ON PERFECT AND NEAR-PERFECT NUMBERS

PAUL POLLACK AND VLADIMIR SHEVELEV

Abstract. We call n a *near-perfect number* if n is the sum of all of its proper divisors, except for one of them, which we term the *redundant divisor*. For example, the representation

$$12 = 1 + 2 + 3 + 6$$

shows that 12 is near-perfect with redundant divisor 4. Near-perfect numbers are thus a very special class of pseudoperfect numbers, as defined by Sierpiński. We discuss some rules for generating near-perfect numbers similar to Euclid's rule for constructing even perfect numbers, and we obtain an upper bound of $x^{5/6+o(1)}$ for the number of near-perfect numbers in $[1, x]$, as $x \to \infty$.

1. Introduction

A *perfect number* is a positive integer equal to the sum of its proper positive divisors. Let $\sigma(n)$ denote the sum of all of the positive divisors of n. Then n is a perfect number if and only if $\sigma(n) - n = n$, that is, $\sigma(n) = 2n$. The first four perfect numbers – 6, 28, 496, and 8128 – were known to Euclid, who also succeeded in establishing the following general rule:

Theorem A (Euclid)**.** *If p is a prime number for which $2^p - 1$ is also prime, then $n = 2^{p-1}(2^p - 1)$ is perfect number.*

It is interesting that 2000 years passed before the next important result in the theory of perfect numbers. In 1747, Euler showed that every even perfect number arises from an application of Euclid's rule:

Theorem B (Euler)**.** *All perfect numbers have the form $n = 2^{p-1}(2^p - 1)$, where p and $2^p - 1$ are primes.*

Recall that primes of the form $2^p - 1$ are called *Mersenne primes*. We do not know whether or not there are infinitely many Mersenne primes, and so we do not know whether or not there exist infinitely many even perfect numbers. Equally mysterious is the question of whether there is any example of an *odd* perfect number. For a survey of the (few) known results and the (many) open problems concerning perfect numbers, we refer the reader to [2, Chapter B] or [9, Chapter 1].

Following Sierpiński [10], the positive integer n is called *pseudoperfect* if n can be written as a sum of some subset of its proper divisors. For example, $36 = 1+2+6+9+18$, and so 36 is pseudoperfect but not perfect. In this paper, we study pseudoperfect numbers of a very special kind. We call n a *near-perfect number* if it is the sum of all of its proper divisors, except *one* of them. The missing divisor d is termed *redundant*. Thus,

$$n \text{ is near-perfect with redundant divisor } d \iff$$
$$d \text{ is a proper divisor of } n, \quad \text{and} \quad \sigma(n) = 2n + d.$$

The first several near-perfect numbers are (cf. our sequence A181595 in [11])

$$12, 18, 20, 24, 40, 56, 88, 104, 196, 224, 234, 368, 464, 650, 992, \dots \tag{1.1}$$

corresponding to the redundant divisors (cf. our sequence A181596 in [11])

$$4, 3, 2, 12, 10, 8, 4, 2, 7, 56, 78, 8, 2, 2, 32, \dots. \tag{1.2}$$

1991 *Mathematics Subject Classification.* 11B83.

We have not yet succeeded in showing that there are infinitely many near-perfect numbers. But we give some strong evidence for this in §2, where we present various rules for constructing near-perfect numbers analogous to Euclid's rule for constructing even perfect numbers. In the final section of this paper, we give an upper bound on the count of the near-perfect numbers: *The number of such integers in* $[1, x]$ *is at most* $x^{5/6+o(1)}$, *as* $x \to \infty$.

Notation and terminology. We use O and o-notation, as well as the associated Vinogradov symbols $\ll$ and $\gg$, with their standard meanings. We recall that an integer m is said to be *squarefull* if p^2 divides m for every prime p dividing m. By the *squarefull part* of an integer n, we mean its largest squarefull divisor. We say that d is a *unitary divisor* of n if n has a decomposition of the form $n = dd'$, where $\gcd(d, d') = 1$. If p^e is a prime power, we write $p^e \parallel n$ to mean that $p^e \mid n$ while $p^{e+1} \nmid n$.

2. Constructing near-perfect numbers

For each integer $k \geq 1$, we let $\mathcal{P}_k$ denote the set of primes of the form $2^t - 2^k - 1$, where $t \geq k+1$. Our first construction of near-perfect numbers is rooted in the following observation:

Proposition 1. *If* $n = 2^{t-1}(2^t - 2^k - 1)$, *where* $2^t - 2^k - 1 \in \mathcal{P}_k$, *then* n *is a near-perfect number with redundant divisor* 2^k.

Proof. Since $k \leq t-1$, we see that $d = 2^k$ is a proper divisor of n. Also, $\sigma(n) = (2^t - 1)(2^t - 2^k)$. Since

$$\sigma(n) - 2n = (2^t - 1)(2^t - 2^k) - 2^t(2^t - 2^k - 1) = 2^k,$$

the proposition follows. □

Unfortunately, the converse of Proposition 1 fails, even if we restrict our attention to even near-perfect numbers. For example, 650 is near-perfect with redundant divisor 2, but does not arise from the construction of Proposition 1.

It appears plausible that for each fixed k, there are infinitely many primes of the form $2^t - 2^k - 1$. (See [1] for a careful discussion of conjectures of this form.) Thus, Theorem 1 suggests the following conjecture.

Conjecture 2. *For each fixed* k, *there exist infinitely many near-perfect numbers with redundant divisor* 2^k.

Let $\mathcal{P} = \bigcup_{k=1}^{\infty} \mathcal{P}_k$ be the collection of all primes which belong to at least one of the sets $\mathcal{P}_k$. The first several primes from $\mathcal{P}$ are (cf. our sequence A181741 in [11])

$$3, 5, 7, 11, 13, 23, 29, 31, 47, 59, 61, 127, 191, 223, 239, \ldots \tag{2.1}$$

Note that all Mersenne primes are in the sequence. Indeed, if a prime p has form $p = 2^r - 1$, then $p = 2^{r+1} - 2^r - 1 \in \mathcal{P}_r$. We also remark that if p is in the sequence (2.1), then it belongs to exactly one set $\mathcal{P}_k$; indeed, k is the unique integer for which $2^k \parallel p + 1$.

Our second construction builds near-perfect numbers from even perfect numbers.

Proposition 3. *A number* n *of the form* $n = 2^j m$, *where* m *is even-perfect, is a near-perfect number if and only if either* $j = 1$ *or* $j = p$, *where* p *is that prime for which* $2^{p-1} \parallel m$.

Proof. By Euclid's Theorem A, we have $m = 2^{p-1}(2^p - 1)$, where p and $2^p - 1$ are prime. Therefore, $n = 2^{p+j-1}(2^p - 1)$. Also,

$$\sigma(n) - 2n = (2^{j+p} - 1)2^p - 2^{j+p}(2^p - 1) = 2^p(2^j - 1).$$

This is a proper divisor of n if and only if either $j = p$ or $j = 1$. □

We see from Proposition 3 that every even perfect number $m = 2^{p-1}(2^p - 1)$ generates two distinct near-perfect numbers $n_1 = 2m$ and $n_2 = 2^p m$. Note that n_1 could also been constructed using Proposition 1 (with $t = p + 1$ and $k = p$), but n_2 is not given by that result.

Our final construction is a very close analogue of Euclid's Theorem A.

Proposition 4. *If both p and $2^p - 1$ are prime numbers, then $n = 2^{p-1}(2^p - 1)^2$ is near-perfect with redundant divisor $2^p - 1$.*

Proof. We have

$$\sigma(n) - 2n = (2^p - 1)((2^p - 1)^2 + (2^p - 1) + 1) - 2^p(2^p - 1)^2 = 2^p - 1. \qquad \square$$

Propositions 3 and 4 have the following amusing consequence: *Every even perfect number is the difference of two near-perfect numbers.* Indeed, if $m = 2^{p-1}(2^p - 1)$ is even-perfect, then $m = n_2 - n_3$, where $n_2 = 2^p m$ and $n_3 = (2^p - 1)m$ are near-perfect.

The numerical data on near-perfect numbers suggests a number of further questions, which we urge upon the interested reader:

- From (1.2), it appears rare for a near-perfect number to have an odd redundant divisor. Is it true that if n is an even near-perfect numbers with an odd redundant divisor, then this divisor is a Mersenne prime (as in Proposition 4)?
- We conjectured above that every power of 2 appears as the redundant divisor of infinitely many near-perfect numbers. Is it true that if ℓ is not a power of 2, then ℓ is the redundant divisor of at most one near-perfect number?

If the answer to both of these questions were affirmative, we would easily obtain the following partial converse of Proposition 4 (compare with Theorem B): *Every even near-perfect number n with odd redundant divisor has the form $n = 2^{p-1}(2^p - 1)^2$, where p and $2^p - 1$ are primes.*

Remark. In 2010 (see sequence A181595 [11]) the second-named author conjectured that all near-perfect numbers are even. It is easy to see that any counterexample must be a perfect square. At the beginning of 2012, Donovan Johnson (private communication) found the counterexample $173369889 = 3^4 \cdot 7^2 \cdot 11^2 \cdot 19^2$.

3. An upper bound on the number of near-perfect numbers

The goal of this section is to establish the following estimate, announced already in the introduction.

Theorem 5. *The number of near-perfect numbers $n \le x$ is at most $x^{5/6+o(1)}$, as $x \to \infty$.*

For comparison, it was established by Hornfeck and Wirsing [4] (compare with [12]) that the number of perfect numbers up to x is $x^{o(1)}$, as $x \to \infty$. It seems plausible that their stronger estimate also holds for the near-perfect numbers, but this seems difficult. We do not even know how to prove such an upper bound for the near-perfect numbers with redundant divisor 1, even though not a single example of such a number is known!

The proof of Theorem 5 requires some preparation. We begin by recalling Gronwall's determination of the maximal order of the sum-of-divisors function [3, Theorem 323].

Proposition 6 (Gronwall)**.** *As $n \to \infty$, we have $\limsup \frac{\sigma(n)}{n \log\log n} = e^\gamma$, where $\gamma = 0.57721\ldots$ is the Euler–Mascheroni constant.*

The next proposition, extracted from [5, Theorem 1.3], asserts that $\gcd(n, \sigma(n))$ is small on average. It may be thought of as a generalization of the Hornfeck–Wirsing upper bound.

Proposition 7. *For each $x \geq 3$, we have*

$$\sum_{n \leq x} \gcd(n, \sigma(n)) \leq x^{1+C/\sqrt{\log\log x}},$$

where C is an absolute positive constant.

The next lemma concerns solutions to the congruence $\sigma(n) \equiv a \pmod{n}$. For a given a, we divide the solutions n to this congruence into two classes: by a *trivial solution*, we mean a natural number

$$n = pm, \quad \text{where } p \text{ is a prime not dividing } m, \quad m \mid \sigma(m), \quad \text{and} \quad \sigma(m) = a. \tag{3.1}$$

(It is straightforward to check that all such n satisfy $\sigma(n) \equiv a \pmod{n}$.) All other solutions are called *sporadic*. Pomerance [8, Theorem 3] showed that for each fixed a, the number of sporadic solutions to $\sigma(n) \equiv a \pmod{n}$ with $n \leq x$ is at most

$$x/\exp((1/\sqrt{2} + o(1))\sqrt{\log x \log\log x}), \tag{3.2}$$

as $x \to \infty$. Theorem 5 requires a stronger bound, with attention paid to uniformity in a.

Proposition 8. *Let $x \geq 3$, and let a be an integer with $|a| < x^{2/3}$. Then the number of sporadic solutions $n \leq x$ to the congruence $\sigma(n) \equiv a \pmod{n}$ at most $x^{2/3+o(1)}$. Here the $o(1)$ term decays to 0 as $x \to \infty$, uniformly in a.*

Remark. In addition to the congruence $\sigma(n) \equiv a \pmod{n}$, Pomerance [8] also treats the congruence $n \equiv a \pmod{\phi(n)}$, proving the same upper bound (3.2) for the number of "nontrivial" solutions $n \leq x$. (Here *nontrivial* has a related, but different, meaning than before.) He returned to this latter congruence in the papers [6], [7], which sharpen the upper bound to $x^{2/3+o(1)}$ and $x^{1/2+o(1)}$, respectively (again, for each fixed a). Our proof of Proposition 8 relies on the method of [6]. It would be interesting to improve the exponent to 2/3 to 1/2, as in [7], but this does not seem easy.

Proof. We may assume that the squarefull part of n is bounded by $x^{2/3}$, since the number of $n \leq x$ for which this condition fails is

$$\ll x \sum_{\substack{m > x^{2/3} \\ \text{squarefull}}} \frac{1}{m} \ll x^{2/3}.$$

(We use here that the counting funciton of the squarefull numbers is $\ll x^{1/2}$.) We also assume, as is clearly permissible, that $n > x^{2/3}$.

Consider first the case when the largest prime factor p of n satisfies $p > x^{1/3}$. Say that $n = mp$, so that $m \leq x^{2/3}$. By our condition on the squarefull part of n, we see that $p \nmid m$. Write $\sigma(n) = nq + a$, where q is a nonnegative integer; from Lemma 6, $q \ll \log\log x$. Observe that

$$\sigma(m)(p+1) = \sigma(mp) = qmp + a,$$

so that

$$p(\sigma(m) - qm) = a - \sigma(m). \tag{3.3}$$

If $\sigma(m) - qm = 0$, then (3.3) implies that $a = \sigma(m)$; referring back to the definitions we see that n is a trivial solution to the congruence $\sigma(n) \equiv a \pmod{n}$, contrary to hypothesis. Thus, $\sigma(m) - qm \neq 0$, and now (3.3) shows that p is uniquely determined given m and q. Since the number of possibilities for m is at most $x^{2/3}$, while $q \ll \log\log x$, the number of n that arise in this manner is $\ll x^{2/3}\log\log x$, which is acceptable for us.

Now suppose that the largest prime factor of n does not exceed $x^{1/3}$. We claim that n has a unitary divisor m from the interval $(x^{1/3}, x^{2/3}]$. The claim obviously holds if every prime power divisor of n is bounded by $x^{1/3}$. Otherwise, $p^e \parallel n$ for some prime power $p^e > x^{1/3}$ (with $e > 1$). In this case, $p^e \leq x^{2/3}$ by our restriction on the squarefull part of n, and so we can take $m = p^e$.

Since m is a unitary divisor of n, it follows that

$$\sigma(n) \equiv 0 \pmod{\sigma(m)} \quad \text{and} \quad \sigma(n) \equiv a \pmod{m}.$$

This places $\sigma(n)$ is a uniquely-defined residue class modulo $[m, \sigma(m)]$. Thus, summing over $m \in (x^{1/3}, x^{2/3}]$, we have that the number of values $\sigma(n)$ that can arise this way is at most

$$\begin{aligned}\sum_{x^{1/3}<m\le x^{2/3}} \left(\frac{x}{\operatorname{lcm}[m,\sigma(m)]}+1\right) &\le x^{2/3} + x \sum_{x^{1/3}<m\le x^{2/3}} \frac{\gcd(m,\sigma(m))}{m\sigma(m)} \\ &\le x^{2/3} + x \sum_{x^{1/3}<m\le x^{2/3}} \frac{\gcd(m,\sigma(m))}{m^2}. \qquad (3.4)\end{aligned}$$

Letting $A(t) = \sum_{m\le t} \gcd(m, \sigma(m))$, the final sum in (3.4) is given by

$$\begin{aligned}\int_{x^{1/3}}^{x^{2/3}} \frac{1}{t^2}\, dA(t) &\le A(x^{2/3})x^{-4/3} + 2\int_{x^{1/3}}^{x^{2/3}} A(t)t^{-3}\, dt \\ &\le x^{-2/3+o(1)} + x^{-1/3+o(1)} = x^{-1/3+o(1)},\end{aligned}$$

where we use the estimate of Proposition 7 for $A(t)$. Referring back to (3.4), we see that the number of values $\sigma(n)$ that can arise is at most $x^{2/3+o(1)}$. Since $\sigma(n) = qn + a$, the values $\sigma(n)$ and q uniquely determine n. Since the number of possible values of q is $\ll \log\log x = x^{o(1)}$ (as above), and there are only $x^{2/3+o(1)}$ possible values of $\sigma(n)$, there are also only $x^{2/3+o(1)}$ possible values of n. $\square$

Proof of Theorem 5. We can assume that $n > x^{5/6}$. Write $\sigma(n) = 2n + d$, where d is a proper divisor of n. If $d > x^{1/6}$, then $\gcd(n, \sigma(n)) = d > x^{1/6}$. By Proposition 7, the number of such $n \le x$ is at most $x^{5/6+o(1)}$.

So suppose that $d \le x^{1/6}$. In this case, we observe that $\sigma(n) \equiv d \pmod{n}$ and apply Proposition 8. Let us check that our near-perfect number n is not a trivial solution to this congruence. If it were, then we could write n in the form (3.1), with 'd' in place of 'a'. Then

$$(p+1)d = (p+1)\sigma(m) = \sigma(mp) = 2mp + d,$$

so that $d = 2m$. But then d and pm have the same number of prime factors (counted with multiplicity), contradicting that d is a proper divisor of n. So n is a sporadic solution, and thus the number of possibilities for n, given d, is at most $x^{2/3+o(1)}$. Summing over values of $d \le x^{1/6}$, we see the number of n that arise in this way is at most $x^{5/6+o(1)}$. $\square$

References

1. M. Filaseta, C. Finch, and M. Kozek, *On powers associated with Sierpiński numbers, Riesel numbers and Polignac's conjecture*, J. Number Theory **128** (2008), no. 7, 1916–1940.
2. R. K. Guy, *Unsolved problems in number theory*, 3rd ed., Problem Books in Mathematics, Springer-Verlag, New York, 2004.
3. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, sixth ed., Oxford University Press, Oxford, 2008.
4. B. Hornfeck and E. Wirsing, *Über die Häufigkeit vollkommener Zahlen*, Math. Ann. **133** (1957), 431–438.
5. P. Pollack, *On the greatest common divisor of a number and its sum of divisors*, Michigan Math. J. **60** (2011), no. 1, 199–214.
6. C. Pomerance, *On composite n for which $\varphi(n)n - 1$*, Acta Arith. **28** (1975/76), no. 4, 387–389.
7. ———, *On composite n for which $\varphi(n) \mid n - 1$. II*, Pacific J. Math. **69** (1977), no. 1, 177–186.
8. Carl Pomerance, *On the congruences $\sigma(n) \equiv a (\mathrm{mod}\ n)$ and $n \equiv a (\mathrm{mod}\ \varphi(n))$*, Acta Arith. **26** (1974/75), no. 3, 265–272.
9. J. Sándor and B. Crstici, *Handbook of number theory. II*, Kluwer Academic Publishers, Dordrecht, 2004.
10. W. Sierpiński, *Sur les nombres pseudoparfaits*, Mat. Vesnik **2 (17)** (1965), 212–213.
11. N. J. Sloane, *The online encyclopedia of integer sequences.*

12. E. Wirsing, *Bemerkung zu der Arbeit über vollkommene Zahlen*, Math. Ann. **137** (1959), 316–318.

University of British Columbia, Department of Mathematics, 1984 Mathematics Road, Vancouver, BC V6T 1Z2 Canada

E-mail address: pollack@math.ubc.ca

Department of Mathematics, Ben-Gurion University of the Negev, Beer-Sheva 84105, Israel

E-mail address: shevelev@bgu.ac.il