Primes, Knots and Po

Barry Mazur

July 22, 2012

For the conference "Geometry, Topology and Group Theory"
in honor of the 80th birthday of Valentin Poenaru
held in Autrans July 1st-6th, 2012

Po and I became instant friends when we met over half a century ago. In the intervening years our friendship has only deepened.

I viewed Po, especially during the time that the photo in front of you was taken, as someone ready—with his own intense energy and centeredness; as someone ready to create—from scratch—his own culture, his own goals, his own mountains to climb, as well as his own language.

Po once commented that to really engage in any aspect of history or science–that is to say, to understand a culture—you're faced with the contradiction of a certain catch22 in that you must manage, somehow, to have already achieved a *critical mass* of prior questions and reflections and knowledge about it, before anything about it comes into focus. Happily, Po is at home in many cultures, many languages, many histories, and he's blessed with this type of intellectual critical mass for so many subjects; physics and mathematics—of course—included.

We first met each other through correspondence—he was in Romania and I in the US—and we were both working on contractible four-manifolds that bound homology three-spheres, each of us having had constructed examples of *nonsimply connected* homology 3-spheres that occur as boundaries of contractible four-manifolds. (Po's article is: Les décompositions de l'hypercube en produit topologique, Bull. Soc. Math. France **88** (1960), 113-129).

Both Po's examples (of contractible 4-manifolds that bound non-simply connected manifolds) and mine were obtained by sewing a thickened 2-disc onto the boundary of $D^3 \times S^1$ along a knot in the boundary that winds its way around the S^1 so as to homotopically kill the S^1. The result—given the particular knots we chose—is the construction of contractible 4-manifolds that with non-simply connected boundary. The kinds of 4-manifolds we construct are simply connected, of course, but—as Po mentioned to me in this conference—an (unpublished) result of Casson implies that they are not *geometrically simply connected* in the sense that it cannot be built as handlebodies having *no* handles of index 1.

The concept of a manifold being *simply connected but not geometrically simply connected* is one that is intimately related to Po's work. This turns out to be uniquely a *dimension four* phenomenon; as Po commented, "strange things happen in dimension four." Indeed, as we now know, for $n \neq 4$ all simply connected compact manifolds are geometrically simply connected. For $n \leq 2$ this is classical; for $n = 3$ it is proved by Perelman and for $n \geq 5$ it is true, thanks to Smale.

As for the related question of whether or not a homology $n-1$-sphere actually bounds a smooth contractible n-manifold, again, and for similar reasons, the case $n = 4$ shows itself to be peculiar. For the answer is *yes* if $n \neq 4$; and the answer is *not always* when $n = 4$, thanks again to an invariant of Casson ([**?**])

It is curious that even now, half a century after this issue was first broached, there are still open problems in this general domain, not the least of which is the still unresolved *smooth* four-dimensional Schoenflies Problem.

Both Po's examples (of homology 3-spheres that bound contractible manifolds) and mine had the further feature that when you doubled them on their boundary—i.e., put two copies of them together by identifying their boundaries—you got a closed differentiable manifold diffeomorphic to the four-dimensional sphere, which means that there is a smooth involution of S^4 (switching the two copies of the doubled manifold) with non-simply-connected fixed point set, and therefore 'exotic' in the sense that the involution is not equivalent to a linear involution. I remember that at the time—the late fifties of the past century—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 S^3 is again (topologically) S^3 giving, therefore, a thoroughly wild and untamable involution of S^3. I imagine that Po was similarly inspired by Bing[1]. The surprising re-creation of S^4 by sewing together the boundaries of two manifolds continued as a theme of Po's work, as in the marvelous theorem that he proved with Francois Laudenbach in the early seventies ([**?**]).

[1]One might also mention that a related issue in the theory of homology $n-1$-spheres is the *double suspension conjecture* that asserts that the double suspension of a homology $n-1$-sphere is homeomorphic to S^{n+1}. This was proved for all n by Cannon ([**?**]) building on earlier work of Edwards [**?**]).

But the great and abiding interest of Po centered on the mysteries of three-dimensional topology, even though—very often—his mode of approach was through four dimensions. The Poincaré Conjecture of course was one of his beloved focal points over decades. Now the way in which Po dealt with the prospect of Perelman's wonderful proof, and the way he engaged in appreciating the insight of Perelman, and at the same time adroitly reshaping his own research projects makes Po one of the truly fine models for our profession: fully at home in the world of ideas for their own sake; and devoted to—and deriving inspiration from—the beauty of that world, their depth, its power of explanation.

Knots and their exquisitely idiosyncratic properties, are the vital essence of three-dimensional topology, the DNA that governs the development, and evolution, of that field. I know that Po has a special love and affinity for them, and I also think that they form a link to many other—seemingly far-flung—aspects of mathematics. For example, when I was trying to get a feel for number theory, I found that a certain 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 and it seems that it might allow two-way traffic, from knots to primes, and from primes to knots. In celebration of Po for this conference, let me explain very briefly what this analogy consists of. For a beautiful introduction to this subject, see M. Morishita's treatise, *Knots and Primes*, [**?**].

In this conference, after listening to a lecture by Michel Boileau, it occurred to me that it might make sense to be somewhat sharper than one traditionally is, when one frames the basic analogy. Perhaps we should be 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[2]). 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[3]. The format of our comparison is then:

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

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

It is interesting to focus on the parallels that can be drawn, as well as the distinctions that can be made.

[2]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'.

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

1 One knot and one prime

1.1 A single knot K embedded in the three-sphere S^3

The separate geometries of the two spaces involved are these: *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 diffeomorphic to S^1. 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. Now consider the knot embedded in S^3,

$$K \ \hookrightarrow \ S^3,$$

and 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:

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

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

Or equivalently, setting

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

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

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

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 that generates the infinite cyclic subgroup

$$N_K \subset T_K \subset X_K.$$

In anticipation of our comparison we might call

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

the *decomposition group* of the knot, and

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

the *inertia subgroup*. The fundamental group of the knot then comes with maps

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

A basic theorem gives us that $V = V_K := H_1(X^{\mathrm{ab}}; \mathbf{Q})$ 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^{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 an attitude to 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?[4] 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?

[4] As I learned in this conference 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.

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

1.2 A single prime number p in the 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,

$$\mathrm{Spec}(\mathbf{F}_p) \hookrightarrow \mathrm{Spec}(\mathbf{Z}),$$

and our analogy begins by thinking of $\mathcal{K} := \mathrm{Spec}(\mathbf{F}_p)$ as 'like' the knot K and $\mathcal{S} := \mathrm{Spec}(\mathbf{Z})$ as 'like" the three-dimensional sphere S^3. To understand this, we should examine, first, the separate geometries of the two schemes $\mathrm{Spec}(\mathbf{F}_p)$ and $\mathrm{Spec}(\mathbf{Z})$. 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 is (canonically) isomorphic to $\hat{\mathbf{Z}}$, the profinite completion of $\mathbf{Z}$. From the étale 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.

The theory for $\mathcal{S} := \mathrm{Spec}(\mathbf{Z})$ requires some class field theory, as reformulated in the vocabulary of étale (and some other Grothendieckian) cohomology theories. Firstly, $\mathcal{S}$ is simply connected, in the sense that every connected finite cover of $\mathcal{S}$ is ramified. Moreover, $\mathcal{S}$ enjoys 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

- $H^i(\mathcal{S}, \mathbf{G}_m)$ 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 $F^* := \mathit{Hom}(F, \mathbf{G}_m)$ its (Cartier) dual finite flat group scheme, then cup-product induces a perfect pairing of flat cohomology groups

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

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

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. If $p > 2$ we can write

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

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 $M_{\mathcal{K}}^i$.

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 $M_{\mathcal{K}}^i$ is a finitely generated $\mathbf{Z}_p$-module, and therefore $V_{\mathcal{K}}^i = M_{\mathcal{K}}^i \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ 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 $L_p(s, \omega^{1-i})$.

1.3 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.

2 Two knots and two primes

2.1 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 $\pi_1(K)$. 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 $X_{K,L} := S^3 - \{K \cup L\}$.

2.2 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.[5])

[5]Po raised the question (in this conference) 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.

3 Borromean primes and 'Cebotarev arrangements'

3.1 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 (cf. [**?**]). 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,

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

as given by Redei (cf. section 8 of [**?**]). 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 $x - y \equiv 1 \mod 4$. Now form $\alpha := x + \sqrt{q}y$ and consider the (non-Galois) extension of $\mathbf{Q}$,

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

Then

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

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

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

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

3.2 '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[6] 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 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 that there is an important theorem in number theory (The Cebotarev density Theorem) that makes 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 brought this up only to have a visualizable counterpart to the type of entanglement represented by the facts of life for prime numbers; and–of course—to offer a birthday greeting for my friend Po!

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

4 Appendix: Cebotarev dynamical systems

In the conference 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[7].

One can formulate analogous conditions regarding dynamical systems in more general, or different, contexts.

1. As Curt McMullen explained to me, beautiful examples can be gotten by considering the collection of knots given by closed geodesics in the spherical tangent bundles of hyperbolic surfaces. Are these 'Cebotarev'?

2. Also, one needn't stick to manifolds: let $f : X \to X$ be any continuous self-mapping of a connected CW-complex X, fixing a basepoint $x_o \in X$. Let $\Pi(X, x_o; f)$ be the quotient group of $\pi_1(X, x_o)$ that *equalizes* f and the identity map; i.e., it is the quotient by the normal subgroup generated by $f(\alpha)\alpha^{-1}$ for all $\alpha \in \pi_1(X, x_o)$.

   Put $I := [0,1]$, and form $X \times I$. Attaching $X \times \{0\}$ to $X \times \{1\}$ by the mapping $(x, 0) \mapsto (f(x), 1)$, construct the space

   $$Y := X \times I / \{(x,0) \sim (f(x),1); x \in X\}.$$

   Identifying $S^1 = \partial D^2$ with the closed loop $C := x_o \times I/\{(x_o, 0) \sim (x_o, 1)\} \subset Y$ (via, say, $\iota : e^{2\pi it} \mapsto (x_o, t) \in Y$ for $t \in I$) form the CW complex Z by adjoining the disc D^2 with the attaching map

   $$\partial D^2 \xrightarrow{\iota} C$$

   to build the space:

   $$Z := Y \cup_\iota D^2.$$

[7] One might also require the maps to have specific dynamical features, such as being Bernoulli ([**?**], [**?**]).

Fix the base point $z_o :=$ the image of $(x_o, 0)$ in Z.

We have (by van Kampen's theorem):

$$(\mathbf{1}) \qquad \pi_1(Z, z_o) \simeq \Pi(X, x_o; f).$$

Any finite f-orbit in X,

$$\mathcal{O} = \{x, fx, f^2x, \ldots, f^{n-1}x\} \subset X$$

with period n (denote this: "$Per(\mathcal{O}) = n$"—so n is the smallest positive number such that $f^n x = x$) gives rise to a loop, i.e., an oriented closed curve, $\gamma_{\mathcal{O}} \subset Z$, defined to be the image of

$$x \times I \sqcup fx \times I \sqcup f^2x \times I \sqcup \cdots \sqcup f^{n-1}x \times I \subset X \times I$$

under the natural mapping

$$X \times I \longrightarrow Z.$$

We give $\gamma_{\mathcal{O}}$ the natural orientation (i.e., 'induced' from the natural orientation of I).

Definition 1. *By the* **Frobenius conjugacy class** *attached to the finite f-orbit $\mathcal{O} \subset X$ we mean the conjugacy class in $\Pi(X, x_o; f)$ determined by the loop $\gamma_{\mathcal{O}} \subset Z$. Specifically, the image of the canonical generator of the fundamental group of the oriented loop $\gamma_{\mathcal{O}}$ into the fundamental group of Z (the map on fundamental groups being given by choosing compatible base points) determines a well-defined conjugacy class of elements in $\pi_1(Z, z_o)$ which we identify with a conjugacy class of elements in $\Pi(X, x_o; f)$ via the isomorphism* **(1)** *above. Denote this Frobenius conjugacy class*

$$\{Frob_{\mathcal{O}}\} \subset \Pi(X, x_o; f).$$

Thus we have a canonical mapping

$$Frob : \{\text{Finite } f - \text{orbits in } X\} \; - - - - - - - \longrightarrow \; \{\text{Conjugacy classes in } \Pi(X, x_o; f)\}.$$

Now consider the following condition regarding the dynamics of f.

Per: The mapping $f : X \to X$ has only finitely many periodic points of any given order, but infinitely many in all.

When $f : X \to X$ is a mapping that satisfies **Per** we order the collection of finite f-orbits in a manner compatible with their periods, and we can begin to ask distribution questions regarding the dynamics of f that are somewhat analogous to the question answered by the Cebotarev Theorem in classical number theory.

The condition most naturally related to the facts of life given by the classical Cebotarev Theorem is the following:

Definition 2. *Let $\rho : \Pi(X, x_o; f) \longrightarrow G$ be a surjective homomorphism onto a finite group G. Say that $f : X \to X$ is* **ρ-Cebotarev** *if for any conjugacy class $\mathcal{C} \subset G$ we have:*

$$\lim_{n \to \infty} \frac{|\{\mathcal{O} \; ; Per(\mathcal{O}) \leq n; \rho(Frob_{\mathcal{O}}) = \mathcal{C}\}|}{|\{\mathcal{O} \; ; Per(\mathcal{O}) \leq n\}} \quad = \quad \frac{|\mathcal{C}|}{|G|}.$$

3. Also, there are other 'Cebotarev'-like questions in this context that have no very close analogues to the types of questions that can be asked in number theoretic contexts. Here, is one: Note that Galois groups in number theory are (finite, or more generally) profinite and therefore *do not admit* homomorphisms to real or complex Lie groups that have infinite image[8]. But it is very possible for the types of groups we are currently interested in—e.g., the groups $\Pi(X, x_o; f)$ of item (2) above—to have homomorphisms to, say, compact real or complex Lie groups with infinite image.

   Definition 3. *Let then $f : X \to X$ satisfy the condition Per as above. Let G be a compact Lie group and let μ be Haar measure on G, normalized to have total mass* 1*. Let*

$$\rho : \Pi(X, x_o; f) \longrightarrow G$$

be a homomorphism with dense image. Say that $f : X \to X$ is **ρ-Cebotarev** *if for every measurable subset $\mathcal{N} \subset G$ closed under conjugation by elements of G, we have:*

$$\lim_{n\to\infty} \frac{|\{\mathcal{O}\ ; Per(\mathcal{O}) \leq n; \rho(Frob_{\mathcal{O}}) \subset \mathcal{N}\}|}{|\{\mathcal{O}\ ; Per(\mathcal{O}) \leq n\}} \quad = \quad \mu(\mathcal{N}).$$

   Note that when G is finite, Definitions **??** and **??** both apply, and are equivalent. Are there any interesting examples of $f : X \to X$ satisfying the condition Per and nontrivial homomorphisms ρ for which $f : X \to X$ is **ρ-Cebotarev**—at least for some of the (nontrivial) ρ's considered in this section?

References

[1] S. Akbulut, J. McCarthy, *Casson's Invariant for Oriented Homology 3-Spheres*, Princeton University Press (1990)

[2] J. W. Cannon: Shrinking cell-like decompositions of manifolds. Codimension three, Ann. Math. **110** (1979), 83-112

[3] R. D. Edwards, Suspensions of homology spheres arXiv:math/0610573v1

[4] 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

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

[6] F. Laudenbach, V. Poénaru, A note on 4-dimensional handlebodies. Bull. Soc. Math. France **100** (1972), 337-344

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

[8] B. Mazur, A note on some contractible 4-manifolds. Ann. of Math. (2) **73** 1961 221-228

[9] V. Poénaru, Les décompositions de l'hypercube en produit topologique, Bull. Soc. Math. France **88** (1960), 113-129.

[8] Some of these groups may, of course, have homomorphisms with infinite image in p-adic Lie groups.