On spectral number theory

Robin Harte

School of Mathematatice, Trinity College Dublin hartere@gmail.com
AMS Classification: 11B25; 15B36
Key words: residual quotient, primes, spectrum

Abstract
Elementary number theory can be made to look like spectral theory.

1 Introduction

Masquerading as part of the Langlands program, this *jeu d'esprit* is really nothing more than an old Littlewood joke. It was sparked, initially, by a rumour that a subtle Japanese attack on Fermat's last theorem involved "square free" integers; then along came the book of "Rosenthal cubed", which proved that a veteran operator theorist could think of turning his hand to number theory. Also Read has demonstrated that "primes" can turn up in unlikely places.

2 Natural numbers

J.E. Littlewood, in his "Miscellany" [5], quotes a nameless savant who maintained that, every once in a while, a scientist should "perform a damfool experiment", such as "playing the trumpet to his tulips". In that spirit, we observe that elementary number theory can be described in language very like spectral theory. Recall

$$\mathbb{N} = \{1, 2, 3, \ldots\} = \bigcup_{n=1}^{\infty} \mathbb{N}_n \tag{2.1}$$

the natural numbers [7],[9], where

$$n \in \mathbb{N} \Longrightarrow \mathbb{N}_n = \{1, 2, \ldots n\} \ , \tag{2.2}$$

is an *initial segment*. The *Principle of Induction* says that, if $K \subseteq \mathbb{N}$ is arbitrary, there is implication

$$\big(1 \in K \ \textit{and} \ K + 1 \subseteq K\big) \Longrightarrow \mathbb{N} \subseteq K \ . \tag{2.3}$$

The apparently stronger principle of complete induction says, with

$$K^{\wedge} = \bigcup_{k \in K} \mathbb{N}_k \ , \tag{2.4}$$

that there is also implication, for $K \neq \emptyset$,

$$K^{\wedge} + 1 \subseteq K \Longrightarrow \mathbb{N} \subseteq K \ . \tag{2.5}$$

Now declare $m \in \mathbb{N}$ to be a *factor* or "divisor" of n, provided

$$n \in \mathbb{N}m \ . \tag{2.6}$$

Equivalently (Green's relation)

$$\mathbb{N}n \subseteq \mathbb{N}m \ . \tag{2.7}$$

The traditional notation is $m|n$; we shall prefer $m \prec n$, or instead

$$m \in \mathbb{N}_{-1}\{n\} \ . \tag{2.8}$$

Here, in contrast to *residual quotients* [3],[6],

$$K^{-1}H = \{x \in A : Kx \subseteq H\} \ ; \ HK^{-1} = \{x \in A : xK \subseteq H\} \ , \tag{2.9}$$

we write

$$K_{-1}H = \{x \in A : H \subseteq Kx\} \ ; \ HK_{-1} = \{x \in A : H \subseteq xK\} \ . \tag{2.10}$$

Thus

$$n \in \mathbb{N}m \Longleftrightarrow m \in \mathbb{N}_{-1}\{n\} \ . \tag{2.11}$$

The *highest common factor* $\mathrm{hcf}(m,n)$ of m and n is defined by setting

$$k = \mathrm{hcf}(m,n) \Longleftrightarrow \mathbb{N}_{-1}\{k\} = \mathbb{N}_{-1}\{n\} \cap \mathbb{N}_{-1}\{m\} \ . \tag{2.12}$$

It is curious how early in the discussion of the natural numbers, the subtleties of factorization present themselves; as "Uncle Petros" tells [1] his nephew, "addition is natural, but multiplication is artificial":

$$\mathbb{N} = \{1, 2, 3, 2^2, 5, 2\cdot 3, 7, 2^3, 3^2, 2\cdot 5, 11, 2^2\cdot 3, 13, 2\cdot 7, 3\cdot 5, 2^4, 17, \ldots\} \ . \tag{2.13}$$

3 Primes

The subset $\mathbb{P} \subseteq \mathbb{N}$ of *primes* is fundamental:

$$\mathbb{P} = \{p \in \mathbb{N} : \mathbb{N}_{-1}\{p\} = \{1, p\}\} \setminus \{1\} \ . \tag{3.1}$$

We shall write, for $n \in \mathbb{N}$,

$$\mathbb{P}_n = \mathbb{P} \cap \mathbb{N}_n \ . \tag{3.2}$$

It is the *fundamental theorem of arithmetic* ([9] Theorem 4.1.1) that

$$\mathbb{N} = \prod \mathbb{P} \ : \tag{3.3}$$

every natural number is (uniquely) a (finite) product of primes. We get about half way there if we observe ([9] Lemma 1.1.1) every non-trivial natural number has at least one prime factor:

$$1 < n \in \mathbb{N} \Longrightarrow N_{-1}\{n\} \cap \mathbb{P} \neq \emptyset \ ; \tag{3.4}$$

now proceed by (complete) induction. It follows that $\mathbb{P}$ is infinite: for if, to the contrary

$$\mathbb{P} \subseteq \mathbb{N}_n \ ,$$

then nowhere in the product $n! + 1$ could there be any primes. Thus

$$\mathbb{P} = \{p_1, p_2, p_3, \ldots\} = \{2, 3, 5, 7, \ldots\} \subseteq \mathbb{N} \ , \tag{3.5}$$

where, as sequences rather than sets,

$$\mathbf{p} = (p_1, p_2, p_3, \ldots) = (2, 3, 5, 7, \ldots) \in \mathbb{N}^{\mathbb{N}} \ ; \tag{3.6}$$

recursively (*Sieve of Erastothenes*)

$$p_{j+1} = \mathrm{Min}(\mathbb{N} \setminus \{1\} \setminus p_j\mathbb{N}) \tag{3.7}$$

with of course

$$p_1 = 2 = \mathrm{Min}(\mathbb{N} \setminus \{1\}) \ .$$

The fundamental theorem of arithmetic now gives the factorization, for $1 < n \in \mathbb{N}$,

$$\prod\{p^{\nu_n(p)} : p \in \mathbb{P}\} = n = \prod_{j=1}^{\infty} p_j^{\nu_j(n)} \ , \tag{3.8}$$

where $\nu_n : \mathbb{P} \to \mathbb{P}$ is the *multiplicity function*, and perversely we write $\nu_j(n) = \nu_n(p_j)$. Formally, if $1 < n \in \mathbb{N}$,

$$\nu_n(p) = \mathrm{Max}\{k \in \mathbb{N} : p^k \in \mathbb{N}_{-1}\{n\}\} \ . \tag{3.9}$$

There is of course no simple formula for the mapping $n \mapsto p_n : \mathbb{N} \to \mathbb{N}$. If we reflect that the *factorial function*

$$n \mapsto n! = 1 \cdot 2 \cdot \ldots \cdot n = \prod \mathbb{N}_n \tag{3.10}$$

has a significant extension to the complex plane (the *Gamma function*), we might wonder whether there could be something similar for the inscrutable "prime function" $\mathbf{p} : n \mapsto p_n$. It is sometimes difficult to be sure that $n \in \mathbb{N}$ is prime: but if we can find $p \in \mathbb{P}$ for which

$$p < n < p^2 \ , \tag{3.11}$$

then we need only search $\mathbb{P}_p$ for factors of n; if there are none then $n \in \mathbb{P}$. It is salutary, if you have a digital clock beside your bed, and are finding it difficult to sleep, to lie there and factorize the time; you will get a new problem every sixty seconds, and will be too drowsy to go and look anything up.

4 Spectrum

If in a Littlewood "damfool experiment" we set [4]

$$\varpi(n) = \{p \in \mathbb{P} : p \in \mathbb{N}_{-1}\{n\}\} \ , \tag{4.1}$$

then we can think of ϖ as some kind of "spectrum". Evidently

$$\varpi(n) \subseteq \mathbb{P}_n \subseteq \mathbb{N}_n \ . \tag{4.2}$$

There is two way implication, for $n \in \mathbb{N}$,

$$n = 1 \Longleftrightarrow \varpi(n) = \emptyset \ . \tag{4.3}$$

If $n \in \mathbb{N}$ and $p \in \mathbb{P}$ then

$$p < n < p^2 \Longrightarrow \varpi(n) \subseteq \bigcup \mathbb{P}_p \cup \{n\} \ . \tag{4.4}$$

$n \in \mathbb{N}$ is a *prime power* provided its spectrum is a singleton

$$\#\varpi(n) = 1 \ , \tag{4.5}$$

and *square free* provided every point of its spectrum has multiplicity one

$$p \in \varpi(n) \Longrightarrow \nu_n(p) = 1 \ . \tag{4.6}$$

Thus a square free prime power is itself a prime. The "spectral mapping theorem" here is [4],[8],([9] Corollary 4.1.3 , Lemma 7.2.2) another sort of logarithmic law:

$$\{m, n\} \subseteq \mathbb{N} \Longrightarrow \varpi(mn) = \varpi(m) \cup \varpi(n) \ . \tag{4.7}$$

Fermat's (little) theorem says ([9] Theorem 5.1.1) that

$$(1 < n \in \mathbb{N} \textit{ and } p \in \mathbb{P}) \Longrightarrow p \in \varpi(n) \cup \varpi(n^{p-1} - 1) \ , \tag{4.8}$$

and *Wilson's theorem* ([9] Theorem 5.2.1) that

$$p \in \mathbb{P} \Longrightarrow p \in \varpi(1 + (p-1)!) \ . \tag{4.9}$$

Finally [4],[9], the *Euclidean Algorithm* demonstrates implication

$$\varpi(m) \cap \varpi(n) = \emptyset \Longrightarrow 1 \in \mathbb{Z}m + n\mathbb{Z} \ : \tag{4.10}$$

spectral disjointness appears to imply "splitting exactness". Indeed there is two way implication

$$\varpi(n) \cap \varpi(m) = \emptyset \Longleftrightarrow \mathrm{hcf}(m, n) = 1 \ , \tag{4.11}$$

and generally

$$\mathrm{hcf}(m, n) \in \mathbb{Z}m + n\mathbb{Z} \ . \tag{4.12}$$

As with linear algebra spectral theory, the spectrum gives only limited information about an element, and "spectral mltiplicity" adds more; indeed here, according to the fundamental theorem of arithmetic, the spectrum $\varpi(n)$ and the multiplicity function ν_n together completely determine $n \in \mathbb{N}$.

Our spectrum lies in the complement of the "totatives" of n: with

$$\mathrm{Tot}(n) = \{k \in \mathbb{N}_n : \mathrm{hcf}(k, n) = 1\} \ , \tag{4.13}$$

we have

$$\varpi(n) \subseteq \mathbb{P}_n \setminus \mathrm{Tot}(n) \ , \tag{4.14}$$

and *Euler's totient function* is defined by the formula

$$\phi(n) = \#\mathrm{Tot}(n) = \#\big(n\mathbb{Z}/(n\mathbb{Z})^{-1}\big) \ . \tag{4.15}$$

For example if $p \in \mathbb{P}$ then $\phi(p) = p - 1$. and if $\{p, q\} \subseteq \mathbb{P}$ are distinct primes then ([9] Theorem 6.1.2)

$$\phi(pq) = (p-1)(q-1) \ . \tag{4.16}$$

5 Polynomials

Complex polynomials in one variable have arithmetic similar to the integers: if

$$p = z^k + \ldots + \alpha_1 z + \alpha_0 \in \mathrm{Poly}_1 \subseteq \mathbb{C}^{\mathbb{C}} \tag{5.1}$$

is a "monic" polynomial, then the *fundamental theorem of algebra* [7],[9] says that

$$p \equiv p(z) = \prod_{j=1}^{k}(z - \lambda_j) = \prod_{\lambda \in \mathbb{C}}(z - \lambda)^{\nu_p(\lambda)} \ \ : \tag{5.2}$$

here there are possible repetitions among the $\{\lambda_j : j \in \{1, 2, \ldots, k\}\}$, while all but finitely many of the $\nu_p(\lambda)$ vanish:

$$p \in \mathrm{Poly}_1 \subseteq \mathbb{C}[z] \Longrightarrow \#\{\lambda \in \mathbb{C} : \nu_p(\lambda) \neq 0\} < \infty \ . \tag{5.3}$$

The "primes" among the monic polynomials are $\{z - \lambda : \lambda \in \mathbb{C}\}$, and $p \in \mathrm{Poly}_1$ has both a "vector-valued" spectrum

$$\varpi(p) = \{z - \lambda_j : j \in \{1, 2, \ldots k\}\} = \{z - \lambda : \nu_p(\lambda) \neq 0\} \ , \tag{5.4}$$

with a multiplicity function $\nu_p : \mathbb{C} \to \mathbb{N} \cup \{0\}$, and a numerical spectrum

$$\sigma(1/p) = p^{-1}(0) \subseteq \mathbb{C} \ . \tag{5.5}$$

The Euclidean algorithm continues to apply: if $\{q, r\} \subseteq \mathrm{Poly}_1$ then

$$q^{-1}(0) \cap r^{-1}(0) = \emptyset \Longrightarrow 1 \in \mathbb{C}[z]q + r\mathbb{C}[z] \ . \tag{5.6}$$

This has an application [2] to the "diagonalization" of a matrix $T \in \mathbb{C}^{k \times k}$: if

$$p \equiv p(z) = \det(T - zI) \tag{5.7}$$

is the *Cayley-Hamilton* polynomial and $\lambda \in p^{-1}(0)$ is an eigenvalue then we can write

$$p = q \cdot r \ \textit{with}\ q = (z - \lambda)^\ell \ \textit{and}\ q^{-1}(0) \cap r^{-1}(0) = \emptyset \ , \tag{5.8}$$

and hence

$$(T - \lambda I)^{-1}(0) \subseteq q^{-1}(0) \subseteq r(T)\mathbb{C}^k \ \ : \tag{5.9}$$

all the eigenvectors $x \in (T - \lambda I)^{-1}(0)$ will be among the columns of the matrix $r(T)$.

6 References

[1] Doxiadis, A. Uncle Petros and Goldbach's conjecture *Bloomsbury* (1992)

[2] Harte, R.E. Cayley-Hamilton for eigenvalues *Irish Math. Soc. Bull.* 22 (1989) 66-68

[3] Harte, R.E. Residual quotients *Funct. Anal. Approx. Comp.* 7 (2015)

[4] Harte, R.E. Spectral dsjointness and the Euclidean algorithm *Math. Proc. Royal Irish Acad.* 118A (2018) 65-69

[5] Littlewood, J.E. A mathematician's miscellany

[6] Northcott, D.G. Ideal theory *Cambridge Tracts in Mathematics* 42 (1960)

[7] O Searcoid, M. Elements of Abstract Analysis *Springer Undergraduate Texts in Mathematics* 515 (2002)

[8] Read, C.J. All primes have closed range *Bull. London Math. Soc.* 33 (2001) 311-346

[9] Rosenthal, D., Rosenthal, D. and Rosenthal, P. A readable introduction to real mathematics *Springer Undergraduate Texts in Mathematics* (2014)