Why is it plausible?

Barry Mazur

January 5, 2012

Rough notes in preparation for a lecture at the joint AMS-MAA conference, Jan. 5, 2012

We mathematicians have handy ways of discovering what stands a chance of being true. And we have a range of different modes of evidence that help us form these expectations; such as: analogies with things that are indeed true, computations, special case justifications, etc. They abound, these methods—explicitly formulated, or not. They lead us, sometimes, to a mere hint of a possibility that a mathematical statement might be plausible. They lead us, other times, to substantially firm—even though not yet justified—belief. They may lead us astray. Our end-game, of course, is understanding, verification, clarification, and most certainly: proof; truth, in short.

Consider the beginning game, though. With the word "plausible" in my title, you can guess that I'm a fan of George Pólya's classic *Mathematics and Plausible Reasoning* ([MPR]).

George Pólya (1887-1985)

I think that it is an important work for many reasons, but mainly because Pólya is pointing to an activity that surely takes up the majority of time, and energy, of anyone engaged in thinking about mathematics, or in trying to work towards a new piece of mathematics. Usually under limited knowledge and much ignorance, often plagued by mistakes and misconceptions, we wrestle with the analogies, inferences, and expectations I've just alluded to; with rough estimates, with partial patterns that hint at more substantial ones, with partial consequences of hypotheses that are true—or seem true—and therefore render it more likely that those hypotheses are true, or at least should be provisionally conjectured, and worked with. We make use of a whole inventory of different rules-of-thumb, and somewhat-systematic heuristics that, when they work, allow us to divine what is true.

Along with this, we are constantly assaying the level of plausibility of any of these conceits, and formulations, that float through our mind as we grapple. A three-level activity:

1. developing possibilities, hypotheses, expectations, through a network of more or less confidence-inspiring heuristics, and at the same time
2. assaying their plausibility, and at the same time
3. "shorting them," to use (metaphorically) an infamous financial term, i.e., working to disprove them,

is what establishes—at least for me, and I imagine for many others—the three voices of the contrapuntal inner music that we experience when we strive to comprehend some idea, new to us, in mathematics (and more broadly, in anything).

How do we gain confidence in mathematical guesses, before we actually prove them? In contrast to the main thrust of Pólya's text, I'm less interested in being pro- or pre-scriptive; that is, I don't have a pedagogical mission presuming to say what one *should not* or *should* do; I'm just aiming at a reflective description of some ways of thinking that come up naturally (to me, and therefore—I assume—to others as well) when one is grappling with judgments regarding plausibility in mathematics. Different mathematicians will surely have different descriptions, and conversations about these differences could be worthwhile. Moreover, a psychologically oriented study of *plausibility in mathematics* in the manner of Tversky and Kahneman might also reveal interesting phenomena.

Here are three distinct modes of reasoning that provide us with plausible inferences:

- *reasoning from consequence*,
- *reasoning from randomness*, and
- *reasoning from analogy.*

The first of these is largely a non-heuristic method, while the other two are heuristic, the distinction being:

- A *heuristic* method is one that helps us actually come up with (possibly true, and interesting) statements, and gives us reasons to think that they are plausible.

- A *non-heuristic* method is one that may be of great use in shoring up our sense that a statement is plausible once we have the statement in mind, but is not particularly good at discovering such statements for us.

In what follows, I'll be discussing each of these modes in turn, noting that this three-part distinction is sometimes blurred by the fact that all three can work surprisingly well together. Among other things, I'll be specifically thinking about what might have been the motivation for Leonhard Euler to have come up with a certain curious conjecture.

Leonhard Euler (1707-1783)

1 Reasoning from Consequence

This is captured by the maxim:

If (**A**) *implies true things we gain confidence in* (**A**).

Depending upon the particular way it is cast, it is sometimes referred to as

- Induction, or
- Experimental confirmation, or

- "Inferential fallacy."

Here is the example we'll focus on.

We learn from Pólya[1] that Euler made the following conjecture:

> Any number of the form $3+8n$ (for n positive) is the sum of a square and the double of a prime[2]:
>
> $$(\mathbf{A}) \qquad 3+8n = a^2 + 2p.$$

This is still today just a conjecture, neither proven nor disproven. How would you have first discovered such a statement, as being potentially true? Having coming up with the statement, how would you garner evidence for its truth? How would you augment or diminish its level plausibility? That is, without actually proving it.

Of course, faced with such a problem, the first thing one might—perhaps should—do is to test it numerically:

$$11 = 1^2 + 2\cdot 5$$
$$19 = 3^2 + 2\cdot 5$$
$$27 = 1^2 + 2\cdot 13$$
$$35 = 1^2 + 2\cdot 17 = 3^2 + 2\cdot 13 = 5^2 + 2\cdot 5$$
$$\dots$$

Now, Euler became interested in this conjecture—Pólya explains—because by assuming it, Euler could prove:

> Any number is a sum of three trigonal numbers:
>
> $$(\mathbf{B}) \qquad n = \frac{x(x+1)}{2} + \frac{y(y+1)}{2} + \frac{z(z+1)}{2},$$

a result he *believed to be true* and had been previously interested in[3]. It is intriguing to follow Euler's (strange, I think) train of thought: *what got him to think that the* (**A**) *he was specifically interested in would be made more plausible by virtue of its implying the* (**B**) *above?*[4]

[1] This is discussed as an example of **Verification of a consequence**: page 3 of Vol. II of *Mathematics and Plausible Reasoning: Patterns of plausible inference.*

[2] Euler could include $n=0$ in his assertion, since he allowed 1 to be a prime—thereby siding with my father, who, whenever he wanted to get my goat, would playfully ask me to defend my bizarre contention that the first prime is 2. Since I have removed 1 as prime, from the initial conjecture conceived by Euler I have ever-so-slightly strengthened it.

[3] Numbers of the form $n(n+1)/2$ are called *trigonal* since they can be thought of as counting an array of points in the plane that have integral coordinates and form—i.e., have as their convex closure—an isosceles right-angle triangle.

[4] A sketch of why **A** implies (**B**) is given in the afterword below.

This latter statement, (**B**), is a special case of Pierre de Fermat's *polygonal number "theorem,"* and even though Euler believed (**B**) to be true, no (published) proof of it existed at the time; (**B**) was proved later by Gauss in 1796 in *Disquisitiones Arithmeticae* (there is an often-quoted line in his diary recording its discovery: "Eureka! num $= \Delta + \Delta + \Delta$").

By describing this turn of Euler's thought, Pólya is pointing to the following intricate zigzag regarding (**A**) and (**B**). Euler *showed* (**A**) $\Longrightarrow$ (**B**) and *believed* (**B**) to be true (but hadn't *proved* (**B**)). As a result, (**A**) was rendered more believable; a kind of transport of plausibility:

$$\begin{array}{c} (\mathbf{A}) \qquad \Longrightarrow \qquad (\mathbf{B}) \\ (\mathbf{B}) \text{ is plausible} \\ \text{------------} \\ (\mathbf{A}) \text{ gains in plausibility} \end{array}$$

We can take this diagram as a "plausibility" companion to the classical *modus ponens* which has the following shape:

$$\begin{array}{c} (\mathbf{A}) \qquad \Longrightarrow \qquad (\mathbf{B}) \\ (\mathbf{A}) \text{ holds} \\ \text{------------} \\ (\mathbf{B}) \text{ holds.} \end{array}$$

Each time a special case of a general statement is something we believe to be true, we acquire a tiny bit more confidence about that general statement. All the better, of course, if that "special case" is *known* by us to be true. We then enact, in our thought, this *inverted modus ponens*:

$$\begin{array}{c} (\mathbf{A}) \qquad \Longrightarrow \qquad (\mathbf{B}) \\ (\mathbf{B}) \text{ holds} \\ \text{------------} \\ (\mathbf{A}) \text{ gains in plausibility.} \end{array}$$

We might think of the above diagram as one of the mainstays of the *calculus of plausibility*, while modus ponens is key in the *calculus of logic.* That there are vast differences between these two brands of "calculus" is so evident that it hardly needs to be said: In the calculus of plausibility, our prior assessments are all important. How *much* (**A**) gains in plausibility, given that (**A**) $\Longrightarrow$ (**B**) and (**B**) holds, depends on judgments about the relevance of (**B**) vis à vis (**A**). It is often influenced by our sense of surprise that (**B**) is true, if we are, in fact, surprised by it.

In contrast, there is no judgment call necessary in the calculus of logic; what you see is what you get: $(\mathbf{A}) \Longrightarrow (\mathbf{B})$ *plus* $(\mathbf{A})$ simply gives you $(\mathbf{B})$.

In view of this distinction between the two modes of thought, it is hardly strange that modifications of formulations which may be *equivalent* to each other in the calculus of logic, may become quite alien to each other in the calculus of plausibility. A famous example of such a modification is passage to the contrapositive, as in the philosophical conundrum, due largely to Carl Gustav Hempel. This is sometimes called *Hempel's paradox*, or the *raven paradox*, and starts with the observation that "logically speaking" the two statements:

All ravens are black
and
No non-black object is a raven

are genuinely equivalent; and yet the natural (*reasoning from consequences*) way of collecting empirical evidence for the first statement is to find raven after raven and check whether or not they are black, whereas the corresponding strategy for the second formulation is to look for objects that aren't black, and then check that they aren't ravens.

Now the first strategy to gain confidence in the assertion seems quixotic perhaps, but vaguely sane to us, while the second is utterly ludicrous. (The essence of this "paradox," as far as I understand it, is that even though the two statements above are equivalent from the vantage-point of the calculus of logic, they present quite different natural strategies for "reasoning from consequence.")

A typical mathematical analogue to Hempel's conundrum—which sheds some light on the initial issue— might be the comparison of the following two modes of building confidence in the Riemann hypothesis, which—formulated in the traditional way—asserts (still conjecturally, of course) that all the zeroes of the Riemann zeta-function, $\zeta(s)$, either lie on the real line (in which case they occur at negative even integer values of s: these are called the *trivial zeroes* of $\zeta(s)$ since the question of vanishing—or nonvanishing—of the zeta function on the real line is known) or else the zeroes lie on the line $Re(s) = 1/2$ in the complex plane. The Hempel conundrum, given this formulation, would be to note the fact that the natural *reasoning from consequence* mode of collecting evidence for the hypothesis as stated, and of its contrapositive, would be—respectively:

- Find a (nontrivial) zero of the Riemann ζ-function and check that it actually lies on the line $Re(s) = \frac{1}{2}$, or:
- find a point s_0 in the complex plane that is (not a trivial zero and) is *off* the line $Re(s) = \frac{1}{2}$, and check that $\zeta(s_0) \neq 0$.

There are a few things to discuss, even with regard to this somewhat frivolous example. As for the second strategy above, if we were to choose an s_0 outside the critical strip, we would learn absolutely nothing we hadn't known—since we already know that all the trivial zeroes lie in the critical strip. Even keeping to the critical strip, however, we do have the prior knowledge that the set of zeroes is discrete, so the chances of hitting on a zero by a random choice of a point is. . . *well*. . . zero. In contrast, the delicacy of the first strategy—requiring something to lie on a given line—is a very demanding test. In brief, this intricate network of "prior assessments" control the calculus of plausibility related to these strategies. What makes *reasoning from consequence* so multi-stranded is illustrated by this example of the Riemann Hypothesis, where there are many equivalent formulations of this very same hypothesis, and each formulation provides us with yet a different natural (*reasoning from consequences*) way of collecting empirical evidence for it. For example, one of the standard equivalent formulations, which is also one of the major reasons for being interested in the conjecture in the first place, is the good approximation implied by the Riemann Hypothesis for the function $\pi(X)$, the number of primes less than or equal to X. Specifically, if $Li(X) := \int_1^X \frac{dt}{\log t}$ then the Riemann Hypothesis is equivalent to the estimate:

$$|Li(X) - \pi(X)| < X^{\frac{1}{2}+\epsilon}$$

for any positive ϵ and $X >> 0$ (the "$>>$" depending on ϵ). With this formulation in mind, the more straightforward way to "reason from consequences" would be to compute $\pi(10^n)$ and $Li(10^n)$ for various n's and compare.

Reasoning from consequences comes in two forms, one that might be called **top-down,** and the other **bottom-up.**

The *top-down* form is where you firmly have an "A" in mind, explicitly formulated, and you want to assess its plausibility by finding "B"s, that are provable and are implied by this A, thereby shoring up your confidence in the truth of A. For example, in our discussion of the Euler conjecture, we recommended making numerical calculations, e.g., $11 = 1^2 + 2 \cdot 5$ etc. as a sequence of confidence builders. This, then, would be an example of the top-down version of reasoning from consequence.

One gambit that seems to fit into this top-down framework is when you have an A as your goal, and you manage to prove a B which is a special case of A. But, there are instances where this B, far from rendering A more plausible, may very well be either neutral or negative for that end; for, depending upon the case at hand, it might be relevant to ask the following disturbing question: how does it happen that your proof of B actually breaks down in the more general context of A, and could that be more of a hint that something goes wrong, rather than right, in that general context?

The *bottom-up* form is where you don't have any general A in mind, but do have a potential B that you know to be true, or more usually, you have a number of potential "B"s and you are looking for a larger framework, an "A," that implies this "B," or these "B"s. An example of this is given by Pólya's discussion regarding Euler's Conjecture, discussed above. For, Pólya tells us that Euler "wanted" the B (any number is a sum of three trigonal numbers) and, in his quest for it, he formulated an A (his conjecture about twice primes) because it would imply his B.

This type of route, a "bottom-up reasoning from consequence," is also a standard strategy for developing demonstrations: we often know what we want to prove, and we "work backwards," so to speak, in that we formulate things that are more and more plausible, more accessible, that imply it.

One might think of *reasoning from consequence* as being in the spirit of what is usually called *scientific induction*, or at least the version of scientific induction that makes sense within the context of mathematical practice. There are big differences, though; the biggest difference being that scientific induction is saturated, either explicitly or implicitly, with issues of causality, that "habit of thought," according to Hume. Now the closest thing to "causality" (as viewed in the empirical sciences) that occurs in the mathematical scheme of things is"logical implication." But these concepts, "causality" and "logical implication" each have elements that are quite foreign to the other, and they each have their own idiosyncratic relationship to "time."

Let us return once more to Pólya's example–i.e., Euler's Conjecture that any number of the form $3 + 8n$ is a square plus twice a prime. Even though, as we've just mentioned, Euler achieved a sense of its plausibility from what we're calling *reasoning from consequence*, there is another plausibility route for this same conjecture. One might come to believe this same conjecture—or at least something qualitatively like that conjecture—via a heuristic method that proposes that once one takes account of all the known constraints, the data is random.

2 Reasoning from Randomness

As mentioned above, this mode of reasoning can be captured by, the following sentiment:

> We know all the relevant systematic constraints in the phenomena that we are currently studying, and ... the rest is random[5].

It is a somewhat hubristic type of reasoning, but it is—as I'm sure you agree—a common, and perfectly natural, way of thinking; it is very often a powerful method that leads to formulating hypotheses that—if not always true—at least often represent "current best guesses." This method, in contrast to "reasoning by consequence," is genuinely heuristic: when it is applicable, it does indeed present us with fairly precise formulations.

Here is a simple example of a problem which will illustrate the power, and the essential limitations of this hubristic method.

> Let a, b, c be a triple of positive integers. Consider the diophantine equation
>
> $$A + B = C$$
>
> where A is allowed to be any positive integer that is a perfect a-th power, B a perfect b-th power and C a perfect c-th power. (So, for example, if $a = b = c = 2$ we are considering Pythagorean triples.) Let X be a large positive integer, and $N(X)$ be the number of solutions of our diophantine equation with $C \leq X$. What can we say about the behavior of $N(X)$ as a function of the bound X?

And here is a rough argument that might lead you to some kind of conjecture regarding this problem. It is in a genre of speculation that almost all mathematicians must have engaged in, at

[5] We form the [measure] space comprising the possible outcomes we are interested in, subject to all constraints that we happen to know of, and then we put what we consider to be some kind of 'even-handed' probability measure on this space. This is sometimes tagged as an application of *the principle of insufficient reason.*

one time or another, in the vocabulary of their fields of interest.(For simplicity I will ignore positive constants independent of X that arise in our error estimates either as multiplicative factors or simply as constants.) Here are possible steps in our deliberation:

1. *Following the dictum for the method, as described above,* we want to think of the two sides, $A+B$ and C, of our diophantine problem:
$$A+B=C$$
as being "random," except, of course, for all our "prior" knowledge about them. So we must take an inventory of what we actually know:

2. *Is there an systematic structure to the collection of solutions?* Here the only thing that comes to my mind is that if d is the least common multiple of a, b, c and (A, B, C) is a solution to our problem, i.e., a contributor to the number $N(X)$, then for every integer
$$k = 1, 2, 3, \ldots (X/C)^{\frac{1}{d}}$$
we have that
$$(k^d \cdot A,\ k^d \cdot B,\ k^d \cdot C)$$
is also a solution.

3. *Hypothesizing the systematic structure away:* There are many ways of dealing with systematic structure, and one way is simply to hypothesize it away! So let us change our problem, and ask questions about the behavior of the function

   $N_o(X) :=$ the number of *relatively prime* triples (A, B, C) that are solutions to our problem.

   Of course this will affect the collection of (A, B, C)'s that are in the game, but as we will see, not by much.

4. *Formulating the probabilistic event:* We get a "hit," i.e., a solution to $A+B=C$ every time we get that the number $A+B-C$ is zero. But—and this is the big assumption—viewing $A+B-C$ as randomly roaming through the allowable range which is roughly of size X as we run through our allowable triples (A, B, C)——the probability that any $A+B-C$ is zero is roughly X^{-1}.

5. *Counting the number of times we are allowed to play the above game:*

   The rough number of *all conceivable* values of A that might appear in a solution in the range $\leq X$ is $X^{\frac{1}{a}}$ and similarly for B and C where we get $X^{\frac{1}{b}}$, and $X^{\frac{1}{c}}$, *respectively.* We now need to confront the requirement that our three numbers (equivalently: any two of them) are relatively prime. This—given the roughness of our calculation—we can ignore, the reason for which I will sketch in this footnote[6].

[6] The possible choices of A are the a-th powers of integers $u := 1, 2, 3, \ldots, X^{\frac{1}{a}}$ and for each of these choices we must choose B's which are the b-th power of $v := 1, 2, 3, \ldots, X^{\frac{1}{b}}$ that are relatively prime to u. So, for each prime p we must throw out all pairs $(u = pu_o, v = pv_o)$ in our range, i.e. roughly $p^{-2}X^{\frac{1}{a}+\frac{1}{b}}$ pairs. Overestimating, then, we throw out at most
$$(\sum_{p \text{ prime}} p^{-2}) \cdot X^{\frac{1}{a}+\frac{1}{b}}$$
pairs. Since $\sum_{p \text{ prime}} p^{-2})$ converges (it is $0.452247\ldots$) we absorb this into our constants, and can ignore it.

So we do have (roughly)

$$X^{\frac{1}{a}} \cdot X^{\frac{1}{b}} \cdot X^{\frac{1}{c}} = X^{\frac{1}{a}+\frac{1}{b}+\frac{1}{c}}$$

shots at this. So the expected number of successes will be $\frac{1}{X}$ times $X^{\frac{1}{a}+\frac{1}{b}+\frac{1}{c}}$, or:

$$X^{\frac{1}{a}+\frac{1}{b}+\frac{1}{c}-1}.$$

To blur things a bit, given that we have been arguing quite naively, we might conjecture:

- When
  $$\frac{1}{a}+\frac{1}{b}+\frac{1}{c} > 1,$$
  we should get:
  $$X^{\frac{1}{a}+\frac{1}{b}+\frac{1}{c}-1-\epsilon} < N_o(X) < X^{\frac{1}{a}+\frac{1}{b}+\frac{1}{c}-1+\epsilon}$$
  for any $\epsilon > 0$, and for $X >> 0$ (with the implied constant in ">>" depending on ϵ).

- When
  $$\frac{1}{a}+\frac{1}{b}+\frac{1}{c} < 1,$$
  the above estimate would give us a *decreasing* number of hits as X tends to infinity; which doesn't make much sense at all, but we interpret it as suggesting

  Conjecture 1 *Fixing exponents a, b, c satisfying the inequality $\frac{1}{a}+\frac{1}{b}+\frac{1}{c} < 1$, there are only finitely many solutions to the diophantine problem $U^a + V^b = W^c$ with (U, V, W) relatively prime positive numbers.*

  We see the classical *Last Theorem of Fermat* as giving a good deal more precise information than the above conjecture for the cases $a = b = c > 3$. This illustrates the structural shortcoming of this probabilistic heuristic: it is quintessentially probabilistic, and could not get one to make as precise a conjecture as Fermat's Last Theorem, even though it might offer, as plausible guess, some affirmation of the qualitative aspect of that Theorem[7].

As I mentioned, every mathematician must have some favorite applications of reasoning from randomness. In number theory, my current favorite is the *Cohen-Lenstra heuristic* that give us guesses for the average values of ideal class groups over various ranges of number fields. This is obtained by imagining the thought-experiment of fabricating an ideal class group by a random process in terms of its generators and relations, subject to the prior constraints that reflect everything we know about the manner in which the ideal class group appears. So far, the Cohen-Lenstra heuristics seem to check out with numerical computations, and these heuristics are regarded as sufficiently

[7] I've left out of the above discussion the case of equality $\frac{1}{a}+\frac{1}{b}+\frac{1}{c} = 1$, which involves just a handful of possibilities: $(3,3,3), (2,3,6), (2,4,4)$ and their permutations; each of them have interesting stories. The discussion above in more general format motivates the work of Masser and Oesterlé with their wonderful, sweeping, *ABC* conjecture; see [ABC]).

plausible, that they have a firm place in the toolkit of conjectures that are helpful—even though not yet proven— guides for reflections and experiments in that branch of number theory[8].

The question: “has *all* the relevant coherent structure of the phenomena been taken into account?” hovers over every plausibility argument in this *reasoning from randomness* category. A famous conjecture in number theory due to Emil Artin predicts the density of the set of prime numbers p relative which a given integer A (not 0 or ± 1) is a primitive root. Clearly, for A to be a primitive root mod p, there *cannot be* a prime number q dividing $p-1$ such that $A^{\frac{p-1}{q}} \equiv 1$ modulo p. Artin initially tallied up the probabilities governing this behavior, and—assuming that these requirements are independent for different primes q—came up with a prospective density for this problem. Further reflection made it clear to him that there were indeed some dependencies (related to the prime 2) between these conditions and required a change of conjecture. For details about this see the Preface (written by by Serge Lang and John Tate) to *The Collected Papers of Emil Artin* Addison-Wesley (1965).

Let us return to the conjecture of Euler regarding numbers of the form *a square plus twice a prime congruent to* 1 *mod* 4 and note that if the conjecture is true, then, in some natural sense, at least one-eighth of all positive numbers are of that form (i.e., any number congruent to 3 mod 8 is of that form). What does the probabilistic heuristic have to say about this conjecture?

Well, the number of squares $< X$ is on the order of $X^{1/2}$, and—by the prime number theorem—the number of integers that are twice a prime and $< X$ is on the order of $X/\log(X)$ (recall we are ignoring positive factors that are constant). Now since the *squares* and *twice primes* have nothing to do with one another except for the relationship modulo 8, as far as we know, and since there are (on the order of) $X^{1/2} \cdot X/\log(X) \ = \ X^{3/2}/\log(X) \quad > X$ pairs of the form:

$$(\textit{square}, \quad \textit{twice a prime congruent to } 1 \textit{ mod } 4)$$

with sum $< X$, the probabilistic heuristic might prompt us to make the following conjecture:

Conjecture 2 *The set of integers of the form a square plus twice a prime congruent to* 1 *mod* 4 *is of positive density in the set of all positive integers.*

But one thing to notice is that, when this probabilistic heuristic suggests such a conjecture *it often suggests much more at the same time* (and in this case, to my mind, it certainly does). For example, by the same reasoning as we have just made, if we let $f(x)$ be any fixed non-constant polynomial with positive integral coefficients and let n be any positive number, it is just as plausible to make the conjecture that the set of numbers of the form

$$f(a) + n \cdot p,$$

as a ranges through all positive integers and p through all primes, is of positive density.

[8] More recently, there have been heuristics, somewhat in the spirit of Cohen-Lenstra, that predict the densities of given ranks of p-Selmer groups over the class of all elliptic curves over a given number field; these heuristics are due to Bjorn Poonen and Eric Rains.

3 Reasoning from Analogy

The fabric of all our thought is woven by the strands of *analogy*—conscious ones as well as unconscious ones— and is decorated by those snap-analogies: *metaphors.* So it is no wonder that mathematical thought is saturated with, and very much colored by, analogies of all sorts.

Here, then, are two somewhat different brands of analogies:

Analogy by expansion is where one has a concept, or a constellation of concepts, or a theory, and one wants to expand the reach of these concepts, retaining their structure as some sort of template. This is often referred to simply as "generalization" but that term—generalization— is, I think, more useful if it were allowed to be a looser descriptive, including, as well, some of the other types of analogical operations that I'll be listing. Analogy by expansion may have the appearance, after the fact, of being a perfectly natural "analytic continuation," so to speak, of a concept—such as the development of zero and negative numbers as an expansion of whole numbers, and from there: rational numbers, etc. BUT, the act itself may be, at the time and even somewhat afterwards, have the shock value of a fundamental change. Even though Grothendieck topologies are half a century old, and are (but only after you've learned the theory!) an utterly direct expansion of the more classical notion of topology—an expansion that gets to the essence of that classical concept—there is still the thrill of it as providing a radical refiguring of what it means to be a topology.

There is, however, a more modest version of *analogy by expansion* that we all, I believe, constantly do: starting from a **(B)** that we either know to be true, or at least firmly believe to be true, we look around for improvements **(A)** that are just a bit more general than **(B)**, for which we can show that

$$(\mathbf{A}) \Longrightarrow (\mathbf{B}).$$

Even relatively small improvements, $(\mathbf{A})$'s that are no more than $(\mathbf{B})+\epsilon$, so to speak, are fair game. Subject to no palpable counter-indication, the proved implication confers a modicum of belief in $(\mathbf{B})+\epsilon$. This is in the style of Amazon's *If you like X you'll like Y*, but here takes the form: *If you believe* $(\mathbf{B})$ *why don't you believe* $(\mathbf{B})+\epsilon$*?* As I hope will be clear from the Afterword (Section 6) below, it is this belief-expansion attitude that (I think) is also a plausible account of how Euler came to his Conjecture.

Analogy as 'Rosetta stone' is where one subject, or branch of a subject—with its specific vocabulary—is perceived as representing something of a model useful to predict what might be happening in another subject, or branch, this latter subject often having quite different vocabulary, axioms, and general set-up.

Here is André Weil's famous paragraph on analogy—expressing a sentiment that I firmly disagree with; nevertheless I keep quoting and re-quoting 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.

What I believe has been shown to be true, time after time, in the development of mathematics is that "yoked theories reveal their common source." That is, analogies between two different theories are often the first indication that there lies in the future a more embracing context that allows each of the theories that are currently yoked by analogy to be simply special instances of the larger picture, their vocabulary merging.

Examples are easily come by, some of vast importance to the nature of our subject such as the grand analogy between *algebra* and *geometry.* In fact, the trace of old mergers of distinct viewpoints can be seen in the combination words that are now titles of basic subjects, such as Algebraic Topology, Algebraic Geometry, Geometric Algebra (which is different, of course), Combinatorial Group Theory, etc.

In recent years, we have witnessed the extraordinary predictive power of analogies that link physics with mathematics—specifically: string theory with aspects of algebraic geometry—these coming from various symmetries and dualities first conceived in physics. The mere extent and number of examples here are staggering, but allow me to mention just one of them: on the basis of what one might term a *physical analogy* Candelas, de la Ossa, Green (and others) conjectured a general formula for the number of rational curves of any degree on a generic quintic threefold; e.g., the number of rational curves of degree 5 was conjectured to be $242,467,530,000$. The general formula was subsequently proved by Givental.

But physics (and physical intuition, broadly interpreted) has been offering mathematics an "analogical laboratory" with predictions that are generally on the mark, for millennia. One need only turn to Archimedes treatise *On the quadrature of the parabola* where he invokes his *mechanical method*—which he does *not* regard as rigorous!—to compute the ratio of the area of a segment of a parabola to the area of a triangle that he constructs based on the geometry of that parabolic segment. Archimedes hints that he had also given what he called a *geometric* (rather than "mechanical") demonstration of this same quadrature, a demonstration that he felt was rigorous. Archimedes performs mechanical method by laminating his parabolic segment, representing it as a continuum of linear cuts, and making a corresponding lamination of the triangle to which he is comparing his parabolic segment. Then, in effect, he "weighs" corresponding linear cuts (as if they had a "weight" in proportion to their length) to obtain the result that the "weight" of his triangle is a simple multiple of the weight of his parabolic segment (See [QP])).

Now if you suspect that this is an argument that, if correct, could easily be affirmed by calculus, you are right; but in Archimedes' conception, *The Method* works on the strength of a correctly guiding analogy that combines previously disparate intuitions that had originated in somewhat different domains: *the experience one has with a certain weighing apparatus* and *the intuition one has via Euclidean geometry.*

4 Summary so far

I have sketched–or at least hinted at—three quite different engines of plausibility: reasoning by consequence, by randomness, and by analogy.

Reasoning by consequence is the backbone of the inductive method. Its shortcoming is that in practicing this method, we often aren't clear whether or not the consequences that we have amassed in support of a general assertion are *telling* consequences. In number theory, for example, there are general conjectures for which an immense amount of numerical data has been collected that actually do *not* (at least significantly) support the general assertion, and in fact would naively suggest a different qualitative guess ... and yet we still (at least currently) believe the general conjectures. For an example of this see [AR].

Reasoning by randomness has the danger that we may not be taking into consideration *all* systematic behavior relevant to the phenomena we are studying. Nevertheless it has two great advantages: it is a starting position, a best current guess, worth contemplating to get what might be the lay of the land, and even if not accurate, it is often an analysis that separates the supposed random aspects (which may show up as 'error terms") from the more regular aspects (which may show up as "dominant terms") of the phenomena. In number theory, those error terms may then also have profound structure (e.g., See[FME])).

But reasoning by analogy is, I think, the keystone: it is present in much (perhaps all) daily mathematical thought, and is also often the inspiration behind some of the major long-range projects in mathematics. And, André Weil was right when he said: "nothing also gives more pleasure to the researcher."

In number theory the Langlands Program is one of the grand analogies—currently being vigorously pursued— connecting representation theory, algebraic geometry, and arithmetic.

The analogy between *number fields* and *function-fields of one variable over finite fields* is a more elementary, and older example.This analogy views the two type of fields we mentioned as a single entity (called a **global field**) that is treatable in a unified way[9].

[9] But, as with all great analogies, its imperfections sparkle, raising questions that may lead to future theories, far deeper than the ones we currently are at home with:

- What is the full story that connects the finite primes of a number field to its archimedean primes, its "primes at infinity"?
- What is the full analogue in the context of number fields of the *genus* of a function field (of one variable) over a finite field?
- Is there an analogue, in the context of number fields, of the product of the smooth projective models of function fields (of one variable) over a finite field?

5 Variants of 'plausible'

In our discussion of Euler's Conjecture, I hope that I've made a convincing argument that one could (and Euler might have) come to believe his conjecture from a mix of the three brands of plausible reasoning that I had labeled as separate categories at the beginning of my essay (*consequence, randomness,* and *analogy*). My feeling is that if we think through the history of any of our personal involvement with any mathematical issue that is important to us, *all* resources available to us will be playing some role in the proceedings. The way these resources interact may be complex, and may be key.

And sometimes *plausibility* itself isn't germaine. Thinking about possible mathematical strategies, it is as natural to focus our attention on issues that are useful wedges, rather than plausible formulations.

It can happen that our ideas are clarified by specifically formulating a particular *yes* or *no* question whose answer we can't guess; and yet the mere fact that we don't have sufficient experience to even make a strongly believed guess focuses the mind (a bit)[10].

Often our thoughts are peppered with fragments of possible patterns, possible formulations, and—even more important—possible organizing principles, for which *truth* is not yet even meaningful, for their truth will depend on their context, and that context is not yet fully determined, or fully formed. There are some organizing principles the truth of which is implicitly *stipulated*, as the lawyers say[11], these principles being of use to us as a guide to finding the context within which they are valid. In Physics, *conservation of energy* served as such a guiding principle: *of course* energy is to be conserved; and if one comes up with a situation where it seems not to be the case, one doesn't throw away the principle, but rather one revises one's idea of what energy *is.*

To illustrate this type of phenomenon with a celebrated mathematical example, consider the Hilbert-Pólya quest for a Hilbert space and Hermitian operator with characteristic series equal, after appropriate normalization and correction, to the Riemann zeta-function. The point here is that if such a Hilbert space and operator could be found, the Riemann hypothesis would follow. Conversely, if the Riemann hypothesis is valid, we can concoct—merely formally—some such Hilbert-Pólya model. So here *plausibility* simply isn't the issue; it is rather a question of whether or not a contemplation of this quest has some utility[12].

The Hilbert-Pólya model has already shown its usefulness, if only because it invites us to think

[10] Hilbert's Tenth Problem over $\mathbf{Q}$ is in my opinion, is one such question: is there a finite algorithm which tells for any given system of polynomial equations in many variables over the rational numbers whether it has a rational solution? Hilbert's Tenth Problem over $\mathbf{Z}$ for polynomials of degree 3 in many variables is another such question: Hilbert's Tenth Problem over $\mathbf{Z}$ has been settled affirmatively for polynomials of degree ≤ 2 by Siegel, and negatively for polynomials of degree 4 (or higher) by Matjasevic; but degree 3 is a vastly different world and despite the fact that there has been an immensely concentrated effort to understand this world, with a rich theory emerging from this, a further step in our knowledge would be represented by our having, at least, a firm consensus for a guess—just a guess—about the outcome (in degree 3) of the algorithmic problem posed by Hilbert.

[11] meaning that we agree without any further discussion to accept the principle

[12] Plausibility giving way to utility suggests that we've slipped into a bit of William James' type pragmatism.

about the zeroes of $\zeta(s)$ as related to the zeroes of analogous zeta-functions of algebraic varieties over finite fields, these being the eigenvalues of a linear operator; and in another direction it connects with Iwasawa's Main Conjecture (which is proved, and) which identifies the zeroes of the p-adic zeta-function companions to Riemann's $\zeta(s)$ with eigenvalues of natural operators; and—going in a completely different direction—the Hilbert-Pólya model invites comparison of the zeroes of $\zeta(s)$ with eigenvalues of random matrices. To be sure, if it *also* inspires a proof of the Riemann Hypothesis, that would be its crowning utility.

6 Afterword: Euler's Conjecture implies Gauss's "Eureka Theorem."

Recall that we want to assume Euler's Conjecture that any integer $n \geq 0$ occurs in an equation $(\mathbf{A})$ with a an integer and p a prime number,

$$(\mathbf{A}) \qquad 3 + 8n = a^2 + 2p,$$

and prove (what will eventually be Gauss's Theorem; i.e.,) that any integer $n \geq 0$ is expressible as a sum of three trigonal numbers. The proof of this is given in a series of steps and hints.

1. For any equation of the form $(\mathbf{A})$ above, the number a is odd, and p is of the form $4t + 1$. (Proof: work the equation $(\mathbf{A})$ modulo 8.)

2. If the prime p occurs in an equation of the form $(\mathbf{A})$ then p is expressible as a sum of two squares:
$$p = u^2 + v^2.$$
(This is *Fermat's Theorem.*)

3. If any number $n \geq 0$ occurs in an equation of the form $(\mathbf{A})$ then any number $n \geq 0$ occurs in an equation of the form
$$(\mathbf{A}') \qquad 3 + 8n = a^2 + b^2 + c^2$$
with a, b, c odd integers. (Proof: If $p = u^2 + v^2$ take
$$b := u + v, \qquad \text{and} \quad c := u - v;$$
then work the equation $(\mathbf{A}')$ modulo 8 to show oddness of a, b, c.) As usual, refer to the proposition that asserts the above fact for any $n \geq 0$ as "$(\mathbf{A}')$."

4. Write
$$a = 2x + 1, b = 2y + 1, c = 2z + 1,$$
for x, y, z integers; compute to get:
$$(\mathbf{B}) \qquad n = \frac{x(x+1)}{2} + \frac{y(y+1)}{2} + \frac{z(z+1)}{2},$$
and going the other way, show that $(\mathbf{B}) \Longrightarrow (\mathbf{A}')$.

5. Conclude that $(\mathbf{A}) \Longrightarrow (\mathbf{A'}) \Longleftrightarrow (\mathbf{B})$.

We can now speculate more exactly about Euler's plausibility thinking here. Euler believed $(\mathbf{B})$, and surely knew that $(\mathbf{B})$ is logically equivalent to $(\mathbf{A'})$. So, of course, he believed $(\mathbf{A'})$, and he knew that the passage from $(\mathbf{A})$ to $(\mathbf{A'})$ consisted in nothing more than replacing, in these contexts,

- the set of numbers that are of the form $2u^2 + 2v^2$ such that $u^2 + v^2$ is an odd *prime* number

by

- the set of numbers that are of the form $2u^2 + 2v^2$ such that $u^2 + v^2$ is an odd number.

So, perhaps, his thoughts went as follows. Fermat has assured us (without revealing his proof) that we get a correct proposition if we allow $u^2 + v^2$ to run through all odd numbers of that form. Can we sharpen things to get a better (and still correct!) proposition by requiring $u^2 + v^2$ to run only through all odd *prime* numbers of that form?

What a subtle guess, especially striking since Euler did not have the advantage of Gauss's guesses approximating $\pi(X)$; nor did he have any serious results giving relevant estimates.

And viewed from this perspective, it would seem that the mode of thought Euler is employing is a straightforward sharpening of a known result, a form of *analogy by expansion.*

References

[MPR] Pólya, G., *Mathematics and Plausible Reasoning, Volume 1: Induction and Analogy in Mathematics*, Princeton University Press (1956); *Volume II Patterns of Plausible Inference*, Princeton University Press (1968)

[ABC] The web is an excellent source for information about this, constantly up-dated. See for example: http://en.wikipedia.org/wiki/Abc_conjecture and http://www.math.unicaen.fr/∼nitaj/abc.html

[QP] Archimedes, *The Quadrature of the Parabola.* See pp.233-252 of *Archimedes' Collected Works*, (Eng. transl.: T.L.Heath) Cambridge University Press (1897). These pages have also been scanned on the web: http://www.math.ubc.ca/∼cass/archimedes/parabola.html

[AR] Bektemirov, B., Mazur, B., Stein, W., Watkins, M., *Average ranks of elliptic curves: Tension between data and conjecture*, Bulletin of the American Mathematical Society **44** (2007) 233 - 254

[FME] Mazur, B., *Finding meaning in error terms*, Bull. Amer. Math. **45** (2008), 185-228.