The Möbius transform and the infinitude of primes

Paul Pollack

Abstract

Say that the pair of arithmetic functions (f, g) is a *Möbius pair* if $f(n) = \sum_{d|n} g(d)$ for all natural numbers n. In this case, one can express g in terms of f by the Möbius inversion formula familiar from elementary number theory. We give a simple proof that if (f, g) is a Möbius pair, then f and g cannot both be of finite support unless they both vanish identically. From this, we deduce another proof of Euclid's famous theorem that there are infinitely many prime numbers.

Recall that the Möbius μ-function from elementary number theory is defined so that $\mu(n) = (-1)^k$ if n is a product of k distinct primes, and $\mu(n) = 0$ if n is divisible by the square of a prime. (So $\mu(1) = (-1)^0 = 1$.) For any arithmetic function f (i.e., any $f\colon \mathbf{N} \to \mathbf{C}$), its Dirichlet transform $\widehat{f}$ is defined by

$$\widehat{f}(n) := \sum_{d|n} f(d),$$

and its *Möbius transform* $\check{f}$ by

$$\check{f}(n) := \sum_{d|n} \mu(n/d) f(d).$$

The well-known Möbius inversion formula ([2, Theorems 266, 267]) says precisely that the Möbius and Dirichlet transforms are inverses of each other: for any f, we have $f = \check{\widehat{f}} = \widehat{\check{f}}$.

Our proof of the infinitude of primes is based on the following lemma. By the *support of* f, we mean the set of natural numbers n for which $f(n) \neq 0$.

Lemma (Uncertainty principle for the Möbius transform)**.** *If f is an arithmetic function which does not vanish identically, then the support of f and the support of $\check{f}$ cannot both be finite.*

Proof. Suppose for the sake of contradiction that both f and $\check{f}$ are of finite support. Let

$$F(z) = \sum_{n=1}^{\infty} f(n) z^n.$$

Then F is entire (in fact, a polynomial function). On the other hand, for $|z| < 1$, we have

$$\begin{aligned} F(z) &= \sum_{n=1}^{\infty}\left(\sum_{d\mid n}\check{f}(d)\right)z^n \\ &= \sum_{d=1}^{\infty}\check{f}(d)\left(z^d + z^{2d} + z^{3d} + \dots\right) = \sum_{d=1}^{\infty}\check{f}(d)\frac{z^d}{1-z^d}. \end{aligned} \tag{1}$$

Here the interchange of summation is justified by observing that

$$\sum_{n=1}^{\infty}\sum_{d\mid n}|\check{f}(d)||z|^n \leqslant A\sum_{n=1}^{\infty}n|z|^n = A\frac{|z|}{(1-|z|)^2} < \infty, \quad \text{where} \quad A := \max_{d=1,2,3,\dots}|\check{f}(d)|.$$

Since f is not identically zero, neither is $\check{f}$ (by Möbius inversion). Let D be the largest natural number for which $\check{f}(D) \neq 0$. The expression on the right-hand side of (1) represents a rational function with a pole at $z = e^{2\pi i/D}$. This contradicts that F is entire (and so bounded in the open unit disc). □

Theorem. *There are infinitely many primes.*

Proof. Suppose that there are only finitely many primes. Then there are only finitely many products of distinct primes; i.e., μ is of finite support. But $\mu = \check{f}$, where f is the function satisfying $f(1) = 1$ and $f(n) = 0$ for $n > 1$. For this f, both f and $\check{f}$ are of finite support, contradicting the lemma. □

Remarks.

(i) We have borrowed the term "uncertainty principle" from harmonic analysis. One of the simplest manifestations of this principle is the theorem that a nonzero function and its Fourier transform cannot both be compactly supported. This has a certain surface similarity to our lemma. The analogy can be more deeply appreciated if one brings into play the fact, first discerned by Ramanujan [3], that many arithmetic functions admit a type of Fourier expansion. For example, if $\sigma(n) := \sum_{d\mid n} d$ denotes the sum-of-divisors function, then

$$\frac{\sigma(n)}{n} = \frac{\pi^2}{6}\left(1 + \frac{1}{2^2}c_2(n) + \frac{1}{3^2}c_3(n) + \dots\right), \quad \text{where} \quad c_q(n) := \sum_{\substack{1\leqslant a\leqslant q \\ \gcd(a,q)=1}} e^{2\pi i\frac{an}{q}}.$$

In general, the (natural) coefficients in the Ramanujan–Fourier expansion of f are intimately connected with the values of $\check{f}$. For suitably "nice" f, the support of $\check{f}$ is finite precisely when the sequence of Ramanujan–Fourier coefficients of f is finitely supported. (Cf. paragraphs 27 and following in [5].)

(ii) The strategy for our proofs goes back to Sylvester [4], who gave an argument in the same spirit for the infinitude of primes $p \equiv -1 \pmod{m}$ when $m = 4$ or $m = 6$. There is also some resonance with Mirsky and Newman's demonstration that there is no exact covering system with distinct moduli greater than 1 (see [1]).

Acknowledgements

I would like to thank Enrique Treviño and Carl Pomerance for helpful comments.

References

[1] P. Erdős, *On a problem concerning congruence systems*, Mat. Lapok **3** (1952), 122–128.

[2] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, sixth ed., Oxford University Press, Oxford, 2008, Revised by D. R. Heath-Brown and J. H. Silverman.

[3] S. Ramanujan, *On certain trigonometrical sums and their applications in the theory of numbers*, Trans. Cambridge Philos. Soc. **22** (1918), 259–276.

[4] J. J. Sylvester, *On the theorem that an arithmetical progression which contains more than one, contains an infinite number of prime numbers*, Proc. London Math. Soc. **IV** (1871), 7–8.

[5] A. Wintner, *Eratosthenian Averages*, Waverly Press, Baltimore, 1943.