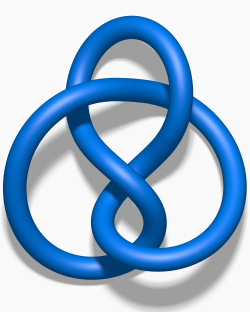
Thoughts about Primes and Knots

Barry Mazur

April 15, 2021


[1]

Contents

[1] Weisstein, Eric W. "Hyperbolic Knot." From MathWorld–A Wolfram Web Resource. https://mathworld.wolfram.com/HyperbolicKnot.html

1 CHAT

I'm delighted to have been asked by Shekar and Chi-Yun to be part of the 'experiment' in this (experimental) series of talks: *CHAT: Career, History and Thoughts*. Shekar has asked me to "take a step back and talk about... larger visions that were then incarnated in specific results... specific influences etc."

This has given me the excuse to think about the various evolutions of interest and focus that I and other mathematicians have had. It may be illuminating to consider those *arcs of interest* that connect different fields and different projects in mathematics—sometimes in more personal than 'formal' ways.

There is, of course, also the evolution of our subjects. Thinking of Algebraic Geometry, how it had its center of gravity in the Italian school—led by Francesco Severi—in the early twentieth century. The temper of that school was *non-rigor*. They were very focused on the 'geometry' —of 'algebraic geometry'—as their primary source of intuition. Among the freedoms they took for themselves was to often assume that the objects they were dealing with could be put "in general position"—and give no formal justification for this.

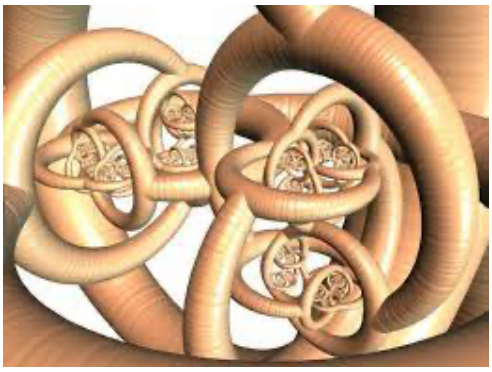
The move towards focusing on the 'algebra' —of 'algebraic geometry'—while, concomitantly, coming up with a rigorous approach to the subject was successfully done by Oscar Zariski (and others) who yoked the powerful commutative algebra of Wolfgang Krull and Emmy Noether (and others) to the intuition of the Italians.

At approximately the same time there were interesting *ultra-algebraic* approaches to aspects of—at least—the algebraic geometry of curves, such as Claude Chevalley's *Introduction to the Theory of Algebraic Functions of One Variable*. If you haven't taken a look at this, do, since it presses a purely algebraic view of the algebraic geometry of curves, without a picture in the book, or even

pictorial language—it is all fields and extensions of fields— it's a curious tour de force with no hint of geometric intuition rather analogous to the way George Perec wrote an entire novel[2] in which the letter "e" never occurs in the text.

In contrast, there was the *Séminaire Chevalley*—that I attended in Paris, in 1957/8—where Chevalley developed his ideas about the foundations of algebraic geometry: a view of the subject that was a precursor to Grothendieck's *Langage des Schémas*.

At the time—the late fifties of the past century—I was a graduate student working in Topology—or, as I would refer to it at the time "Pure Topology," meaning that I felt its true mission to be to understand topological truths unencumbered by crutches such as smoothness hypotheses—or, heavens forbid!—algebraic structure. In my thesis I proved the Schoenflies Conjecture that says that any reasonably collared $(n-1)$-dimensional sphere in n-space was (topologically) the 'standard' $(n-1)$-dimensional sphere.[3] I was very much in awe of the magical construction of R.H. Bing who showed that the double of the closure of the *bad* component of the complement of the Alexander horned sphere in the three-dimensional sphere S^3 is again (topologically) S^3 giving, therefore, a thoroughly wild and untamable involution of S^3:



[4]

And I was fascinated by knots in S^3. Knots and their exquisitely idiosyncratic properties, are the vital essence of three-dimensional topology; these have the DNA that governs the development, and evolution, of that field; and knots form a link to many other—seemingly far-flung—aspects of mathematics.

In time, I found myself drawn more and more toward algebraic geometry—initially in work with Michael Artin where we applied Nash theory (i.e., real algebraic geometry) to the study of periodic points of diffeomorphisms. A natural move for me was to try to understand algebraic geometry per se; and then, later, the extraordinarily powerful view of mathematics afforded by Grothendieck's

[2] *La Disparition*

[3] Subsequently people have proved that (for all $n \neq 4$) smoothly embedded $(n-1)$-dimensional spheres are smoothly standard; the 4-dimensional case is *still open*.

[4] Courtesy of Cameron Brown

theory of schemes. And how it launched a true fusion of *arithmetic, algebra* and *geometry*. "Arithmetic Algebraic Geometry" is a phrase quite familiar nowadays—and certainly very familiar to many in this seminar—but at the inception of the *Langage des Schémas* that fusion of different viewpoints, and techniques had a brilliant newness to it—and deepened each of the three subjects[5]; it was something I couldn't keep away from.

It was natural, then, for me to work with Mike Artin in the formulation of *Étale Homotopy Theory* which brought into play the full context of homotopy types, but connected directly to algebraic geometry–and even more intriguingly, to arithmetic. As I muse over this now I recall that one other project I had in mind—never to be developed at all, at least by me—was to associate to each étale homotopy type, a full Postnikov tower (algebraic geometric—very likely: necessarily with infinite-dimensional objects).

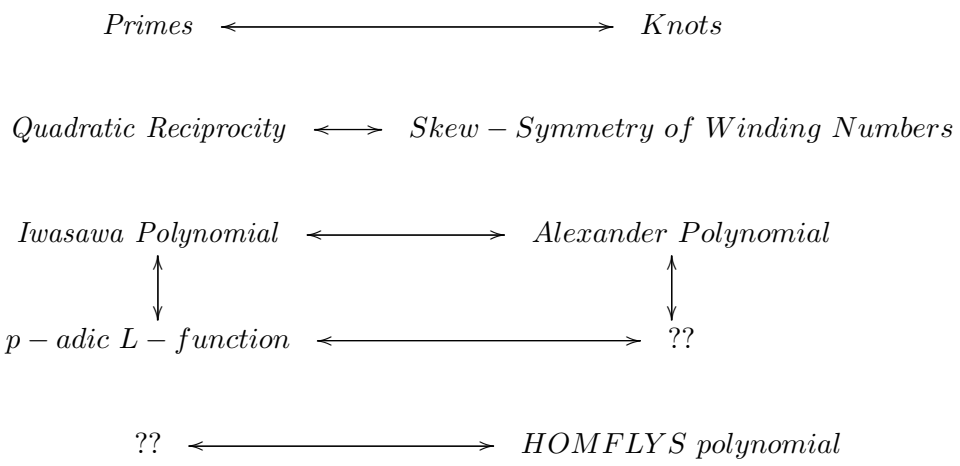
When I was trying to get a feel for number theory, I found that a certain illuminating analogy between the knot theory that I knew as a topologist and the phenomenology of prime numbers (that I was trying to become at home with) was exceedingly helpful, as a bridge. I've returned to it often as a learning device; it allows two-way traffic, from knots to primes, and from primes to knots. It got me to beam in on cyclotomic extensions—the objects that were once referred to by Serge Lang as "the backbone of number theory"— since they are analogous to abelian coverings of the three-dimensional sphere ramified at links. It made me immediately 'at home' in number theory. I imagine that many mathematicians have examples of similar levers that allow them to move from one type of intuition to another.

For a recent beautiful introductory account of the analogy between number theory and knot theory, see M. Morishita's treatise, *Knots and Primes*, [6] and his archiv survey: [8].

So, this is what I want to "CHAT" about. This basic analogy *Primes* $\leftrightarrow$ *Knots* pairs purely arithmetic structures with topological structures, such as:

[5]This is reminiscent of René Descartes' [3]:

> ... there is no need to impose any restrictions on our mental powers; for the knowledge of one truth does not, like skill in one art, hinder us from discovering another; on the contrary it helps us... It must be acknowledged that all the sciences are so closely interconnected that it is much easier to learn them all together than to separate one from the other. If, therefore, someone seriously wishes to investigate the truth of things, he ought not to select one science in particular, for they are all interconnected and interdependent. ...



The question-marks in this framework are worth further exploration, I think. I've actually talked about this a few times, the latest being in a celebration conference for my very good friend Valentin Poenaru's 80-th birthday. (This paper is a rewriting—in the direction of a "CHAT"— of *Primes, Knots, and Po* [9]; i.e., the notes to my talk at that conference.)

I realized, after having given that lecture that one could be even more precise, by making the comparison between *prime numbers* and—more specifically—the class of *hyperbolic knots* (which, in contrast to the class of *all* knots have very few members, conjecturally, in each commensurability class[6]). This choice also has the virtue of allowing us to make use of the hyperbolic volume of the complement of the knot, $vol(K)$, as a ready-made analogue to the logarithm of the norm of the prime[7].

The format of our comparison is then:

$$\textbf{Prime Numbers } p \quad \leftrightarrow \quad \textbf{Hyperbolic Knots } K$$

$$\log p \quad \leftrightarrow \quad vol(K)$$

So what I'll say today will recall a bit of what I said there, but go a bit further.

2 The Underlying Analogy: $\mathcal{S} := \mathrm{Spec}(\mathbf{Z})$ *as* The "three-dimensional sphere."

First, any connected finite extension of the ring of integers $\mathbf{Z}$ is ramified—so $\mathcal{S}$ is simply connected.

[6]Two knots K, K' are said to be **commensurate** if there are finite covers M, M' of their respective knot complements such that M is homeomorphic to M'.

[7]As Morishita commented on an early draft of these notes, one might also take the closely related *Gromov norm* of the knot complement.

As for the cohomology of $\mathcal{S} := \mathrm{Spec}(\mathbf{Z})$ one needs some class field theory, but reformulated in the vocabulary of étale (and some other Grothendieckian) cohomology theories. The scheme $\mathcal{S}$ possesses a three-dimensional 'Poincaré-type' duality theorem for étale and flat cohomology with values in the multiplicative group $\mathbf{G}_m$ in the sense that—at least ignoring a bit of 2-torsion[8]—

- $H^i(\mathcal{S}, \mathbf{G}_m)$ is (canonically) equal to $\{\pm 1\}, 0, 0, \mathbf{Q}/\mathbf{Z}$, and 0 for $i = 0, 1, 2, 3$, and > 3 respective;
- If F is a finite flat group scheme over $\mathcal{S}$ and $F^* := \underline{Hom}(F, \mathbf{G}_m)$ its (Cartier) dual finite flat group scheme, then cup-product induces a perfect pairing of cohomology groups (for the flat—fppf—topology over $\mathcal{S}$—again ignoring a bit of 2-torsion, or working with H^*_c as in Theorem 1.1 of [2]):

$$H^i(\mathcal{S}, F) \otimes H^{3-i}_c(\mathcal{S}, F^*) \longrightarrow H^3_c(\mathcal{S}, \mathbf{G}_m) = \mathbf{Q}/\mathbf{Z}.$$

  In a word, $\mathcal{S}$ is morally 2-connected and enjoys a 3-dimensional Poincaré duality "oriented" by the coefficient sheaf $\mathbf{G}_m$.

2.1 A prime ideal (p) in the ring of integers Z

The algebra here is just given by the natural "reduction mod p" homomorphism

$$\mathbf{Z} \to \mathbf{Z}/p\mathbf{Z} = \mathbf{F}_p.$$

We will avoid the prime $p = 2$ since some minor differences would have to be acknowledged at various points otherwise; so *prime* will mean *odd prime* in the discussion below. We will be taking the standard viewpoint of modern algebraic geometry, and think of this surjective homomorphism as giving us an embedding of schemes,

$$\mathcal{K} := \mathrm{Spec}(\mathbf{F}_p) \hookrightarrow \mathrm{Spec}(\mathbf{Z}) = \mathcal{S},$$

making this embedding ''like" the embedding of a knot in the three-dimensional sphere S^3. To understand this, we should examine, first, the separate geometries of the schemes $\mathcal{K} = \mathrm{Spec}(\mathbf{F}_p)$, $\mathcal{S} = \mathrm{Spec}(\mathbf{Z})$, and $\mathcal{S} \setminus \mathcal{K}$.

The facts of life of the theory of finite fields tells us that for every positive integer n, up to isomorphism, there is a unique field of cardinality p^n, $\mathbf{F}_{p^n}$ given as a field extension $\mathbf{F}_{p^n}/\mathbf{F}_p$ which is Galois, cyclic, and degree n. Moreover the (cyclic) Galois group of this field extension has a canonical generator: the Frobenius automorphism $x \mapsto x^p$. In a word

$$\mathrm{Spec}(\mathbf{F}_{p^n}) \to \mathbf{F}_p$$

is a cyclic (unramified!) Galois cover with Galois group canonically $\mathbf{Z}/n\mathbf{Z}$. An algebraic closure $\bar{\mathbf{F}}/\mathbf{F}_p$ is an appropriate union of these field extensions, and its Galois group—i.e., the fundamental group of $\mathcal{K}$— is (canonically) isomorphic to $\hat{\mathbf{Z}}$, the profinite completion of $\mathbf{Z}$. From the étale

[8] that can be gotten rid of by appropriately taking account of the infinite prime...

homotopy perspective, $\mathrm{Spec}(\bar{\mathbf{F}})$ is contractible, and therefore $\mathcal{K} = \mathrm{Spec}(\mathbf{F}_p)$ is homotopically a $K(\hat{\mathbf{Z}}, 1)$-space.

So, we view our prime p as a *knot*: $\mathcal{K} \hookrightarrow \mathcal{S}$; and two primes p and q as a *link*: $\mathcal{K} \sqcup \mathcal{L} \subset \mathcal{S}$.

2.2 An (actual, topological) knot K in the three-sphere S^3

Let K be (a **knot**; i.e.,) diffeomorphic to S^1 and smoothly embedded in S^3,

$$K \hookrightarrow S^3.$$

The ambient three-sphere S^3 is 2-connected and enjoys a 3-dimensional Poincaré duality with a canonical isomorphism $H^3(S^3; \mathbf{Z}) \simeq \mathbf{Z}$ while *the knot* K is a $K(\pi, 1)$ where its fundamental group π is infinite cyclic. For technical reasons I will always take K to be given with an orientation–i.e., with a canonical isomorphism $H^1(K; \mathbf{Z}) \simeq \mathbf{Z}$—so K is (canonically) a $K(\mathbf{Z}, 1)$-space—i.e., the fundamental group of K has a canonical generator, just as $\mathcal{K} = \mathrm{Spec}(\mathbf{F}_p)$ does.

As for the knot complement

$$X = X_K := S^3 - K \hookrightarrow S^3,$$

Alexander duality establishes a $\mathbf{Z}$-duality between $H^1(X; \mathbf{Z})$ and

$$\partial : H_2(S^3, K; \mathbf{Z}) \xrightarrow{\simeq} H_1(K; \mathbf{Z}) = \mathbf{Z},$$

giving us a canonical isomorphism:

$$H^1(X_K; \mathbf{Z}) = \mathbf{Z}$$

which tells us that all finite abelian covering spaces of S^3 branched at the knot, but unramified outside it, have *cyclic* groups of deck transformations, that these cyclic groups have canonical compatible generators, and that

$$\begin{array}{c} X_K^{\mathrm{ab}} \\ \Big\downarrow \Gamma \\ X_K \end{array} \quad \simeq \quad \mathbf{Z}$$

the maximal abelian covering space of X_K, has group of deck transformations Γ canonically isomorphic to $\mathbf{Z}$.

Or equivalently, setting

$$\Pi_K := \pi_1(X_K, x),$$

with suitable base point x—the *fundamental group of the knot*—we have

$$\Pi_K^{ab} := \Pi_K/[\Pi_K, \Pi_K] \simeq \mathbf{Z}.$$

Up to isotopy, the knot complement X_K may be viewed as compact manifold with torus boundary, $T_K = \partial X_K$, and within that torus—up to homotopy—there's a normal ('meridianal') loop m within a plane the intersects the knot at some point, tracing out a cycle

$$\{m\} = N_K \subset T_K \subset X_K.$$

In anticipation of our comparison we might call the image of

$$\mathcal{D}_K = \pi_1(T_K) = \mathbf{Z} \times \mathbf{Z}$$

in Π_K the *decomposition group* of the knot, and, perhaps, the image of

$$\mathcal{I}_K = \pi_1(N_K) = \mathbf{Z}$$

the *inertia subgroup*. The fundamental group of the knot, in any event, comes with maps

$$\begin{array}{ccccc} & & \mathcal{I}_K & \xrightarrow{\hookrightarrow} & \mathcal{D}_K \\ & & \downarrow \simeq & & \downarrow \\ \mathbf{Z} & \xleftarrow[\simeq]{} & \Pi_K^{\mathrm{ab}} & \longleftarrow & \Pi_K \end{array}$$

A basic theorem gives us that $V = V_K := H_1(X_K^{\mathrm{ab}}; \mathbf{Q})$ is a *finite dimensional* $\mathbf{Q}$*-vector space*. The natural action of the canonical generator of the group of deck transformations $\Gamma \simeq \mathbf{Z}$ on X_K^{ab} induces an automorphism of V_K whose characteristic polynomial $P_K(T)$ is the *Alexander Polynomial of the knot* K.

There are multiple ways of approaching, and understanding, the information in $P_K(T)$ (e.g., through the combinatorial braid group theory around HOMFLYS).

Here is a view of the *zeroes* of the Alexander Polynomial that is natural enough: for any nonzero complex number z consider the homomorphism $\psi_z : \Pi_K \to \mathbf{C}^*$ that sends the generator of $\Pi^{ab} := \Pi/[\Pi, \Pi]$ to z. This defines a linear system (of complex vector spaces of dimension one) $V(z)$ over X. We have that $\dim_{\mathbf{C}} H_1(X, V(z))$ is equal to the order of vanishing of the Alexander polynomial $P_K(T)$ at $T = z$.

Since the analogue (in number theory) to the topological fundamental group is the *étale fundamental group*—which for a smooth complex variety is the profinite completion of the topological fundamental group—we might prepare for this, in anticipation of our analogy, by defining two knots K, K' to be **profinitely equivalent** if there is an isomorphism between the profinite completions of their basic group diagrams,

$$(\hat{\mathbf{1}}) \quad \hat{\mathcal{I}}_K \hookrightarrow \hat{\mathcal{D}}_K \longrightarrow \hat{\Pi}_K.$$

and

$$(\hat{\mathbf{1}}') \quad \hat{\mathcal{I}}_{K'} \hookrightarrow \hat{\mathcal{D}}_{K'} \longrightarrow \hat{\Pi}_{K'};$$

and similarly for links.

This raises two questions:

1. Are profinitely equivalent knots, or links, isomorphic?[9] Are knots that are *profinitely trivial* actually trivial?
2. Let us say, casually—not precisely—that a knot invariant has a "profinite definition" if it can be computed directly from the profinite completions ($\hat{\mathbf{1}}$). Which of the knot invariants have profinite definitions (and therefore carry over directly to the context of primes numbers) and which do not?

For example, the Alexander polynomial does have a "profinite definition" but it is not obvious that the general HOMFLYS does; perhaps it doesn't.

3 Going back to the number field case: $\mathcal{K} \hookrightarrow \mathcal{S}$

Now consider our prime p viewed as 'knot' $\mathcal{K}$ embedded in $\mathcal{S}$,

$$\mathcal{K} \hookrightarrow \mathcal{S},$$

and form the 'knot complement'

$$\mathcal{X} := \mathcal{S} - \mathcal{K} = \mathrm{Spec}(\mathbf{Z}[1/p] \hookrightarrow \mathcal{S}.$$

An argument very akin to Alexander duality (given the cohomological facts we have just recalled) establishes a canonical isomorphism

$$H_1(\mathcal{X}; \mathbf{Z}) \simeq \mathbf{Z}_p^*$$

(where $\mathbf{Z}_p^*$ is the group of units in the ring $\mathbf{Z}_p$ of p-adic integers). Another way of saying this is that the maximal abelian extension of $\mathbf{Q}$ unramified outside the prime p consists of the field generated over $\mathbf{Q}$ by the union of all p-power roots of unity, and the Galois group of that field extension is canonically isomorphic to $\mathbf{Z}_p^*$.

If $p > 2$ we can write

$$\mathbf{Z}_p^* \simeq F_p^* \times \Gamma$$

[9] As I learned from Norbert A'Campo and Louis Funar, there has been some–not yet published—investigation of this. So, perhaps,in a later draft of these notes I will be able to include some discussion of this.

where Γ is the infinite cyclic pro-p-group of 1-units in $\mathbf{Z}_p$ and is generated, for example, by the 1-unit $1+p$:

$$\Gamma = (1+p)^{\mathbf{Z}_p}.$$

In particular, all finite abelian covering spaces of $\mathcal{S}$ branched at $\mathcal{K}$—i.e., finite abelian extensions of $\mathbf{Q}$ unramified except at the prime p (and ∞)—have Galois groups that are cyclic, and canonically isomorphic to the finite quotients $(\mathbf{Z}/p^m\mathbf{Z})^*$ of the topological group $\mathbf{Z}_p^*$. In anticipation of things to come, set:

$$\Lambda := \mathbf{Z}_p[[\mathbf{Z}_p^*]]$$

noting that this ring is isomorphic to a direct product of $p-1$ copies of the power series ring in one variable $\mathbf{Z}_p[[T]]$, where if i is an integer modulo $p-1$ the i-th factor of Λ is given by the surjective $\mathbf{Z}_p$-algebra homomorphism

$$\chi_i : \Lambda \longrightarrow \mathbf{Z}_p[[T]].$$

This is the unique $\mathbf{Z}_p$-algebra homomorphism that extends the continuous group homomorphism from $\mathbf{Z}_p^* =\simeq F_p^* \times (1+p)^{\mathbf{Z}_p} \subset \Lambda^*$ to $\mathbf{Z}_p[[T]]^*$ obtained by the stipulations that

- $x \in F_p^*$ be sent to
$$(x^i, 1) \in F_p^* \times \Gamma = \mathbf{Z}_p^* \subset \mathbf{Z}_p[[T]]$$
and
- $(1+p) \in \Gamma$ be sent to $1+T \in \mathbf{Z}_p[[T]]$.

Set

$$\Pi_{\mathcal{K}} := \pi_1^{et}(\mathcal{X}, x),$$

with suitable base point x —the *étale fundamental group of our knot* $\mathcal{K}$—we have that in relatively standard parlance,

$$\Pi_{\mathcal{K}} = G_{\mathbf{Q},\{p,\infty\}},$$

i.e., is the quotient of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}$ that is the Galois group of the maximal extension of $\mathbf{Q}$ in an algebraic closure $\bar{\mathbf{Q}}$ that is unramified except at p and ∞.

As with topological knots the 'fundamental group of the prime,' comes with inertia and decomposition groups

$$\mathcal{I}_{\mathcal{K}} \hookrightarrow \mathcal{D}_{\mathcal{K}} \longrightarrow \Pi_{\mathcal{K}} = G_{\mathbf{Q},\{p,\infty\}}.$$

From our previous discussion,

$$\Pi_{\mathcal{K}}^{ab} := \Pi_{\mathcal{K}}/[\Pi_{\mathcal{K}}, \Pi_{\mathcal{K}}] \simeq \mathbf{Z}_p^*,$$

and if $\mathcal{X}^{\mathrm{ab}} \to \mathcal{X}$ is the maximal unramified abelian (connected) cover, then we can also say

$$\text{“}\mathrm{Gal}(\mathcal{X}^{\mathrm{ab}}/\mathcal{X})\text{”} = \Pi_{\mathcal{K}}^{ab} = \mathbf{Z}_p^*.$$

A natural analogue to the finite dimensional $\mathbf{Q}$-vector space $V_K := H_1(X^{\mathrm{ab}}; \mathbf{Q})$ discussed above is the étale 1-st homology group, taken first, with p-adic *integral* coefficients,

$$M_{\mathcal{K}} := H_1^{et}(\mathcal{X}^{\mathrm{ab}}; \mathbf{Z}_p) = \lim_n H_1^{et}(\mathcal{X}^{\mathrm{ab}}; \mathbf{Z}/p^n\mathbf{Z}),$$

or—tensoring with $\mathbf{Q}_p$—we get the vector space

$$V_{\mathcal{K}} := H_1^{et}(\mathcal{X}^{\mathrm{ab}}; \mathbf{Z}_p) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p.$$

The module $M_{\mathcal{K}}$ is naturally a Λ-module, and $V_{\mathcal{K}}$ a $\Lambda \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$-module. Tensoring $M_{\mathcal{K}}$ with the $p-1$ projection operators χ_i described above, we get for each i mod $p-1$ a $\mathbf{Z}_p[[T]]$-module that we'll call $M^i_{\mathcal{K}}$.

The behavior of these modules depends crucially on the parity of i. It is a marvelous theorem in Iwasawa theory that if i is 'odd' (which makes sense since our prime p is not 2) then our module $M^i_{\mathcal{K}}$ is a finitely generated $\mathbf{Z}_p$-module, and therefore $V^i_{\mathcal{K}} = M^i_{\mathcal{K}} \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ is a finite dimensional $\mathbf{Q}_p$-vector space.

By definition–but subject to possibly different normalization—the **Iwasawa polynomial** for the pair (p, i) (i odd, modulo $p-1$) is the characteristic polynomial $g_p(i;T) \in \mathbf{Z}_p[T]$ of the operator T acting on this vector space $V_{\mathcal{K}}$. These polynomials $g_p(i;T)$ or, more precisely, their zeroes are crucial for much number theoretic phenomena. For example, if for a given p and all odd i mod $p-1$, they are all 1—i.e., have no zeroes—the prime p is what is called *regular* and Kummer's relatively easy procedure of proving Fermat's Last Theorem for exponent p can be made to work. In general, by what is known as the 'main conjecture" (which is a theorem) the zeroes of $g_p(i;T)$ correspond in a one-one fashion, and in a natural way, to the zeroes of the Leopold-Kubota L-function $L_p(s, \omega^{1-i})$.

3.1 Brief comments on comparison and differences

- If by **unknotted** one means that the fundamental group of the knot is abelian, every prime is 'knotted.'
- A serious distinction between knots and primes has to do with what is called *wild inertia* a phenomenon that exists, and is of crucial importance in number theory, but there's no corresponding complexity in our analogous situation in knot theory.
- There is a duality in the structure of the Alexander polynomial (it is invariant under inversion $t \mapsto t^{-1}$; hence if θ is a root, so is θ^{-1}). But there is nothing like that for Iwasawa polynomials.

  Given the G_m-orientation of $\mathcal{S}$, the corresponding duality for the Iwasawa polynomial would—if it existed—send the index i to $j := 1 - i$ and since j would then be even, $g_j(T)$ has not been defined. Of course, you could simply, by fiat, define $g_j(T)$ so that it exhibits the duality, but lacking (yet) any number theoretic motivation, that would be too formal a move to contemplate.

4 Two knots and two primes

4.1 A pair of (disjoint) knots K, L embedded in the three-sphere S^3

Here we can consider the embeddings:

$$K \quad \hookrightarrow \quad X_L := S^3 - L$$

and

$$L \quad \hookrightarrow \quad X_K := S^3 - K$$

Choose arbitrary base points and consider the induced homomorphisms of π_1,

$$\pi_1(K) \quad \longrightarrow \quad \Pi_L.$$

In anticipation of the analogy to come, let

$$\{Frob_K\} \in \Pi_L$$

denote the conjugacy class of the image of the canonical generator of $\pi_1(K)$ in Π_L. This is indeed well-defined, independent of the choice of base points. Similarly we have

$$\{Frob_L\} \in \Pi_K.$$

To be sure, we can't yet compare these conjugacy classes, since they live in different groups. But passing to the abelian quotient groups of Π_K and Π_L, both are canonically isomorphic to $\mathbf{Z}$ we can indeed compare the images of $\{Frob_K\}$ and $\{Frob_L\}$ in

$$\Pi_K^{\mathrm{ab}} = \mathbf{Z} = \Pi_L^{\mathrm{ab}},$$

and those images are given— respectively—by the linking number of K in L and the linking number of L in K, these being *equal* with opposite sign. The proof of this equality is usually given by identifying these numbers with the cup product of the fundamental classes in $H^1(X_K)$ and $H^1(X_L)$ in $H^2(X_{K,L}) = \mathbf{Z}$ where $X_{K,L} := S^3 - \{K \cup L\}$.

4.2 A pair of (distinct) primes p, q

In parallel with our previous subsection, let $\mathcal{K} := \mathrm{Spec}(\mathbf{F}_p)$ and $\mathcal{L} := \mathrm{Spec}(\mathbf{F}_q)$. Consider the embeddings:

$$\mathcal{K} \quad \hookrightarrow \quad X_{\mathcal{L}} := \mathrm{Spec}(\mathbf{Z}[1/p])$$

and

$$\mathcal{L} \quad \hookrightarrow \quad X_{\mathcal{K}} := \mathrm{Spec}(\mathbf{Z}[1/q])$$

Choose arbitrary base points and consider the induced homomorphisms of the étale fundamental groups

$$\pi_1^{et}(\mathcal{K}) \quad \longrightarrow \quad \Pi_{\mathcal{L}}.$$

Denote by

$$\{Frob_{\mathcal{K}}\} \in \Pi_{\mathcal{L}}$$

the conjugacy class of the image of the canonical generator of $\pi_1^{et}(\mathcal{K})$ which is independent of the choice of base points. Similarly we have

$$\{Frob_{\mathcal{L}}\} \in \Pi_{\mathcal{K}}$$

.

Here again, we can't yet compare these conjugacy classes, since they live in different groups. Even passing to the abelian quotient groups of $\Pi_{\mathcal{K}}$ and $\Pi_{\mathcal{L}}$, which are canonically $\mathbf{Z}_p^*$ and $\mathbf{Z}_q^*$ respectively, and where the image of $\{Frob_{\mathcal{K}}\}$ is the element $p \in \mathbf{Z}_q^*$ and the image of $\{Frob_{\mathcal{L}}\}$ is the element $q \in \mathbf{Z}_p^*$, we simply have elements in different groups and so are not (yet) comparable. In a word, the linking "number" of p with q (in that order) is the element p in $\mathbf{Z}_q^*$, while the linking "number" of q with p (in that order) is the element q in $\mathbf{Z}_p^*$–no clear way to make any correspondence, yet. Nevertheless each of these groups $\mathbf{Z}_p^*$ and $\mathbf{Z}_q^*$ have unique subgroups of index two (consisting of 'squares' of elements) and the famous comparison to be made here is to ask whether p being a square in $\mathbf{Z}_q^*$ (or equivalently, mod q) has anything to do with q being a square in $\mathbf{Z}_p^*$ (or equivalently, mod p). Indeed it does, as given by the classical *quadratic reciprocity theorem*. Namely, p is a square mod q if q is a square mod p , except in the case where both p and q are both congruent to -1 mod 4, in which case p is a square mod q if and only if q is not a square mod p. (One of the many proofs of this follows the lines of the proof I hinted at above of skew-symmetry of linking number.[10])

5 Borromean primes and 'Cebotarev arrangements'

5.1 Borromean primes

The *Borromean Ring* is that well-known link of three disjoint 'unknots' that has the property that if you ignore any of the three unknots the other two are unlinked, yet the three taken all together are somehow linked. John Milnor defined a class of invariants that serve as obstructions to linkage of the above sort, these being secondary (or higher) linking numbers that can be defined—in analogy with standard linking numbers—as secondary (or higher) cohomology operations related to the vanishing of cup-products, the Massey triple product being the first example of these. The clean general structure corresponds to what is called an A_∞-algebra structure on chain complexes, such as was discussed by Francois Laudenbach in this conference (he obtained it from Morse functions on the knot manifold with Dirichlet and Neumann conditions on the boundary).

One can establish a striking analogy to this, with prime numbers, obtaining secondary (or higher) versions of the quadratic reciprocity theorem, as is done in the work of Morishita, Redei, and others

[10]Po raised the question of whether Gauss himself—who, after all, had introduced the integral formula for the linking number—might have seen some analogy between that concept and the structure surrounding the quadratic reciprocity theorem.

(cf. [6], [7], and Section 4 of citeM2). Specifically, given three distinct primes p, q, r all congruent to 1 mod 4 and each a quadratic residue of any of the others, there is a mod 2 invariant which gauges how triply-entangled the three primes are; moreover, as is the case with old-fashioned linking numbers, the natural definition of this invariant is given somewhat asymmetrically in terms of the roles played by p, q and r; yet, the theorem is that the invariant itself is independent of permutation of these.

Here is the description of this invariant,

$$link(p, q, r) \in \{\pm 1\},$$

as given by Redei (cf. section 8 of [6]). Under the assumptions of the previous paragraph there is a nontrivial integral zero (x, y, z) of the quadratic form

$$X^2 - qY^2 - rZ^2$$

and moreover, one can assume that $g.c.d((x, y, z) = 1$, y is even, and $x - y \equiv 1$ modulo 4. Now form $\alpha := x + \sqrt{q}y$ and consider the (non-Galois) extension of $\mathbf{Q}$,

$$K := \mathbf{Q}(\sqrt{q}, \sqrt{\alpha}).$$

Then

$$link(p, q, r) = 1 \in \{\pm 1\}$$

if and only if the prime p splits completely in K. Otherwise, $link(p, q, r) = -1$.

An example of linked Borromean triples of primes is given (by D. Vogan—cf. loc.cit.) by

$$(p, q, r) = (13, 61, 937).$$

5.2 'Cebotarev arrangements'

Here is a thought-experiment that I once mused about a long time ago, but will try to sharpen a bit here: I think of it *not at all* as a problem to be resolved[11] but rather as just a somewhat casual way of appreciating *visually* how vastly *entangled* the collection of all primes are.

Imagine choosing one hyperbolic knot in every commensurable equivalence class of hyperbolic knots, and then arranging these knots (up to equivalence) in S^3 so that they form a mutually disjoint ensemble:

$$\mathcal{C} := \sqcup_i K_i \ \subset S^3$$

where we have ordered them compatibly with their hyperbolic volume. By an **admissible Galois cover of S^3 (relative to $\mathcal{C}$)** let us mean a finite cover $f : M^3 \to S^3$, Galois and ramified over at worst a finite subcollection of knots $\Sigma = K^{(1)} \sqcup K^{(2)} \sqcup \cdots \sqcup K^{(n)}$ of $\mathcal{C}$ in the natural sense; i.e., such that f restricted to $Y := M^3 - f^{-1}\Sigma$ the pullback of $S^3 - \Sigma$ is a locally trivial covering space

[11] although the easiest is just to formulate it as a 'question'

of $X := S^3 - \Sigma$ with free action of a finite group G on M^3 (the "Galois group "of the cover) such that $Y/G = X$.

A knot in $\mathcal{C}$ which is branched in $M^3 \to S^3$ we say is *ramified in the cover* and if it isn't we say it is *unramified in the cover*. Any unramified knot K in an admissible cover $M^3 \to S^3$ gives rise to a conjugacy class of elements in $G = \mathrm{Gal}(M^3/S^3)$ by the analogue of the Frobenius construction alluded to earlier. Thus, for all but finitely many knots in $\mathcal{C}$ we have a well-defined conjugacy class

$$\{Frob_K(M^3/S^3)\} \subset G.$$

Let us say that the collection $\mathcal{C}$ is a **Cebotarev Arrangement** if the following statistical rule holds for every admissible cover M^3/S^3 and every conjugacy class $\{c\} \subset G = \mathrm{Gal}(M^3/S^3)$

$$\lim_{k\to\infty} \frac{1}{k} \#\big[K_i, i \leq k \mid \{Frob_{K_i}(M^3/S^3)\} = \{c\}\big] \quad = \quad \frac{|\{c\}|}{|G|},$$

where the limit here is compiled by ordering the knots compatibly with their hyperbolic volume.

In effect, one is asking that—with these conventions–the Frobenius conjugacy classes are uniformly distributed in fundamental groups.

The only reason for my formulating this notion is to connect it to The Cebotarev Density Theorem, the closely analogous statement for primes.

Is there such a Cebotarev arrangement? If so, how bewilderingly complex, and yet somehow organized, this entangled collection would be, each knot winding about infinitely many others according to various proportions! As I said, I initially brought this up—in [9]—only to have a visualizable counterpart to the type of entanglement represented by the facts of life for prime numbers; I did this in my original formulation of these thoughts as a birthday greeting for my friend Po's 80-th birthday!

In the conference for PO's 80-th birthday Jérome Los mentioned to me that he has constructed (unpublished as of yet) a dynamical system in S^3 whose closed orbits run through all knot types. So one might sharpen one's quest by insisting that the knots in the Cebotarev arrangements (as formulated above) all be closed orbits of some globally defined dynamical system.

As I understand it, Los has a spin-construction that realizes many elements in the braid group. It begins with a self-mapping of the disc $f : D^2 \to D^2$ which is used to patch the top and bottom of $D^2 \times [0, 1]$ together to get a solid torus T which is then imbedded in the natural way in S^3 to finish up with an appropriate dynamical system on S^3 . This dynamical system has the property that going "one circuit" through T effects the mapping f; hence following through n contiguous circuits effect the n-th iterate of f. Of course, one can consider a version of this spin-construction of Los for any topological automorphism f of any connected 2-manifold M^2 that has finitely many periodic points of any specific period, but infinitely many periodic point in all. For any such self-map, form the 3-manifold $M^2 \times [0, 1] \to M^3$ obtained by attaching the 'bottom' $M^2 \times \{0\}$ of $M^2 \times [0, 1]$ to the 'top' $M^2 \times \{1\}$ via the mapping f and viewing the periodic orbits of the dynamical system $f : M^2 \to M^2$ as an interesting collection of knots nicely organized by period (or equivalently, by

length). If f has a fixed point $m \in M^2$ one has the further option of taking m as base point, killing the loop $[0,1] \times \{m\} \subset M^3$ by the adjunction of a thickened two-disc and viewing the preceding collection of knots as being in the 3-manifold N^3 obtained from M^3 by the corresponding surgery[12].

One can formulate analogous conditions regarding dynamical systems in more general, or different, contexts. As Curt McMullen explained to me—and see his [5]—beautiful 'Cebotarev examples' can be gotten by considering the collection of knots given by closed geodesics for pseudo-Anososov flows in the spherical tangent bundles of hyperbolic surfaces.

References

[1] H. Hu, Y. Pesin, A,Talitskaya, Every compact manifold carries a hyperbolic Bernoulli flow. Modern dynamical systems and applications, Cambridge Univ. Press, (2004) 347-358

[2] C.Demarche, D.Harari, Artin-Mazur-Milne duality for fppf cohomology, (2018) arXiv:1804.03941v3

[3] R. Descartes, Rules for the Direction of our Native Intelligence. In J. Cottingham, R. Stoothoff, D. Murdoch, & A. Kenny (Eds.), Descartes: Selected Philosophical Writings (pp. 1-19). Cambridge: Cambridge University Press. (1988) doi:10.1017/CBO9780511805059.003

[4] A. Katok, Bernoulli Diffeomorphisms on Surfaces, Annals of Mathematics, Second Series, **110** No. 3 (1979), 529-547

[5] C. McMullen, Knots which behave like the prime numbers, Compositio Mathematica, **149** (2013) 1235-1244

[6] M. Morishita, *Knots and Primes,* Springer (2011)

[7] M. Morishita, "Milnor invariants and Massey products for prime numbers" Compositio Math. **140** (2004) 69-83 (See the abstract: `https://www.cambridge.org/core/journals/compositio-mathematica/article/milnor-invariants-and-massey-products-for-prime-numbers/83068A12C7889910D3D54B9ADEB3905C`)

[8] M. Morishita, Analogies between knots and primes, 3-manifolds and number rings, Archiv: `https://arxiv.org/pdf/0904.3399.pdf`

[9] B. Mazur, Primes, Knots and Po, `http://people.math.harvard.edu/~mazur/papers/Po8.pdf`

[12] One might also require the maps to have specific dynamical features, such as being Bernoulli ([4], [1]).