THE FACES OF EVIDENCE *(IN MATHEMATICS)*

BARRY MAZUR

Notes for the presentation and discussion at Museion, February 5, 2014

1. What is evidence?

In contrast to the complex evolution and unfolding of the meanings—through centuries of usage—of many of the words we currently use, the word *evidence* has a seemingly uncomplicated history. It comes to English around the 1300s, meaning then, as now, "appearance from which inferences may be drawn." It was a loan-word from Late Latin *evidentia*, i.e., proof. Originally it meant *distinction, clearness,* from Latin ex+videre.

But in each field of inquiry the term will generally have a different complexion, reflecting the distinct role *evidence* plays in producing a consensus regarding what is considered "progress" in that field; each discipline (*Mathematics, Physics,. . . , Art History*) has, perhaps, a different kind of goal—let alone a different specific goal.

In the Fall semester 2012 I had the pleasure of co-running a seminar-course—*The Nature of Evidence*— in the Harvard Law School with Noah Feldman. The seminar-course was structured as an extended conversation between different practitioners and our students, and us. We found it very useful to learn, in some specificity, from people in different fields–via concrete examples graspable by people outside the field–what evidence consists of in *Physics, Economics, Biology, Art History, History of Science, Mathematics, and Law.* We heard about the very articulated internal debate in Economics on the relative merits of randomized control experiments, natural experiments, and more discursive modes of argument. We heard about issues in Biology regarding the use of genetic data. In Physics, about the structure of evidence that determined the existence of the Higgs boson, in the History of Physics, about the evolution of the cloud chamber. And Law, which has its own precise rules explicitly formulated.

I'm hoping that this evening is an occasion to continue this dialogue to compare a bit of the structure of evidence as it occurs within each of our specific experiences: what is the nature of the evidence that must be presented to reach a consensus conclusion about a 'new result" or perhaps a new promising direction of research? Let's also aim for a

comprehensive view and not merely a fragmented "evidence-in-X, evidence-in-Y, etc." with no matrix that ties these bits together. For there are indeed general formats and attitudes towards evidence that can bear some discussion.

For example, compare these (standard, but cartoon) formats for the treatment of evidence:

- the classical Baconian view, where data is (supposedly) gathered as evidence to *test* explicit hypotheses;
- the Bayesian view, where evidence is fed back to modify the (meta-)hypotheses—i.e., to 'educate' the *priors*;
- a recent strident claim: given that it is dead easy to amass as much 'Big' data as one wants—the data itself is meant to stand as some pure source of 'evidence-without-a-specific-intent,' independent of any hypothesis, any model, and simply mined whenever needed.

It is striking, though, how different branches of knowledge—the Humanities, the Sciences, Mathematics—justify their findings so very differently; they have, one might say, quite incommensurate rules of evidence. Often a shift of emphasis, or framing, of one of these disciplines goes along with, or derives from, a change of these rules, or of the repertoire of sources of evidence, for justifying claims and findings in that field.

The way the word *evidence* is used in a field, and how its meaning evolves, can already tell us much about the profile, and the development, of an intellectual discipline.

Consider, for example, Charles Darwin's language in *The Origin of Species*—specifically, his use of the words *fact* and *evidence*—as offering us clues about the types of argumentation that Darwin counts in support, or in critique, of his emerging theory of evolution[1]. Sometimes Darwin provides us with a *sotto voce* commentary on what *shouldn't* count—or should only marginally count—as evidence, such as when he writes:

> But we have better evidence on this subject than mere theoretical calculations.

He spends much time offering his assessment of what one can expect—or not expect—to glean from the fossil record. He gives quick characterizations of types of evidence—'historical evidence' he calls 'indirect' (as, indeed, it is in comparison with the evidence

[1]As is perfectly reasonable, Darwin reserves the word *fact* for those pieces of data or opinion that have been, in some sense, vetted, and are not currently in dispute; The word *evidence* in *The Origin of Species* can refer to something more preliminary, yet to be tested and deemed admissible or not. Sometimes, if evidence is firmer than that, Darwin will supply it with an adjective such as *clear evidence* or *plainest evidence*; it may come as a negative, such as "there isn't a shadow of evidence."

one gets by having an actual bone in one's actual hands). These types of judgments frame the project of evolution.

The subsequent changes in Darwin's initial repertoire, such as evidence obtained by formulating various mathematical models, or the formidable technology of gene sequencing, etc. mark changes in the types of argument evolutionary biologists regard as the constituting a genuine result in the field—in effect, changes of what they regard *evolutionary biology* to be.

2. **Evidence in Math**

To start a conversation, I'll show that this notion, *evidence,* is not cut and dried, even in mathematics, where people often construe it to mean proof, and nothing more[2]. Although clarity is the signature of mathematics, the shape of evidence relevant to understanding mathematics, or working with mathematics, is not at all straightforward. For example, consider how versatile Mathematics is in importing traces of evidence from the world around, or from other fields. Consider how, at times, Mathematics merges with Physics, where each of these fields provides a bounty of insights, evidence, and direction, for the other. One need only think of Archimedes' method, or the Calculus, or the Dirichlet Principle[3] or the current relationship between Algebraic Geometry and String Theory.

But sticking to *evidence in Mathematics* per se, here are two distinct discussions that one might have:

- The issue of proof, the vaguaries of rigor, formal structures, logic and the limits of logic, and the well-known crises in the foundations of mathematics.

This is a conversation that has been steady, is on-going, and is a mainstay in the philosophy of mathematics. It is astonishing how intense, how rock solid, the consensus of agreement

[2]A close version of what I am about to present has already been published as **Shadows of Evidence** in the Science Newsletter of the Simons Foundation: `https://www.simonsfoundation.org/mathematics-and-physical-science/shadows-of-evidence/`. A complementary 'take' on some of the same issues—specifically: *Plausible reasoning* in mathematics—can be found in my essay **Is it Plausible?** [3].

[3]E.g., the back and forth segue, in Felix Klein's exposition of Riemann's work [4], between physical issues surrounding Dirichlet's Principle, and purely mathematical ones, are explained by Klein as follows:

> The physical method seemed the true one for my purpose. For it is well known that Dirichlet's Principle is not sufficient for the actual foundation of the theorems to be established; moreover, the heuristic element which to me was all-important was brought out far more prominently by the physical method.

among mathematicians is, regarding whether a result is established or not[4]. This is not to say that a disagreement can't occur, but when it does and persists it often has a *name* and star-billing, such as the *Hilbert-Brouwer Controversy*. Nevertheless, when you are working within mathematics you often feel how vastly more there is left to be done: most of this edifice is yet to be conceived, designed, built. Languages wait to be fashioned, that are needed even to set down the architectural plans of these future structures.

So there is also:

- the more personal, more individual, modes of evidence that persuade the mathematician to think that a certain direction is promising, another not—that this formulation may be wrong-headed (even if not wrong)—that this definition is important—that this statement is likely true.

Usually under limited knowledge and much ignorance—often plagued by mistakes and misconceptions—we wrestle with analogies, inferences, expectations, rough estimates, partial patterns, heuristics. The Emily Dickinson line "Tell it true but tell it slant" is second nature to us since *slant* is often the way we find the truth in the first place. We depend on "evidence" in order to proceed—to assess the promise of an approach to a problem—to guess where to look and what to look for—and the evidence often comes from unexpected places, and sometimes in unexpected vocabulary.

I suspect that every discipline has such two-tiered levels of possible discussion. But it is the second of these possible 'discussions' that I will focus on, for through sometimes intangible shadows of evidence mathematicians negotiate and develop their conjectures, guesses, aspirations. This second discussion, being broader than being confined to the concrete sort of evidence, might even need a descriptive word more evocative than *evidence* to embrace its various aspects. As Curt McMullen commented: one is also after "a mathematician's sense of smell, i.e. how do we as detectives or truffle hounds find something interesting to explore?"

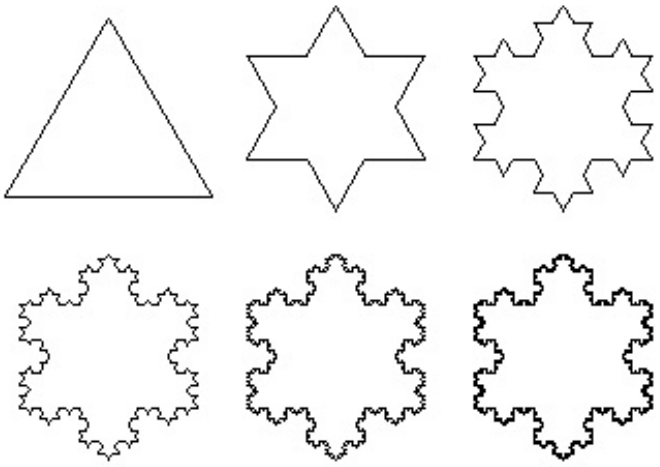
For reasons of time I can't give examples illustrating all the species of evidence playing such a role in mathematics. I will only talk about the following three categories.

[4]Even when a result is understood to be definitively proved, that is often hardly the end of the game: we bolster our understanding, and belief, of the proof by what might be called 'after-proof remarks'—auxiliary evidence, therefore— that provide a 'double-check.' Showing that something that you've just proved has an alternative proof, or that the result actually checks out by using it to prove something you already know to be true—are important items in the expositor's toolkit. An example, suggested by Curt McMullen in comments he made on an early draft of this presentation, is John Conway's verification of the classification of even unimodular lattices in dimension 24 – the Niemeier lattices – by plugging the known the lattices into Siegel's mass formula, and observing that equality holds.

- Evidence stemming from 'visual' intuition
- Numerical evidence
- Analogy.

3. Evidence stemming from 'visual' intuition

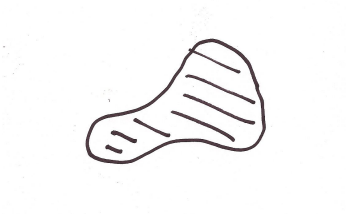
This is so ubiquitous, that it almost doesn't need any concrete example to illustrate it, but here's a dramatic emergence of an energized direction of research stemming from new pictures. I'm referring to the rise of the *fractals* of Benoit Mandelbrot —whose precursors include infinitely wiggly sets that are—in comparison—easily visualized, such as the Koch snowflake. This *Koch snowflake* is a closed curve obtained by taking the limit of an infinite sequence of crinkle-operations. Start with an equilateral triangle and on an interval one third the size of each side construct a small equilateral triangle. At each stage you are faced with a longer curve, and in the limit you have seemingly nicely contained curve within a finite region that is so crinkly so as to have—in effect—infinite length. The diagram below illustrates the first few stages.



Up to the end of the First World War, the theory that was the progenitor of the 'fractals' we will be discussing was called Fatou-Julia theory. That theory studied the structure of certain regions in the plane (very) important for issues related to dynamics. By 'dynamics' here I mean a subject that might be called 'mathematical dynamics,' which is the study of the qualitative, or quantitative, teleological phenomena that occur when you iteratively apply the same transformation (or a systematically modified transformation) to a space, a 'phase space' for example. If I use this description, mathematical dynamics is

everywhere: any differential equation is such[5], or any algorithm that can be iteratively applied. Take–for example–Newton's method for finding the zero of a function (which we will talk about, below).

Surely, given the resources available at the time, Fatou or Julia would not have been able to make too exact a numerical plot of regions related to the teleological nature of orbits arising from such iterations, if those regions are not utterly simple. And unless you plotted such a region very accurately, it would very likely show up as blob in the plane with nothing particularly interesting about its perimeter–something like this:



Partly due to the ravages of the first world war, and partly from the general consensus that the problems in this field were essentially *understood*, there was a lull, of half a century, in the study of such planar regions—a particular class of them now called *Julia sets*[6].

But in the early 1980s Mandelbrot made (as he described it)"a respectful examination of mounds of computer-generated graphics." His pictures of such Julia sets and related planar regions were significantly more accurate, and tended to look like the figures below (which is actually of a different dynamical problem than the one considered by Julia, and has a slightly more modern cast than ones Mandelbrot[7] produced in the 80s—nevertheless it has features characteristic of many of them).

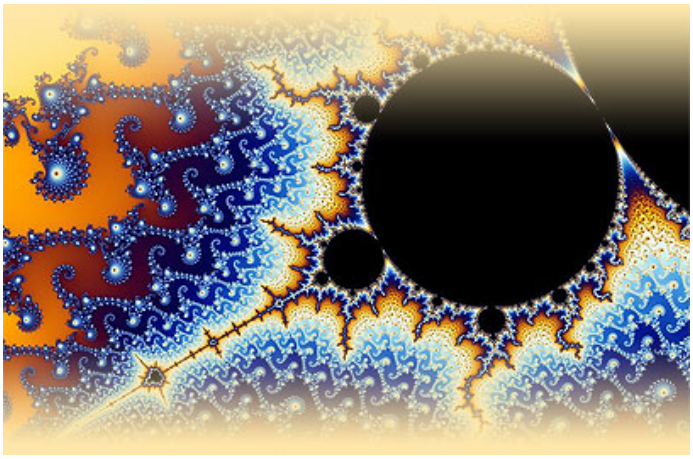
[5]And most computational algorithms offering numerical approximation of solutions of differential equations, in effect, turn the differential equation into a discrete dynamical system.

[6]If $f : \mathbf{P}^1 \to \mathbf{P}^1$ is a rational function on the complex projective plane, then its **Julia set**, $J(f)$ is the closure of the set of its repelling periodic points. Recall that a point z is *periodic, of period* $n \geq 1$ for f if $f^{(n)}(z) = z$ where $f^{(n)} = f \circ f \circ f \cdots \circ f$ is the n-th iterate of f. Such a periodic point z is *repelling* if the derivative of $f^{(n)}$ at the point z is strictly greater than 1 in absolute value. For an excellent survey of the basic theory, see [1].

[7]The image in color is called the **Mandelbrot set for the polynomial transformation** $z \mapsto z^2 + c$ which is the locus of complex numbers c for which the orbit of 0 under iteration of that transformation, i.e.:

$$0, c, c^2 + c, (c^2 + c)^2 + c, \ldots,$$

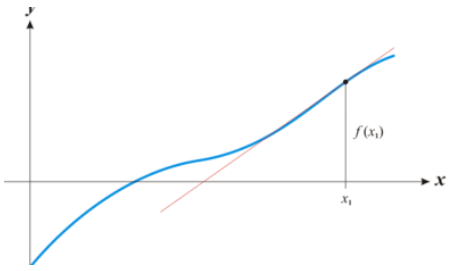
remains bounded. The coloring scheme for the points c in that image is according to some code that corresponds to how rapidly the above sequence diverges, if at all. For more, see the (very informative and colorful) Wikipedia entry for *Mandelbrot set*.



Iterative methods tend to provide a richness of structure when accurately visualized, and they tend to lead to new applications, new theoretical considerations.

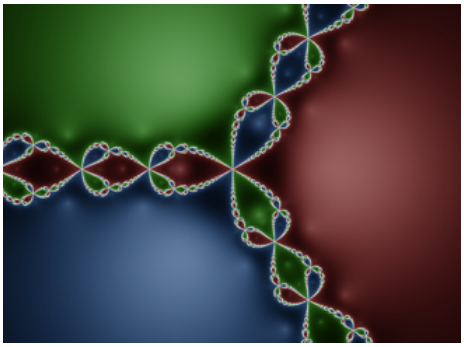
For example, consider Newton's method, which allows you to find (successive approximations to) a *zero* of a real valued (smooth) function $f(x)$. If you're sensible, and are interested in it as a handy method for the job of locating a zero of a given function, you begin by looking for a starting point x_1 at which the function f has a value close to zero. So, x_1 is *your prior*. You then correct your starting guess x_1 by the (pre-designated) procedure:

$$x_2 := x_1 - f(x_1)/f'(x_1)$$



making x_2 as your better guess, and then do this again (and again). This is enormously useful, and has amply paid its way in the straightforward mission of finding close approximations to zeroes of functions. But mathematics being what it is, one is ineluctably led to ask the question: what is the inherent structure of Newton's method, qua mathematical object in its own right, separated from its (merely historical) mission?

It becomes, from this perspective, a full-fledged dynamical system: operation that can be performed on *any* point in the complex plane and iterated indefinitely—and not only on select points that are already close to a zero. The diagram below invites us to visualize this dynamical system in the complex plane, and see it unfold in a way that suggests much more of a rich theoretical framework than its germane historical application might have hinted at[8].



From pictures alone—when initially presented by Mandelbrot in the 80s– it became evident that there is an immense amount of structure to such depicted regions and to their perimeters. This almost immediately re-energized and broadened the field of research, making it clear that very little of the basic structure inherent in these Julia sets had been perceived, let alone understood. It also suggested new applications. Mandelbrot proclaimed—with some justification—that "Fatou-Julia theory 'officially' came back to life" on the day when, in a seminar in Paris he displayed his illustrations.

Computers nowadays (as we all know) can accumulate and manipulate massive data sets. But they also play the role of *microscope* for pure mathematics, allowing for a type of extreme visual acuity that is, itself, a powerful kind of evidence.

4. Numerical evidence

How many instances constitutes enough *numerical evidence* to offer us sufficient reason to expect that one thing rather than another is the case, in mathematics? Lacking a general theoretical result about some question about which one hopes one has correctly guessed the answer, one naturally resorts to checking particular cases to bolster confidence

[8]Here, Newton's method is applied to arbitrary points in the complex plane in order to "find" the zeroes of the function $f(z) = z^3 - 1$. The Julia set for f consists of the points colored white.

in the guess. But how many instances is enough? How much numerical data do you need to strengthen your confidence? Or to weaken it?

I'll allude here to two utterly different types of contemporary examples of numerical issues, perhaps somewhat contrary to each other. I say 'allude to" because I'll give no real details for either, but still hope that the contrariness will come through.

- **Elliptic curves** The first question has to do with a certain class of algebraic curves[9] (given with rational number coefficients). It asks for the percentage of these curves that have *infinitely many* rather than *finitely many* solutions[10]. People have computed something on the order of 100 million such curves to produce evidence for the answer. When computed 'only' for these 100 million curves, however, you get that around 60% of them have infinitely many solution[11]. What is curious here is
  - People (who know about the resources available for computation) are not hopeful that one can expect, in our lifetime, to make vastly more than those 100 million computations. That is, as far as numerics go, we won't see any change in the data. Yet:
  - There is a firm consensus (of belief in certain conjectures that imply) that the ultimate percentage is not "about 60%" but rather it is *exactly* 50%.

  So much for the power of mere numerical computation—however massive—to revise an opinion based solely on conjecture and shadows of evidence! For more on this, see [2].

- **Moonshine** The second issue, with a spirit quite different from the first, involves a *single* computation, one that any of us can do:

$$196884 = 1 + 196883.$$

[9] these are elliptic curves ordered systematically in terms of the size of their conductor

[10] I.e., *rational points*, but experts will realize that I'm using a very firm classical conjecture to interpret the data this way.

[11] and this has been relatively flat over an impressive range up to 100 million

In the early seventies, the mathematician John McKay made that simple computation, but coupled it with a very important observation. What is peculiar about this formula is that the left-hand-side of the equation, i.e., the number 196884, is well-known to most practitioners of a certain branch of mathematics (*complex analysis*, and the *theory of modular forms*) while 196883 which appears on the right is well-known to most practitioners of (what was in the 1970s) quite a different branch of mathematics (*The theory of finite simple groups*) Mckay took this 'coincidence"—the closeness of those two numbers[12] —as evidence that there had to be a very close relationship between these two disparate branches of pure mathematics; and he was right!

Here are a few more words about this.

The 'lefthand side' of McKay's 'equation' above, 196884, is the first interesting Fourier coefficient of a basic function in that branch of mathematics, the elliptic modular function:

$$j(z) = \sum_{n=-1}^{\infty} c_n e^{2\pi i n z} \;=\; e^{-2\pi i z} + 744 + \mathbf{196884} e^{2\pi i z} + 21493760 e^{4\pi i z} + 864299970 e^{6\pi i z} \ldots$$

As for the 196883 that appears on the righthand side, we have quite a different story to tell: 196883 is the smallest dimension of a Euclidean space that has the largest sporadic simple group (*the 'Monster group'*) as a subgroup of its symmetries. The four lowest dimensions of irreducible representations of the Monster group are

$$1,\ 196883,\ 21296876,\ 842609326.$$

Noting that the sum of the lowest first three dimensions of irreducible representations of the Monster group is equal to the second interesting Fourier coefficient of the elliptic modular function, i.e.,

$$1 \ + \ 196883 \ + \ 21296876 \ = \ 21493760.$$

And, tantalizingly, the third interesting Fourier coefficient is equal to a similar linear combination, with strikingly small coefficients, of dimensions of irreducible representations of the Monster group:

$$2 \times 1 \ + \ 2 \times 196883 \ + \ 21296876 \ = \ 864299970$$

we see (i.e., McKay saw) that surely *something* is going on here: the successive Fourier coefficients c_n of the elliptic modular function seem to be interpretable as the dimensions of representations (call them provisionally T_n) of the Monster group, and—moreover—the irreducible representations that occur in these T_n's have striking low multiplicities. It is perfectly reasonable, then, to ask whether there is, in fact, a *natural* sequence of representations T_n that play a suitable role

[12]McKay gave a convincing interpretation of the "1" in the formula as well!

> here, and... beyond that, what in the world is going on? What has been developed in various directions is so surprising that it has taken on the nickname *monstrous moonshine*, and involves the beautiful work of many people now, including John McKay, John Conway, Simon Norton, John Thompson, Richard Borcherds, Igor Frenkel, James Lepowsky, Arne Meurman, and others. And, it began with McKay's surmise.

5. Analogy

I'm annoyed by André Weil's famous paragraph on analogy in mathematics, but feel that it tends to start discussions with a bang, so I'll quote it:

> Nothing is more fruitful—all mathematicians know it—than those obscure analogies, those disturbing reflections of one theory on another; those furtive caresses, those inexplicable discords; nothing also gives more pleasure to the researcher. The day comes when this illusion dissolves: the presentiment turns into certainty; the yoked theories reveal their common source before disappearing. As the Gita teaches, one achieves knowledge and indifference at the same time.

My annoyance, by the way, is with the somewhat curious importation of the sentiment of 'indifference.' I don't know Sanscrit but discover that Weil's sentence relates to Verse 52 of the *As it is* Chapter 2 in the Bhagavad-G$\bar{\imath}$t$\bar{a}$:

> yad$\bar{a}$ te moha-kalilaṁ
> buddhir vyatitari∫yati
> tad$\bar{a}$ gant$\bar{a}$si nirvedaṁ
> śrotavyasya śrutasya ca

which, I'm told, means:

> When your intelligence has passed out of the dense forest of delusion, you shall become indifferent to all that has been heard and all that is to be heard.

In contrast to the state (of indifference) signaled by the Bhagavad-G$\bar{\imath}$t$\bar{a}$, "yoked theories" in mathematics having revealed "their common source" simply become instances of a grander theory[13].

[13]One need only think of *prime ideal* instantiated as "point" on an affine algebraic variety—in *Algebraic Geometry*—and as an appropriate notion of "prime" in Algebraic Number Theory. I'm not clear where the 'indifference' resides.

It is also notable that in mathematics—in contrast to some other fields—when one successfully establishes a significant viewpoint that allows one to unite two 'analogous concepts' one can, at times, formulate *one* truly united concept, so that each of the analogized concepts are now direct instances of the new synthesis. This is rare, I think, in similar analogies that occur in other fields. For example, the historical (simple) analogy between electric circuits and hydraulic systems allowed one to see in what manner the formulae relating their behavior coincided. But electric circuits and hydraulic systems were not viewed as instances of one more general object. The ultimate distinctness of two analogized instances is all the more apparent in any literary analogy or simile ("My love is like a red, red rose")[14].

Now mathematics is built on analogy. The history of mathematics is studded with analogies between theories A and B, where the analogy has the force—of some degree—of evidence, in that things true about A, appropriately translated to B may not be deemed true yet for B, but perhaps are thought to be sufficiently plausible—based merely on the 'evidence' of the analogy—that it may be worth your time to look for a proof of it in the theory B. Some of these analogies are so successful, and in fact so universally acknowledged as to become almost transparent, 'evident.' We all 'have' those analogies in our central nervous system.

Here, then, is a medley of some classical and modern examples of analogies in mathematics that have played their important roles, and I'll begin with the analogy of *Time* as *Distance*, the most transparent analogy of all:

(1) **Time as distance** We say "far in the future," or "a long time ago" without (usually) acknowledging the depth of insight that some proto-mathematician must have had in order to utter this quintessentially mathematical leap of imagination. I think this is indeed a leap of the imagination and should not be under-estimated, even though, on the one hand,

- absolutely any *linearly order-able* thing (or notion) begs—given its ordering—to be geometrized, or at least to be thought of analogically as 'geometrical' such as temperature on a thermometer, or anything read by a gauge.

And on the other hand,

[14]Curt McMullen mentioned to me a comment of Borges, relevant to this thought—namely, that "imminence of revelation" is appropriately in the realm of the aesthetic, rather than the logical, as long as it is *always* in the state of the never-quite-emerging. This captures the romantic element of Kant's view of aesthetic judgment and suggests an attitude toward those 'presentiments'(as Weil described) of analogies that refuse to be subsumed in a single overarching theory, i.e. those which are destined to fall into—or ascend to– an aesthetic rather than an epistemological realm. As McMullen commented, this fits well with Woodin's view of his "ultimate L" and its relation to the Continuum Hypothesis which has, surely, an aesthetic quality, but Woodin argues for it on epistemological—and 'extra-logical'—grounds.

- the Time/Distance analogy, ubiquitous as it is, isn't all that strong: for example, *time*—in our experience—is uni-directional.

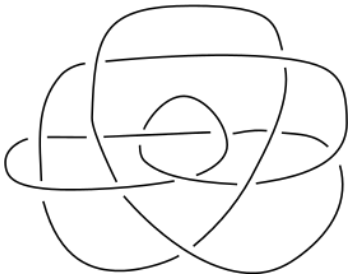
(2) **Conic sections** One example is the Euclidean study of *ellipses, parabolas, hyperbolas.* These were viewed fruitfully as analogous—until—at the time of Appolonius of Perga—that "presentiment turned into certainty," when they were all three of these types of mathematical objects were viewed as 'the same thing,' i.e., conic sections.

(3) **Archimedes** Another example is Archimedes 'Method' where volumes were taken to be like objects that have weight and were laminated into a continuous stream of cross-sections, each of which was weighed on a lever (using 'Archimedes law of the lever') to heuristically show his famous quadrature theorem.

(4) **Knots and Primes** But to give another example of an analogy, a contemporary analogy that might be surprising to some:

Knots $\iff$ **Prime numbers**

Now, a **Knot** is something like this:



and a **Prime number** is something like this:

37.

So, how in the world can these distinct kinds of mathematical objects be analogous?[15] Nevertheless, the analogy between them is staggeringly strong, so that if we know some particular thing about one of these kinds of objects, we have motivation, at least, to take this knowledge as analogical *evidence* that the corresponding 'thing' might possibly hold for the other kind of object.

Here is one simple example. (Of many!)

Certain ways of measuring the 'interaction' between two different prime numbers carry over directly—via this analogy—to ways of measuring the 'interaction' or the linking of two different knots. To give you a sense of what it might mean for primes to interact with each other, let P and Q be two primes—for example:

$$P = 2^{57,885,161-1} \text{ and } Q = 2^{43,112,609-1}.$$

Now ask yourself the following two (very different, but linked) questions:

1: Is there a solution (in whole numbers X and Y) to the equation:

$$P = X^2 + QY?$$

2: Is there a solution (in whole numbers X and Y) to the equation:

$$Q = X^2 + PY?$$

The quadratic reciprocity theorem of Gauss tells us that for any pair of prime numbers P and Q, no matter how difficult, or easy, it is to answer either one of those YES or NO questions, the answers to them are linked. By 'linked,' I mean that it is *dead easy* to tell, for a given P and Q, whether the answers agree (i.e., YES to both or NO to both) or disagree (i.e., one of them gets a YES and the other gets a NO)[16] even though you may have a slightly more difficult time pinning a definitive YES or NO to either of these questions[17] .

The analogous result in the world of knots has to do with what is called the *linking number of two knots* K and L which says how intertwined the two are with each other[18].

[15]As already mentioned in the previous footnote, Algebraic Geometry has already seen for well over a century—thanks to the efforts of Weber and Kronecker— a different—and in the end, equally mysterious—analogy between *primes* and *points on algebraic varieties*. This could be a side-discussion.

[16]That's the case for $P = 2^{57,885,161-1}$ and $Q = 2^{43,112,609-1}$.

[17]The very linking of those two question given by the quadratic reciprocity theorem leads to a log-fast solution of both of them, which is an added bonus!

[18]The corresponding "Question 1" for knots would compute this linking number by–in effect–measuring in an appropriate way how many times K winds around L (the definition needed here is elegant) and the "Question 2" for knots would reverse the roles of the two knots in that computation. The theorem, again says that a response to "Question 1" gives us a response to "Question 2" and, of course, vice versa.

(5) **'Duality' as analogy**

One doesn't usually think of the duality inherent in projective geometry—say, the geometry of the projective plane—as a type of analogy, so let me try to frame it in this way:

$$\{\textit{Points} \text{ are related to } \textit{Lines}\} \quad \overset{\text{just as}}{\longleftrightarrow} \quad \{\textit{Lines} \text{ are related to } \textit{Points}\}$$

on the projective plane. For example:

Two points determine (i.e., generate) a line

just as

Two lines determine (i.e., intersect at) a point.

The standard duality theorems for finite dimensional vector spaces may be viewed as what is behind the duality just described for the projective plane; those duality theorems can be considered a natural linear way of expressing the *line-point* analogy described above, and, in fact, a generalization of it in arbitrary dimensions.

There are natural further extensions of such types of duality. For example, one has a general duality theory for *abelian* locally compact groups, the prototype being the duality between the circle group and the discrete group of integers with its direct connection to the classical theory of *Fourier series*.

Things get even more interesting (and somewhat more puzzling) when one formulates a beguiling extension of duality theory for abelian locally compact groups to yield a *non-abelian* version of duality in the context of general Lie groups (specifically: connected semisimple, or reductive groups). Thanks to the theory of Lie, Killing and Cartan, the essential data determining a connected simply connected semisimple group G is cleanly given by a maximal torus T in that group together with some extra structure on that torus; for brevity let me just call that extra structure ϵ. Since the torus is a commutative group, we can apply the theory of duality for abelian groups and pass to the dual torus, $\hat{T}$. As it happily turns out, one can make use of the extra structure ϵ on T to give rise to a corresponding 'extra structure' $\hat{\epsilon}$ on $\hat{T}$, thereby producing essential data for some other semisimple, or reductive group, $\hat{G}$, called the *dual group to* G.

Linked by the duality between these abelian groups, i.e., their maximal tori, and essential extra data, the groups themselves are considered to be in 'duality' correspondence

$$G \qquad \longleftrightarrow \qquad \hat{G}.$$

So far, this is not terribly radical for we have no more than a proclaimed 'duality' between objects of the same species: continuous groups.

It was Robert Langlands who made use of this duality between *nonabelian* Lie groups as a mere springboard for a much bolder analogy—in fact a profound close correspondence—between quite disparate fields of mathematics. This analogy is, at present, extensively developed into a full-fledge theory known as

The Langlands program, or **Langlands duality**,

one of its fundamental goals being to establish a close analogy—indeed a specific correspondence—between the two fields of mathematics:

Algebraic Number Theory $\longleftrightarrow$ Automorphic Representations[19].

This program is still far from fully developed and is something about which one is anything but 'indifferent." Mathematics is simply laced with analogies that are bearers of evidence from one field to another!

References

[1] McMullen, C.T., Frontiers in complex dynamics, Bull. Amer. Math. Soc. **31** (1994), 155-172.
[2] Bektemirov, B., Mazur, B., Stein, W., Watkins, M., Average ranks of elliptic curves: Tension between data and conjecture, Bull. Amer. Math. Soc. **44** (2007), 233-254.
[3] Mazur, B., *Is it Plausible?* (On my homepage: `abel.math.harvard.edu/~mazur/papers/Plausibility.Notes.3.pdf?` and to appear in print in *The Mathematical Intelligencer*, and currently on-line: `http://link.springer.com/article/10.1007%2Fs00283-013-9398-0`)
[4] Klein, F., *On Riemann's Theory of Algebraic Functions and their Integrals: A Supplement to the Usual Treatises*, (tr.: Frances Hardcastle) MacMillan and Bowes, (1893)

[19]The 'Algebraic Number Theory' comes into the picture by consideration of representations of Galois groups of number fields into certain towers of finite groups related to a reductive algebraic group G. The 'Automorphic Representations' come into the picture by considering (usually) infinite-dimensional representations of the dual group $\hat{G}$.