Arithmetic functions. . .
old and new

Paul Pollack

MSRI workshop on "Recent developments in analytic number theory"

May 2017

PART I: Some not-so-recent developments

Let $s(n) := \sum_{d|n, d<n} d$ be the sum of the proper divisors of n, and let $\sigma(n) = \sum_{d|n} d$ be the sum of all positive divisors of n. So, e.g.,

$$s(4) = 1 + 2 = 3, \qquad \sigma(4) = 1 + 2 + 4 = 7.$$

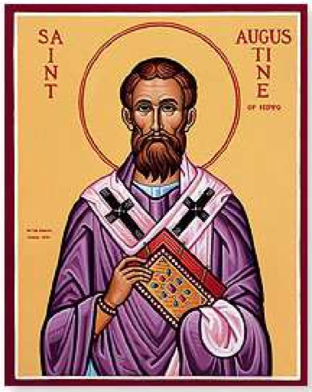
A natural number n is called **perfect** if $s(n) = n$ (equivalently, $\sigma(n) = 2n$), and **amicable** if $s(n) \neq n$ and $s(s(n)) = n$. For example, $s(6) = 6$, so 6 is perfect. Also,

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

and so 220 is amicable (as is 284; we say 220 and 284 form an amicable pair).

The number Six .... which is said to be perfect ... was called Marriage by the Pythagoreans, because it is produced from the intermixing of the first meeting of male and female; and for the same reason this number is called Holy and represents Beauty, because of the richness of its proportions. — Iamblichus (ca. 300 AD)

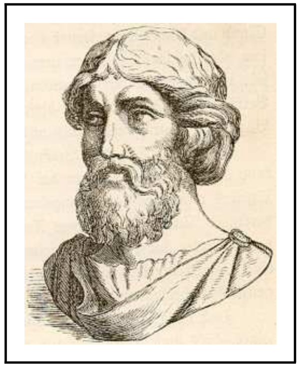
The number Six .... which is said to be perfect ... was called Marriage by the Pythagoreans, because it is produced from the intermixing of the first meeting of male and female; and for the same reason this number is called Holy and represents Beauty, because of the richness of its proportions. — Iamblichus (ca. 300 AD)



Six is a number perfect in itself, and not because God created all things in six days; rather, the converse is true. God created all things in six days because the number is perfect. Augustine (ca. 400 AD)

Pythagoras (6th century BCE), when asked what a friend was, replied:

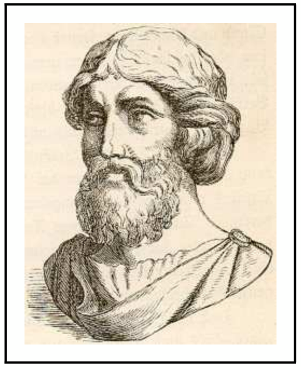
One who is the other I, such as 220 and 284.



Pythagoras (6th century BCE), when asked what a friend was, replied:

One who is the other I, such as 220 and 284.

Persons who have concerned themselves with talismans affirm that the amicable numbers 220 and 284 have an influence to establish a union or close friendship between two individuals. – Ibn Khaldun (14th century AD)



Pythagoras (6th century BCE), when asked what a friend was, replied:

One who is the other I, such as 220 and 284.

Persons who have concerned themselves with talismans affirm that the amicable numbers 220 and 284 have an influence to establish a union or close friendship between two individuals. – Ibn Khaldun (14th century AD)

Al-Majriti (10th century AD) claims to have

tested the erotic effect of . . . giving any one the smaller number 220 to eat, and himself eating the larger number 284.

A deep thought

We tend to scoff at the beliefs of the ancients.

A deep thought

We tend to scoff at the beliefs of the ancients.
But we can't scoff at them personally, to their faces, and this is what annoys me.

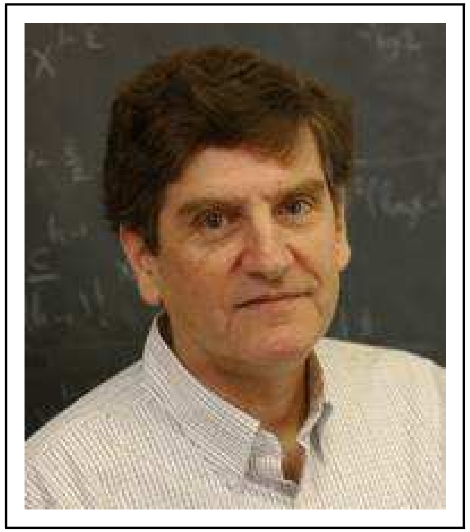
– *Jack Handey*

The distribution of amicable numbers

There are over ten million amicable pairs known, but we have no proof that there are infinitely many.

Theorem (Erdős, 1955)

Almost all numbers are not amicable.



Theorem (Pomerance, 2015)

The number $V_2(x)$ of amicable numbers $n \le x$ satisfies

$$V_2(x) \le x/\exp((\log x)^{1/2})$$

for large x.

Erdős's 1955 proof

Proposition (Erdős)

Let $\epsilon > 0$. For almost all n — meaning, all n except for a set of density 0 — we have

$$\frac{s(s(n))}{s(n)} > \frac{s(n)}{n} - \epsilon.$$

In other words, if we define the *abundancy* of a number n by the ratio $s(n)/n$, then almost all of the time, the abundancy of $s(n)$ is $\gtrapprox$ the abundancy of n.

Proposition (Erdős)

Let $\epsilon > 0$. For almost all n — meaning, all n except for a set of density 0 — we have

$$\frac{s(s(n))}{s(n)} > \frac{s(n)}{n} - \epsilon.$$

Sketch of proof.

First, one argues that $f(n) := s(n)/n$ is "essentially determined" by small divisors. To make sense of this claim, observe that

$$f(n) = \sum_{d|n,\ d>1} \frac{1}{d}.$$

This representation suggests a natural truncated version, namely

$$f_y(n) = \sum_{\substack{d|n \\ 1<d\leq y}} \frac{1}{d}.$$

Clearly $f(n) \geq f_y(n)$, and

$$\sum_{n \leq x} (f(n) - f_y(n)) = \sum_{d > y} \frac{1}{d} \sum_{\substack{n \leq x \\ d \mid n}} 1 \leq x \sum_{d > y} \frac{1}{d^2} < x/y.$$

Thus, on average, $f(n)$ and $f_y(n)$ differ by $O(1/y)$.

We think of y as large and fixed (in a way to be specified momentarily).

The next step is to show, using the sieve, that n and $s(n) = \sigma(n) - n$ share the same set of divisors $\leq y$, away from a set of density zero.

The next step is to show, using the sieve, that n and $s(n) = \sigma(n) - n$ share the same set of divisors $\leq y$, away from a set of density zero.

The sets of divisors $\leq y$ certainly coincide whenever $\sigma(n) \equiv 0$ modulo d, for every $d \leq y$. That is, whenever

$$\sigma(n) \equiv 0 \pmod{M} \quad \text{for} \quad M = \operatorname{lcm}[1, 2, \ldots, y].$$

That this congruence holds for almost all n is an easy application of the sieve. Indeed, there is usually a prime $p \equiv -1 \pmod{M}$ that shows up to the first power in the prime factorization of n, ensuring that

$$M \mid p + 1 \mid \sigma(n).$$

We can now finish up. Since n and $s(n)$ have the same set of divisors $\le y$, for almost all n, we have

$$f_y(s(n)) = f_y(n) \qquad \text{for almost all } n.$$

Thus, for almost all n,

$$\frac{s(s(n))}{s(n)} = f(s(n)) \ge f_y(s(n)) = f_y(n).$$

Since $f_y(n)$ and $f(n)$ differ by $O(1/y)$ on average, and so

$$f_y(n) > f(n) - \epsilon = \frac{s(n)}{n} - \epsilon$$

away from a set of upper density $O(\epsilon^{-1}/y)$. Inserting this above and taking $y \to \infty$ finishes the proof.

Proposition (Davenport, 1933)

For each real $u \geq 0$, consider the set

$$\mathcal{D}_s(u) = \{n : s(n)/n \leq u\}.$$

This set always possesses an asymptotic density $D_s(u)$. Considered as a function of u, D_s is continuous, with $D_s(0) = 0$ and $D_s(\infty) = 1$.

Davenport's motivation was to answer a 1929 question of Bessel-Hagen about the counting function of the abundant, deficient, and perfect numbers, defined by the conditions $s(n) > n$, $s(n) < n$, and $s(n) = n$. Davenport's theorem implies that all three sets have a density, and that the perfects have density 0.

The previous two propositions have the following consequence.

Theorem

All abundant numbers n, apart from a density zero set of exceptions, are such that $s(n)$ is also abundant.

Proof.

Since $s(n)$ is abundant, $s(n)/n > 1$.

Let $\delta > 0$ be a small, fixed parameter. We can assume $s(n)/n > 1 + \delta$, at the cost of excluding a set of density

$$D_s(1 + \delta) - D_s(1).$$

By Erdős's Proposition, all of the remaining n apart from a density zero set of exceptions have $s(s(n))/s(n) > 1 + \delta/2 > 1$, and hence have $s(n)$ abundant.

Now send $\delta \downarrow 0$, using continuity of D_s at 1.

Amicables have density 0

Now we are home free!

To prove that the set of numbers belonging to an amicable pair has density zero, note that it is enough to show this for the smaller members of each pair.

But if n is the smaller member of an amicable pair, then n is abundant, since $s(n) > n$, but $s(n)$ is deficient, since $s(s(n)) = n < s(n)$. So n is one of the members of the density-zero exceptional set in the theorem we just proved.

We showed:

Proposition (Erdős)

Let $\epsilon > 0$ for almost all n — meaning, all n except for a set of density 0 — we have

$$\frac{s(s(n))}{s(n)} > \frac{s(n)}{n} - \epsilon.$$

What about Erdős in reverse?

We showed:

Proposition (Erdős)

Let $\epsilon > 0$ *for almost all* n *— meaning, all* n *except for a set of density* 0 *— we have*

$$\frac{s(s(n))}{s(n)} > \frac{s(n)}{n} - \epsilon.$$

What about Erdős in reverse?

Proposition

Let $\epsilon > 0$ *for almost all* n *— meaning, all* n *except for a set of density* 0 *— we have*

$$\frac{s(s(n))}{s(n)} < \frac{s(n)}{n} + \epsilon.$$

Is this true?

It is tempting to try the same proof! After all, we showed

$$f_y(n) = f_y(s(n))$$

for almost all n, and this equation is symmetric in n and $s(n)$.

But there is a subtle asymmetry.

Our proof relied on knowing that $f(n)$ and $f_y(n)$ are usually nearby, for y large. For this variant, one would want the same for $f(s(n))$ and $f_y(s(n))$.

Our proof relied on knowing that $f(n)$ and $f_y(n)$ are usually nearby, for y large. For this variant, one would want the same for $f(s(n))$ and $f_y(s(n))$.

We know that if $s(n)$ and $f_y(s(n))$ differ significantly, then $s(n)$ is placed in a small set. But does this mean n is placed in a small set?

Conjecturally, yes.

Conjecture (Erdős, Granville, Pomerance, Spiro, 1990)

If $\mathcal{A}$ is any subset of the positive integers with density 0, then $s^{-1}(\mathcal{A})$ also has density 0.

Theorem (EGPS, conditional on the conjecture)

Fix $\epsilon > 0$ and fix a nonnegative integer K. Then for almost all n,

$$\frac{s_{k+1}(n)}{s_k(n)} > \frac{s(n)}{n} - \epsilon \quad \textit{for } k = 1, 2, \ldots, K$$

and

$$\frac{s_{k+1}(n)}{s_k(n)} < \frac{s(n)}{n} + \epsilon \quad \textit{for } k = 1, 2, \ldots, K.$$

"Abundancy generally persists" for any finite number of iterations.

The lower bound was proved unconditionally earlier by Erdős (1976), following his work on the $K = 1$ case discussed earlier.

EGPS proved the upper bound unconditionally for $K = 1$.

For density zero sets $\mathcal{A}$ with arithmetic structure, it is often tractable to show that $s^{-1}(\mathcal{A})$ has density 0.

Theorem (P., 2014)

The count of $n \leq x$ for which $s(n)$ is prime is $O(x/\log x)$.

Theorem (Troupe, 2015)

The normal number of prime factors of $s(n)$ is $\log\log n$. In other words, $s^{-1}(\mathcal{A}_\epsilon)$ has density zero for each of the sets

$$\mathcal{A}_\epsilon = \{m : |\omega(m) - \log\log m| > \epsilon \log\log m\}.$$

(Same holds for Ω replacing ω.)

Since we certainly have

$$\mathcal{A} \subset s^{-1}(s(\mathcal{A})),$$

the EGPS conjecture implies that whenever $\mathcal{A}$ does not have density zero, $s(\mathcal{A})$ can also not have density zero.

If we take $\mathcal{A} = \mathbb{Z}^+$, we see that $s(\mathcal{A})$ should have positive upper density. One can prove this directly: by the results towards Goldbach, most odd numbers are $p + q + 1 = s(pq)$.

What about $\mathcal{A} = 2\mathbb{Z}^+$? That $s(\mathcal{A})$ has positive upper density (in fact, positive lower density!) was shown only in 2015, by Luca and Pomerance.
equivalently: a positive proportion of even numbers are in $s(\mathbb{Z}^+)$.

A result towards the EGPS conjecture

Theorem (Thompson, Pomerance, P.)

Let $\epsilon(x)$ be any positive-valued function tending to 0 as $x \to \infty$. If $\mathcal{A}$ is any collection of $x^{\frac{1}{2}+\epsilon(x)}$ integers, then

$$\#\{n \le x : s(n) \in \mathcal{A}\} = o(x), \quad \text{as } x \to \infty,$$

uniformly in the choice of $\mathcal{A}$.

We borrow some ideas from a recent preprint of Andy Booker, who shows that $\#s^{-1}(2n) \ll_\epsilon n^{1/2+\epsilon}$.

The theorem only gets stronger if $\epsilon(x)$ gets larger, so can assume $\epsilon(x) \geq 1/\log\log x$.

Now let $\mathcal{A}$ be a set of at most $x^{1/2+\epsilon(x)}$ integers.

When counting $n \leq x$ with $s(n) \in \mathcal{A}$, we can immediately discard inconvenient n, including

- $n \leq x^{1/2}$,
- n with no prime factor up to $\log x$,
- n with a squarefull part $> x^{2\epsilon(x)}$,
- n with $\gcd(n, \sigma(n)) > \log x$,
- n with a divisor between $x^{1/2-10\epsilon(x)}$ and $x^{1/2+10\epsilon(x)}$.

Indeed, we throw out $o(x)$ integers each time.

The strategy is to show that for each $a \in \mathcal{A}$, the number of remaining $n \le x$ with $s(n) = a$ is

$$\le x^{1/2 - 2\epsilon(x)}.$$

Since $\#\mathcal{A} \le x^{1/2+\epsilon(x)}$, this "pointwise" bound on the number of preimages is enough to complete the proof that

$$\#\{n \le x : s(n) \in \mathcal{A}\} = o(x).$$

Where does this pointwise bound come from?

Write $n = de$ where d is the largest divisor of n not exceeding $\sqrt{x}$. Note $e > 1$.

The overall plan is to bound the number of possibilities for e, given d, then to sum on d.

Our assumptions on n imply that

$$d < x^{1/2 - 10\epsilon(x)}$$

but that

$$dp^{-}(e) > x^{1/2 + 10\epsilon(x)}.$$

One can deduce from these inequalities and the fact that n has small squarefull part that

$$\gcd(d, e) = 1.$$

Now consider the equation

$$s(de) = a.$$

Using the definition of s and the multiplicativity of σ, high school algebra yields

$$\sigma(d)s(e) + s(d)e = a.$$

We see that it is enough to bound the number of possibilities for $s(e)$, given d, since d and $s(e)$ determine e, and hence determine $n = de$.

We also see, looking modulo $s(d)$, that

$$\sigma(d)s(e) \equiv a \pmod{s(d)}.$$

Given d, this puts $s(e)$ in a uniquely determined residue class modulo $s(d)/\gcd(s(d), \sigma(d))$.

So where are we at?

Given d, we want to count the number of possibilities for $s(e)$. And we know that $s(e)$ is a determined residue class mod $s(d)/\gcd(s(d),\sigma(d))$.

We would like an upper bound on $s(e)$. A *lower bound* is easy: $s(e) \geq e/p^{-}(e)$.

This isn't helpful for us. But it is easy to prove that this lower bound is not too far from the truth:

$$s(e) \ll \log x \cdot \frac{e}{p^{-}(e)}$$

This isn't helpful for us. But it is easy to prove that this lower bound is not too far from the truth:

$$s(e) \ll \log x \cdot \frac{e}{p^-(e)}$$

Since $de = n \le x$, we have $e \le x/d$, and so

$$s(e) \ll \log x \cdot \frac{x}{dp^-(e)}.$$

But remember $d \cdot p^-(e) \ge x^{1/2+10\epsilon(x)}$, and so

$$s(e) \ll \log x \cdot x^{1/2-10\epsilon(x)}.$$

OK, so $s(e)$ is in a determined residue class modulo $s(d)/\gcd(s(d), \sigma(d))$ and $s(e) \ll \log x \cdot x^{1/2-10\epsilon(x)}$. The number of possibilities for $s(e)$, given d, is thus

$$\ll \log x \cdot x^{1/2-10\epsilon(x)} \cdot \frac{\gcd(s(d), \sigma(d))}{s(d)} + 1.$$

We have $s(d) \geq d/p^{-}(d) \geq d/\log x$.

Also, $\gcd(s(d), \sigma(d)) = \gcd(d, \sigma(d))$, and this divides $\gcd(n, \sigma(n))$. Therefore, $\gcd(s(d), \sigma(d)) \leq \log x$.

So our upper bound is

$$\ll (\log x)^3 \cdot x^{1/2-10\epsilon(x)}/d + 1.$$

Finally sum over $d \leq x^{1/2-10\epsilon(x)}$: result is $< x^{1/2-2\epsilon(x)}$.

A strong variant of the EGPS conjecture

One also finds in [EGPS] the following hypothesis:

Hypothesis

For each fixed K, the number of preimages of n not exceeding Kn is $O_K(1)$.

Note that there are n with arbitrarily many preimages: take an n for which $n-1$ has many representations $p+q$, and note that $s(pq)=p+q+1=n$. But only $O_K(1)$ of the numbers pq are $< Kn$.

About this, they write:

> *We are not sure we believe this hypothesis, and in fact it may be possible to disprove it. We note though that it implies [the EGPS conjecture].*

This variant turns out to be too strong.

Disproof.

We will show that there are m which have arbitrarily many preimages of the form $2pq$, with p and q distinct odd primes.

Note that $m = s(2pq) \geq pq$, so that each preimage $2pq \leq 2m$, and so this disproves the conjecture for $K = 2$.

Simple algebra shows that

$$s(2pq) = (p+3)(q+3) - 6,$$

so it is enough to show that there are numbers with arbitrarily many representations in the form $(p+3)(q+3)$. For this we used a variant of a 1936 construction of Erdős (who had this with $p+3$ and $q+3$ replaced by $p-1$ and $q-1$).

By an elaboration on these methods, we show:

Theorem (Thompson, Pomerance, P.)

Fix $\alpha > 0$ and $\epsilon > 0$. Then there are infinitely many n for which $s^{-1}(n)$ intersects $((\alpha - \epsilon)n, (\alpha + \epsilon)n)$ in more than $n^{c/\log\log n}$ elements.

In the last section of this talk, I'd like to revisit a theorem of Davenport that came up earlier.

Proposition (Davenport, 1933)

For each real $u \geq 0$, consider the set

$$\mathcal{D}_s(u) = \{n : s(n)/n \leq u\}.$$

This set always possesses an asymptotic density $D_s(u)$. Considered as a function of u, the function D_s is continuous, with $D_s(0) = 0$ and $D_s(\infty) = 1$.

Putting Davenport in his place

A function $F\colon \mathbb{R} \to [0,1]$ is called a *distribution function* if

- F is increasing,
- F is right-continuous,
- $F(-\infty) = 0$ and $F(\infty) = 1$.

Example

If X is a (real-valued) random variable on a probability space, and F is defined as

$$F(t) := \Pr(X \leq t),$$

then F is a distribution function.

In fact, all examples arise this way.

Putting Davenport in his place, ctd.

If f is a real-valued arithmetic function, we say that f has a *limit law* (or *possesses a distribution function*) if there is a distribution function F such that

$$F(t) = \text{density of } n \text{ with } f(n) \leq t$$

for every real t at which F is continuous.

Davenport's theorem says precisely that $f(n) = \frac{s(n)}{n}$ has a continuous distribution function. Equivalently — and what Davenport actually proved — $\frac{\sigma(n)}{n}$ has a distribution function. (Notice $\frac{s(n)}{n} = \frac{\sigma(n)}{n} - 1$.)

Putting Davenport in his place, ctd.

Davenport's result is a special case of a celebrated theorem of Erdős–Wintner (1939) for *additive* functions.

Theorem

Let f be a real-valued additive function. Then f has a distribution function if and only if the following the three series all converge:

$$\sum_{|f(p)|>1} \frac{1}{p}, \qquad \sum_{|f(p)|\le 1} \frac{f(p)}{p}, \qquad \sum_{|f(p)|\le 1} \frac{f(p)^2}{p}.$$

The distribution function is continuous unless

$$\sum_{f(p)\neq 0} \frac{1}{p} < \infty.$$

Putting Davenport in his place, ctd.

Davenport's result is a special case of a celebrated theorem of Erdős–Wintner (1939) for *additive* functions.

Theorem

Let f be a real-valued additive function. Then f has a distribution function if and only if the following the three series all converge:

$$\sum_{|f(p)|>1} \frac{1}{p}, \quad \sum_{|f(p)|\le 1} \frac{f(p)}{p}, \quad \sum_{|f(p)|\le 1} \frac{f(p)^2}{p}.$$

The distribution function is continuous unless

$$\sum_{f(p)\neq 0} \frac{1}{p} < \infty.$$

Davenport: take $f(n) = \log \frac{\sigma(n)}{n}$.

It seems natural to ask what happens if one combines additive functions.

For example, suppose $f_1, \ldots, f_k$ are additive functions all of which possess distribution functions. If P is a polynomial in k variables, does $P(f_1, \ldots, f_k)$ possess a distribution function?

Yes!

If all the f_i have continuous distribution functions, does $P(f_1, \ldots, f_k)$ also have a continuous distribution function?

No! e.g., take $P(x, y) = x + y$. Then $P(f, -f) = 0$.

Whenever P is linear and $f_1, \ldots, f_k$ are additive, $P(f_1, \ldots, f_k)$ is again additive function (up to an additive constant).

Referring back to the necessary and sufficient condition for continuity in the E–W theorem, it is easy to arrange situations where all $f_1, \ldots, f_k$ have continuous distribution functions but $P(f_1, \ldots, f_k)$ does not.

In fact, linear polynomials provide the only essential obstruction.

Theorem (Lebowitz-Lockard and P., 2017+)

Let $f_1, \ldots, f_k$ be additive functions. Suppose that every $\mathbb{R}$-linear combination

$$c_1 f_1 + \cdots + c_k f_k$$

with not all $c_i = 0$ possesses a continuous distribution function. Then for any nonconstant polynomial $P(x_1, \ldots, x_k) \in \mathbb{R}[x_1, \ldots, x_k]$, the function $P(f_1, \ldots, f_k)$ also has a continuous distribution function.

Products of additive functions

Corollary

Let $f_1, \ldots, f_k$ *be additive functions each possessing a continuous distribution function. Then the product* $f_1 \cdots f_k$ *also possesses a continuous distribution function.*

Let me sketch a proof $k = 3$.

First, a piece of terminology. If $g_1, \ldots, g_\ell$ are additive functions with limit laws, we say the g_i are *independent* if every nontrivial linear combination of them has a continuous distribution function.

When f_1, f_2, f_3 are independent, the claim of the corollary is immediate from the theorem. (Take $P(x_1, x_2, x_3) = x_1 x_2 x_3$.)

Suppose, for illustration, that $\{f_1, f_2\}$ are independent but $\{f_1, f_2, f_3\}$ is not. (Other cases are similar.)

Then there are constants c_1, c_2 for which

$$g := f_3 - c_1 f_1 - c_2 f_2$$

has a discontinuous distribution function. Thus,

$$f_3 = c_1 f_1 + c_2 f_2 + g$$

where g is an additive function having a discontinuous limit law. Hence,

$$f_1 f_2 f_3 = f_1 f_2 (c_1 f_1 + c_2 f_2 + g).$$

Hence,

$$f_1 f_2 f_3 = f_1 f_2 (c_1 f_1 + c_2 f_2 + g).$$

If g were identically 0, the continuity of the limit law for $f_1 f_2 f_3$ would follow from the Main Theorem applied to $P(x, y) = xy(c_1 x + c_2 y)$. (Here we use that f_1 and f_2 are independent.)

In fact, if g assumed only finitely many values, say $\gamma_1 = 0, \ldots, \gamma_r$, we could deduce continuity by applying the theorem to the n polynomials

$$xy(c_1 x + c_2 y + \gamma_i),$$

for $i = 1, 2, \ldots, n$.

Since g has a discontinuous distribution function, E–W tells us

$$\sum_{p:\ g(p)\neq 0} \frac{1}{p} < \infty.$$

This implies that g assumes "essentially" only finitely many values: for each $\epsilon > 0$, there is a finite set of values $\{\gamma_i\}$ such that the n with $g(n)$ not any of the γ_i has upper density $< \epsilon$.

This allows the proof to be completed more-or-less as before.

Two footnotes

- One could also look at a polynomial in multiplicative functions. These are all linear combinations of mult. functions.

  By a variant of the method, Lebowitz–Lockard and I can handle many of these too; e.g.,

  $$\frac{\sigma(n)\cdot(-1)^{\Omega(n)}}{n} - 17\frac{\phi(n)}{\sigma(n)} + \pi \exp\left(\sum_{p\mid n}\frac{1}{\log p}\right)$$

  has a continuous distribution function.

- One could also look at polynomials in “large” additive functions like $\omega(n)$. (Think Erdős–Wintner vs. Erdős–Kac.) Martin and Troupe have results in this direction.

Thank you!