The Möbius transform and the infinitude of primes

Paul Pollack

Paul Pollack received his Ph.D. from Dartmouth College in 2008. He is currently finishing a postdoctoral appointment at the University of Illinois, Urbana, Illinois, USA. His research focuses on easily-stated problems in the theory of numbers.

Recall that the Möbius $\mu$-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 $f : \mathbb{N} \to \mathbb{C}$), its Dirichlet transform $\hat{f}$ is defined by

$$\hat{f}(n) := \sum_{d \mid n} f(d),$$

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

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

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

$$f = \check{f} = \hat{f}.$$
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 M"obius transform).** If \( f \) is an arithmetic function which does not vanish identically, then the support of \( f \) and the support of \( \hat{f} \) cannot both be finite.

**Proof.** Suppose for the sake of contradiction that both \( f \) and \( \hat{f} \) 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

\[
F(z) = \sum_{n=1}^{\infty} \left( \sum_{d|n} \hat{f}(d) \right) z^n = \sum_{d=1}^{\infty} \hat{f}(d) (z^d + z^{2d} + z^{3d} + \ldots) = \sum_{d=1}^{\infty} \hat{f}(d) \frac{z^d}{1-z^d}.
\]

(1)

Here the interchange of summation is justified by observing that

\[
\sum_{n=1}^{\infty} \sum_{d|n} |\hat{f}(d)||z|^n \leq A \sum_{n=1}^{\infty} n|z|^n = A \frac{|z|}{(1-|z|)^2} < \infty,
\]

where \( A := \max_{d=1,2,3,\ldots} |\hat{f}(d)| \).

Since \( f \) is not identically zero, neither is \( \hat{f} \) (by M"obius inversion). Let \( D \) be the largest natural number for which \( \hat{f}(D) \neq 0 \). 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). \( \square \)

**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., \( \mu \) is of finite support. But \( \mu = \hat{\mu} \), where \( \mu \) is the function satisfying \( \mu(1) = 1 \) and \( \mu(n) = 0 \) for \( n > 1 \). For this \( \mu \), both \( f \) and \( \hat{f} \) are of finite support, contradicting the lemma. \( \square \)

**Remarks.**

1) 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

\[
\frac{\sigma(n)}{n} = \frac{\pi^2}{6} \left( 1 + \frac{1}{2^2} c_2(n) + \frac{1}{3^2} c_3(n) + \ldots \right),
\]

where

\[
c_q(n) := \sum_{1 \leq a \leq q, \gcd(a,q) = 1} e^{2\pi i \frac{an}{q}}.
\]

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

2) 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]).

Acknowledgement

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

References


Paul Pollack
Department of Mathematics
University of Illinois at Urbana-Champaign
Urbana, Illinois 61801, USA
e-mail: twonth@gmail.com