THREE THEOREMS OF SIERPINSKI AND THEIR UNITARY ANALOGUES

V. Sitaramaiah
Department of Mathematics
Pondicherry Engineering College
Pondicherry 605014
India
sitaramaiah@vsnl.net

M.V. Subbarao*
Department of Mathematical Sciences
University of Alberta
Edmonton, Alberta
Canada T6G 2G1
m.v.subbarao@ualberta.ca

May 8, 2003

Abstract

In 1963, Sierpinski proved that (a) $\sigma(n)$ is a power of 2 if and only if n is a product of distinct Mersenne primes (b) $\varphi(n)$ is a power of 2 if and only if n is a product of distinct Fermat primes (c) $\sigma(n)$ is a power of 3 only when $n = 1$ or 2. In this paper we show that similar theorems are valid for their unitary analogues $\sigma^*(n)$ and $\varphi^*(n)$.

1 The Sierpinski Theorems

In 1963, Sierpinski [3] proved the following:

*Supported in part by an NSERC Grant
AMS (1991) Subject Classification: 11A25
Key words and phrases: $\sigma(n), \varphi(n), \sigma^*(n), \varphi^*(n)$, Mersenne and Fermat primes

1.1. Theorem A. *There exist infinitely many integers n such that $\sigma(n)$ is a power of 2 if and only if there exist infinitely many Mersenne primes; $\sigma(n)$ is a power of 2 if and only if n is a product of distinct Mersenne primes.*

1.2. Theorem B. *There exist infinitely many odd numbers n such that $\varphi(n)$ is a power of 2 if and only if there exist infinitely many Fermat primes; $\varphi(n)$ is a power of 2 if and only if n is a product of distinct Fermat primes.*

1.3. Theorem C (Schinzel). *$\sigma(n)$ is equal to a power of 3 only when $n = 1$ or 2.*

Here $\sigma(n)$ denotes the sum of the divisors of n and $\varphi(n)$ is the Euler totient.

One might raise the question: are there similar theorems valid for their unitary analogues $\sigma^*(n)$ and $\varphi^*(n)$? We prove in this paper that there are indeed equally elegant analogues. At the end of the paper, we consider the interesting equation $\varphi^*(\varphi^*(n)) = n - 2$ and show it has an infinity of solutions if and only if there exist infinitely many Fermat primes or infinitely many Mersenne primes.

Here $\sigma^*(n)$ denotes the sum of the unitary divisors of n and $\varphi^*(n)$ is the unitary totient function with the evaluations (see [1]):

$$\sigma^*(n) = \underset{p^a \| n}{\overrightarrow{\quad}} \prod (p^a + 1); \quad \varphi^*(n) = \underset{p^a \| n}{\overrightarrow{\quad}} \prod (p^a - 1).$$

Throughout $p, p_1, \ldots, p_r$ represent primes.

2 The Analogous Theorems

Theorem A*. *$\sigma^*(n)$ equals a power of 2 if and only if n is a product of distinct Mersenne primes.*

Theorem B*. *$\varphi^*(n)$ is a power of 2 if and only if n is a product of distinct Fermat primes, with the exception that if the Fermat prime 3 occurs as a factor, then it may occur to the first or second power.*

Theorem C*. *$\sigma^*(n)$ is a power of 3 only for $n = 1, 2$ and 8.*

We also establish

Theorem D*. *The only solutions of the equation $\varphi^*(\varphi^*(n)) = n - 2$ are given by $n = 9$ or n is a Fermat prime or $n - 1$ is a Mersenne prime.*

Theorem E*. *The only solutions of the equation* $\sigma^*(\sigma^*(n)) = n+2$ *are given by* $n = 8$ *or* n *is a Mersenne prime or* $n+1$ *is a Fermat prime.*

3 Some Lemmas

3.1. Lemma. *Let* $a > 1$ *and odd. If* $2^x \| a^\alpha + 1$, *where* α *is odd, then* $2^x \| a^d + 1$ *for every divisor* d *of* α. *(Here* $2^x \| N$ *means that* $2^x | N$ *and* $2^{x+1} \not| N$).

Proof: We can assume that $\alpha > 1$ and $1 \le d < \alpha$. Let $a^\alpha + 1 = 2^x u$, where $x \ge 1$ and u odd. Since α is odd and $d|\alpha$, $a^d + 1 | a^\alpha + 1$. Hence we can write $a^d + 1 = 2^{x_1} t$, where $x_1 \ge 1$, t odd and $t|u$. Let $r = \alpha/d$ so that $r \ge 3$ and r odd. We have

$$a^\alpha = (a^d)^r = (2^{x_1}t - 1)^r = -1 + \sum_{k=1}^{r} \binom{r}{k} (-r)^{r-k} 2^{x_1 k} t^k$$

so that

$$a^\alpha + 1 = 2^{x_1}\left\{rt + \sum_{k=2}^{r} \binom{r}{k} (-1)^{r-k} 2^{x_1(k-1)} t^k\right\} = 2^{x_1}.$$

m, m odd, since r and t are odd. Hence $x_1 = x$ so that $2^x \| a^d + 1$.

Corollary. *If* a *is odd and* > 1, *then* $a^\alpha + 1 = 2^x$ *implies that* $\alpha = 1$.

Proof: Suppose $\alpha > 1$. If α is odd, by Lemma 3.1, $a + 1 = 2^x$, which is not possible. It α is even, since $y^2 \equiv 1 (\text{mod } 4)$, when y is odd, we have

$$2^x = a^\alpha + 1 = (a^{\alpha/2})^2 + 1 \equiv 2 (\text{mod } 4),$$

which is not possible since $x \ge 2$. Hence $\alpha = 1$.

3.2. Lemma. *If* p *is an odd prime,* α *and* β *are positive integers with* $\beta \ge 2$, *then* $2^\alpha + 1 = p^\beta$, p *prime, if and only if* $p = 3$, $\alpha = 3$ *and* $\beta = 2$.

Proof: Let $\beta \ge 2$ and $2^\alpha + 1 = p^\beta$. Then

$$\begin{aligned} 2^\alpha = p^\beta - 1 &= (p-1)(1 + p + p^2 + \cdots + p^{\beta-1}) \\ &= (p-1)\sigma(p^{\beta-1}), \end{aligned}$$

so that $\sigma(p\beta - 1) = 2^a$ for some positive integer a. By Sierpinski's result (Theorem A above), we get $\beta = 2$, so that $p = 2^a - 1$, a Mersenne prime. Hence $2^\alpha + 1 = p^\beta = p^2 = (2^a - 1)^2 = 2^{2a} - 2^{a+1} + 1$, giving $2^{\alpha-a-1} = 2^{a-1} - 1$. This implies that $a = 2$ and $\alpha = 3$, which yields $p = 3$, thus establishing the lemma.

4 Proofs of the Theorems

Proof of Theorem A*. Say $n = p_1^{a_1} \dots p_r^{a_r}$, so that

$$\sigma^*(n) = (p_1^{a_1} + 1) \dots (p_r^{a_r} + 1).$$

Suppose that $\sigma^*(n) = 2^b$, $b \geq 1$. It follows that p_i is odd and $p_i^{a_i} + 1$ is a power of 2 for each $i = 1, 2, \dots, r$. By Corollary to Lemma 3.1, $a_i = 1$, for $i = 1, 2, \dots, r$. This proves Theorem A*.

Proof of Theorem B*. Let $n = p_1^{a_1} \dots p_r^{a_r}$. Then $\varphi^*(n) = (p_1^{a_1} - 1) \dots (p_r^{a_r} - 1)$ and this is a power of 2 if and only if each factor on the right is a power of 2. This implies that $p_1, \dots, p_r$ are odd. For an odd prime p, suppose that $p^a - 1 = 2^b$, $a \geq 1$, $b \geq 1$, so that $p^a = 2^b + 1$. If $a = 1$, then p is a Fermat prime. If $a > 1$, then by Lemma 3.2 we must have $p = 3$, $a = 2$ and $b = 3$.

Theorem B* now follows.

Proof of Theorem C*. If $n = p_1^{a_1} \dots p_r^{a_r}$ and if $\sigma^*(n) = (p_1^{a_1} + 1) \dots (p_r^{a_r} + 1) = 3^b$, then no p_i is odd. For $p_1 = 2$, Lemma 3.2 shows that the equation $2^{a_1} + 1 = 3^b$ is possible only when $b_1 = 1$, $a_1 = 1$ or $b_1 = 2$, $a_1 = 3$.

This proves Theorem C*.

Proof of Theorem D*. Let $n = 2^\alpha$ be a solution so that $2^\alpha - 2 = \varphi^*(\varphi^*(2^\alpha)) = \varphi^*(2^\alpha - 1)$. Thus $\varphi^*(m) = m - 1$ where $m = 2^\alpha - 1$, so that $m = p^\beta$ for some odd prime p and a positive integer β. Now Corollary to Lemma 3.1 implies that $\beta = 1$ and hence $n - 1$ is a Mersenne prime. We may note that $\varphi^*(m)$ is odd if and only if $m = 2^\alpha$ for some $\alpha \geq 0$. If n is an odd solution, since $\varphi^*(\varphi^*(n))$ must be odd in that case, we must have that $\varphi^*(n) = 2^\alpha$ for some $\alpha \geq 1$. Hence $n - 2 = \varphi^*(\varphi^*(n)) = \varphi^*(2^\alpha) = 2^\alpha - 1$ so that $n = 2^\alpha + 1$. Thus $2^\alpha = \varphi^*(n) = \varphi^*(2^\alpha + 1)$ and hence $2^\alpha + 1 = p^\beta$ for some odd prime p and a positive integer β. If $\beta = 1$, $n = 2^\alpha + 1$ is a Fermat prime. If $\beta \geq 2$, Lemma 3.2 implies that $p = 3$, $\alpha = 3$ and $\beta = 2$, so that $n = 2^\alpha + 1 = 9$. If $n = 2u$ is a solution where $u > 1$ is odd, we obtain $2u - 2 = n - 2 = \varphi^*(\varphi^*(n)) = \varphi^*(\varphi^*(2u)) = \varphi^*(\varphi^*(u)) \leq u - 2$, a contradiction. Let $n = 2^\alpha u$, where $\alpha \geq 2$ and $u > 1$ is odd, be a solution. Let $\varphi^*(n) = 2^a q_1^{\beta_1} \dots q_k^{\beta_k}$, where $a \geq 1$ and $q_1, \ldots, q_k$ are distinct odd primes. From the equation $n-2 = \varphi^*(\varphi^*(n))$, we obtain

$$2(2^{\alpha-1}u - 1) = (2^a - 1)(q^{\beta_1} - 1)\ldots(q_k^{\beta_k} - 1). \tag{1}$$

Since $\alpha \geq 2$, the left hand side of (1) is of the form $2m$ where m is odd. Since 2^k is a factor of the right hand side of (1), it follows that $k = 1$. Denoting q_1 by q and β_1 by β, we have the equations

$$(2^\alpha - 1)\varphi^*(u) = 2^a q^b \tag{2}$$

and

$$(2^a - 1)(q^\beta - 1) = 2^\alpha u - 2. \tag{3}$$

From (2), $2^\alpha - 1 | q^\beta$ so that $2^\alpha - 1 = q^\gamma$ for some $\gamma \geq 1$. Lemma 3.1 implies that $\gamma = 1$, so that $2^\alpha - 1 = q$. Using in (3) and (2), we obtain

$$\begin{aligned}(q+1)u - 2 &= 2^\alpha u - 2 \\ &= (2^a - 1)(q^\beta - 1) \\ &< 2^a q^\beta \\ &= (2^\alpha - 1)\varphi^*(u) \\ &= q\varphi^*(u) \\ &< qu,\end{aligned}$$

a contradiction.

We can similarly prove Theorem E*.

5 Some Remarks

The problem when $\sigma(n)$ or $\varphi(n)$ is a power of a prime is, in general, a difficult one to settle. For example, from a deep result of [2], it follows that $\sigma(p^k)$ is a square only for $k = 4$, $p = 7$ and $k = 5$, $p = 3$. In a later paper we shall examine these and other problems in detail.

The latest available information on the internet shows that there are now thirty-nine known Mersenne primes, the last one being $2^{13466917} - 1$, with 4053946 digits. It was discovered by a young Canadian, aged twenty, by the name of Michael Cameron on November 14, 2001.

As for Fermat primes, only five are known, namely F_0, F_1, F_2, F_3, F_4, where $F_n = 2^{2^n} + 1$.

References

[1] Eckford Cohen, Arithmetic functions associated with the unitary divisors of an integer *Math. Z.* **34** (1960), 66-80.

[2] W. Ljunggren, Noen setringer om ubestmete likninger av formen $(x^n - 1)/(x - 1) = y^q$. *Norsk. Tids* **25** (1943), 17-29, MR39#5463.

[3] W. Sierpinski, Sur les nombres dont la somme de diviseurs est une puissance du nombra 2, *Calcutta Math. Soc. Golden Jubilee Commemoration* **(1758-59)**, Part I, pp. 7-9, Calcutta Math. Soc., Calcutta 1963, MR A30-24 32#5584.