BOLYAI SOCIETY
MATHEMATICAL STUDIES, 25

Erdős Centennial
pp. 515–533.

Paul Erdős and the Rise of Statistical Thinking in Elementary Number Theory

PAUL POLLACK and CARL POMERANCE*

1. Introduction

It might be argued that elementary number theory began with Pythagoras who noted two-and-a-half millennia ago that 220 and 284 form an amicable pair. That is, if $s(n)$ denotes the sum of the proper divisors of n ("proper divisor" means $d \mid n$ and $1 \le d < n$), then

$$s(220) = 284 \quad \text{and} \quad s(284) = 220.$$

When faced with remarkable examples such as this it is natural to wonder how special they are. Through the centuries mathematicians tried to find other examples of amicable pairs, and they did indeed succeed. But is there a formula? Are there infinitely many? In the first millennium of the common era, Thâbit ibn Qurra came close with a formula for a subfamily of amicable pairs, but it is far from clear that his formula gives infinitely many examples and probably it does not.

A special case of an amicable pair m, n is when $m = n$. That is, $s(n) = n$. These numbers are called perfect, and Euclid came up with a formula for some of them (and perhaps all of them) that probably inspired that of Thâbit for amicable pairs. Euler showed that Euclid's formula covers all even perfect numbers, but we still don't know if Euclid's formula gives infinitely many examples and our knowledge about odd perfects, even whether any exist, remains rudimentary.

These are colorful and attractive problems from antiquity, but what is a modern mathematician to make of them? Are they just curiosities? After

*The authors would like to thank Enrique Treviño and the anonymous referee for their helpful suggestions. The second author was supported in part by NSF grant DMS-1001180.

L. Lovász et al. (eds.), *Erdős Centennial*

all, not all problems are good. Ancient people wondered why and how the planets wandered through the stellar constellations, and such musings became the foundation of astronomy, trigonometry, and modern physics. They also wondered why the sun and moon are the same apparent size, with such musings leading nowhere!

Euclid also studied another special subset of the natural numbers: the primes. Already he had a proof of their infinitude. Euler was able to quantify the reciprocal sum for primes in $[1, x]$ as $x \to \infty$, and so we had the birth of a statistical viewpoint in number theory. This led to the prime-counting conjectures of Gauss and Lagrange, the estimates of Chebyshev, the provocative outline of Riemann, and the proofs of Hadamard, de la Vallée Poussin, Erdős, and Selberg. There is a great story here which we feel sure will be told in another essay.

So we have a prime number theorem, but is there a perfect number theorem, an amicable number theorem, and others of this sort? By asking such questions about the statistical distribution of special sets of numbers one opens the door to a host of interesting problems in which modern mathematicians can participate in this millennia-old quest. And leading the way was Paul Erdős.

2. Distribution

The function s defined in the Introduction partitions the positive integers into 3 sets: those n with $s(n) < n$, those with $s(n) = n$, and those with $s(n) > n$. Perhaps, it is not so natural to consider such a partition, but it is historically correct, going back thousands of years. Numbers with $s(n) < n$ are called *deficient* and those with $s(n) > n$ are called *abundant*, with the case of equality already met as the perfect numbers. Putting these concepts into modern garb, we have the immediate question of asymptotic density. It is clear at least that the lower density of the abundant numbers is positive, since any multiple of 6 that is larger than 6 is abundant. But it is not so clear that the abundant numbers possess an asymptotic density.[1]

In 1933, Davenport [5] resolved the problem by proving that the sets of abundant numbers and deficient numbers each possesses a positive asymptotic density, while the set of perfect numbers has asymptotic density 0. In fact, Davenport proved a much more general theorem. Let σ denote the sum-of-divisors function, so that $\sigma(n) = s(n) + n$. And let $h(n) := \frac{\sigma(n)}{n}$.

[1] It is also clear that the deficient numbers have positive lower density since it is easy to see that $s(n)/n$ has mean value $\pi^2/6 - 1$, which is smaller than 1.

So, for example, n is perfect when $h(n) = 2$ and abundant when $h(n) > 2$. Davenport's result is the following:

Theorem 1. *For each real number u, let $\mathscr{D}(u) = \{n \in \mathbf{N} : h(n) \leq u\}$. The set $\mathscr{D}(u)$ always possesses an asymptotic density. Denoting this density by $D(u)$, the function $D(u)$ is continuous and strictly increasing for $u \geq 1$. Moreover, $D(1) = 0$ and $\lim_{u\to\infty} D(u) = 1$.*[2]

Since $D(u)$ is continuous, it follows immediately that the perfect numbers have density zero. We subsequently deduce that the deficient numbers have density $D(2)$, where $0 < D(2) < 1$, and that the abundant numbers comprise a set of density $1 - D(2)$. The numerical values of these densities were investigated by Behrend [2, 3], who succeeded in showing that the density of the abundant numbers lies between 0.241 and 0.314. Later authors (Salié [58], Wall [62], and Deléglise [6]) have tightened these bounds; the current state of the art, due to Kobayashi [42], is that the density of the abundants has decimal expansion starting with 0.2476.

Davenport's proof of this result was decidedly analytic, requiring a study of the complex moments of the function $h(n)$. In this respect, he was following a model laid down by Schoenberg [59], who had earlier proved the analogue of Theorem 1 for the closely-related function $n/\varphi(n)$, where φ is Euler's function. The non-elementary nature of Davenport's argument would surely have irked Erdős, and in the mid-1930s, Erdős took it upon himself to give a purely arithmetic proof of Theorem 1. This resulted in a series of three papers [9, 11, 12], culminating in what we now know as the sufficiency half of the Erdős–Wintner Theorem (see [30]), one of the foundational results in the field known as *probabilistic number theory*. Studying distribution functions eventually led to the landmark collaboration of Erdős and Kac and their celebrated theorem on the normal distribution of the number of prime factors of an integer. As these subjects are discussed elsewhere in this volume, we do not dwell on them here, but rather return to the theme of elementary number theory.

3. Amicables

Recall from the Introduction that a pair n, m of positive integers is said to be amicable if $s(n) = m$ and $s(m) = n$, with the perfect numbers corresponding to the degenerate case of $n = m$. We have seen that the perfect numbers have asymptotic density 0, but do the amicables?

[2]Davenport did not prove that $D(u)$ is strictly increasing; this was established a few years later by Schoenberg [60].

A first approach to counting amicable numbers is suggested by the following simple observation: Suppose that n and m form an amicable pair, with $n < m$. Then $s(n) = m > n$, so that n is abundant. Thus, the upper density of the amicable numbers is at most twice the density of the abundant numbers, and so from [6] or [42], the upper density of the amicables is smaller than $\frac{1}{2}$.

When one considers that essentially none of the theory of amicable pairs was used in this argument, this result seems quite respectable!

In fact, all we used above was that the smaller member of a non-perfect amicable pair is abundant. An equally simpleminded observation, dual to the first, is that the larger member is deficient. Putting these together, we see that if n is the smaller member of a non-perfect amicable pair, then n is an abundant number for which $s(n)$ is deficient. Erdős had the great insight that this two-fold condition on n should be quite restrictive. His argument in [15] that the amicable numbers have asymptotic density zero is actually a proof of the following theorem:

Theorem 2. *The set of abundant natural numbers n for which $s(n)$ is deficient has asymptotic density zero.*

Erdős's proof of Theorem 2 is naturally split into three identifiable components. The first of these is an immediate consequence of the continuity of the function $D(u)$ appearing in Davenport's Theorem 1.

Lemma 3. *Let $\epsilon > 0$ be arbitrary. For a certain $\delta > 0$, depending on ϵ, the set of solutions n to*

$$2 < h(n) < 2 + \delta$$

has asymptotic density less than ϵ.

For every positive integer n, the bijection between divisors d of n and their co-divisors n/d permits us to write $h(n) = \frac{1}{n}\sum_{d|n} d = \sum_{d|n} \frac{1}{d}$. This expression for $h(n)$ suggests that the small divisors of n play the largest role in determining the size of $h(n)$. To make this precise, we let $y > 0$, and we define the truncated function

$$h_y(n) := \sum_{\substack{d|n \\ d \le y}} \frac{1}{d}.$$

The second leg on which Erdős's argument rests is the following lemma.

Lemma 4. *Let $x > 0$ and let y be a positive integer. For each $\delta > 0$ the number of $n \le x$ for which $h(n) - h_y(n) \ge \delta$ does not exceed $\delta^{-1}x/y$.*

Proof. A simple interchange of the order of summation shows that

$$\sum_{n\le x}(h(n)-h_y(n)) = \sum_{d>y}\frac{1}{d}\sum_{\substack{n\le x\\ d\mid n}} 1.$$

The inner sum here is at most $\frac{x}{d}$, from which it is easy to see that the entire sum is at most $\frac{x}{y}$. The claim follows immediately. ■

It seems likely that Erdős would have considered the key innovation in the proof of Theorem 2 to be its third component, which we formulate as follows.

Lemma 5. *Fix $y > 0$. For all natural numbers n outside of a set of asymptotic density zero, n and $s(n)$ share the same set of divisors in $[1, y]$.*

Proof. Let M be the least common multiple of the natural numbers not exceeding y. It suffices to show that $\sigma(n)$ is a multiple of M unless n belongs to a set of density zero. Indeed, if $M \mid \sigma(n)$, then the relation $s(n) = \sigma(n) - n$ implies that

$$s(n) \equiv -n \pmod{d}$$

for all $d \le y$. Thus, $d \mid s(n)$ if and only if $d \mid n$. Now if p is a prime that exactly divides n, then $p+1$ divides $\sigma(n)$. Thus, M divides $\sigma(n)$ whenever there is a prime $p \equiv -1 \pmod{M}$ for which $p \parallel n$. For any particular prime $p \equiv -1 \pmod{M}$, we see that $p \parallel n$ precisely when n falls into one of the $(p-1)$ residue classes $p, 2p, 3p, \dots, (p-1)p \pmod{p^2}$. So if the relation $p \parallel n$ fails for all $p \le z$ from the residue class $-1 \pmod{M}$, then n avoids $p-1$ residue classes modulo p^2 for every such p. By the Chinese remainder theorem, this restricts n to a set of asymptotic density

$$\prod_{\substack{p\equiv -1 \pmod{M}\\ p\le z}} \left(1 - \frac{1}{p} + \frac{1}{p^2}\right).$$

This product can be made arbitrarily small by taking z sufficiently large, since by Dirichlet, the sum of the reciprocals of the primes $p \equiv -1 \pmod{M}$ diverges. The lemma follows. ■

Remark. The proof of Lemma 5 shows that for a fixed M, the number $\sigma(n)$ is almost always divisible by M. When M is a power of 2, this was previously observed by Kanold [40], who used this to prove that the amicable numbers have upper density less than 0.204.

It is now a simple matter to assemble Lemmas 3–5 to prove Theorem 2.

Proof of Theorem 2. Let n denote a generic abundant natural number for which $s(n)$ is deficient. We will show that for each fixed $\epsilon > 0$, the set of all such n has upper density smaller than 2ϵ. By Lemma 3, we may fix $\delta > 0$ small enough so that the set of solutions to $2 < h(n) < 2 + \delta$ has density less than ϵ. Thus, discarding a set of density less than ϵ, we can assume that

$$h(n) \geq 2 + \delta.$$

We now apply Lemma 4 with

$$y := \left\lceil \frac{1}{\delta\epsilon} \right\rceil$$

and find that discarding a set of upper density bounded by ϵ, we can assume that

$$h_y(n) > h(n) - \delta \geq 2.$$

Discarding a further set of density zero, we can assume (by Lemma 5) that n and $m = s(n)$ have the same set of divisors up to y. But then

$$h(m) \geq h_y(m) = h_y(n) > 2,$$

contradicting that m is deficient. So n must have belonged to one of the exceptional sets described above, which have combined upper density smaller than 2ϵ. ∎

In the introduction to [15], Erdős asserted that his method, suitably refined, would show that the count $A(x)$ of amicable numbers in $[1, x]$ satisfies

$$A(x) \ll \frac{x}{\log\log\log x}. \tag{1}$$

Details appeared twenty years later in joint work with Rieger [28] (cf. Rieger's weaker solo result [57]). The Erdős–Rieger upper bound was soon improved by Pomerance [53], who established that

$$A(x) \leq x/\exp(c(\log_3 x \log_4 x)^{1/2}) \tag{2}$$

for a certain constant $c > 0$ and all large x (note the subscripts indicate iterated logs). In both cases, what is actually estimated is the count of abundant $n \leq x$ for which $s(n)$ is deficient. (The key innovation in [53] is

the use of Erdős's theory of *primitive abundant numbers;* see [8].) A few years later, and by different methods, Pomerance [54] established the bound

$$A(x) \leq x/\exp(c(\log x \log_2 x)^{1/3}),$$

for some positive constant c and all large x. This bound has not yet been improved, nor do we know that there are infinitely many amicable numbers. Erdős has a heuristic argument suggesting that $A(x) > x^{1-o(1)}$ as $x \to \infty$.

Fix $\epsilon > 0$. Arguing as in the proof of Theorem 2, one finds that for almost all natural numbers n, we have $h(s(n)) > h(n) - \epsilon$. In the concluding remarks to [15], Erdős claimed that the complementary inequality $h(s(n)) < h(n) + \epsilon$ also holds for almost all n. A proof of this last result eventually appeared in joint work with Granville, Pomerance, and Spiro (see [22, Theorem 5.1]). Hence, $h(s(n)) = h(n) + o(1)$, as $n \to \infty$ in a set of asymptotic density 1. For another application of their method of proof, see [51].

4. Sociables

One can revisit the definition of an amicable pair from the viewpoint of function iteration. Let $s_k(n)$ denote the kth iterate of $s(n)$. Then n is amicable precisely when $s_2(n) = n$. Generalizing, we say that n is *k-sociable* if $s_k(n) = n$ but $s_j(n) \neq n$ for $1 \leq j < k$, and we call the set $\{n, s(n), \ldots, s_{k-1}(n)\}$ an *aliquot k-cycle.* Note that the 1-sociable numbers are exactly the perfect numbers, whose distribution is discussed in detail in the next section.

Questions about the iterates of $s(n)$ began to be asked at the end of the 19th century. For a natural number n, the *aliquot sequence at n* is the sequence $n, s(n), s_2(n), \ldots$, where we stop if we reach 0. For instance, the aliquot sequence at 24 is 24, 36, 55, 17, 1, 0, while the aliquot sequence at 25 is $25, 6, 6, 6, \ldots$. In 1888, Catalan [4] proposed the empirical theorem that these two examples exhaust the possible behaviors of an aliquot sequence; more precisely, every aliquot sequence either terminates or hits a perfect number.

'Empirical theorems', like champion athletes, are always in danger of losing their title. Soon after Catalan's conjecture appeared, Perrott [47] pointed out that the aliquot sequence at 220 was a counterexample. This led Dickson [7] to propose a somewhat tamer, modified conjecture – commonly known today as the *Catalan–Dickson conjecture* – that all aliquot sequences terminate or are eventually periodic. This has been verified numerically for

$n < 276$. However, when $n = 276$, more than 1700 terms of the sequence have been computed [64], with no end in sight.

When Dickson put forward his modified conjecture in 1913, no aliquot cycles of length > 2 were known. The first examples, of lengths 5 and 28, were given by Poulet in 1918. Currently there are 217 such cycles known [45], all but 11 of which have length 4.

What can we prove about the distribution of these cycles? The first asymptotic result on this problem is due to Erdős [21]. Note that the case $k = 2$ is contained in Erdős's earlier work on amicable pairs.

Theorem 6. *Fix $\epsilon > 0$ and fix an integer $k \geq 2$. Then for all n outside of a set of asymptotic density zero, we have*

$$h(s_j(n)) > h(n) - \epsilon \quad \text{for all } \ 0 < j < k. \tag{3}$$

One consequence of Theorem 6 is that for each fixed k, almost all abundant numbers are *k-times abundant*: $n < s(n) < s_2(n) < \cdots < s_k(n)$. Suppose now that n is the smallest member of a sociable k-cycle, where $k > 1$. Then n is abundant, but not k-times abundant (since $s_k(n) = n$), and so n belongs to a set of density zero. As a corollary, the set of k-sociable numbers has asymptotic density zero for each fixed k. For quantitative results of this kind, see [43] and [49].

The proof of Theorem 6 employs the same reasoning seen in the previous section, but with Lemma 5 replaced by the following generalization.

Lemma 7. *Fix $y > 0$, and fix $k \geq 2$. For all natural numbers n outside of a set of asymptotic density zero, all of n, $s(n)$, $\ldots$, $s_{k-1}(n)$ share the same set of divisors in $[1, y]$.*

One can ask whether Theorem 6 remains true with (3) replaced by the complementary inequality $h(s_j(n)) < h(n) + \epsilon$. As mentioned above, this is known to be so when $k = 2$, by later work of Erdős et al. [22]. For larger values of k, this constitutes an attractive open problem. Note that the claim of a general proof, made in [21], is retracted in [22].

For more recent developments on sociable numbers, see [43]. For example, it is shown there that if one lumps together all sociable numbers (i.e., one takes the union of the k-sociables over all k), then after discarding a certain set of asymptotic density zero, the remaining elements are all both odd and abundant.

5. Perfects

From Euclid and Euler, we know that an even number is perfect precisely when it can be written as $2^{p-1}(2^p-1)$, where 2^p-1 is prime. Thus, the distribution of the even perfect numbers is inextricably linked with the distribution of primes of the form 2^p-1, known as *Mersenne primes.* While almost nothing is known rigorously about the distribution of Mersenne primes, Lenstra, Pomerance, and Wagstaff have (independently) given heuristic arguments suggesting that probably

$$\#\{p \le x : 2^p - 1 \text{ prime}\} \sim \frac{\mathrm{e}^\gamma}{\log 2} \log x, \quad \text{as } x \to \infty.$$

Here γ is the familiar Euler–Mascheroni constant. (See, for example, [61].) The validity of this conjecture would imply that the count of even perfect numbers up to x is asymptotic to $\frac{\mathrm{e}^\gamma}{\log 2} \log\log x$.

What about odd perfect numbers? We have already noted that from Davenport's Theorem 1, these numbers have asymptotic density zero. But this is a rather weak result. There is a short and pretty argument of Hornfeck [38] showing that in fact, the count $P(x)$ of odd perfects in $[1, x]$ is smaller than $x^{1/2}$, for every $x > 1$. We cannot resist reproducing it here. By a classical result of Euler, we can write an odd perfect n as $n = p^e m^2$ where p is a prime not dividing m and $p \equiv e \equiv 1 \pmod 4$. (This uses only that n is odd and $\sigma(n) \equiv 2 \pmod 4$.) Since n is perfect,

$$2p^e m^2 = \sigma(p^e)\sigma(m^2), \quad \text{so that} \quad \frac{2m^2}{\sigma(m^2)} = \frac{\sigma(p^e)}{p^e}.$$

But the fraction $\sigma(p^e)/p^e$ is already in lowest terms, since the numerator $\sigma(p^e) = 1 + p + \cdots + p^e$ is not divisible by p. Hence, the prime power p^e is uniquely determined from m. If we assume that $n \le x$, then $1 < m \le \sqrt{x}$, and so Hornfeck's bound follows.

The problem of obtaining improved bounds for $P(x)$ attracted some attention in the late 1950s, with several number theorists throwing their hats into the ring. It was Erdős [16] who gave the first significant improvement over Hornfeck's bound, getting $P(x) \le x^{1/2-c}$ for a certain $c > 0$ and all large x. His idea is both ingenious and, at least in hindsight, quite natural. We sketch an improvement that obtains the estimate $P(x) \le x^{1/4+o(1)}$. (A result of this same quality was obtained by Kanold [41] shortly after Erdős's paper appeared.)

Erdős's starting point is the following 'greedy' algorithm for extracting from an integer M a divisor D of M with D coprime to both M/D and $\sigma(D)$:

Algorithm:

Factor $M = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, where $p_1 > p_2 > \cdots > p_k$.
$D \leftarrow 1$ `// Initialize`
for $i = 1$ **to** k **do** `// Loop over prime power divisors of` M
if $\gcd(\sigma(p_i^{e_i} D), p_i^{e_i} D) = 1$ **then**
  $D \leftarrow p_i^{e_i} D$
end
return D

In certain special cases, Erdős proved that the output D of this algorithm is bounded below by a fixed power of the input M. However, for our present purposes, the argument is clearer (and stronger) if it is instead made to rest upon the following near-injectivity property, whose proof – given in [52] – involves the same circle of ideas as in [16].

Proposition 8. *Let $\epsilon > 0$. For all sufficiently large values of x, depending on the choice of ϵ, at most x^ϵ inputs $M \le x$ of the Algorithm correspond to the same output D.*

We now show that $P(x) \le x^{1/4+o(1)}$ as $x \to \infty$. Write an odd perfect number $n \le x$ as $p^e m^2$ as above and apply the Algorithm to $M = m^2$. It produces a divisor D of m^2 coprime to m^2/D and to $\sigma(D)$. Thus $D = d^2$ for some $d \mid m$. Letting v^2 be the co-divisor of d^2 in m^2, we have $n = p^e v^2 d^2$. Since n is perfect, we have

$$2p^e v^2 d^2 = \sigma(n) = \sigma(p^e v^2)\sigma(d^2).$$

Since d^2 is coprime to $\sigma(d^2)$, we have $d^2 \mid \sigma(p^e v^2)$. If $p^e v^2 \le x^{1/2}$, then $d^2 \le 2x^{1/2}$ so that $d < 2x^{1/4}$. But if $p^e v^2 > x^{1/2}$, then $d^2 = n/(p^e v^2) < x^{1/2}$, so in either case, $d < 2x^{1/4}$. So, by Proposition 8 there are at most $x^{1/4+\epsilon}$ inputs m^2 to the Algorithm (for each fixed $\epsilon > 0$ and x sufficiently large depending on ϵ). But by the Hornfeck–Euler argument, m^2 determines n, which proves the theorem that $P(x) \le x^{1/4+o(1)}$ as $x \to \infty$.

A year after Erdős's article appeared, Hornfeck and Wirsing [39] published a proof that $P(x) \le x^{o(1)}$ as $x \to \infty$. Two years later, Wirsing [63] showed that for an absolute constant W, one has $P(x) < x^{W/\log\log x}$ for all $x > \mathrm{e}$. In fact, the same is true for the distribution of those n with

$\sigma(n)/n = r$ for any fixed rational number r. Wirsing's upper bound has not been improved in fifty years, but it is still a rather long way from the widespread belief that $P(x)$ is identically zero.

While Erdős's results on $P(x)$ are now primarily of historical interest, his approach to the problem has borne other fruit. For instance, as Erdős noted at the time in [16], one can use these methods to show that n and $\sigma(n)$ rarely have a large common factor. For a detailed discussion of these problems, see [50], which was written in part to correct and substantiate some of the unproved assertions of [16]. See also [52].

6. Iteration

It was not always the case, but we now view functions as interesting mathematical objects in and of themselves. For example, for a function whose values are contained in its domain, we can view the function as creating a dynamical system. We discussed this above in the context of the function s, the sum-of-proper-divisors function, where we have sociable cycles and the Catalan–Dickson conjecture.

Euler's function φ provides another attractive dynamical system. Given a positive integer n and the sequence $n, \varphi(n), \varphi(\varphi(n)), \ldots$, we note that it is strictly decreasing until it reaches 1. Thus, we may define $k(n)$ as the minimal number $k \geq 1$ of iterates necessary for n to reach 1. For example, $k(13) = 4$, since the sequence is $13, 12, 4, 2, 1, 1, \ldots$. Seemingly a very exotic function, there is some unexpected structure here! Let $k^*(n) = k(n)$ for n even and $k^*(n) = k(n) - 1$ for n odd. It is not hard to see that $k^*(n)$ is completely additive ($k^*(mn) = k^*(m) + k^*(n)$ for all m, n) and it is inductively defined on the primes by $k^*(2) = 1$ and $k^*(p) = k^*(p-1)$ for $p > 2$. Erdős and his collaborators show in [22] that under the assumption of the Elliott–Halberstam conjecture (a widely believed conjecture on the distribution of primes in residue classes) there is a positive constant α such that $k(n) \sim \alpha \log n$ as $n \to \infty$ on a set of asymptotic density 1.

Euler chains $n, \varphi(n), \varphi(\varphi(n)), \ldots$ arise in other contexts, for example, primality testing and algebraic number theory. See the very recent paper of Ford [32] and the references therein.

7. Values

The set of values of an arithmetic function can also give rise to interesting questions. Take the function s. If p, q are different primes, then $s(pq) =$

$p+q+1$. So a slightly stronger form of Goldbach's conjecture, namely all even numbers at least 8 are a sum of two distinct primes, implies that all odd numbers at least 9 are in the image of s. Since $s(2)=1$, $s(4)=3$, and $s(8)=7$, presumably the only odd number missing from the image of s is 5. From what we know about the possible exceptional set in Goldbach's conjecture, it follows that the set of odds not in the form $s(n)$ has asymptotic density 0. But what of even numbers? Here, Erdős in [20] showed by a clever argument that a positive proportion of even numbers are missing from the image of s. We still don't know if the image of s has a density or if the range of s contains a positive proportion of even numbers. The issue of numbers of the form $n-\varphi(n)$ was also raised in [20], but here even less is known. See [56] for a recent paper in this area with references to other work.

Here is a proof of the result in [20] that a positive proportion of even numbers are missing from the image of s. If $s(n)$ is even and n is odd, then $\sigma(n)$ must be odd too, and so n is a square, say m^2. If $s(m^2)\le x$ and q is the least prime factor of m, then $x\ge s(m^2)>m^2/q$. If m is composite, then $q\le m^{1/2}$, so that $m^{3/2}<x$ and there are at most $x^{2/3}$ possibilities. If $m=q$ is prime, then $q<x$ and there are at most $\pi(x)=O(x/\log x)$ possibilities. Hence the number of even numbers $s(n)$ in $[1,x]$ with n odd is $o(x)$ as $x\to\infty$. So we may assume that n is even, which in turn implies that $x\ge s(n)\ge n/2$. Hence $n\le 2x$. Consider values of s in $[1,x]$ that are divisible by 12. By Lemma 5, but for $o(x)$ choices for $n\le 2x$, we may assume that $12\mid n$. Thus, $x\ge s(n)\ge \frac{4}{3}n$, so that $n\le \frac{3}{4}x$. We conclude that the number of values of $s(n)\le x$ divisible by 12 is at most $\frac{1}{12}\cdot\frac{3}{4}x+o(x)\sim\frac{1}{16}x$, leaving asymptotically at least 25% of the multiples of 12 not in the range of s.

In 1929 S. S. Pillai [48] proved that the image of Euler's function φ has density 0. Here is the idea of the proof. For each fixed positive integer k consider numbers n with at most k distinct prime factors. It is easy to see that the set of these numbers has density 0 as does their image under φ. But if n is not in this set, then $2^k\mid\varphi(n)$, so we see that the image of φ has upper density at most 2^{-k}. Since k is arbitrary, this proves that the image of φ has density 0. Pillai was able to quantify this result by taking k as a function of x and obtaining an estimate of $O(x/(\log x)^{\frac{1}{e}\log 2})$ for the number of values of φ in $[1,x]$. Since φ is 1-1 on the primes, we immediately have a lower bound of magnitude $x/\log x$.

So what is the correct exponent here?

Erdős's answer: "1." This was in [10], a wonderful and seminal paper submitted to the Quarterly Journal of Mathematics when he was 21. That is, the number of values of φ in $[1,x]$ is $x/(\log x)^{1+o(1)}$ as $x\to\infty$. The idea is to look not only at the number of factors 2 in $\varphi(n)$, but at the total

number of prime factors. If $\Omega(n)$ is the number of prime factors of n counted with multiplicity, Erdős knew after Hardy and Ramanujan that normally $\Omega(n) \sim \log\log n$. Moreover, exceptional numbers with $\Omega(n) < \epsilon \log\log x$ or $\Omega(n) > \frac{1}{\epsilon}\log\log x$ are so sparse that they are negligible. Erdős then showed (in an early and inventive use of Brun's sieve method) an analog of the Hardy–Ramanujan theorem for "shifted primes", that is, he showed that $\Omega(p-1)$ is normally near $\log\log p$, with exceptional primes p, with $\Omega(p-1)$ far from this normal order, being quite rare. So, but for very few numbers n, they are divisible by a fair number of non-exceptional primes p. Since $\Omega(\varphi(n)) \geq \sum_{p|n} \Omega(\phi(p))$, we find that $\Omega(\varphi(n))$ is much larger than $\log\log n$, meaning that $\phi(n)$ is quite exceptional! This is all worked out in exquisite detail, not only solving Pillai's problem, but introducing extraordinarily useful tools in the statistical study of elementary number theory.

The problem of the distribution of φ values was taken up later by Erdős and Hall [23, 24], Maier and Pomerance [46], and by Ford [31]. However, we still don't have an asymptotic formula nor do we know if a natural one exists.

The same theorems carry over to the range of σ. Erdős also raised the attractive question (for instance, in [18]) of whether the images of φ and σ have an infinite intersection. If p and $p+2$ are both primes, then $\sigma(p) = p+1 = \varphi(p+2)$, so the answer is affirmative if there are infinitely many twin primes. Also if $2^p - 1$ is prime, then $\sigma(2^p-1) = 2^p = \varphi(2^{p+1})$, so the answer is again 'yes' if there are infinitely many Mersenne primes (and so 'yes' if there are infinitely many even perfect numbers). In a recent paper, Ford, Luca, and Pomerance [33] showed unconditionally that there are infinitely many pairs of integers m, n with $\sigma(m) = \varphi(n)$, and Ford and Pollack [34, 35] have some finer results in this direction.

8. Order

Euler's function $\varphi(n)$ gives the order of the multiplicative group $(\mathbf{Z}/n\mathbf{Z})^*$. A closely related function, $\lambda(n)$ gives the maximal order of an element in this group. When $(\mathbf{Z}/n\mathbf{Z})^*$ is cyclic, we have $\lambda(n) = \varphi(n)$. We always have $\lambda(n) \mid \varphi(n)$, and since $(\mathbf{Z}/n\mathbf{Z})^*$ is abelian, for all integers a coprime to n, $a^{\lambda(n)} \equiv 1 \pmod{n}$. For this reason, $\lambda(n)$ is referred to as the *universal exponent function.*

Carmichael used the notation λ, but the function appears in Gauss a century earlier. It is easy to give a formula for $\lambda(n)$ based on the prime factorization of n: for a prime power p^α, we have $\lambda(p^\alpha) = \varphi(p^\alpha)$ except

if $p = 2$ and $\alpha \geq 3$ in which case, $\lambda(2^\alpha) = \frac{1}{2}\varphi(2^\alpha)$. (Note that $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$.) Further, for all n, $\lambda(n)$ is the lcm of $\lambda(p^\alpha)$ for prime powers $p^\alpha \mid n$.

Being so closely related to φ, one might expect that statistically λ is quite similar. Here is φ's story: We know (from Schoenberg, or more generally the Erdős–Wintner theorem) that for each real number $u \in (0,1]$, the set $\{n : \varphi(n) \leq un\}$ has a positive asymptotic density that varies continuously and strictly monotonically with u. Further, from Mertens' theorem in analytic number theory, it follows that $\varphi(n) \geq (\mathrm{e}^{-\gamma} + o(1))n/\log\log n$ as $n \to \infty$. And on average, $\varphi(n)$ behaves like cn, with $c = 6/\pi^2$.

Erdős took up the normal and average orders of $\lambda(n)$ in [17], stating some results without proof. Full proofs of more precise results, including the minimal order of $\lambda(n)$, were worked out in Erdős–Pomerance–Schmutz [27] in 1991. The function is amazingly different from φ. On average it is not like cn, but rather like $n/(\log n)^{1+o(1)}$, where the "$o(1)$" is asymptotically $c/\log\log\log n$, with c explicitly worked out. The normal order is not of the shape $\asymp n$, but rather much smaller at $n/(\log n)^{\log\log\log n + c + o(1)}$ for a different explicit c. And the minimal order, instead of the large function $n/\log\log n$, is instead the tiny function $(\log n)^{c\log\log\log n}$ (here the precise value of c is still not known), a result that has found application in the analysis of some primality tests. These results have not been improved over the past 2 decades, and there is indeed room for improvement. For example, does $\lambda(n)$ have a "nice" distribution function? That is, for $\varphi(n)$ we compare it with n; what should $\lambda(n)$ be compared with?

The image of λ is also different than the image of φ. In [27] it is shown that there is some $c > 0$ such that the number of λ-values in $[1, x]$ is $O(x/(\log x)^c)$, a result which strongly uses an earlier result of Erdős and Wagstaff in [29]. It has been announced by Luca and Pomerance that there is some $c' > 0$ such that the count is at least $x/(\log x)^{1-c'}$ for all large x. Probably the truth is $x/(\log x)^{\alpha+o(1)}$ as $x \to \infty$, where $\alpha = 1 - (1 + \log\log 2)/\log 2 = 0.086\ldots$, the Erdős–Tenenbaum–Ford constant, and maybe this is provable.

The iteration of λ also has its surprises, see Harland [37] for some recent work.

From its definition, we see that λ is related to the order-of-an-element function. For n a positive integer and $\gcd(a, n) = 1$, we follow Erdős in using the notation $\ell_a(n)$ for the order of a in $(\mathbf{Z}/n\mathbf{Z})^*$. Thus, $\ell_a(n) \mid \lambda(n)$, and for some number a we have $\ell_a(n) = \lambda(n)$. In a surprisingly difficult paper, Erdős in [19] (he spoke on this at the International Conference of Mathematicians in Nice in 1970), began the statistical study of $\ell_a(n)$. Further developments can be tracked in [25] and in [44].

A pseudoprime to the base a is a composite integer n for which $a^{n-1} \equiv 1 \pmod{n}$. Note that the congruence holds if and only if $\ell_a(n) \mid n-1$. Pseudoprimes are a useful concept since all primes n not dividing a satisfy the congruence and the congruence itself is easily checkable numerically. Thus, pseudoprimes stand as an obstruction against using the congruence as a primality test. Known from experience that pseudoprimes are rare compared with primes, it took some time for this to be proved. Erdős was the first to do so in [14] (announced earlier in [13]). Currently the best upper bound known for their distribution is in Pomerance [55], and a number of other statistical results are discussed in Erdős–Pomerance [26].

Some composites n have the property that $a^{n-1} \equiv 1 \pmod{n}$ for all integers a coprime to n. From what we have said above, this congruence is equivalent to $\lambda(n) \mid n-1$. It is easy to see that this then forces n to be squarefree. In 1899, Korselt essentially gave this criterion for a number n to satisfy $a^{n-1} \equiv 1 \pmod{n}$ for all a coprime to n, but did not give any composite examples. In 1910 and apparently unaware of Korselt's criterion, Carmichael did give some examples, such as 561, 1105, and 1729. Now known as Carmichael numbers, Erdős was the first to prove a result about their distribution, in [17]. He showed that the number of Carmichael numbers in $[1, x]$ is at most $x^{1-c \log\log\log x/\log\log x}$ for some fixed $c > 0$. And he gave a heuristic argument that the count exceeds $x^{1-\epsilon}$ for each fixed $\epsilon > 0$ and all sufficiently large x depending on ϵ.

This was all the more remarkable in that at that time we did not have a proof that there are infinitely many Carmichael numbers and the numerical evidence seemed to indicate a much slower growth rate for the counting function. Shanks was notably vocal in challenging Erdős on this point. It is now known that there are infinitely many Carmichael numbers, Alford–Granville–Pomerance [1]. The proof largely follows the Erdős heuristic in [17], which in turn is based on a proof in [10] that there are numbers $v \le x$ such that $\varphi(n) = v$ has more than x^c solutions n. In Granville–Pomerance [36] the two incompatible viewpoints of Erdős and Shanks were shown to both have elements of truth, though there is still much to be learned here.

9. Conclusion

We have touched on a few of our favorite problems and results of Erdős in elementary number theory, particularly those involving the elementary number theoretic functions. We have not attempted to be encyclopedic, and for a more thorough and complete treatment, we recommend the article of

Schinzel in this volume, as well as the original papers of Erdős, most of which are freely available online.

The point we have tried to make is that viewing classical problems in elementary number theory through a statistical lens allows the tools of modern mathematics to prove interesting and sometimes beautiful theorems. It is through this lens that the mathematics of the ancients lives on. Paul Erdős was an early and consistent exponent of this point of view, changing for the better the entire landscape of elementary number theory.

References

[1] W. R. Alford, A. Granville, and C. Pomerance, *There are infinitely many Carmichael numbers,* Ann. of Math. (2) **139** (1994), 703–722.

[2] F. Behrend, *Über numeri abundantes. I,* Sitzgsber. Akad. Berlin (1932), 322–328.

[3] ———, *Über numeri abundantes. II,* Sitzgsber. Akad. Berlin (1933), 289–293.

[4] E. Catalan, *Propositions et questions diverses,* Bull. Soc. Math. France **16** (1888), 128–129.

[5] H. Davenport, *Über numeri abundantes,* Sitzgsber. Akad. Berlin (1933), 830–837.

[6] M. Deléglise, *Bounds for the density of abundant integers,* Experiment. Math. **7** (1998), 137–143.

[7] L. E. Dickson, *Theorems and tables on the sum of the divisors of a number,* Q.J. Math. **44** (1913), 264–296.

[8] P. Erdős, *On primitive abundant numbers,* J. London Math. Soc. **10** (1935), 49–58.

[9] ———, *On the density of some sequences of numbers,* J. London Math. Soc. **10** (1935), 120–125.

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

[11] ———, *On the density of some sequences of numbers, II,* J. London Math. Soc. **12** (1937), 7–11.

[12] ———, *On the density of some sequences of numbers, III,* J. London Math. Soc. **13** (1938), 119–127.

[13] ———, *On the converse of Fermat's theorem,* Amer. Math. Monthly **56** (1949), 623–624.

[14] ———, *On almost primes,* Amer. Math. Monthly 57 (1950), 404–407.

[15] ———, *On amicable numbers,* Publ. Math. Debrecen **4** (1955), 108–111.

[16] ———, *On perfect and multiply perfect numbers,* Ann. Mat. Pura Appl. (4) **42** (1956), 253–258.

[17] ———, *On pseudoprimes and Carmichael numbers,* Publ. Math. Debrecen **4** (1956), 201–206.

[18] ———, *Remarks on number theory, II. Some problems on the σ function,* Acta Arith. **5** (1959), 171–177.

[19] ———, *On the sum* $\sum_{d|2^n-1} d^{-1}$*,* Actes du Congrés International des Mathématiciens (Nice, 1970), Tome 3, and Israel J. Math. **9** (1971), 43–48.

[20] ———, *Über die Zahlen der form* $\sigma(n) - n$ *und* $n - \varphi(n)$*,* Elem. Math. **28** (1973), 83–86.

[21] ———, *On asymptotic properties of aliquot sequences,* Math. Comp. **30** (1976), no. 135, 641–645.

[22] P. Erdős, A. Granville, C. Pomerance, and C. Spiro, *On the normal behavior of the iterates of some arithmetic functions,* Analytic number theory (Allerton Park, IL, 1989), Progr. Math., vol. 85, Birkhäuser Boston, Boston, MA, 1990, pp. 165–204.

[23] P. Erdős and R. R. Hall, *On the values of Euler's φ-function,* Acta Arith. **22** (1973), 201–206.

[24] ———, *Distinct values of Euler's φ-function,* Mathematika **23** (1976), 1–3.

[25] P. Erdős, P. Kiss, and C. Pomerance, *On the prime divisors of Mersenne numbers,* Acta Arith. **57** (1991), 267–281.

[26] P. Erdős and C. Pomerance, *On the number of false witnesses for a composite number,* Math. Comp. **46** (1986), 259–279.

[27] P. Erdős, C. Pomerance, and E. Schmutz, *Carmichael's lambda function,* Acta Arith. **58** (1991), 363–385.

[28] P. Erdős and G. J. Rieger, *Ein Nachtrag über befreundete Zahlen,* J. Reine Angew. Math. **273** (1975), 220.

[29] P. Erdős and S. S. Wagstaff, Jr., *The fractional parts of the Bernoulli numbers,* Illinois J. Math. **24** (1980), 104–112.

[30] P. Erdös and A. Wintner, *Additive arithmetical functions and statistical independence,* Amer. J. Math. **61** (1939), 713–721.

[31] K. Ford, *The distribution of totients,* Ramanujan J. **2** (1998), 67–151. (Updated version on the author's web page.)

[32] K. Ford, *Sieving by very thin sets of primes and Pratt trees with missing primes,* preprint, 2012, `arXiv:1212.3498 [math.NT]`, IMRN, to appear.

[33] K. Ford, F. Luca, and C. Pomerance, *Common values of the arithmetic functions* ϕ *and* σ*,* Bull. Lond. Math. Soc. **42** (2010), 478–488.

[34] K. Ford and P. Pollack, *On common values of* $\varphi(n)$ *and* $\sigma(m)$*, I,* Acta Math. Hungarica **133** (2011), 251–271.

[35] ———, *On common values of* $\varphi(n)$ *and* $\sigma(m)$*, II,* Algebra Number Theory **6** (2012), 1669–1696.

[36] A. Granville and C. Pomerance, *Two contradictory conjectures concerning Carmichael numbers,* Math. Comp. **71** (2001), 883–908.

[37] N. Harland, *The number of iterates of the Carmichael lambda function required to reach* 1*,* preprint, 2012, `arXiv:1203.4791 [math.NT]`.

[38] B. Hornfeck, *Zur Dichte der Menge der vollkommenen Zahlen,* Arch. Math. (Basel) **6** (1955), 442–443.

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

[40] H. J. Kanold, *Über die Dichten der Mengen der vollkommenen und der befreundeten Zahlen,* Math Z. **61** (1954), 180–185.

[41] ———, *Über die Verteilung der vollkommenen Zahlen und allgemeinerer Zahlenmengen,* Math. Ann. **132** (1957), 442–450.

[42] M. Kobayashi, *On the density of abundant numbers,* Ph.D. thesis, Dartmouth College, 2010.

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

[44] P. Kurlberg and C. Pomerance, *On a problem of Arnold: the average multiplicative order of a given integer,* Algebra and Number Theory, to appear.

[45] D. Moews, *A list of aliquot cycles of length greater than* 2, internet resource, `http://djm.cc/sociable.txt`.

[46] H. Maier and C. Pomerance, *On the number of distinct values of Euler's ϕ-function,* Acta Arith. **49** (1988), 263–275.

[47] J. Perrott, *Sur une proposition empirique énoncée au Bulletin,* Bull. Soc. Math. France **17** (1889), 155–156.

[48] S. S. Pillai, *On some functions connected with $\varphi(n)$,* Bull. Amer. Math. Soc. **35** (1929), 832–836.

[49] P. Pollack, *A remark on sociable numbers of odd order,* J. Number Theory **130** (2010), no. 8, 1732–1736.

[50] ———, *On the greatest common divisor of a number and its sum of divisors,* Michigan Math. J. **60** (2011), no. 1, 199–214.

[51] ———, *Quasi-amicable numbers are rare,* J. Integer Seq. **14** (2011), no. 5, Article 11.5.2, 13 pages.

[52] P. Pollack and C. Pomerance, *Prime-perfect numbers,* Integers **12A** (2012), article A14, 19 pages.

[53] C. Pomerance, *On the distribution of amicable numbers,* J. Reine Angew. Math. **293/294** (1977), 217–222.

[54] ———, *On the distribution of amicable numbers. II,* J. Reine Angew. Math. **325** (1981), 183–188.

[55] ———, *On the distribution of pseudoprimes,* Math. Comp. **37** (1981), 587–593.

[56] C. Pomerance and H.-S. Yang, *Variant of a theorem of Erdős on the sum-of-proper-divisors function,* Math. Comp., to appear.

[57] G. J. Rieger, *Bemerkung zu einem Ergebnis von Erdős über befreundete Zahlen,* J. Reine Angew. Math. **261** (1973), 157–163.

[58] H. Salié, *Über die Dichte abundanter Zahlen,* Math. Nachr. **14** (1955), 39–46.

[59] I. J. Schoenberg, *Über die asymptotische Verteilung reeller Zahlen mod* 1, Math. Z. **28** (1928), 171–199.

[60] ———, *On asymptotic distributions of arithmetical functions,* Trans. Amer. Math. Soc. **39** (1936), 315–330.

[61] S. S. Wagstaff, Jr., *Divisors of Mersenne numbers,* Math. Comp. **83** (1983), 385–397.

[62] C. R. Wall, *Density bounds for the sum of divisors function,* The theory of arithmetic functions (Proc. Conf., Western Michigan Univ., Kalamazoo, Mich., 1971), Lecture Notes in Math., vol. 251, Springer, Berlin, 1972, pp. 283–287.

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

[64] P. Zimmerman, *Aliquot sequences,* internet resource, `http://www.loria.fr/ zimmerma/records/aliquot.html`.

Paul Pollack
University of Georgia,
Department of Mathematics,
Athens, GA 30602,
USA
`e-mail: pollack@uga.edu`

Carl Pomerance
Dartmouth College,
Department of Mathematics,
Hanover, NH 03755,
USA
`e-mail: carlp@math.dartmouth.edu`