Finiteness theorems for perfect numbers and their kin

Paul Pollack

Abstract

Since ancient times, a natural number has been called *perfect* if it equals the sum of its proper divisors; e.g., $6 = 1+2+3$ is a perfect number. In 1913, Dickson showed that for each fixed k, there are only finitely many odd perfect numbers with at most k distinct prime factors. We show how this result, and many like it, follow from embedding the natural numbers in the *supernatural numbers* and imposing an appropriate topology on the latter; the notion of sequential compactness plays a starring role.

1 Introduction.

Quick: You're handed an infinite sequence of points in a compact subset of $\mathbf{R}^n$ – what do you do? Probably your first instinct is to pass to a convergent subsequence and examine the limit. This fruitful proof technique in analysis does not have an obvious analogue in number theory. Certainly an unbounded sequence of natural numbers has a subsequence that tends to infinity, but this is seldom useful information; it is clear that the standard topology on $\mathbf{N}$ was prescribed by analysts and not more arithmetically-minded individuals. What would matters be like if number theorists ran the world and could define convergence the way they saw fit?

Our purpose in this article is two-fold. First, to provide a glimpse into this utopia (dystopia?). Second (but primarily), to highlight some results about perfect numbers, amicable numbers, and their close relatives that deserve to be better known and whose demonstrations underscore the usefulness of these "sequential" methods.

Recall that a *perfect number* is a number N for which $s(N) = N$, where $s(N) := \sum_{D|N,\ D<N} D$ denotes the sum of the proper divisors of N. For example, $N = 28$ is perfect, since $28 = 1+2+4+7+14$. The study of such numbers goes back at least to Euclid (ca. 300 BCE), who showed in his *Elements* that if $2^n - 1$ is prime, then

$$N := 2^{n-1}(2^n - 1) \tag{1}$$

is a perfect number. Two thousand years later, Euler showed that every *even* perfect number arises in this manner. We expect, but cannot prove, that $2^n - 1$ is prime infinitely often; to date, 47 examples of such *Mersenne primes* have

been found, the largest corresponding to $n = 43112609$. The situation for odd perfect numbers is less satisfactory. We know of no examples, but despite over two thousand years of effort, we cannot prove that none exist.

Short of such a proof, one could hope to prove something a bit weaker. Perhaps one can show that there are at most finitely many odd perfect numbers? Again, this seems difficult. We know from work of Hornfeck and Wirsing ([20]; see also [37]) that the odd perfect numbers are sparsely distributed; for any $\epsilon > 0$, the number of such up to x is $< x^\epsilon$, once $x > x_0(\epsilon)$. If we insist on finiteness, then the best result we have is the following 1913 theorem of Dickson [9]. We write $\omega(N) := \sum_{p|N} 1$ for the number of distinct prime divisors of N.

Theorem 1. *For each positive integer k, there are at most finitely many odd perfect numbers N with $\omega(N) \leq k$.*

If N has the form (1), where $2^n - 1$ is prime, then $\omega(N) = 2$. So one consequence of Dickson's theorem is that there are no infinite families of odd perfect numbers which are as easy to write down as the (presumably) infinite family (1) of even perfects.

What does Dickson's theorem have to do with the arithmetician's dream-world alluded to at the start of this article? As shown by Shapiro [31], Dickson's theorem can be proved very simply using the notion of compactness, once one writes down the correct topology! We turn to a description of this topology in the next section. It will transpire that Dickson's theorem is just one of several results that suddenly become visible from this topological perspective.

To avoid misunderstanding, it should be emphasized that compactness already plays a well-recognized, fundamental role in many number theoretic arguments. Indeed, topological considerations are so prevalent in the algebraic-analytic theory that Weil includes Haar measure on locally compact groups as a prerequisite for his book titled *Basic Number Theory* [36] (such choices on Weil's part were not without controversy, however; e.g., see the anecdote of [33, p. 139]). Also, in that part of combinatorial number theory that overlaps with Ramsey theory, compactness arguments are routinely used to show that if no infinite colorings of a certain kind exist, then the same is true for sufficiently large finite colorings; see [15, §1.5] for a general theorem of this kind. What we are offering is a bit different; we take existing theorems of the sort that could be presented in a first number theory course and propose a new, unifying topological perspective on their proofs that both clarifies and motivates the arguments. In this program, we have been inspired by Furstenberg's topological proof of the infinitude of primes [11].

2 What could be more natural?

Let $\mathbf{N}$ denote the set of natural numbers (positive integers), and let $\mathbf{N}_{\geq 0} := \mathbf{N} \cup \{0\}$ be the set of nonnegative integers. Define a *supernatural number* (also called a *Steinitz number*) as a formal product $\prod_p p^{v_p}$, where p runs over all primes and each $v_p \in \mathbf{N}_{\geq 0} \cup \{\infty\}$. The set $\mathscr{S}$ of all supernatural numbers forms

a multiplicative semigroup with multiplication defined by exponent addition, and the multiplicative semigroup of natural numbers $\mathbf{N}$ embeds into it by unique factorization.

If N is a supernatural number, we will write $v_p(N)$ for the exponent of p appearing in N. The *support* of N is the set of primes p for which $v_p(N) > 0$. If D and N are supernatural numbers, we say that D *divides* N, written $D \mid N$, if $N = DD'$ for some supernatural D', or equivalently, if $v_p(D) \leq v_p(N)$ for all primes p.

The supernatural numbers were introduced in Steinitz's influential 1910 paper *Algebraische Theorie der Körper* ([34]; see also [30]), which was the first systematic development of field theory from an axiomatic viewpoint. They arise in Steinitz's description of the algebraic closure $\bar{\mathbf{F}}_p$ of the prime field $\mathbf{F}_p$: For each supernatural N, the elements of $\bar{\mathbf{F}}_p$ algebraic of degree dividing N form a subfield; conversely, every subfield of $\bar{\mathbf{F}}_p$ arises in this way from a uniquely determined supernatural number N.

We are interested in the supernatural numbers for a different reason: They allow us to assign arithmetically meaningful limits to certain sequences of natural numbers. Our fundamental idea is to choose a topology on $\mathscr{S}$ so that if $\{N_i\}_{i=1}^{\infty}$ is a sequence of supernatural numbers, and $N \in \mathscr{S}$, then

$$\lim_{i\to\infty} N_i = N \iff \text{for every prime } p, \quad \lim_{i\to\infty} v_p(N_i) = v_p(N), \tag{2}$$

where the limit on the right-hand side is the usual limit from elementary calculus (adopting the standard conventions about infinite limits).

Such a topology is not hard to come by. Write $\widehat{\mathbf{N}} := \mathbf{N}_{\geq 0} \cup \{\infty\}$, and view $\widehat{\mathbf{N}}$ as the closure of $\mathbf{N}_{\geq 0}$ in $\widehat{\mathbf{R}} := \mathbf{R} \cup \{\infty\}$, the one-point compactification of $\mathbf{R}$. Using subscripts on X to denote a copy of the space X, identify $\mathscr{S}$ with $\prod_p \widehat{\mathbf{N}}_p$, mapping $\prod_p p^{e_p}$ to the exponent vector $(e_2, e_3, e_5, \dots)$. It follows quickly from the definition of the product topology that our desired convergence criterion (2) holds.

Given all the fuss we have made over compactness, one might hope that this topology makes $\mathscr{S}$ into a sequentially compact space. This is indeed true! Each factor $\widehat{\mathbf{N}}_p$ is sequentially compact for the boring reason mentioned in the introduction. A sequence of natural numbers is either bounded or has a subsequence that tends to infinity. And by a well-known diagonalization argument, a countable product of sequentially compact spaces is sequentially compact.

How do sums of divisors enter the picture? For a natural number N, its *abundance* is defined by $h(N) := \sigma(N)/N$, where $\sigma(N) := \sum_{D|N} D$ is the usual sum-of-divisors function from elementary number theory (in contrast with the definition of s, note that the number N itself appears in the sum). For example, N is perfect precisely when $h(N) = 2$. While σ does not seem to have a useful extension to $\mathscr{S}$, the function h does; namely, put

$$h(p^\infty) = \lim_{v\to\infty} h(p^v) = \lim_{v\to\infty} \left(1 + \frac{1}{p} + \cdots + \frac{1}{p^v}\right) = \frac{p}{p-1},$$

and define $h(\prod_p p^{v_p}) = \prod_p h(p^{v_p})$, where the product is understood as ∞ if divergent.

In the sequel, we will need the following two properties of h, which respectively describe how h interacts with the topology on $\mathscr{S}$ and the lattice structure of $\mathscr{S}$:

(i) For each natural number B, let $\mathscr{S}^B$ denote the set of supernatural numbers whose support has size bounded by B. We leave as an exercise the task of checking that $\mathscr{S}^B$ is a closed subset of $\mathscr{S}$, and that the restriction of h to $\mathscr{S}^B$ defines a continuous function to $\widehat{\mathbf{R}}$.

(ii) The function h is monotonic along the divisor lattice. More precisely, if N and N' are two supernatural numbers for which $N \mid N'$, and $h(N') < \infty$, then $h(N) \leq h(N')$, with equality only if $N = N'$. This is immediate from the definitions, noting that for each fixed prime p, the function $h(p^v)$ is strictly increasing in v, for $0 \leq v \leq \infty$.

One more piece of notation before we see some applications: If D and N are supernatural numbers, we say that D is *a unitary divisor* of N, and write $D \parallel N$, if $v_p(D) = v_p(N)$ for every prime p dividing D. The key example is the following: If $N_i \to N$, and D is a natural number for which $D \parallel N$, then $D \parallel N_i$ for all but finitely many indices i.

3 Getting something for (almost) nothing: Ω results.

As a first illustration of how these topological ideas are useful, let us consider the following simpler variant of Dickson's theorem. We write $\Omega(N) := \sum_{p^k \mid N} 1$ for the total number of prime divisors of N, counted with multiplicity.

Theorem 2. *Let α be a rational number, and let k be a positive integer. There are only finitely many natural numbers N for which $\sigma(N)/N = \alpha$ and $\Omega(N) \leq k$.*

Theorem 2 is in one sense weaker than Dickson's theorem, since requiring that $\Omega(n)$ be bounded is much stronger than requiring the same for $\omega(n)$. Note, though, that Theorem 2 is not restricted to odd N, and that the result is stated for any α, not just $\alpha = 2$. When $\alpha = 2$, Hare [17] showed that there are in fact no odd solutions with $\Omega(N) < 75$ and Nielsen [26] that there are none with $\omega(N) < 9$.

After our mini-course on supernatural topology, the proof of Theorem 2 is almost an exercise in definition-chasing.

Proof of Theorem 2. For our later attack on Theorem 1 (and Theorem 5 below), it is convenient to prove the result in the following alternative formulation. If $\{N_i\}_{i=1}^{\infty}$ is an infinite sequence of distinct natural number solutions to $h(N_i) = \alpha$ all of which satisfy $\omega(N_i) \leq k$, then the sequence $\{\Omega(N_i)\}_{i=1}^{\infty}$ is unbounded.

Passing to a convergent subsequence of the N_i in the supernatural topology, we can suppose that $N_i \to N_\infty$ (say), where $N_\infty \in \mathscr{S}$. Since each $N_i \in \mathscr{S}^k$, the limit $N_\infty \in \mathscr{S}^k$. Since $h|_{\mathscr{S}^k}$ is continuous, $h(N_\infty) = \lim h(N_i) = \alpha$. Thus, we may write

$$N_\infty = N' N''^\infty,$$

where N' and N'' are relatively prime natural numbers with N'' squarefree. Here N' encodes the contribution to N_∞ from those primes p for which the exponents $v_p(N_i)$ stabilize (as $i \to \infty$), while N'' is the product of those primes p for which the exponents $v_p(N_i)$ shoot off to infinity.

We know that $N' \parallel N_i$ for all but finitely many i and that there is at most one value of i with $N' = N_i$. Hence, N' is a proper divisor of N_i for all large i. Choosing such an i and recalling the monotonicity property of h, we find that $h(N') < h(N_i) = \alpha$. Since $h(N_\infty) = \alpha$, clearly $N' \neq N_\infty$, so that $N'' > 1$.

Now pick a prime p dividing N''. The total number $\Omega(N_i)$ of prime factors of N_i satisfies $\Omega(N_i) \geq v_p(N_i)$ for each i, while our convergence criterion (2) gives that $v_p(N_i) \to v_p(N_\infty) = \infty$. The theorem follows. □

What else is this method good for? Recall that an *amicable pair* is a pair of distinct natural numbers N and M for which each is the sum of the proper divisors of the other; in other words, $s(N) = M$ and $s(M) = N$. For example, $N = 220$ and $M = 284$ form an amicable pair, since

$$\begin{aligned} 220 &= 1 + 2 + 4 + 71 + 142, \quad \text{while} \\ 284 &= 1 + 2 + 4 + 5 + 10 + 11 + 20 + 22 + 44 + 55 + 110. \end{aligned}$$

The amicable numbers, like their perfect brethren, have an ancient pedigree. According to the Neoplatonic philosopher Iamblichus, writing in the third century CE (see [35, pp. 122–123]):

> ... 284 and 220 are [amicable numbers]; for the parts of each are generative of each other according to the nature of friendship, as was shown by Pythagoras. For someone asking him what a friend was, he answered ἕτερος εγω [=another I], which is demonstrated to take place in these numbers.

We have all the tools necessary to prove the following amicable pair analogue of Theorem 2. A stronger result will be established as Theorem 8 in §5.

Theorem 3. *Fix a natural number k. Then there are only finitely many amicable pairs (N, M) for which $\Omega(NM) \leq k$.*

Proof of Theorem 3, following Borho [5, §5]. We follow our nose, attempting to mimic the proof of Theorem 2. We will suppose that $\{(N_i, M_i)\}_{i=1}^\infty$ is an infinite sequence of distinct amicable pairs for which $\omega(N_i M_i)$ is bounded and will show that this forces $\Omega(N_i M_i)$ to be unbounded. Since $\mathscr{S} \times \mathscr{S}$ is sequentially compact, after passing to a subsequence, we can assume that $(N_i, M_i) \to (N_\infty, M_\infty)$.

Since $\omega(N_i M_i)$ is bounded, it follows that N_∞ and M_∞ are both supported on at most finitely many primes. Thus, we can write

$$M_\infty = M' M''^\infty \quad \text{and} \quad N_\infty = N' N''^\infty,$$

where M', M'', N', N'' are natural numbers, $\gcd(M', M'') = \gcd(N', N'') = 1$, and M'', N'' are squarefree. Comparing with the proof of Theorem 2, we see it is enough to show that either $N'' > 1$ or $M'' > 1$.

The proof of Theorem 2 depended on taking the limit of the sequence of equations $h(N_i) = 2$. An analogue in the amicable case is

$$\begin{aligned}(h(N_i) - 1)(h(M_i) - 1) &= \left(\frac{\sigma(N_i) - N_i}{N_i}\right)\left(\frac{\sigma(M_i) - M_i}{M_i}\right) \\ &= \frac{s(N_i)}{N_i}\frac{s(M_i)}{M_i} = \frac{M_i}{N_i}\frac{N_i}{M_i} = 1,\end{aligned}$$

which, upon passing to the limit, gives

$$(h(N_\infty) - 1)(h(M_\infty) - 1) = 1. \tag{3}$$

Now choose i large enough that N' and M' are unitary divisors of N_i and M_i (respectively) and so that the pair $(N', M') \neq (N_i, M_i)$. Then by the monotonicity of h,

$$1 = (h(N_i) - 1)(h(M_i) - 1) > (h(N') - 1)(h(M') - 1). \tag{4}$$

Comparing (3) and (4), we see that $(N', M') \neq (N_\infty, M_\infty)$. So either $N'' > 1$ or $M'' > 1$, as desired. □

In the early part of the 20th century, two competing generalizations of amicable pairs were introduced:

- Meissner [24, p. 200] proposed investigating what are now known as *sociable numbers*. Here $N \in \mathbf{N}$ is called *k-sociable* if the sequence of iterates N, $s(N)$, $s(s(N))$, ... is purely periodic with exact period k (see [23] for more of the history and some recent results). Then the perfect numbers are exactly the sociable numbers of order 1, while the sociable numbers of order 2 are precisely those integers which belong to an amicable pair. Higher-order sociable numbers exist as well; e.g., Poulet [28] discovered that iterating the map s produces the 5-element cycle

$$\cdots \mapsto 12496 \mapsto 14288 \mapsto 15472 \mapsto 14536 \mapsto 14264 \mapsto 12496 \mapsto \cdots.$$

- Dickson [8] proposed calling $(N_1, \ldots, N_k)$ an *amicable k-tuple* if

$$\sigma(N_i) = N_1 + \cdots + N_k \quad \text{for all } 1 \leq i \leq k,$$

  and he gave a handful of examples when $k = 3$ (many more examples were collected by Poulet in his tract *La Chasse aux Nombres* [29, Chapitre IV]). It is simple to check that two distinct integers N_1 and N_2 form an amicable pair precisely when (N_1, N_2) is an amicable 2-tuple in Dickson's sense.

The following theorem of Borho (cf. [5, §5]) generalizes Theorem 3 in both directions.

Theorem 4. *Let k and K be natural numbers, with $k \geq 2$.*

(i) There are only finitely many k-sociable numbers N for which the product of the elements $N, s(N), \ldots, s_{k-1}(N)$ has at most K prime factors, counted with multiplicity.

(ii) There are only finitely many amicable k-tuples $(N_1, \ldots, N_k)$ for which the product $N_1 \cdots N_k$ has at most K prime factors, counted with multiplicity.

At this point, the proof of Theorem 4 can be safely left as an exercise. Part (i) follows the proof of Theorem 3. The proof of (ii) is similar, but one should first observe that the definition of an amicable k-tuple gives

$$\begin{aligned}\frac{1}{h(N_1)} + \frac{1}{h(N_2)} + \cdots + \frac{1}{h(N_k)} &= \frac{N_i}{\sigma(N_i)} + \cdots + \frac{N_k}{\sigma(N_k)} \\ &= \frac{N_1}{N_1 + \cdots + N_k} + \frac{N_2}{N_1 + \cdots + N_k} + \cdots + \frac{N_k}{N_1 + \cdots + N_k} = 1. \quad (5)\end{aligned}$$

4 Dickson's theorem revisited.

We have already seen how to prove some variants of Theorem 1. In order to prove Theorem 1 itself, we have to work a little harder, but not much. The argument below is due to Shapiro [31] (compare to Gradstein [14, Chapter II, §§3–7]).

Proof. We start exactly as in Theorem 2. Fix a natural number k, and suppose that there are infinitely many odd perfect N with $\omega(N) \leq k$. Take an infinite sequence N_i of distinct such N. Passing to a subsequence, we can assume that $N_i \to N_\infty$. Exactly as in the proof of Theorem 2, we may write $N_\infty = N'N''^\infty$, where N' and N'' are coprime natural numbers and N'' is squarefree. Since each N_i is odd, we see easily that $N'N''$ is also odd. From the proof of Theorem 2, we have $N'' > 1$.

Let us write q for the primes dividing N' and r for those dividing N''. Since $N'' > 1$, there is at least one such r. Writing $v_q = v_q(N')$, we have

$$2 = h(N_\infty) = h(N')h(N''^\infty) = \prod_q \frac{q^{v_q+1} - 1}{q^{v_q}(q-1)} \prod_r \frac{r}{r-1}, \quad (6)$$

and thus

$$2\left(\prod_q q^{v_q}\right)\prod_r (r-1) = \prod_q \frac{q^{v_q+1}-1}{q-1}\prod_r r.$$

Since each r is coprime to $2\prod q^{v_q}$, it follows that

$$\prod_r r \mid \prod_r (r-1).$$

But this is impossible; the left-hand side is larger than the right. □

A clever modification of this argument gives Theorem 1 with the number "2" replaced by any rational α.

Theorem 5. *Let α be a rational number, and let k be a positive integer. There are only finitely many odd natural numbers N for which $\sigma(N)/N = \alpha$ and $\omega(N) \le k$.*

Proof. We imitate the proof of Theorem 1 up until (6), which now takes the shape $\alpha = h(N') \prod_r \frac{r}{r-1}$. Choose an index i large enough to guarantee that $N' \parallel N_i$. Writing $N_i = N'Q_i$ gives $\alpha = h(N')h(Q_i)$, and so $h(Q_i) = \prod_r \frac{r}{r-1}$. Thus,

$$\prod_s \frac{1 + s + s^2 + \cdots + s^{v_s}}{s^{v_s}} = \prod_r \frac{r}{r-1},$$

where s runs over the prime divisors of Q_i and $v_s := v_s(Q_i)$. This is absurd; the right-hand product has even denominator in lowest terms (since there is at least one r), while the left has odd denominator. □

This proof of Theorem 5 is due to Artjuhov [2], who is perhaps best-known for anticipating [1] the Selfridge–Miller–Rabin strong pseudoprimality test implemented in most computer algebra systems (for details of this test, see, e.g., [7, §3.5]).[1] It may seem that the proof of Theorem 5 renders Shapiro's argument obsolete, but this is not the case; Shapiro's method (but not Artjuhov's) also gives results for what are called *primitive α-abundant* numbers. See Shapiro's papers [31, 32] for details.

By methods beyond the scope of this article, Kanold [22] proved the following elegant common generalization of Theorems 1, 2, and 5 (a narrower form of which was conjectured in [21]).

Theorem 6. *Let α be a rational number, and let k be a positive integer. Among all solutions N to the equation $\sigma(N)/N = \alpha$ for which $\omega(N) \le k$, all but finitely many have the form $N = AB$, where A is an even perfect number, $\sigma(B)/B = \alpha/2$, and $\gcd(A, B) = 1$.*

It is somewhat satisfying that Kanold's argument makes essential use of Siegel's theorem, perhaps the best-known finiteness theorem in number theory, which states that a curve of positive genus has only finitely many integral points.

5 A more perfect result on amicable numbers.

We saw in Theorem 3 that for any prescribed bound k, there are only finitely many amicable pairs with $\Omega(NM) \le k$. Ideally, we would like to have the same result with Ω replaced by ω. Even if this is true – and no one has presented compelling arguments either way – it appears hopeless to prove.

[1] Correction: What Artjuhov describes is the Solovay–Strassen test, not the Selfridge–Miller–Rabin test. Thanks to Keith Conrad for pointing this out to me.

To justify this pessimistic assessment, it is helpful to recall a theorem of the ninth century CE mathematician/astronomer Thābit ibn Qurra (see [10, p. 39]).

Proposition 7 (Thābit's rule)**.** *Suppose that for the integer $n > 1$, all three of*

$$p := 3 \cdot 2^{n-1} - 1, \quad q := 3 \cdot 2^n - 1, \quad r := 9 \cdot 2^{2n-1} - 1 \tag{7}$$

are prime numbers. Then $N := 2^n \cdot p \cdot q$ and $M := 2^n \cdot r$ form an amicable pair.

Once written down, Thābit's rule is straightforward to verify. The divisors of N are precisely the integers of the form $2^a p^b q^c$, where $0 \leq a \leq n$ and $b, c \in \{0, 1\}$. Hence,

$$\begin{aligned}\sigma(N) &= \sum_{a=0}^{n} \sum_{b \in \{0,1\}} \sum_{c \in \{0,1\}} 2^a p^b q^c \\ &= \left(\sum_{a=0}^{n} 2^a \right) (1+p)(1+q) = (2^{n+1} - 1) \cdot 9 \cdot 2^{2n-1}.\end{aligned}$$

By a direct calculation, this last expression coincides with the sum $N + M$. Hence, $s(N) = \sigma(N) - N = M$. Similarly, the divisors of M are the numbers $2^a r^b$, where $0 \leq a \leq n$ and $b \in \{0, 1\}$. Thus,

$$\sigma(M) = (2^{n+1} - 1)(1 + r) = (2^{n+1} - 1) \cdot 9 \cdot 2^{2n-1} = N + M,$$

so that $s(M) = \sigma(M) - M = N$. Hence, N and M form an amicable pair. It is not clear how Thābit discovered Proposition 7; see [6] for some speculations.

Of course, the relevance of Proposition 7 to the present discussion is that if N and M come out of Thābit's rule, then $\omega(NM) = 4$.

One might think of Proposition 7 as an analogue of Euclid's rule for generating perfect numbers, quoted in the introduction. However, there is a key respect in which we believe that Euclid was luckier than Thābit. On probabilistic grounds (see, e.g., [7, §1.3]), we expect that there are infinitely many primes of the form $2^n - 1$, so that Euclid's formula (1) should yield infinitely many perfect numbers. But those same heuristic arguments suggest that for large n, *at most one* of p, q, and r in (7) is prime, so that Thābit's rule never gets off the ground. This is borne out by computation; in fact, of the numbers $n \leq 191600$, Thābit's rule applies only for $n = 2, 4$, and 7 (see [12]).

So it would be quite surprising if Thābit's rule actually yields infinitely many amicable pairs. However, given the current state of number-theoretic technology, it would be almost as surprising if anyone were to prove this any time soon! Rigorously (vs. heuristically) understanding arithmetic properties of exponentially-growing expressions like those in (7) is still something of a pipe dream (cognoscenti can consult the last chapter of [19] for a discussion of some of the difficulties involved here). Moreover, even if one could show that Thābit's rule applies only finitely often, there are many other sources of amicable pairs

which would have to be better understood (cf. [4, §6]) in order to prove that $\omega(NM)$ cannot remain bounded. The upshot is that any proof of the analogue of Theorem 3 for distinct prime factors must lie very deep.

So perhaps we should not aim so high. The following theorem is a happy medium between the unattainable and the trivial.

Theorem 8. *Let k be a natural number. There are only finitely many amicable pairs (N, M) for which $\omega(NM) \leq k$ and $\Omega(\gcd(N, M)) \leq k$.*

There is a still-unresolved folklore conjecture (going back at least to Gmelin [13, §10]) that in each amicable pair, the numbers N and M share a common factor > 1. Hagis [16] has shown that there are no counterexamples with $\omega(NM) \leq 21$. Theorem 8 implies that the number of counterexamples with $\omega(NM) \leq k$ is finite for each fixed k.

Theorem 8 is due to Borho [4]; a similar but weaker theorem was published by Artjuhov [3]. Rather than attack Theorem 8 directly, we prove a somewhat stronger (but less easily-stated) result.

Proposition 9. *Let $\{(N_i, M_i)\}_{i=1}^{\infty}$ be an infinite sequence of distinct amicable pairs for which $\omega(N_i M_i)$ is bounded. Then for a certain prime q, each power of q divides some $\gcd(N_i, M_i)$.*

Note that even if there were an infinite sequence of amicable pairs produced by Thābit's rule, this would not contradict Proposition 9, whose conclusion would then hold with $q = 2$.

It will be convenient for the proof of Proposition 9 to abuse notation slightly and, in addition to our earlier use of v_p, to also use $v_p(x)$ for the power of p appearing in the nonzero rational number x (the so-called *p-adic valuation of x*). In other words, if $x \in \mathbf{Q}^{\times}$ has the form $p^n a/b$, where $p \nmid ab$, we write $v_p(x) = n$. Any confusion this may cause is benign, since both definitions of v_p agree on $\mathbf{N} = \mathbf{Q}^{\times} \cap \mathscr{S}$.

Since the following important fact is sometimes omitted from a first course in number theory, we reproduce the proof here.

Lemma 10 (Ultrametric triangle inequality)**.** *Let p be a prime number. If x and y are any rational numbers, then $v_p(x + y) \geq \min\{v_p(x), v_p(y)\}$, with equality unless $v_p(x) = v_p(y)$. Here we interpret $v_p(0)$ as ∞ when it appears.*

Proof. Scaling x and y by an appropriate integer, we may assume that x and y are themselves integral. If either x or y is zero, the claims of the lemma are obvious, so suppose $xy \neq 0$. Let v_1 and v_2 be the largest nonnegative integers for which $p^{v_1} \mid x$ and $p^{v_2} \mid y$. Without loss of generality, $v_1 \leq v_2$. The lower bound in the lemma is just the assertion that p^{v_1} divides $x+y$, which is clear since p^{v_1} is a common divisor of x and y. Suppose now that $v_p(x) \neq v_p(y)$, so that $v_1 < v_2$. If $p^{v_1+1} \mid x+y$, then (since $v_2 \geq v_1+1$) we would have that $p^{v_1+1} \mid (x+y)-y = x$, which is false. Hence, $v_p(x + y) = v_1 = \min\{v_p(x), v_p(y)\}$. □

Proof of Proposition 9, following Borho [4]. We start the argument exactly as in the proof of Theorem 3. Thus, we assume we have passed to a subsequence

where $(N_i, M_i) \to (N_\infty, M_\infty)$, and we suppose that N', M', N'', M'' have the same meaning as in that prior argument. We know from the proof of Theorem 3 that either $N'' > 1$ or $M'' > 1$. So interchanging the roles of N and M if necessary, we can assume that $M'' > 1$. Let q be the largest prime factor of M''. It suffices to show that q also divides N'', for then each fixed power of q divides $\gcd(N_i, M_i)$ for all but finitely many i.

Since N_i and M_i form an amicable pair, (5) gives that $1/h(N_i)+1/h(M_i) = 1$, and so $1/h(N_\infty) + 1/h(M_\infty) = 1$. Since $h(p^\infty) = p/\phi(p)$ (with ϕ the familiar Euler function), this can be rewritten as

$$\frac{N'}{\sigma(N')}\frac{\phi(N'')}{N''} + \frac{M'}{\sigma(M')}\frac{\phi(M'')}{M''} = 1. \tag{8}$$

We will use (8) to establish the desired link between q, which divides the denominator of the second summand, and N'', which appears in the denominator of the first summand.

The number $\phi(M'')$ is a product of terms $r - 1$, with each $r \le q$, so that $q \nmid \phi(M'')$. Since $q \mid M''$ and $\gcd(M', M'') = 1$, also $q \nmid M'$. It follows that the q-adic valuation of the second summand in (8) is negative. Since $v_q(1) = 0$, Lemma 10 forces

$$v_q\left(\frac{N'}{\sigma(N')}\frac{\phi(N'')}{N''}\right) = v_q\left(\frac{M'}{\sigma(M')}\frac{\phi(M'')}{M''}\right) < 0. \tag{9}$$

Assume for the sake of contradiction that $q \nmid N''$. Then (9) shows that $v_q(N'/\sigma(N')) < 0$. For i large enough to ensure that $N' \parallel N_i$, it follows that

$$\begin{aligned} v_q(N_i/\sigma(N_i)) &= v_q(N'/\sigma(N')) + v_q\left(\frac{N_i/N'}{\sigma(N_i/N')}\right) \\ &< v_q\left(\frac{N_i/N'}{\sigma(N_i/N')}\right). \end{aligned}$$

Since $q \nmid N''$, the relation $v_q(N_i) \to v_q(N_\infty)$ shows that eventually $v_q(N_i) = v_q(N')$, and so $v_q(N_i/N') = 0$. We conclude that

$$v_q(N_i/\sigma(N_i)) < 0 \quad \text{for all but finitely many } i. \tag{10}$$

With (10) established, we are nearly out of the woods. Since $N_i/\sigma(N_i) + M_i/\sigma(M_i) = 1$, Lemma 10 and (10) imply that $v_q(M_i/\sigma(M_i)) < 0$. But $v_q(M_i) \to \infty$, since $q \mid M''$. So it must be that $v_q(\sigma(M_i)) \to \infty$ also. Since N_i and M_i form an amicable pair, $N_i = \sigma(M_i) - M_i$, and so $v_q(N_i) \to \infty$ by Lemma 10. This implies that $q \mid N''$, contrary to our assumption. □

Theorem 8 says that only finitely many amicable pairs satisfy given bounds on $\omega(NM)$ and $\Omega(\gcd(N, M))$. Rather than impose a hypothesis on $\gcd(N, M)$, we could instead strengthen the ω-condition by prescribing the actual elements of the support of NM. This also leads to a finiteness result. More precisely, for any finite set of primes $\mathscr{P}$, there are only finitely many amicable pairs for which

the support of NM is a subset of $\mathscr{P}$ (the obvious generalizations for sociable cycles and amicable tuples also hold). We won't prove this here, although the proof is simple and uses nothing beyond the tools that have been on display throughout this article. If the paper had been an infomercial for sequential compactness, now is where we would ask the reader to make that leap of faith and commit. What do you have to lose? There's even a money-back guarantee!

6 Parting shots.

We conclude with some open questions intended as an invitation to further research.

- Because our proofs rely on limiting processes, they appear deafeningly silent on how to compute (even in principle) the finite sets which they assert exist. But already in 1925, Gradstein showed how to convert our proof of Theorem 1 into a procedure to find all odd perfect N with $\omega(N) \leq k$ "by a finite number of tests" (see [14, Theorem 1]). In the more general situation of Kanold's Theorem 6, Pomerance [27] gave an algorithm to compute an upper bound on the finite set in question; in principle, one can then individually examine all numbers up to this upper bound, by brute force. His work easily implies corresponding upper bounds in Theorems 1, 2, and 5.

  For the specific case of odd perfect numbers, one has the following effective version of Theorem 1, which is a sharpening due to Nielsen [25] of a theorem of Heath–Brown [18]. If N is odd perfect and $\omega(N) \leq k$, then $N < 2^{4^k}$. Borho [5, Satz 2] states a cognate result in the situation of Theorem 3: If N and M form an amicable pair with $\Omega(NM) \leq k$, then $NM < k^{2^k}$. This suggests the following question: What about Theorems 4 and 8? For example, is there a doubly-exponential upper bound on the number of coprime amicable pairs satisfying $\omega(NM) \leq k$?

- Theorem 8 is a partial ω-analogue of Theorem 3, one which we were able to obtain by adding an extra condition on the greatest common divisor of M and N. In the generalized-amicable situation of Theorem 4, what conditions should be added to establish an ω-analogue?

- Our final question is more broad. What have we missed? It does not seem too presumptuous to expect that this simple and transparent method has number-theoretic implications beyond those described here.

Acknowledgements. Thanks are owed to Greg Martin, Michael Pollack, Carl Pomerance, Jonah Sinick, Enrique Treviño, Erick Wong, and the referees for helpful comments and conversations.

References

[1] M. M. Artjuhov, Certain criteria for primality of numbers connected with the little Fermat theorem, *Acta Arith.* **12** (1966/1967) 355–364.

[2] ———, On the problem of odd h-fold perfect numbers, *Acta Arith.* **23** (1973) 249–255.

[3] ———, On problems of the theory of amicable numbers, *Acta Arith.* **27** (1975) 281–291.

[4] W. Borho, Befreundete Zahlen mit gegebener Primteileranzahl, *Math. Ann.* **209** (1974) 183–193.

[5] ———, Eine Schranke für befreundete Zahlen mit gegebener Teileranzahl, *Math. Nachr.* **63** (1974) 297–301.

[6] S. Brentjes and J. P. Hogendijk, Notes on Thābit ibn Qurra and his rule for amicable numbers, *Historia Math.* **16** (1989) 373–378.

[7] R. Crandall and C. Pomerance, *Prime numbers: A Computational Perspective*, second edition, Springer, New York, 2005.

[8] L. E. Dickson, Amicable number triples, *Amer. Math. Monthly* **20** (1913) 84–92.

[9] ———, Finiteness of the odd perfect and primitive abundant numbers with n distinct prime factors, *Amer. J. Math.* **35** (1913) 413–422.

[10] ———, *History of the Theory of Numbers. Vol. I: Divisibility and Primality*, AMS Chelsea, Providence, 2002.

[11] H. Furstenberg, On the infinitude of primes, *Amer. Math. Monthly* **62** (1955) 353.

[12] M. García, J. M. Pedersen, and H. te Riele, Amicable pairs, a survey, in *High primes and misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams*, Fields Inst. Commun., vol. 41, American Mathematical Society, Providence, RI, 2004. 179–196.

[13] O. Gmelin, *Über vollkommene und befreundete Zahlen*, Ph.D. thesis, Heidelberg University, Heidelberg, 1917.

[14] I. S. Gradstein, On odd perfect numbers, *Mat. Sbornik* **32** (1925) 476–510.

[15] R. L. Graham, B. L. Rothschild, and J. H. Spencer, *Ramsey Theory*, second edition, Wiley-Interscience Series in Discrete Mathematics and Optimization, Wiley, New York, 1990.

[16] P. Hagis, Jr., On the number of prime factors of a pair of relatively prime amicable numbers, *Math. Mag.* **48** (1975) 263–266.

[17] K. G. Hare, New techniques for bounds on the total number of prime factors of an odd perfect number, *Math. Comp.* **76** (2007) 2241–2248.

[18] D. R. Heath-Brown, Odd perfect numbers, *Math. Proc. Cambridge Philos. Soc.* **115** (1994) 191–196.

[19] C. Hooley, *Applications of Sieve Methods to the Theory of Numbers*, Cambridge Tracts in Mathematics, no. 70, Cambridge University Press, Cambridge, 1976.

[20] B. Hornfeck and E. Wirsing, Über die Häufigkeit vollkommener Zahlen, *Math. Ann.* **133** (1957) 431–438.

[21] H.-J. Kanold, Über einen Satz von L. E. Dickson, *Math. Ann.* **131** (1956) 167–179.

[22] ———, Über einen Satz von L. E. Dickson. II, *Math. Ann.* **132** (1956) 246–255.

[23] M. Kobayashi, P. Pollack, and C. Pomerance, On the distribution of sociable numbers, *J. Number Theory* **129** (2009) 1990–2009.

[24] O. Meissner, Über einige zahlentheoretische Funktionen, *Arch. der Math. u. Phys.* **12** (1907) 199–202.

[25] P. P. Nielsen, An upper bound for odd perfect numbers, *Integers* **3** (2003) article A14, 9 pp. (electronic).

[26] ———, Odd perfect numbers have at least nine distinct prime factors, *Math. Comp.* **76** (2007) 2109–2126.

[27] C. Pomerance, Multiply perfect numbers, Mersenne primes, and effective computability, *Math. Ann.* **226** (1977) 195–206.

[28] P. Poulet, Question 4865, *L'interméd. des Math.* **25** (1918) 100–101.

[29] ———, *La Chasse aux Nombres. I: Parfaits, Amiables et Extensions*, Stevens, Bruxelles, 1929.

[30] P. Roquette, In memoriam Ernst Steinitz (1871–1928), *J. Reine Angew. Math.* **648** (2010) 1–11.

[31] H. N. Shapiro, Note on a theorem of Dickson, *Bull. Amer. Math. Soc.* **55** (1949) 450–452.

[32] ———, On primitive abundant numbers, *Comm. Pure Appl. Math.* **21** (1968) 111–118.

[33] G. Shimura, *The Map of My Life*, Springer, New York, 2008.

[34] E. Steinitz, Algebraische Theorie der Körper, *J. Reine Angew. Math.* **137** (1910) 167–309.

[35] T. Taylor, *Theoretic Arithmetic*, printed for the author by A. J. Valpy, London, 1816; available at `http://books.google.ca/ebooks?id=kGoUAAAAQAAJ`.

[36] A. Weil, *Basic Number Theory*, Classics in Mathematics, Springer, Berlin, 1995.

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

Paul Pollack received his B.S. from the University of Georgia in 2003 and his Ph.D. from Dartmouth College in 2008. From 2008–2011, he was an NSF postdoc at the University of Illinois. He is presently working as a Postdoctoral Fellow at the University of British Columbia and Simon Fraser University before returning to the University of Georgia in 2012 to begin an assistant professorship. When not pondering the puzzles posed by the positive integers, he can often be found catching up on genre television or reading about the relationship between religious narratives and social justice.
Department of Mathematics, University of British Columbia, Vancouver, BC Canada V6T 1Z2
Department of Mathematics, Simon Fraser University, Burnaby, BC Canada V5A 1S6
pollack@math.ubc.ca