VARIANT OF A THEOREM OF ERDŐS ON THE SUM-OF-PROPER-DIVISORS FUNCTION

CARL POMERANCE AND HEE-SUNG YANG

Abstract. In 1973, Erdős proved that a positive proportion of numbers are not of the form $\sigma(n) - n$, the sum of the proper divisors of n. We prove the analogous result where σ is replaced with the sum-of-unitary-divisors function σ^* (which sums divisors d of n such that $(d, n/d) = 1$), thus solving a problem of te Riele from 1976. We also describe a fast algorithm for enumerating numbers not in the form $\sigma(n)-n$, $\sigma^*(n)-n$, and $n-\varphi(n)$, where φ is Euler's function.

1. Introduction

If $f(n)$ is an arithmetic function with nonnegative integral values it is interesting to consider $V_f(x)$, the number of integers $0 \le m \le x$ for which $f(n) = m$ has a solution. That is, one might consider the distribution of the image of f within the nonnegative integers. For some functions $f(n)$ this is easy, such as the function $f(n) = n$, where $V_f(x) = \lfloor x \rfloor$, or $f(n) = n^2$, where $V_f(x) = \lfloor \sqrt{x} \rfloor$. For $f(n) = \varphi(n)$, Euler's φ-function, it was proved by Erdős [Erd35] in 1935 that $V_\varphi(x) = x/(\log x)^{1+o(1)}$ as $x \to \infty$. Actually, the same is true for a number of multiplicative functions f, such as $f = \sigma$, the sum-of-divisors function, and $f = \sigma^*$, the sum-of-unitary-divisors function, where we say d is a unitary divisor of n if $d \mid n$, $d > 0$, and $\gcd(d, n/d) = 1$. In fact, a more precise estimation of $V_f(x)$ is known in these cases; see Ford [For98].

The arithmetic function $s(n) := \sigma(n) - n$ has been considered since antiquity. In studying $V_s(x)$ one immediately sees that if p, q are distinct primes, then $s(pq) = p + q + 1$. Assuming that every even number $m \ge 8$ can be represented as a sum $p + q$, where p, q are distinct primes (a slightly stronger form of Goldbach's conjecture), it follows that all odd numbers $m \ge 9$ are values of s. We do know that even a stronger form of Goldbach's conjecture is almost always true – see [MV75] for example – so as a consequence all odd numbers, except for those in a set of asymptotic density 0, are values of s. But what of even values? In 1973, Erdős [Erd73] showed that if U is the set of positive numbers such that no $s(n) \in U$, then U has positive lower density. The set U is popularly known as the set of "non-aliquot" or "untouchable" numbers. It is not known if U possesses an asymptotic density nor if the upper density of U is smaller than $\frac{1}{2}$. It is known that the lower density of the non-aliquot numbers is at least 0.06, see [CZ11].

In his thesis in 1976, te Riele [tR76] described an algorithm for enumerating all members of $s(\mathbb{N})$ to a given bound x. He did not compute the complexity of this algorithm, but it seems to be of the shape $x^{2+o(1)}$. In fact, his algorithm does more than enumerate: it computes all solutions to the inequality $s(n) \le x$ with n composite. In this paper we describe an

Date: 30 July 2012.

2010 *Mathematics Subject Classification.* 11A25, 11Y70, 11Y16.

Key words and phrases. Unitary untouchable numbers, untouchable numbers, noncototients.

algorithm that achieves the more modest goal of enumerating $s(\mathbb{N})$ (or equivalently, U) to x. Our algorithm has running time of the shape $x^{1+o(1)}$. The algorithm of te Riele is based on an earlier one of Alanen [Ala72]. Alanen was able to count U to 5,000, while with te Riele's improvements, he got the count to 20,000. We provide some statistics to $x = 10^8$ indicating that the density of U perhaps exists.

te Riele [tR76] also suggested some problems similar to the distribution of $s(\mathbb{N})$. Let $s^*(n) := \sigma^*(n) - n$ and let $s_\varphi(n) := n - \varphi(n)$. (te Riele did not consider the latter function.) In both cases, we again have almost all odd numbers in the image, since for p, q distinct primes, $s^*(pq) = s(pq) = p + q + 1$ and $s_\varphi(pq) = p + q - 1$. Positive numbers missing from the image of s^* are sometimes called "unitary untouchable" numbers and numbers missing from the range of s_φ are known as "noncototients". Solving a problem of Sierpiński, it has been shown that there are infinitely many noncototients (see [BS95, FL00, GM05]), but we do not know if their lower density is positive. Nothing seems to be known about $s^*(\mathbb{N})$. Let $U^* = \mathbb{N} \setminus s^*(\mathbb{N})$, the set of positive integers not of the form $s^*(n)$. te Riele used a version of his algorithm to enumerate U^* to 20,000, finding only 160 members; perhaps a reasonable interpretation of that data might lead one to think that U^* has density 0. In this paper we apply our algorithm to enumerate both U^* and $\Phi := \mathbb{N} \setminus \varphi(\mathbb{N})$ to 10^8 leading us to conjecture that both sets have a positive asymptotic density, though the density of U^* seems to be small. The previous best count of U^* was to 10^5, a result of David Wilson, as recorded in Guy's *Unsolved Problems in Number Theory*. The previous best count for Φ was to 10^4, by T. D. Noe, as recorded in the Online Encyclopedia of Integer Sequences.

Our principal result is the following.

Theorem 1.1. *The set $U^* = \mathbb{N} \setminus s^*(\mathbb{N})$ has a positive lower density.*

Our proof follows the same general plan as that of Erdős [Erd73], except that an important special case is dealt with via covering congruences. That covering congruences should arise in the problem is not totally unexpected. As noted by te Riele [tR76], if the conjecture of de Polignac [dP49] that every large odd number can be represented as $2^w + p$, where $w \geq 1$ and p is an odd prime[1], then since $s^*(2^w p) = 2^w + p + 1$, it would follow that U^* has asymptotic density 0. However, Erdős [Erd50] and van der Corput [vdC50] independently showed that de Polignac's conjecture is false. As an important ingredient in our proof of Theorem 1.1, we use the Erdős argument for disproving de Polignac's conjecture, an argument which involves covering congruences.

Though it is not known if the set $U = \mathbb{N} \setminus s(\mathbb{N})$ has upper density smaller than $\frac{1}{2}$ nor if the set Φ of noncototients has upper density smaller than $\frac{1}{2}$, we can achieve such a result for U^*.

Theorem 1.2. *The set U^* has upper density smaller than $\frac{1}{2}$.*

Our proof of this theorem follows from noting that de Polignac's conjecture, mentioned above, does hold for a positive proportion of numbers.

[1]Note that de Polignac allowed $p = 1$ in his conjecture, but the set of numbers $2^w + 1$ has density 0.

2. Proof of Theorem 1.1

The set of positive lower density that we identify will be a subset of the integers that are 2 (mod 4). We begin with the following result.

Lemma 2.1. *Let n be a positive integer. If $n > 1$ is odd or if n is divisible by 4 and also two distinct odd primes, then $s^*(n) \not\equiv 2 \pmod 4$.*

Proof. If p^a is a power of an odd prime p, then $\sigma^*(p^a) = 1 + p^a$ is even. Thus, if $n > 1$ is odd, then $\sigma^*(n)$ is even, so that $s^*(n)$ is odd; in particular, we have $s^*(n) \not\equiv 2 \pmod 4$. Similarly, if n is divisible by k distinct odd primes, then $2^k \mid \sigma^*(n)$. Hence, if $k \geq 2$ and $4 \mid n$, then $s^*(n) \equiv 0 \not\equiv 2 \pmod 4$. This concludes the proof of the lemma. □

We would like to handle the case of $4 \mid n$ and n is divisible by only one odd prime. The following result almost shows that such numbers are negligible.

Lemma 2.2. *The set of numbers $s^*(2^w p^a)$ where p is an odd prime and $a \geq 2$ has asymptotic density 0.*

Proof. We have $s^*(2^w p^a) = 1 + 2^w + p^a$. If $s^*(2^w p^a) \leq x$, we have

$$2^w \leq x \text{ and } p^a \leq x.$$

The number of choices for 2^w is thus $O(\log x)$ and the number of choices for p^a with $a \geq 2$ is thus $O(\sqrt{x}/\log x)$. Thus, in all there are just $O(\sqrt{x})$ numbers $2^w p^a$ to consider, and so just $O(\sqrt{x})$ numbers $s^*(2^w p^a) \leq x$. Hence such numbers comprise a set of asymptotic density 0, proving the lemma. □

For the case of $s^*(2^w p)$ we invoke the proof using covering congruences that shows that a certain positive proportion of integers are not of this form.

Proposition 2.3. *There are integers c, d with d odd such that if p is an odd prime, w is a positive integer, then $s^*(2^w p) \not\equiv c \pmod d$.*

Proof. It is easy to verify that each integer w satisfies at least one of the following congruences:

$$\begin{aligned} w &\equiv 1 \pmod 2, \quad w \equiv 1 \pmod 3, \\ w &\equiv 2 \pmod 4, \quad w \equiv 4 \pmod 8, \\ w &\equiv 8 \pmod{12}, \quad w \equiv 0 \pmod{24}. \end{aligned} \tag{1}$$

For each modulus $m \in \{2, 3, 4, 8, 12, 24\}$ we find an odd prime q such that the multiplicative order of 2 modulo q is exactly m. Valid choices for q are listed in the table below. With a pair m, q, note that for any integer b, if $w \equiv b \pmod m$, then $s^*(2^w p) \not\equiv 1 + 2^b \pmod q$ for $p \neq q$. Choices for b are given in the above chart, and the consequently forbidden residue class for $N = s^*(2^w p)$ is given in the table below.

m	b	q	$2^b \bmod q$	$N \bmod q$	Conclusion:
2	1	3	2	$N \equiv p$	$N \not\equiv 0 \pmod 3$ or $p = 3$
3	1	7	2	$N \equiv 3 + p$	$N \not\equiv 3 \pmod 7$ or $p = 7$
4	2	5	-1	$N \equiv p$	$N \not\equiv 0 \pmod 5$ or $p = 5$
8	4	17	-1	$N \equiv p$	$N \not\equiv 0 \pmod{17}$ or $p = 17$
12	8	13	-4	$N \equiv -3 + p$	$N \not\equiv -3 \pmod{13}$ or $p = 13$
24	0	241	1	$N \equiv 2 + p$	$N \not\equiv 2 \pmod{241}$ or $p = 241$

Upon applying the Chinese Remainder Theorem to the six forbidden residue classes in the last column, i.e.,

$$\begin{aligned} &N \equiv 0 \pmod 3, \quad N \equiv 0 \pmod 5, \\ &N \equiv 3 \pmod 7, \quad N \equiv -3 \pmod{13}, \\ &N \equiv 0 \pmod{17}, \quad N \equiv 2 \pmod{241}, \end{aligned} \tag{2}$$

we obtain the residue class $c \pmod d$, where $c = -1518780$ and $d = 3 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 241 = 5592405$.

To summarize the argument so far, suppose $s^*(2^w p) \equiv c \pmod d$. Since the congruences (1) cover all integers, we must have $w \equiv b \pmod m$ for one of the six choices for $b \pmod m$ in (1). In particular, unless p is the prime q corresponding to m, we have $s^*(2^w p)$ forbidden from the corresponding residue class modulo q in (2). And in particular $s^*(2^w p)$ cannot be in the residue class $c \pmod d$.

We finally consider numbers of the form $s^*(2^w q)$ where $q \in \{3, 5, 7, 13, 17, 241\}$. Suppose $N \equiv c \pmod d$ and $N = s^*(2^w q)$. Since $N \equiv 3 \pmod 7$ and none of the expressions

$$2^w + 4,\ 2^w + 14,\ 2^w + 18,\ 2^w + 242$$

can be 3 (mod 7), we can rule out $q = 3, 13, 17$, and 241. Since $2^w + 6$ cannot be 0 (mod 17), we can rule out $q = 5$. To rule out $q = 7$ we note that $2^w + 8 \equiv 2 \pmod{241}$ has no solutions. This proves the proposition. $\square$

Remark 2.4. The last part of the proof shows that none of the numbers of the form $s^*(2^w q)$ with $q \in \{3, 5, 7, 13, 17, 241\}$ lie in the residue class $c \pmod d$. We note that such numbers comprise a set of asymptotic density 0, so even without this last part of the proof, we would have asymptotically almost all of the numbers in the residue class $c \pmod d$ not of the form $s^*(2^w p)$.

Proposition 2.5. *Let*

$$Q = 2 \cdot 3^\alpha \cdot 5^\beta \cdot 17^\gamma,$$

where α, β, γ are positive integers. If $s^*(Q)/Q > 1$ then the set of members of U^* which have Q as a unitary divisor has lower density at least

$$\left(1 - \frac{Q}{s^*(Q)}\right) \frac{384}{dQ},$$

where d is as in Proposition 2.3.

Proof. Consider the residue class $c \pmod d$ of Proposition 2.3. We have $c \equiv 0 \pmod{3 \cdot 5 \cdot 17}$. Thus the conditions that a number lie in the residue class $c \pmod d$ and have Q as a unitary divisor are compatible and there are exactly $\varphi(510) = 128$ such residue classes modulo $2dQ$. (Note that the least common multiple of d and Q is $dQ/255$, so there are 510 residue classes modulo $2dQ$ that are $c \pmod d$ and $0 \pmod Q$. Of these, $\varphi(510) = 128$ have Q as a unitary divisor.) Fix one of these residue classes, call it r. We first show that the proportion of numbers $r \pmod{2dQ}$ that are not in the form $s^*(n)$ is at least $1 - Q/s^*(Q)$. By Lemmas 2.1 and 2.2 we may assume that $n \equiv 2 \pmod 4$ or n is divisible by 4 and just one odd prime to the first power. Since we are only looking at values in the residue class $c \pmod d$, Proposition 2.3 shows the latter case does not occur, that is, we must have $n \equiv 2 \pmod 4$. Then n has the unitary divisor $n/2$ so that $s^*(n) > n/2$. In particular, if we are counting values $s^*(n) \le x$, then we must have $n < 2x$. It follows from [tR76, Lemma 9.2] (which is attributed to [Sco73]) that the number of $n < 2x$ with $\sigma^*(n) \not\equiv 0 \pmod{2dQ}$ is $o(x)$ as $x \to \infty$. Thus, we may assume that $\sigma^*(n) \equiv 0 \pmod{2dQ}$, which in turn implies that $n \equiv -r \pmod{2dQ}$, and so Q is a unitary divisor of n. This implies that

$$s^*(n) = \sigma^*(n) - n = \sigma^*(Q)\sigma^*(n/Q) - n \ge \sigma^*(Q)n/Q - n = (s^*(Q)/Q)n.$$

Since $s^*(n) \le x$, we have $n \le (Q/s^*(Q))x$. Thus, the number of values of $s^*(n) \equiv r \pmod{2dQ}$ in $[1, x]$ is at most $(Q/s^*(Q))(x/2dQ) + o(x)$ as $x \to \infty$. Hence, within the residue class $r \pmod{2dQ}$ the lower density of U^* is at least $(1 - Q/s^*(Q))/2dQ$. Noting that there are 128 values of $r \pmod{2dQ}$, we get that the lower density of U^* within the residue class $c \mod d$ and with Q as a unitary divisor is at least $(1 - Q/s^*(Q))128/2dQ = (1 - Q/s^*(Q))64/dQ$.

Note that $384 = 6 \cdot 64$. The 6-fold improvement in the proposition is explained as follows. In the proof of Proposition 2.3, after we choose the residue classes 1 (mod 2), 2 (mod 4), and 4 (mod 8), there are actually 6 choices for the remaining congruence classes mod 3, 12, and 24. In the proof we chose 1, 8, and 0, respectively. Instead we could have chosen 1, 0, 8, or 2, 0, 16, or 2, 4, 0, or 0, 4, 8, or 0, 8, 16. Each of the 6 choices leads to a residue class $c_j \pmod{d}$ for $j = 1, 2, \ldots, 6$ for which the above argument works just as well.

This completes the proof of the proposition. □

Let $Q = 2 \cdot 3 \cdot 5 \cdot 17 = 510$. We have

$$\frac{s^*(Q)}{Q} = \frac{3 \cdot 4 \cdot 6 \cdot 18}{510} - 1 = \frac{131}{85} > 1,$$

so that Proposition 2.5 implies that the lower density of those members of U^* with Q as a unitary divisor is at least

$$\left(1 - \frac{85}{131}\right) \frac{384}{5592405 \cdot 510} > 4.727 \times 10^{-8}. \tag{3}$$

This immediately proves Theorem 1.1.

We can improve our estimate for the lower bound of the lower density of U^* as follows. First, instead of choosing α, β, γ as 1, 1, 1 in the definition of Q, we can choose α, β, γ as 1, 1, 2, or 1, 2, 1, or 1, 3, 1, or 2, 1, 1. These choices in turn lead to estimates for the lower density of the set of those numbers in U^* with these unitary divisors of

$$2.29 \times 10^{-9}, \quad 4.53 \times 10^{-9}, \quad 6.3 \times 10^{-10}, \quad 4.72 \times 10^{-9},$$

respectively. A further improvement can be made by changing the residue class 4 (mod 8) in our covering to 0 (mod 8). This in turn changes our choice for residue classes modulo 3, 12, and 24 in the proof of Proposition 2.3 to 1, 8, 12 plus 5 other triples. In this case we do not have 17 as a divisor of our value (before, the residue class modulo 17 was $2^4 + 1 \equiv 0 \pmod{17}$, but now it is $2^0 + 1 \equiv 2 \pmod{17}$). Thus, we have an analogous version of Proposition 2.5 with $Q = 2 \cdot 3^\alpha \cdot 5^\beta$. Using this with $Q = 30$ leads to an estimate for the lower density of the set of members of U^* with 30 as a unitary divisor and not divisible by 17 of

$$\left(1 - \frac{30}{s^*(30)}\right) \frac{24}{5592405 \cdot 30} > 4.087 \times 10^{-8}.$$

There are of course other small improvements to be made, but the estimates so far imply that the lower density of U^* is greater than 10^{-7}.

Remark 2.6. It is not too hard to use these ideas to show that the set $U \cap U^*$ of numbers that are simultaneously not of the form $s(n)$ nor $s^*(m)$ has positive lower density. In fact, it is possible to show this set has lower density larger than 10^{-8}. To do this one can exploit the fact that for n squarefree we have $s(n) = s^*(n)$. Thus, in trying to find values for s or s^* with 510 as a unitary divisor and in the residue class $c \pmod d$, for both problems we are restricted to searching over the set A of numbers $n \le (510/s(510))x$ with $n \equiv c \pmod d$ and with 510 as a unitary divisor. The only point of departure between the two counts comes from those members of A that are not squarefree. But a simple calculation shows that more than 97% of the members of A are squarefree, so there are not enough of the non-squarefree members to appreciably affect our estimates. That is, (3) with "$1 - 85/131$" replaced with "$0.97 - 85/131$" holds as a lower bound for the lower density of $U \cap U^*$. Probably with a little work, the lower bound 10^{-8} can be improved to 10^{-7}.

3. Proof of Theorem 1.2

We again focus on numbers $s^*(2^w p)$ with $w \ge 1$ and p an odd prime, but instead of looking at even numbers not of this form, we look at even numbers that are of this form. We have

$$s^*(2^w p) = 2^w + p + 1.$$

Thus, Theorem 1.2 will follow if we show that the set of numbers of the form $2^w + p$ has a positive lower density. (The case $w = 0$ is not permitted in our problem, since $s^*(2^0 p) = 1$, but the set of numbers of the form $2^0 + p$ has density 0. In addition, the case $p = 2$ is not permitted in our problem, but again the set of numbers of the form $2^w + 2$ has density 0.)

Though it is not hard to prove the result directly using the Cauchy–Schwarz inequality and sieve methods, this theorem is already in the literature. In particular, in 1934, Romanov [Rom34] proved that the lower density of numbers of the form $2^w + p$ is positive. Chen and Sun [CS04] proved that the lower density is at least 0.0868, and this was improved in Habsieger and Roblot [HR06], Lü [L07], and Pintz [Pin06] to 0.09368. It follows that

$$10^{-7} < \underline{d}\, U^* \le \bar{d}\, U^* \le 0.40632,$$

where $\underline{d}$ denotes lower asymptotic density and $\bar{d}$ denotes upper asymptotic density.

4. The enumeration of U^*

In this section we introduce our methods on numerically enumerating U^*. We begin with the following elementary observation.

Proposition 4.1. *Let m, j be positive integers with m odd. Then*
(i) $s^*(2m) = 3\sigma^*(m) - 2m$,
(ii) $s^*(2^{j+1}m) = 2s^*(2^j m) - \sigma^*(m)$.

Proof. This follows immediately from the fact that $\sigma^*(2^j m) = (2^j + 1)\sigma^*(m)$. □

We now can describe our procedure. Say we wish to enumerate the even members of U^* $[1, x]$. For each odd number $m \le x$ we compute $\sigma^*(m)$ (more on this later). Then starting with $t = 3\sigma^*(m) - 2m$ we iterate the recurrence $t \mapsto 2t - \sigma^*(m)$ until we exceed x. Each number t visited is an even member of $s^*(\mathbb{N})$. Thus, after exhausting this procedure, we have visited every even member of $s^*(\mathbb{N})$ in $[1, x]$, so the even numbers not visited comprise the even members of U^* in $[1, x]$.

In our implementation we used trial division to factor each odd number m in $[1, x]$. Instead one might use the method of Moews and Moews [MM06] which can compute each $\sigma^*(m)$ for m up to x in time $\tilde{O}(x)$. (The expression $\tilde{O}(x)$ denotes the bound $x(\log x)^{O(1)}$.)

Since it is time consuming to manage set membership in the set of even members of $s^*(\mathbb{N})$, we instead initialize a function f defined as identically 1 for all even numbers up to x. Whenever we visit an even number t in $s^*(\mathbb{N}) \cap [1, x]$, we reassign $f(t)$ to 0. At the end of the procedure, our function f is then the characteristic function of the even members of U^* in $[1, x]$.

There remains the task of finding the odd members of U^* in $[1, x]$. Note that 3, 5, and 7 are all in U^*. As remarked earlier, it follows from a slightly stronger form of Goldbach's conjecture (namely, every even number starting at 8 is the sum of two distinct primes) that every odd number $n \geq 9$ is of the form $s^*(pq) = p + q + 1$ where p, q are distinct primes. Thus, to enumerate the odd members of U^* to x it suffices to verify this slightly stronger form of Goldbach's conjecture to x. On the webpage [Oli12] (maintained by Oliveira e Silva) the verification of this stronger form of Goldbach's conjecture is reported to $x = 4 \times 10^{18}$. In our calculation of U^* we search only to 10^8, so the numbers 3, 5, and 7 are the only odd ones in this range. Concerning the time bound of $\tilde{O}(x)$, this too can stand as a time bound for verifying the slightly stronger form of Goldbach's conjecture that we are using, modulo the reasonable assumption that every even $n \geq 8$ has a decomposition as $p + q$ where p, q are primes and $p \leq (\log n)^{O(1)}$. Even without such an assumption, since exceptions are rare, the theoretical time bound of $\tilde{O}(x)$ might still be achievable.

In the table below we record counts to 10^8 for U^*. Here, $N(x)$ denotes the number of members of U^* up to x, $D(x) = N(x)/x$ denotes the density of $U^* \cap [1, x]$ in $[1, x]$, and Δ records the difference from the prior entry.

x	$N(x)$	Δ	$100D(x)$	x	$N(x)$	Δ	$100D(x)$
100000	862	862	0.862	6000000	60257	10176	1.00428
200000	1846	984	0.923	7000000	70518	10261	1.0074
300000	2811	965	0.937	8000000	80987	10469	1.01234
400000	3790	979	0.9475	9000000	91087	10100	1.01208
500000	4841	1051	0.9682	10000000	101030	9943	1.0103
600000	5795	954	0.965833	20000000	203113	102083	1.01557
700000	6810	1015	0.972857	30000000	304631	101158	1.01544
800000	7828	1018	0.9785	40000000	405978	101347	1.01495
900000	8865	1037	0.985	50000000	509695	103717	1.01939
1000000	9903	1038	0.9903	60000000	615349	105654	1.02558
2000000	19655	9752	0.98275	70000000	720741	105392	1.02963
3000000	29700	10045	0.99	80000000	821201	100460	1.0265
4000000	40302	10602	1.00755	90000000	923994	102793	1.02666
5000000	50081	9779	1.00162	100000000	1028263	104269	1.02826

All of our calculations were done with Mathematica, using their FactorInteger function to factor each odd number m appearing. It should be expected that with a more serious implementation using the techniques of [MM06], one could go considerably further.

5. The enumeration of Φ and U

The algorithms for enumerating $\Phi = \mathbb{N} \setminus s_\varphi(\mathbb{N})$ and $U = \mathbb{N} \setminus s(\mathbb{N})$ are more or less similar to the algorithm introduced in the previous section. However, the relations we employ are different. The following statement is an elementary exercise.

Proposition 5.1. *Let $s_\varphi(n) := n - \varphi(n)$. Suppose also that m, j are positive integers with m odd. The following statements hold:*
(i) $s_\varphi(2m) = 2m - \varphi(m)$,
(ii) $s_\varphi(2^{j+1}m) = 2s_\varphi(2^j m)$.

Since $s_\varphi(n) \equiv n \pmod 2$ when $n > 2$, to count even noncototients it suffices to consider only $n = 2^j m$ with m, j positive integers and m odd. Further, for such a number n, we have $s_\varphi(n) > m$, so if we are enumerating to x, we need only consider odd numbers $m < N$. Thus, we have an entirely analogous algorithm as for U^*.

We record below our counts for noncototients to 10^8. Let $N_\varphi(x)$ denotes the number of noncototients up to x and let $D(x)$ denote their density. As before Δ records the difference in the count from the prior entry.

x	$N_\varphi(x)$	Δ	$D(x)$	x	$N_\varphi(x)$	Δ	$D(x)$
100000	10527	10527	0.10527	6000000	674884	113034	0.112481
200000	21433	10906	0.107165	7000000	788080	113196	0.112583
300000	32497	11064	0.108323	8000000	901478	113398	0.112685
400000	43559	11062	0.108898	9000000	1014711	113233	0.11274
500000	54757	11198	0.109514	10000000	1128160	113449	0.112816
600000	65938	11181	0.109897	20000000	2262697	1134537	0.113135
700000	77115	11177	0.110164	30000000	3398673	1135976	0.113289
800000	88306	11191	0.110383	40000000	4534957	1136284	0.113374
900000	99554	11248	0.110616	50000000	5671818	1136861	0.113436
1000000	110786	11232	0.110786	60000000	6808454	1136636	0.113474
2000000	223337	112551	0.111669	70000000	7944836	1136382	0.113498
3000000	335920	112583	0.111973	80000000	9081939	1137103	0.113524
4000000	448955	113035	0.112239	90000000	10218937	1136998	0.113544
5000000	561850	112895	0.11237	100000000	11355049	1136112	0.11355

The case for $s(n)$ is somewhat different. First note that we have the analogous elementary exercise.

Proposition 5.2. *Let $s(n) := \sigma(n) - n$. Suppose also that m, j are positive integers and m is odd. The following statements hold:*
(i) $s(2m) = 3\sigma(m) - 2m$,
(ii) $s(2^{j+1}m) = 2s(2^j m) + \sigma(m)$.

In the case of U, it is *not* enough to check the numbers $s(2^j m) \le x$ for odd $m \le x$. We have $s(n)$ even if and only if

1. n is even and not a square nor twice a square, or
2. n is an odd square.

When enumerating the even values of $s(n)$ in $[1, x]$, in case 1 it suffices to take $s(2^j m)$ for odd $m < x$ (since $s(2^j m) > m$) with m not a square. In case 2, we must consider $s(m^2)$

for odd $m < x$ (since $s(m^2) > m$). Case 1 is entirely analogous to the enumeration of U^* and Φ except that if $\sigma(m)$ is odd (signifying that m is a square), we do not enter a loop that increases the power of 2, and we pass over this m. To deal with the odd squares, it is helpful to use the case 1 calculation to find $s(p^2)$ for prime $p < x$. These are detected as follows. If $\sigma(m) = m + 1$, signifying that m is a prime, we record the number $m + 1$ as an even value of s since it is $s(m^2)$. This would leave the values of $s(m^2) \le x$ with m odd and composite. In this case, we have that $m < x^{2/3}$. Indeed, if $g \mid m$ and $m^{1/2} \le g < m$, then $s(m^2) > gm \ge m^{3/2}$. Thus, we may run a small side program for odd composite numbers $m < x^{2/3}$, computing $s(m^2)$ in each case.

We conclude that as with the enumeration of U^*, both the enumeration of Φ and U can be achieved in time $\tilde{O}(x)$. Here are our counts of U to 10^8, where $N_\sigma(x)$ is the number of members of U in $[1, x]$ and $\Delta, D(x)$ are as before.

x	$N_\sigma(x)$	Δ	$D(x)$	x	$N_\sigma(x)$	Δ	$D(x)$
100000	13863	13863	0.13863	6000000	936244	158572	0.156041
200000	28572	14712	0.14286	7000000	1095710	159466	0.15653
300000	43515	14940	0.14505	8000000	1255016	159306	0.156877
400000	58459	14944	0.146148	9000000	1414783	159767	0.157198
500000	73565	15106	0.14713	10000000	1574973	160190	0.157497
600000	88828	15263	0.148047	20000000	3184111	1609138	0.159206
700000	104062	15234	0.14866	30000000	4804331	1620220	0.160144
800000	119302	15240	0.149128	40000000	6430224	1625893	0.160756
900000	134758	15456	0.149731	50000000	8060163	1629939	0.161203
1000000	150232	15474	0.150232	60000000	9694467	1634304	0.161574
2000000	305290	155058	0.152645	70000000	11330312	1635845	0.161862
3000000	462110	156820	0.154037	80000000	12967239	1636927	0.16209
4000000	619638	157528	0.15491	90000000	14606549	1639310	0.162295
5000000	777672	158034	0.15553	100000000	16246940	1640391	0.162469

6. Discussion

We have been able to get considerably farther than prior enumerations for U^*, Φ, and U. As remarked earlier, our algorithm is essentially linear, while the earlier methods seem to have traversed over a substantially larger search space. The method of te Riele elaborates on an earlier method of Alanen [Ala72], and we have not seen any other algorithms discussed.

In [tR76], te Riele suggests an interesting random model that possibly could predict the approximate number of members of our various sets to x. Namely, in each case, one might compute the number $M(x)$ of integers that the functions s^*, s_φ, s take to even numbers in $[1, x]$. Assuming randomness, the number of even numbers not represented would be about $\frac{1}{2}x(1 - 2/x)^{M(x)}$. This is an appealing thought, and it should be remarked that via the continuity of the distribution functions for $\sigma^*(n)/n$, $\varphi(n)/n$, and $\sigma(n)/n$, in each case, we have $M(x) \sim cx$ for a positive constant c that is appropriate for the particular function. (In the case of s^* one needs to add in $x/\log 2$ to what the distribution-function argument gives, coming from the density-0 set of integers $2^w p$.) te Riele found that when $x = 20{,}000$, the number of even members of U is 2565, compared with a prediction of 2610. For U^*, the number of even ones is 157 compared with a prediction of 90.

We have worked out this computation at $x = 10^8$. In the case of s^*, we found that there are 290,100,230 numbers n with $s^*(n)$ even and at most 10^8. This suggests that there are about

$$\frac{1}{2}10^8\left(1-\frac{2}{10^8}\right)^{290,100,230} \approx 151{,}075$$

members of U^* to 10^8 compared with the actual number of 1,028,263. Thus, the heuristic model seems not too good for U^*.

It is better for Φ. In the case of s_φ, there are 85,719,597 values of n with $s_\varphi(n)$ even and at most 10^8. This would suggest that there are about

$$\frac{1}{2}10^8\left(1-\frac{2}{10^8}\right)^{85,719,597} \approx 9{,}003{,}659$$

noncototients to 10^8, compared with the actual number of 11,355,049.

It is better still for U. There are 62,105,426 values of n with $s(n)$ even and at most 10^8. The model suggests then that there are about

$$\frac{1}{2}10^8\left(1-\frac{2}{10^8}\right)^{62,105,426} \approx 14{,}433{,}734$$

members of U to 10^8, compared with the actual number of 16,246,940.

We record some open problems. The data suggest that in all the cases we considered, the density exists. Can this be proved? Is there a positive proportion of even numbers in $s(\mathbb{N})$? The same question for $s_\varphi(\mathbb{N})$. Can one prove that the lower density of Φ is positive?

7. Acknowledgments

We thank Paul Pollack for helping us find some of the references related to Romanov's theorem. This paper is based on the second-named author's undergraduate honor's thesis at Dartmouth College in 2012, written under the supervision of the first-named author. The first-named author was supported in part by NSF grant DMS-1001180.

References

[Ala72] J. D. Alanen, *Empirical study of aliquot series*, Ph.D. thesis, Yale University, 1972.

[BS95] J. Browkin and A. Schinzel, *On integers not of the form $n - \varphi(n)$*, Colloq. Math. **68** (1995), no. 1, 55–58.

[CS04] Y.-G. Chen and X.-G. Sun, *On Romanoff's constant*, J. Number Theory **106** (2004), 275–284.

[CZ11] Y.-G. Chen and Q.-Q. Zhao, *Nonaliquot numbers*, Publ. Math. Debrecen **78** (2011), no. 2, 439–442.

[dP49] A. de Polignac, *Six propositions arithmologiques dédits du crible de d'eratosthène*, Nouv. Ann. Math. **8** (1849), 130–133.

[Erd35] P. Erdős, *On the normal number of prime factors of $p - 1$ and some related problems concerning Euler's φ-function*, Quart. J. Math. **6** (1935), 205–213.

[Erd50] ———, *On integers of the form $2^k + p$ and some related problems*, Summa Brasil. Math. **2** (1950), 113–123.

[Erd73] ———, *Über die Zahlen der Form $\sigma(n) - n$ und $n - \varphi(n)$*, Elem. Math. **11** (1973), 83–86.

[FL00] A. Flammenkamp and F. Luca, *Infinite families of noncototients*, Colloq. Math. **86** (2000), no. 1, 37–41.

[For98] K. Ford, *The distribution of totients*, Ramanujan J. **2** (1998), 67–151.

[GM05] A. Grytczuk and B. Mędryk, *On a result of Flammenkamp–Luca concerning noncototient sequence*, Tskukuba J. Math. **29** (2005), 533–538.

[HR06] L. Habsieger and X.-F. Roblot, *On integers of the form $p + 2^k$*, Acta Arith. **122** (2006), 45–50.

[L07] G. Lü, *On Romanoff's constant and its generalized problem*, Adv. Math. (Beijing) **36** (2007), 94–100.
[MM06] D. Moews and P. C. Moews, *A search for aliquot cycles and amicable pairs*, Acta Arith. **122** (2006), 45–50.
[MV75] H. L. Montgomery and R. C. Vaughan, *The exceptional set in Goldbach's problem*, Acta Arith. **27** (1975), 353–370.
[Oli12] T. Oliveira e Silva, *Goldbach conjecture verification*, last updated April 2012, accessed 5 June 2012. `http://www.ieeta.pt/~tos/goldbach.html`.
[Pin06] J. Pintz, *A note on Romanov's constant*, Acta Math. Hungar. **112** (2006), 1–14.
[Rom34] N. P. Romanov, *Über einige Satze der additives Zahlentheorie*, Math. Ann. **109** (1934), 668–678.
[Sco73] E. J. Scourfield, *Non-divisibility of some multiplicative functions*, Acta Arith. **22** (1973), 287–314.
[tR76] H. J. J. te Riele, *A theoretical and computational study of generalized aliquot sequences*, Ph.D. thesis, Universiteit van Amsterdam, 1976, Mathematical Centrum Tracts No. 74, Mathematisch Centrum, Amsterdam, 1976.
[vdC50] J. G. van der Corput, *On de Polignac's conjecture*, Simon Stevin **27** (1950), 99–105.

Department of Mathematics, 6188 Kemeny Hall, Dartmouth College, Hanover, NH 03755
E-mail address: `carl.pomerance@dartmouth.edu`

Department of Mathematics, 6188 Kemeny Hall, Dartmouth College, Hanover, NH 03755
E-mail address: `hee-sung.yang.12@dartmouth.edu`