

The Möbius transform and the infinitude of primes

Autor(en): **Pollack, Paul**

Objektyp: **Article**

Zeitschrift: **Elemente der Mathematik**

Band (Jahr): **66 (2011)**

PDF erstellt am: **09.08.2024**

Persistenter Link: <https://doi.org/10.5169/seals-283499>

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.

Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.

Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

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 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 $f: \mathbf{N} \rightarrow \mathbf{C}$), its Dirichlet transform \hat{f} is defined by

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

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

$$f = \check{\hat{f}} = \hat{\check{f}}.$$

Es gibt eine Vielzahl von Beweisen zur Unendlichkeit der Menge \mathbb{P} der Primzahlen. Der vermutlich den meisten Lesern bekannte Beweis geht von der Annahme $\mathbb{P} = \{p_1, \dots, p_m\}$ aus und führt diese Annahme durch Betrachtung der natürlichen Zahl $n = p_1 \cdots p_m + 1$ zum Widerspruch, da diese Zahl einen Primteiler p mit $p \notin \mathbb{P}$ besitzt; dieser Beweis wird Euklid zugeschrieben. Ein anderer, auf Euler zurückgehender Beweis, basiert auf der Eulerschen Produktentwicklung der Riemannschen Zetafunktion $\zeta(s)$ und der Tatsache, dass $\zeta(s)$ an der Stelle $s = 1$ einen Pol erster Ordnung hat. In der vorliegenden Arbeit finden wir einen weiteren Beweis zur Unendlichkeit von \mathbb{P} , der elementare Eigenschaften arithmetischer Funktionen f, g , welche die Beziehung $f(n) = \sum_{d|n} g(d)$ ($n \in \mathbb{N}$) erfüllen, verwendet.

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

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

Here the interchange of summation is justified by observing that

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

where $A := \max_{d=1,2,3,\dots} |\check{f}(d)|$.

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). \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., 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. \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 $\sigma(n) := \sum_{d|n} d$ denotes the sum-of-divisors function, then

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

where

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

In general, the (natural) coefficients in the Ramanujan-Fourier expansion of f are intimately connected with the values of \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].)

- 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

- [1] Erdős, P.: On a problem concerning congruence systems. *Mat. Lapok* 3 (1952), 122–128.
- [2] Hardy, G.H.; Wright, E.M.: *An introduction to the theory of numbers*. Sixth ed., Oxford University Press, Oxford 2008. Revised by Heath-Brown, D.R.; Silverman, J.H.
- [3] Ramanujan, S.: On certain trigonometrical sums and their applications in the theory of numbers. *Trans. Cambridge Philos. Soc.* 22 (1918), 259–276.
- [4] Sylvester, J.J.: 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] Wintner, A.: *Eratosthenian Averages*. Waverly Press, Baltimore 1943.

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