The multiplier 128 is from the set $\{2, 8, 128, 32768, 2147483648\}$ of multipliers of the form $\phi(a_k)$ where $a_k = 2^k - 1$ with $k \in \{2, 4, 8, 16, 32\}$ as in the proof of Theorem 2. (These numbers all satisfy $2\phi(m) = \phi(2\sigma(m))$ and are therefore multipliers although none of them satisfies **3.** Since each is twice a perfect square, this does not violate Theorem 4.)

Beyond $n = 175$, *new* solutions to **3.** from Moreno's list include only $\{357, 608, 646, 1071, 1292, 1508, 2295, 4641, 4845\}$. The theory of the solutions of **3.** which is emerging consists of *three* sequences: the *terms* of the sequence (i.e. the solutions of **3.**); the *generator* sequence (*including* all $p = 2q - 1$ where p and q are odd primes but containing other numbers as well); and the *multipliers* (i.e. the numbers m with $2\phi(m) = \phi(2\sigma(m))$). The *terms* of the sequence, in general, are the products of *generators* times *multipliers*, subject to compatibility constraints. It is thus clear that 119 is a *generator*, since Moreno's list of *terms* includes $357 = 3 \times 119$, $1071 = 9 \times 119$, and $4641 = 39 \times 119$. (The compatibility requirements for multipliers m of 119 appear to be $(\sigma(m), 3) = 1$ and $(m, 119) = 1$.) Another family is $646 = 2 \times 323$, $1292 = 4 \times 323$, and $4845 = 15 \times 323$. However, a modification of Theorem 4 to describe the multipliers of non-prime generators seems to be needed in this case. The only terms on Moreno's list still "unexplained" are $608 = 2^5 \cdot 19$, $1508 = 2^2 \cdot 13 \cdot 29$, and $2295 = 3^3 \cdot 5 \cdot 17$.