

ON A PROBLEM OF ORE

Ognian Trifonov¹

Department of Mathematics, University of South Carolina, Columbia, SC 29229, USA
trifonov@math.sc.edu

Sharon E. Behum

Johns Hopkins University Applied Physics Laboratory, Laurel, MD 20723, USA
sharon.behum@jhuapl.edu

Received: 12/30/05, Accepted: 5/18/06

Abstract

Let k_α be the least positive integer such that $2^\alpha k_\alpha$ is not a value of Euler's phi-function. In the 1960s P. Bateman and J. Selfridge showed that k_α exists for all positive integers α and computed k_α for $\alpha \leq 2312$. Bateman also formulated a certain conjecture concerning the numbers k_α . We show that Bateman's conjecture does not hold and prove that a modified version of the conjecture holds.

Also, let v_α be the least positive integer such that $2^\alpha v_\alpha$ is not a value of the σ function. We show that $v_\alpha \leq 509203$ for all α , and establish a connection between a certain property of the Mersenne primes and the behavior of the sequence $\{v_\alpha\}$.

1. Introduction

In 1961, Oystein Ore [7] posed the following problem in the American Mathematical Monthly:

“Prove that for each exponent α there is a smallest odd integer k_α such that the equation $\varphi(x) = 2^\alpha k_\alpha$ has no solution. Determine k_2, k_3, k_4 . Try to find bounds for k_α .”

(It is well-known and easy to check that $k_1 = 7$.) Solutions by John Selfridge [9] and Paul Bateman [2] appeared in the journal.

¹supported by NSF DMS Grant #9970455

Definition 1. Let $k \in \mathbb{N}$. Define the Sierpinski exponent, $s(k)$ to be the least positive integer n such that $k \cdot 2^n + 1$ is prime, if such an n exists. If $k \cdot 2^n + 1$ is composite for all $n \in \mathbb{N}$, we define $s(k) = +\infty$ and we call k a *Sierpinski number*.

Bateman’s solution is based on the two lemmas below:

Lemma 1. (Bateman) *Suppose α is a given positive integer. Let l_α be the smallest odd prime number such that $s(l_\alpha) > \alpha$ and $l_\alpha \neq 2^t + 1$ for $t = 1, 2, \dots, \alpha$. Then there is no integer x such that $\varphi(x) = 2^\alpha l_\alpha$. Thus k_α exists and $k_\alpha \leq l_\alpha$.*

By definition, $\{l_\alpha\}$ is a non-decreasing sequence.

Also, in [10] Sierpinski showed that $N = 271129 \cdot 2^n + 1$ is composite for any $n \in \mathbb{N}$. That is, 271129 is a Sierpinski number. Moreover, 271129 is prime number and $271129 \neq 2^k + 1$, so $l_\alpha \leq 271129$ for any $\alpha \in \mathbb{N}$.

Lemma 2. (Bateman) *Suppose α is a given positive integer. Let h_α be the smallest odd positive integer whose Sierpinski exponent is greater than α . Then $k_\alpha \geq h_\alpha$.*

Bateman proves the above lemma by showing

$$s(k_\alpha) > \alpha. \tag{1}$$

Again, the definition of h_α implies that the sequence $\{h_\alpha\}$ is non-decreasing.

In 1962 John Selfridge showed that 78557 is a Sierpinski number. Thus, $h_\alpha \leq 78557$ for all α . Note that 78557 is composite, $78557 = (17)(4621)$.

So, Bateman showed $h_\alpha \leq k_\alpha \leq l_\alpha$ for all α , and by direct computation he obtained $h_1 = k_1 = l_1 = 7$, $h_2 = k_2 = l_2 = 17$, $h_\alpha = k_\alpha = l_\alpha = 19$ for $3 \leq \alpha \leq 5$, and $h_\alpha = k_\alpha = l_\alpha = 31$ for $6 \leq \alpha \leq 7$. Furthermore, Selfridge [9] showed $k_\alpha = 47$ for $8 \leq \alpha \leq 582$, and $k_\alpha = 383$ for $583 \leq \alpha \leq 2312$ and computations show that $h_\alpha = k_\alpha = l_\alpha$ for all $\alpha \leq 2312$.

Bateman wrote [2]: “It is conceivable that $h_\alpha = l_\alpha$ for all values of α but this would be difficult to decide.”

We will show that, $h_\alpha = k_\alpha = l_\alpha$ for all $\alpha \leq 33287$. However, $h_\alpha \neq l_\alpha$ for $33288 \leq \alpha \leq 50010$. Thus, Bateman’s hypothesis does not hold. However, a modified version of the hypothesis holds:

Theorem 1. *For all $\alpha \in \mathbb{N}$, $k_\alpha = l_\alpha$.*

We also consider the version of Ore’s problem where one replaces Euler’s phi-function by σ (the sum of divisors function).

Definition 2. Let $\alpha \in \mathbb{N}$. Define v_α to be smallest positive odd integer such that the equation $\sigma(n) = 2^\alpha v_\alpha$ has no solution, if such an integer exists.

We prove

Lemma 3. *For all $\alpha \in \mathbb{N}$, v_α is well-defined and $v_\alpha \leq 509203$.*

There is a significant difference between the original Ore problem and its modified form. It stems from the fact that the equation $\varphi(m) = 2^n$ has a solution for all $n \in \mathbb{N}$, while this is not the case for the equation $\sigma(m) = 2^n$. It is easy to show (and we do in Section 3) that the equation $\sigma(m) = 2^n$ has a solution if and only if there exist distinct Mersenne primes $p_1 = 2^{q_1} - 1, p_2 = 2^{q_2} - 1, \dots, p_s = 2^{q_s} - 1$ such that $q_1 + q_2 + \dots + q_s = n$.

If the Wagstaff-Pomerance-Lenstra [11] heuristic holds, then there exist infinitely many “sufficiently large” gaps between Mersenne numbers, so that the following hypothesis is true:

Hypothesis 1. *There exist infinitely many positive integers n such that the equation $\sigma(m) = 2^n$ has no solution.*

The validity of Hypothesis 1 determines the behavior of the the sequence $\{v_\alpha\}$.

Definition 2. Let $r \in \mathbb{N}$. We say that r is a *Riesel* number if $r2^n - 1$ is composite for all $n \in \mathbb{N}$.

Theorem 2. *(i) If Hypothesis 1 holds, then there exist infinitely many positive integers α such that $v_\alpha = 1$. (ii) If Hypothesis 1 does not hold, then there exist $n_0 \in \mathbb{N}$ such that $v_\alpha = r$ for all $\alpha \geq n_0$ where r is the smallest prime Riesel number.*

The paper is organized as follows: Section 2 is on Bateman’s conjecture and Section 3 deals with the numbers v_α .

2. Bateman’s Conjecture

Recall that l_α is the smallest odd prime number such that $s(l_\alpha) > \alpha$ and $l_\alpha \neq 2^t + 1$ for $t = 1, 2, \dots, \alpha$. First, we show that the requirement $l_\alpha \neq 2^t + 1$ can be dropped.

Indeed, l_α is prime and if $l_\alpha = 2^t + 1$ then it is a Fermat prime. As noted in Section 1, we know $l_\alpha \leq 271129$ for all α . Thus, if $l_\alpha = 2^t + 1$ then l_α is one of the numbers 3, 5, 17, 257, 65537. Now, the sequence $\{l_\alpha\}$ is non-decreasing and its first six distinct values are 7, 17, 19, 31, 47, 383. Also, $s(65537) = 287$ and $s(47) = 583$, and thus $65537 \notin \{l_\alpha\}$. Since 17 is the smallest prime whose Sierpinski exponent is > 2 , the requirement $17 \neq 2^t + 1$ for $t = 1, 2$ is unnecessary.

So, l_α is the smallest prime whose Sierpinski exponent is $> \alpha$, and h_α is the smallest positive odd integer whose Sierpinski exponent is $> \alpha$.

Next, we list the first ten positive integers k such that $s(k) > 1000$. This list is due to Jaeshke [6], Buell and Young [3], and the project “Seventeen or Bust” [5]. (Note: in the

following tables, each composite is marked with the symbol *.)

k	383	881	* 1643	2897	3061	* 3443	* 3829	* 4847	4861	5297
$s(k)$	6393	1027	1465	9715	33288	3137	1230	3321063	2429	50011

Using the list we get

$$h_\alpha = k_\alpha = l_\alpha = 383 \text{ for } 583 \leq \alpha \leq 6392;$$

$$h_\alpha = k_\alpha = l_\alpha = 2897 \text{ for } 6393 \leq \alpha \leq 9714;$$

$$\text{and } h_\alpha = k_\alpha = l_\alpha = 3061 \text{ for } 9715 \leq \alpha \leq 33287.$$

However, for $33288 \leq \alpha \leq 50010$, $h_\alpha = 4847 = (37)(131)$ but $l_\alpha = 5297$, so $h_\alpha \neq l_\alpha$ in this range. Thus, Bateman’s conjecture does not hold. What is the value of k_α when $33288 \leq \alpha \leq 50010$? Is it 4847 or 5291? We can determine it by using the following lemma.

Lemma 4. *Let $n = d_1d_2$ where d_1 and d_2 are distinct integers greater than 1. If $s(d_1) + s(d_2) \leq \alpha$, then $k_\alpha \neq n$.*

Proof. Let $A = s(d_1)$ and $B = s(d_2)$. Then $p_1 = d_12^A + 1$ and $p_2 = d_22^B + 1$ are distinct primes ($d_1 \neq d_2$), and $\varphi(2^{\alpha-A-B+1}p_1p_2) = 2^\alpha d_1d_2$, completing the proof of the lemma.

Since $s(37) + s(131) < 2000$, $k_\alpha \neq 4847$ for $\alpha > 2000$. We obtain $k_\alpha = l_\alpha = 5297$ for $33288 \leq \alpha \leq 50010$.

Let us determine the next few values of k_α and l_α . We use the list of the first five positive integers k such that $s(k) > 50011$ (again from [12], [3], and [5]).

k	* 4847	* 5359	7013	8423	10223
$s(k)$	3321063	5054502	126113	55157	$> 8 \times 10^6$

Recall that $s(k_\alpha) > \alpha$. Since $5359 = (23)(233)$, using Lemma 4 we get $k_\alpha = l_\alpha = 7013$ for $50011 \leq \alpha \leq 126112$. Next, 10223 is prime, so $k_\alpha = l_\alpha = 10223$ for $126113 \leq \alpha \leq s(10223) - 1$, and $s(10223) > 8 \times 10^6$. So, we have shown $k_\alpha = l_\alpha$ for all $\alpha \leq s(10223)$. To finish the proof of Theorem 1 we need to show $k_\alpha = l_\alpha$ for all α such that $8 \times 10^6 < \alpha \leq s(10223)$.

If k_α is prime for some α , the simplified definition of l_α implies $l_\alpha = k_\alpha$. Next, we show that k_α is prime for all $\alpha > 8 \times 10^6$. Say that k_α is composite for some $\alpha > 8 \times 10^6$. First, consider the case in which k_α has at least three prime divisors. In this case $k_\alpha = p_1p_2l$, with $p_1 \leq p_2 \leq l$. If $p_2 \geq 5$, set $d_1 = p_2$, $d_2 = p_1l$; otherwise set $d_1 = p_1p_2 = 9$ and $d_2 = l$. So, k_α can be represented as $k_\alpha = d_1d_2$ with $5 \leq d_1 < d_2 < 271129/5 < 78557$. Taking into account Lemma 4 we get that $s(d_1) + s(d_2) > 8 \times 10^6$. Thus, either $s(d_1) > 4 \times 10^6$, or $s(d_2) > 4 \times 10^6$.

In the quest to prove that 78557 is the smallest Sierpinski number, bounds for the Sierpinski exponents of all but 8 odd integers less than 78557 have been found. It is known [5]

that the only odd integers < 78557 , which could have a Sierpinski exponent $> 4 \times 10^6$, are in the set $\mathcal{A} = \{5359, 10223, 19249, 21181, 22699, 24737, 27653, 28433, 33661, 55459, 67607\}$.

Let us deal with the multiples of 5359 that do not exceed 271129. These are $5359 \cdot (2j-1)$, $j = 1, \dots, 25$. Well, $5359 = (23)(233)$, so $5359 \cdot (2j-1) = (233) \cdot (23 \cdot (2j-1))$. Now, $233 < 5359$ and $23 \cdot (2j-1) < 5359$, so Lemma 4 implies that k_α is never a multiple of 5359. We deal similarly with the multiples of $21181 = (59)(359)$, $24737 = (29)(853)$, $33661 = (41)(821)$, and $55459 = (31)(1789)$. Next we deal with the odd, composite multiples of the members of the set $\mathcal{B} = \{10223, 19249, 22699, 27653, 28433, 67607\}$ that do not exceed 271129 (all numbers in \mathcal{B} are prime). There are 32 such multiples. The Sierpinski exponents of all but two of these multiples do not exceed 20. The two exceptions are $235129 = (10223)(23)$ and $249689 = (22699)(11)$. But $s(235129) = 26$ and $s(249689) = 25$.

Thus, k_α always has at most two prime divisors.

Now, consider the case when $k_\alpha = p_1 p_2$ where p_1 and p_2 are primes. If $5 \leq p_1 < p_2$ the above argument still holds (set $d_1 = p_1$ and $d_2 = p_2$). The argument also holds if $p_1 = 3$ and $p_2 < 78557$. Thus, either $p_1 = 3$ and $p_2 \in [78557, 90373]$, or $p_1 = p_2$.

First, let $k_\alpha = 3p$ with p a prime in $[78559, 90373]$. Direct computation shows that for all but two of the primes in the above range either $s(p) \leq 30$ or $s(3p) \leq 30$. The two exceptions are 82891 and 88951. However $s(3 \cdot 82891) = 40$ and $s(3 \cdot 88951) = 80$.

The final opportunity for k_α being composite is $k_\alpha = p^2$ with p prime. Since $k_\alpha \leq 271129$, $p \leq 509$. Direct computation shows that for all but six primes in the above range $s(p^2) < 200$. The six exceptions are 61, 83, 149, 379, 433, 509. However $s(61^2) = 444$, $s(83^2) = 326$, $s(149^2) = 396$, $s(379^2) = 1212$, $s(433^2) = 466$, and $s(509^2) = 384$.

We have exhausted all possibilities for k_α being composite and have completed the proof of Theorem 1.

There are still many open problems on inverting the Euler function. We refer the interested reader to the exciting paper [4] on this subject which appeared recently.

3. The Numbers v_α

First we state a well-known lemma and provide a short proof.

Lemma 5. Suppose $\sigma(p^a) = 2^t$ for some prime p and some positive integers a, t . Then $a = 1$ and p is a Mersenne prime.

Proof. Clearly p must be an odd prime, so a is odd, say $a = 2k - 1$, $k \in \mathbb{N}$. Then we have $\sigma(p^a) = \frac{p^k - 1}{p - 1} (p^k + 1) = 2^t$. Since $\gcd(p^k - 1, p^k + 1) = 2$ and $\frac{p^k - 1}{p - 1} \neq 2$, we get $\frac{p^k - 1}{p - 1} = 1$

and $k = 1$.

Lemma 5 implies the following corollary which we mentioned in the introduction:

Corollary 1. Let $t \in \mathbb{N}$. The equation $\sigma(n) = 2^t$ has a solution if and only if there exist distinct Mersenne primes $p_1 = 2^{q_1} - 1, p_2 = 2^{q_2} - 1, \dots, p_s = 2^{q_s} - 1$ such that $q_1 + q_2 + \dots + q_s = t$.

Recall that r is a Riesel number if $r \cdot 2^n - 1$ is composite for all $n \in \mathbb{N}$. In 1956 H. Riesel [8] showed that 509203 is a Riesel number.

Next, we prove the following lemma:

Lemma 6. Let r be a prime Riesel number such that $2r - 1$ is not the square of a Mersenne prime. Also, assume that the equation $\sigma(p^k) = r$ has no solutions with $k \in \mathbb{N}$ and p prime. Thus, the equation $\sigma(m) = r \cdot 2^\alpha$ has no solutions with $m, \alpha \in \mathbb{N}$ and p prime.

Proof. Since r is prime, it is sufficient to show that

$$\sigma(p^a) = r \cdot 2^\alpha \tag{2}$$

has no solutions with p prime, $a \in \mathbb{N}$, and α a non-negative integer.

For a contradiction, assume this is false. Let $\alpha \geq 0$ be the least non-negative integer for which Equation (2) has a solution. By the conditions of the lemma, $\alpha \geq 1$.

Since $\alpha \geq 1$, p must be an odd prime and a an odd integer, say $a = 2k - 1$. If $k = 1$, then $a = 1$, and the equation becomes $p = r \cdot 2^\alpha - 1$, contradicting the fact that r is a Riesel number.

Now, let $k > 1$. Then $a = 2k - 1 > k > 1$. We get $\frac{p^k - 1}{p - 1}(p^k + 1) = r \cdot 2^\alpha$. Thus, $\sigma(p^{k-1}) = \frac{p^k - 1}{p - 1} = 2^\beta$ or else $\sigma(p^{k-1}) = r \cdot 2^\beta$ with $0 \leq \beta < \alpha$.

Suppose $\sigma(p^{k-1}) = r \cdot 2^\beta$. By the conditions of the lemma, $\beta \geq 1$. This contradicts the fact that α is the least positive solution of Equation (2).

Finally, let $\sigma(p^{k-1}) = 2^\beta$. Lemma 5 implies $k = 2$, $a = 3$, and p is Mersenne prime.

We obtain $(1 + p)(1 + p^2) = r \cdot 2^\alpha$.

Now, $p^2 + 1 \equiv 2 \pmod{4}$. Therefore $p^2 + 1 = 2r$. This contradicts the condition that $2r - 1$ is not the square of a Mersenne prime. So, our assumption is false and the proof of the lemma is complete.

Lemma 3 (which is stated in the Introduction) follows directly from Lemma 6.

Proof of Lemma 3. It suffices to check that 509203 satisfies the conditions of Lemma 6. Note that 509203 is a Riesel number (see [8]), and 509203 is prime too. Also, $2 \cdot 509203 - 1 =$

(5)(353)(577) is not a perfect square. Finally, the equation

$$1 + p + \dots + p^k = 509203 \tag{3}$$

has no solutions with p prime and $k \in \mathbb{N}$.

Indeed, if Equation (3) holds, then $p|509202 = 2 \cdot 3^2 \cdot 28289$. A quick check shows that none of the primes 2, 3, 28289 gives a solution to Equation (3).

Finally, we prove Theorem 2.

Proof of Theorem 2. (i) If Hypothesis 1 holds, then there exist infinitely many positive integers α such that 2^α is not a value of the σ function. For each such α , $v_\alpha = 1$.

(ii) Here we will use the results of the computations of the Riesel Problem project aiming to show that 509203 is the smallest Riesel number. The idea is to find, for every odd positive integer k less than 509203, an exponent $e_k \in \mathbb{N}$ such that $k \cdot 2^{e_k} - 1$ is prime. This has been achieved for all but seventy-six integers. Denote the set of these seventy-six integers by \mathcal{C} . For the complete list of the elements of \mathcal{C} see [1].

Assume that Hypothesis 1 does not hold. Then there exists α_0 such that for each $\alpha \geq \alpha_0$ there exists $n_\alpha \in \mathbb{N}$ with $\sigma(n_\alpha) = 2^\alpha$. Lemma 5 implies that n_α is a squarefree number whose prime divisors are Mersenne primes. The set \mathcal{C} has several properties which we will use in the proof. These properties are:

- (i) No element of \mathcal{C} is a multiple of another element of \mathcal{C} ;
- (ii) Each element of \mathcal{C} is either prime or it has at least two distinct prime divisors;
- (iii) No element of \mathcal{C} is a Mersenne prime;
- (iv) If $q \in \mathcal{C}$ is prime, then $2q - 1$ is not the square of a Mersenne prime;
- (v) No element of \mathcal{C} is of the form $n^2 + n + 1$ with $n \in \mathbb{N}$;
- (vi) If $q \in \mathcal{C}$ is prime, then the equation $\sigma(p^k) = q$ has no solutions with $k \in \mathbb{N}$ and p prime.

Properties (i) and (ii) are easy to check by considering the factorizations of the elements of \mathcal{C} . It is also straightforward to establish properties (iii), (iv), and (v). To establish (vi), assume $\sigma(p^k) = q$ for some primes p and q with $q \in \mathcal{C}$ and $k \in \mathbb{N}$. By property (iii), we have $p \neq 2$. Thus, p is an odd prime and k is even. Note that $q < 509203$. So, if $k \geq 6$, then $p < 10$; that is, $p = 3, 5, \text{ or } 7$. No element of \mathcal{C} is of the form $1 + p + \dots + p^k$ with $k \in \mathbb{N}$ and $p = 3, 5, \text{ or } 7$. If $k = 4$ we check that the numbers $1 + p + p^2 + p^3 + p^4$ are not in \mathcal{C} when $p \in \{11, 13, 17, 19, 23\}$ ($29^4 > 700000$). Finally, property (v) ensures that there are no solutions with $k = 2$. Thus, property (vi) holds.

Denote by r be the smallest Riesel prime number. Let k be an odd integer in the interval $[1, r)$. If $k \notin \mathcal{C}$ then there exists e_k such that $p_k = k \cdot 2^{e_k} - 1$ is prime. If $k \in \mathcal{C}$, then k is composite ($k < r$). By properties (i) and (ii), k has the factorization $k = uv$ with $\gcd(u, v) = 1$ and $u \notin \mathcal{C}$, $v \notin \mathcal{C}$. Thus, there exist primes p_u, p_v , and an integer $\alpha_k \in \mathbb{N}$ such that $\sigma(p_u p_v) = uv \cdot 2^{\alpha_k}$. We showed that for each odd integer in the interval $[1, r)$ there exist positive integers m_k, α_k such that $\sigma(m_k) = k \cdot 2^{\alpha_k}$. Moreover, m_k is either prime or a

product of two distinct primes, and no Mersenne prime divides m_k . Let $\alpha > \alpha_k + \alpha_0$. Set $\beta = \alpha - \alpha_k$. Then $\sigma(n_\beta \cdot m_k) = k \cdot 2^\alpha$. Thus, the equation $\sigma(m) = k \cdot 2^\alpha$ has a solution for all $\alpha > \alpha_k + \alpha_0$. Let $\mathcal{M} = \alpha_0 + \max\{\alpha_k\}$ where the maximum is taken over all odd integers in the interval $[1, r)$. Thus, the equation $\sigma(m) = k \cdot 2^\alpha$ has a solution whenever k is an odd integer in $[1, r)$ and $\alpha > \mathcal{M}$. Therefore

$$v_\alpha \geq r \text{ for all } \alpha > \mathcal{M}. \quad (4)$$

On the other hand, r satisfies all conditions of Lemma 6. (It is a prime Riesel number by definition and the remaining conditions of Lemma 6 hold due to properties (iv) and (vi)). Therefore the equation $\sigma(m) = r \cdot 2^\alpha$ has no solution for any α . We get

$$v_\alpha \leq r \text{ for all } \alpha \in \mathbb{N}. \quad (5)$$

Combining (4) and (5) we get $v_\alpha = r$ for all $\alpha > \mathcal{M}$.

References

- [1] R. Ballinger and W. Keller, *The Riesel Problem: Search status for the remaining candidates*, <http://www.prothsearch.net/rieselsearch.html>, December (2005).
- [2] P. Bateman, *Solution of Problem 4995*, American Mathematical Monthly **70** (1963) 101–102.
- [3] D. Buell and J. Young, *Some large primes and the Sierpinski problem*, SRC Technical Report 88-004, SRC, Lantham MD, (1988).
- [4] MR2197003 S. Contini, E. Croot, I. Shparlinski, *Complexity of inverting the Euler function*, Math. Comp. **75** (2006), no. 254, 983–996 (electronic).
- [5] L. Helm and D. Norris, *Seventeen Or Bust*, <http://www.seventeenorbust.com/>, December (2005).
- [6] G. Jaeschke, *On the smallest k such that all $k \cdot 2^n + 1$ are composite*, Math. Comp. **40** (1983) 381–384.
- [7] O. Ore, *Problems for solution pr.4955*, The American Mathematical Monthly **68** (1961) 1010.
- [8] H. Riesel, *Some large primes (in Swedish)*, Elementa **39** (1956) 258–260.
- [9] J. Selfridge, *Solution of Problem 4995*, The American Mathematical Monthly **70** (1963) 101.
- [10] W. Sierpinski, *Sur un probleme concernant les nombres $k \cdot 2^n + 1$* , Elem. Math. **15** (1960) 73–74.
- [11] S. Wagstaff, *Divisors of Mersenne numbers*, Math. Comp. **40** (1983) 385–397.
- [12] J. Young, *Primes submitted to Chris Caldwell's list*, <http://www.prothsearch.net/sierp.html>, August (1997).