PRIMES AND RIEMANN ZEROS

LUCIAN M. IONESCU
ILLINOIS STATE UNIVERSITY AND I.H.E.S.

Abstract. Intuitively, prime numbers of "Number systems" (rings) are the building blocks of their elements.

We start from natural numbers and Gaussian integers to explain more general frameworks, like the structure theorem for finitely generated Abelian groups.

We end with a 1 million dollar puzzle, the Riemann Hypothesis, and point to the fact that prime numbers are dual to the Riemann zeros.

Some easy references are provided.

Contents

1. Fundamental Theorem of Arithmetic 1
1.1. Rational primes 1
1.2. Gaussian primes 1
1.2.1. ... and the Two Squares Theorem of Fermat 1
1.3. On Mathematical Structures 2
1.3.1. Numbers as Shadows of Mathematical Structures 2
2. Structure of Prime Numbers 2
2.1. Generating primes 2
2.1.1. What is the structure of Primes Numbers? 2
2.1.2. Generating the Prime Numbers 3
2.2. Deconstructing primes 3
2.2.1. Deconstructing primes 3
2.3. The POSet of Prime Numbers 3
2.3.1. The POSet of Primes 4
2.3.2. Parameters and Properties 4
3. The Duality Primes - Riemann Zeros 5
3.1. Riemann Zeta Function Zeros 5
3.2. The Duality 5
3.2.1. A first connection with Primes 5
3.2.2. The Prime-Zeros Duality 5
3.3. Behind Riemann Zeros: shadows of ... what? 5
3.3.1. Finite fields and primes 6

Date: April 18, 2022.

3.3.2. Riemann zeros and ... what? 6
3.3.3. ... and Fundamental Theorem of Discrete Calculus 6
3.3.4. ... and Weyl Zeros 7
References 7

1. Fundamental Theorem of Arithmetic

1.1. **Rational primes.** Primes $2, 3, 5...$ are the natural numbers that cannot be factored.

Through multiplication they generate all natural numbers:

$$(N, \cdot) =< 2, 3, 5, ... >$$

This is known as the *Fundamental Theorem of Arithmetic*

Theorem 1. Any natural number can be represented as a product of primes, in a unique way modulo order:

$$n = \prod p_1^{k_1} ... p_l^{k_l}, \qquad ex. : 12 = 2^2 \cdot 3.$$

This is the "free case", where the generators are independent, and we may think of elements as *functions*: $Q = F(Spec(Z), Z)$ (extending the framework to ring of rational numbers).

1.2. **Gaussian primes.** If we extend $(Z, +, \cdot)$ to *Gaussian integers*, which are complex numbers of the form $n + im$, with n and m integers, we have an analog of such elements that cannot be factored non-trivially, called *Gaussian primes*.

Examples: $1 + i$, $1 + 2i$, $2 + 3i$ etc. Some rational primes are still Gaussian primes: $3, 7, 11$ etc.

Since we have enlarged the number system from Z to $Z[i]$, we expect more factorizations of integers are possible, hence some of the *rational primes* are no longer irreducible here:

$$2 = (1 + i)(1 - i), \quad 5 = (1 + 2i)(1 - 2i) \quad \cdots$$

1.2.1. *... and the Two Squares Theorem of Fermat.* A beautiful theorem due to Pierre de Fermat, a French "amateur" mathematician from 17th century, tells us which rational primes factor into a product of Gaussian primes (*split*), and which do not (are *inert*).

Theorem 2. An odd rational prime p factors as a Gaussian integer iff $p \cong 1$ *mod* 4. Then we have:

$$p = (m + in)(m - in) \Leftrightarrow p = m^2 + n^2.$$

Example $13 = (2+3i)(2-3i), 13 = 2^2 + 3^2$, where indeed $13 \cong 1$ *mod* 4.

Why *mod* 4? ... to have a congruence arithmetic analog of i, i.e. an element of order four $i^4 = 1$, so we would have a 2D analog of the Gaussian plane / integers (a torus here).

The analog of the Fundamental Theorem of Arithmetic holds true in this Number System.

It is not true that il will hold in more general extensions. For example

$$2 \cdot 3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

provides two distinct factorizations of 6 in $Z[\sqrt{-5}]$.

1.3. **On Mathematical Structures.**

1.3.1. *Numbers as Shadows of Mathematical Structures.* For the Abstract Algebra aficionado, we mention that natural numbers are sizes of Abelian groups ("integrals" with respect to counting measure) and the Fundamental Th. of Arithmetic is the "shadow" of the *Fundamental Theorem for (finitely generated) Abelian Groups.*

For example $6 = 2 \cdot 3$ "comes from" the Chinese reminder Theorem saying in this case $Z/6 = Z/2 \times Z/3$.

Specifically, taking the number of elements of abelian groups in the FT for Finitely Generated Abelian Groups yields the FTA for natural numbers.

Example: for $n = 12$ we have, with notation $Z_n := Z/n$:

$$Z/12 \cong Z_{2^2} \times Z_3, \quad 12 = |Z_{12}| = |Z_{2^2} \times Z_3| = 2^2 \cdot 3,$$

The linear version of this is taking the dimension of vector spaces.

2. Structure of Prime Numbers

2.1. **Generating primes.**

2.1.1. *What is the structure of Primes Numbers?* While $N =< Primes >$, what about $Primes =< \cdots >$? How can we **generate the prime numbers**?

For example, *new primes can be generated by the Euclid "trick"*, used in his proof that there are infinitely many prime numbers:

$$N = p_1 p_2 ... + 1 = \prod q_i.$$

We use here the term "generated" in the sense that *new primes* q_i result from the factorization of N.

For example:

$$2 \cdot 3 \cdot 5 + 1 = 31$$

but the 6-th *primorial* fails to yield in this way a prime:

$$N(p_{5\#}) = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 59 \cdot 509.$$

2.1.2. *Generating the Prime Numbers.* The ancient method for determining prime numbers less then a given bound, and hence "generating" prime numbers, is the well-known Erathostene's Sieve.

There is a new procedure for generating prime numbers invented by McCanney (2006) [3, 2], using primorials.

Specifically, apply Erathostene Sieve elimination of multiples of previously found primes, to the integers generated by a generalization of Euclid's trick:

$$N = p_{\#n} \pm q.$$

Here we add or subtract q, which is either the unit as in Euclid's trick, or a prime already generated, but bigger than p_n. Example: with $2, 3$ already found, $N_1 = 2 \cdot 3 \pm 1$

gives $5, 7$ and $N_2 = 6 + 5 = 11, N_3 = 6 + 7 = 13$. We get in one iteration four more primes.

2.2. **Deconstructing primes.**

2.2.1. *Deconstructing primes.* The reverse procedure of *deconstructing a prime* works every time:

$$13 - 1 = 2^2 \cdot 3, \quad 31 - 1 = 2 \cdot 3 \cdot 5.$$

This is the *shadow* of the Chinese Reminder Theorem applied to the group of automorphisms of the primary abelian groups $(Z/p, +)$; or if you like better, the group of units of the ring $(Z/p, +, \cdot)$, which happens (for a reason) to be a field [1].

For example:

$$F_{13}^* = (Z/13, +, \cdot)^* \cong Z/12 = Z/2^2 \times Z/3.$$

Lazlo Fuchs-like Question: when Euclid's trick yields a prime? Equivalently when multiplying primary abelian groups yields the group of units of a ring, and when is that ring a field?

2.3. **The POSet of Prime Numbers.**

[1] this may be confusing at first reading ...

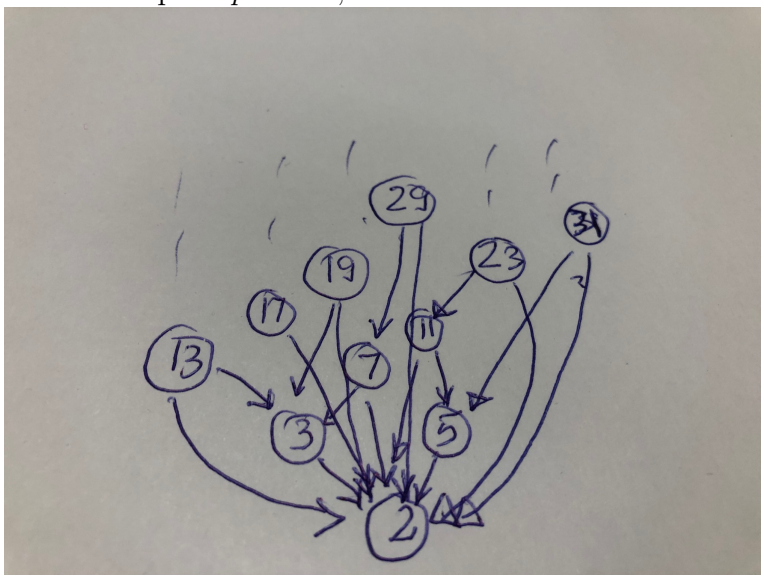
2.3.1. *The POSet of Primes.* This leads to a partial order set structure on the set of primes: to each prime we can associate a rooted tree, by repeatedly deconstructing primes (see my paper [1]).

For example $13- > (2, 3)$ and $3- > 2$ while 2 is a final node in such a rooted tree. Another example for $p = 47$ can be found in [1].

The rooted tree comes from the graph representing the partial order, with 2 as a final node.

If we consider all primes, we have an infinite graph originating from 2, extending "upwards", representing the *POSet of Prime Numbers*.

More examples: $p = 131$, ...



2.3.2. *Parameters and Properties.* There are several parameters / weights that "grade" the primes, refining the linear order defined by their sizes (position on the x-axis):

1) *Depth* of the graph associated to a prime; ex. $d(31) = 3$, depth of Fermat primes is 1;

2) *Width* of the POSet at a given *height*; e.g. $w(1) = 2$ etc.

One has obvious candidates for "refining" The Prime Number Theorem: how many primes are there at a given height, correlation depth / size etc.

Note there are other properties associated to primes, like the *branching rank* rk; for Sophie Germain primes $q = 2p + 1$ (safe primes) it is $rk = 1$ (number of cyclic generators of symmetries; 2 is a reflection in F_q).

Here we have disregarded the powers of primes entering as descendants (symmetries) of a prime (finite field).

3. The Duality Primes - Riemann Zeros

3.1. **Riemann Zeta Function Zeros.** Riemann zeros are the non-trivial zeros of the Riemann zeta function, which is an analytic function of a complex variable s:

$$\zeta(s) = \sum_{n=1,2,3...} n^{-s} = \prod \frac{1}{1-p^{-s}}.$$

These are zeros in the sense of analitic continuation ($\ln \zeta(s)$ has *periods* there: Cauchy loop integrals).

All the zeros computed are of the form $s_k = x_k + iy_k$, with $x_k = 1/2$. The first few ordinates are $y_k : 14.1..., 21.0..., 25.0..., 31.4...$, for $k = 1..3$.

Riemann Conjecture. *All Riemann zeros are situated on the vertical line $z = 1/2$.*

It is one of the Millennium Problems, with a 1 mil dollars price on its proof.

3.2. **The Duality.**

3.2.1. *A first connection with Primes.* Note the presence of primes in Euler's product form of the RZF.

Assuming RC and rewriting, yields:

$$p_j^{-s_k} = p_j^{-\frac{1}{2}} p_j^{-iy_k} = \sqrt{p_j} e^{2\pi i (y_k/2\pi) \ln p_j},$$

we see $\ln p$ pop-out ... What *are* these polar angles, we don't know (may be an analog / related to Gauss periods and Weyl zeros that we understand in connection with finite fields and Weyl conjectures: see my articles on this subject, as well as [4]).

3.2.2. *The Prime-Zeros Duality.* There is an Fourier-like transform (Dirichlet transform as a discrete Melin transform) that relates *prime powers and zeros*: a series on prime powers localizes at R-zeros and a series on R-zeros that localizes at prime powers, in the sense of distributions (generalized functions, like Dirac delta function).

See [5] for details and the easy books [6, 7].

3.3. **Behind Riemann Zeros: shadows of ... what?**

3.3.1. *Finite fields and primes.* Numbers are shadows of Abelian groups (f. gen.):

$$Z/6 = Z/2 \times Z/3, \quad 6 = 2 \cdot 3.$$

Prime powers are shadows of finite fields F_{p^k} and of primary abelian groups Z/p^k:

$$|F_7| = 7, \quad |F_7^* \cong Z_2 \times Z_3| = 6 = 2 \cdot 3.$$

The later are truncations of p-adic numbers!

Categorically speaking, integration on f. gen. Abelian groups is a multiplicative functor: Fundamental Theorems for Abelian groups / natural numbers.

Note also that the multiplicative group of a finite field F_p^* is $Aut(Z/p, +)$ is a torsor ("loop group" / algebraic fundamental group), and the POSet's nodes are obtained by repeatedly applying $Aut()$.

3.3.2. *Riemann zeros and ... what?* Since primes and zeros are in duality, what is the mathematical object analog to a finite field F_p, via this duality?

Note that the finite field is really the tautological representation:

$$F_p^* \cong Aut(Z/p, +) \xrightarrow{\rho} Aut(Z/p, +).$$

If $p = |F_p|$ is thought of as a "discrete period" (cardinal as a measure) then what corresponds to a Riemann zero, or better as a *pole* of the inverse of RZF?

So, the "primes-zeros game" is played in the category $Ab_{f.g.}$ with some Fourier Transform (group rings and arithmetic functions?) ...

Indeed ...

3.3.3. *... and Fundamental Theorem of Discrete Calculus.* Recall that Mobius function μ and the constant function 1 are inverse to one another with respect to convolution and that Dirichlet Transform D is a homomorphism:

$$1(n) \star \mu(n) = \delta(n) \text{ and } D(1) = RZF \Rightarrow \quad D(\mu) = 1/RZF.$$

Now convolution with 1 is summation (discrete integration) and convolution with μ is finite difference operator (differentiation).

These two operators $\int(f) = 1 \star f$ and $d(f) = \mu \star f$ are "inverse" to one another, satisfying the Fundamental Theorem of Discrete Calculus for arithmetic functions.

... so, what else!?

3.3.4. *... and Weyl Zeros.* Finite fields allow to consider algebraic curves (group ring and polynomials) and the theory of Weyl zeros at a prime.

Riemann zeros should be related to Weyl zeros in some way; finite fields are "Spec" (irred. / tangent spaces in the sense of Deformation Theory) of Ab, so we expect R-Spec to be in some sense global periods of collections of Weyl zeros ...

These is just food for thought, of course, with a millenium price for understanding this RH "puzzle" (with so many math pieces interconnected).

References

[1] L. M. Ionescu, A natural partial order on prime numbers, https://arxiv.org/abs/1407.6659

[2] McCanney, Procedure for generating prime numbers, Google slides by L. M. Ionescu: https://docs.google.com/presentation/d/1MFpiHlg4fYlSMeYrMTAGHJQzmWXakV6VwNQoSP_b_kU/edit#slide=id.gbec6ef573_11

[3] M. J. McCanney, Calculate prime numbers - Direct propagation of prime numbers, https://www.amazon.com/Calculate-Primes-Direct-Propagation-Prime-Numbers/dp/0972218661

[4] L. M. Ionescu, A note on the statistic of prime numbers, https://arxiv.org/pdf/1903.09318.pdf

[5] L. M. Ionescu, On prime Numbers and the Riemann Zeros, Journal of Advances in Applied Mathematics, Vol. 2, No. 4, October 2017, pp.208-219, http://www.isaacpub.org/1/1423/2/4/10/2017/JAAM.html; https://arxiv.org/abs/2204.00899;

[6] B. Mazur, W. Stein, Primes: What is Riemann's Hypothesis?, (draft), http://modular.math.washington.edu/rh/rh.pdf

[7] Marcus de Satoy, The Music of the Primes: Searching to Solve the Greatest Mystery in Mathematics, Harper Perennial, 2012.