11 Enrico Bombieri: On Intuition

Enrico Bombieri is one of the world leaders in many areas of mathematics, including number theory, algebraic geometry, and analysis. He has won many awards, and is a Fields Medalist.

We will discuss the notion of intuition in mathematics. I am curious what it is, how to get it, and how to use it.

One story, perhaps an urban legend, is that a senior expert in real analysis was once sent a paper that "proved" a surprising theorem. The expert looked at the proof, and was immediately skeptical. The "theorem" seemed to be too surprising. His intuition, based on his great experience, was that the theorem could not be true. Yet even after hours of studying the proof he could not find any mistakes. But his intuition continued to bother him. He finally looked even more carefully, and found the problem. The author of the proof had used a lemma from a famous topology book. He had used the lemma *exactly* as it was stated in the famous textbook. But there was a typo in the book. Somehow the words "closed" and "open" had been exchanged in the statement of the lemma. This made the lemma false, caused a gap in the proof of the surprising theorem, and left the poor author with a buggy paper.

Proving theorems is not mechanical. Yes it does require formal manipulation. Yet proving theorems also requires the use of intuition, the ability to see what is reasonable or not, and the ability to put all components together. Blindly using a lemma from even the most famous textbook can be dangerous, as the story shows.

I once lost several months of hard work trying to use a published theorem to solve an open problem. I almost had a proof, but eventually—as in the story—I found a bug in the published result. The result was the sole result of a friend's PhD thesis. Oh well. This is not an urban legend; I was there, but I will leave it to another time.

For now let's turn to the discussion of intuition in mathematics.

In mathematics you don't understand things. You just get used to them. John von Neumann

R.J. Lipton, K.W. Regan, *People, Problems, and Proofs*,
DOI 10.1007/978-3-642-41422-0_11, © Springer-Verlag Berlin Heidelberg 2013

11.1 Number Theory

I think that it is not too hard to have a reasonable intuition in number theory, especially concerning the behavior of prime numbers. A pretty fair approximation is to try the distribution of primes as “random.” That is primes in the range $[N, N + \Delta]$ are roughly randomly selected odd numbers with the correct density: the number of primes in such an interval for Δ is about $\Delta / \ln N$. This of course follows from the prime number theorem.

A classic example of this is the conjectured behavior of twin primes. If primes are random, then one would expect that there are about

$$CN/\ln^2 N$$

twin primes in $[1, N]$ where C is a constant. Godfrey Hardy and John Littlewood made an even more detailed conjecture, which included the value of the constant C. They guessed that C is

$$\prod_{p \geq 3} \frac{p(p-2)}{(p-1)^2} \approx 0.6601\ldots.$$

Of course there are local properties that need to be added to the model. The number of primes p so that $p + 2$ and $p + 4$ are also primes is not

$$CN/\ln^3 N,$$

but one. This follows since one of p, $p + 2$, $p + 4$ is divisible by 3: so p must be equal to 3.

I once had a proof that needed only a lemma about the structure of the primes to be complete. It was about a communication complexity lower bound that I was working on at the time with Bob Sedgewick. We could not prove the lemma, nor could we find any references to anything like it. So we made an appointment to see the famous number theorist, Enrico Bombieri. He is a member of the Institute for Advanced Study, and was there at the time. So Bob and I went over to ask him about our lemma.

Bombieri listened very politely, asked a question or two for clarification, and said, “Yes, that lemma is surely correct.” We were thrilled, since this would make our proof complete. I then asked him for a reference. He looked at me and said:

> Of course the lemma about primes is true, but it is completely hopeless to prove it.

He had great intuition about primes, but proving certain results was then and still is today completely beyond anything anyone can do.

11.2 Geometry

My intuition in geometry, especially in high dimensions, is very poor. I have proved basic geometry theorems that hold in n dimensions, but I have terrible geometric intuition.

I am not sure why. I am not sure what makes geometry so hard for me, but it is very different from the study of prime numbers. There are plenty of geometric questions that I would not have any idea how to conjecture what is true. Perhaps it is just a defect in my abilities, but geometry seems to be orders of magnitude trickier than number theory.

John Moller of the University of Utah writes a blog titled "On Topology," and gave some helpful insights into high-dimensional geometry in a March 3, 2009 post titled "Reasoning in Higher Dimensions: Hyperspheres" (referenced in the end notes).

11.3 Groups

My intuition about finite groups is even worse than my geometric intuition. No, that is not quite right. In a sense my intuition about groups is really very good. Over the years I have hit upon a rule in thinking about groups. I figured out that if I thought that X was a reasonable theorem that should hold for finite groups, then X was likely to be false.

Of course, this is a bit silly. It is like having a really poor sense of picking stocks—if you were always wrong, then there would be a great strategy. But, somehow I do believe there is something to what I am saying. My intuition is so bad that after a while I just started to guess the opposite of whatever I first thought.

Chapter 10 is a perfect example. At the time, I had a series of conjectures about solvable groups. The conjecture I listed took an expert, Colin Reid, a few minutes to disprove. He is a group theorist. I should have known better, as my intuition about groups is terrible, even though groups may play an important role in our understanding of computer science theory.

11.4 Reid's Proof

Colin Reid posted his proof that a problem I had called $\mathcal{SOLVE}$ is impossible in the comments section of the post on which Chap. 10 is based. The parts of his comments using angle brackets were snipped as HTML-style tags, so the following is an expanded version fixing the glitches. Ken and I have also replaced his quotient-subgroup notation by homomorphism notation.

Let G be a non-trivial solvable group—some say soluble group. The *composition series* is defined by $G_0 = G$, and for $i \geq 1$, $G_i = [G_{i-1}, G_{i-1}] =$ the subgroup generated by the *commutators* $[u, v] = uvu^{-1}v^{-1}$ for $u, v \in G_i$. Solvability of G means that some G_i is the trivial subgroup $\{1\}$, whereupon the series terminates. The important facts are that not only is every G_i normal in its predecessor, it is normal in the entire group G, and that the immediate quotients G_{i-1}/G_i are Abelian. This means that we can define a homomorphism π on all of G whose kernel is G_i, and for all $c, d \in G_{i-1}$, $\pi(c)$ and $\pi(d)$ commute. The reason for the latter is that

$$dc = cdk \quad \text{where } k \text{ is the commutator } \left[d^{-1}, c^{-1}\right],$$

so $\pi(d)\pi(c) = \pi(dc) = \pi(cdk) = \pi(c)\pi(d)\pi(k) = \pi(c)\pi(d)$, since k is in the kernel G_i.

Now recall that $\mathcal{SOLVE}$ asserted the existence in G of elements a, b, c, d such that some conjugates xax^{-1} of a and yby^{-1} of b are in $\langle c, d\rangle$, where $x, y \in G$, and likewise some conjugates of c and d are in $\langle a, b\rangle$, with a third condition on the orders of these elements in G. The condition is that $o(a)o(b)$ be relatively prime to $o(c)o(d)$, and this is what finally prevents the existence of a, b, c, d.

For contradiction, suppose a solvable group G with such elements exists. Then in the composition series, there is some i such that G_{i-1} contains all of a, b, c, d, but G_i does not. By symmetry, without loss of generality, we can suppose G_i does not have a. Take $a' = xax^{-1}$ as above, so $a' \in \langle c, d\rangle$. It does not matter whether c or d belongs to G_i; that both belong to G_{i-1} is enough. Since a' is a conjugate, $o(a') = o(a)$. Now take the homomorphism π with G_i as kernel, and observe:

(1) $\pi(a') \in \langle\pi(c), \pi(d)\rangle$.

(2) $o(\pi(c))$ divides $o(c)$, $o(\pi(d))$ divides $o(d)$, and $o(\pi(a'))$ divides $o(a') = o(a)$.

(3) Since c and d are in G_{i-1}, $\pi(c)$ and $\pi(d)$ commute.

(4) Hence $\pi(c)$ and $\pi(d)$ can generate at most $m = o(\pi(c))o(\pi(d))$ different elements.

(5) Put more strongly, the subgroup $\langle\pi(c), \pi(d)\rangle$ they generate is also a subgroup of the Abelian group generated by $\pi(c)$ and $\pi(d)$, which has exactly m elements. Hence by Lagrange's theorem the order of $\langle\pi(c), \pi(d)\rangle$ divides m.

(6) Since $\pi(a')$ is in $\langle\pi(c), \pi(d)\rangle$, it follows that $o(\pi(a'))$ divides m, which divides $o(c)o(d)$.

(7) However, since $o(\pi(a'))$ divides $o(a)$ which is relatively prime to $o(c)o(d)$, the only way this can happen is $o(\pi(a')) = 1$.

(8) That means $\pi(a') = 1$, so $a' \in G_i$ since G_i is the kernel of π.

(9) But G_i is normal in G, not just in G_{i-1}, so $xa'x^{-1}$ is in G_i. This puts a into G_i, which yields a contradiction.

To someone with good algebraic intuition this comes trippingly off the tongue, which is why it is a service to communicate in public. So we thank Colin Reid—and we will see if the insight gained works against our more-complicated stratagems of this kind. At the time he was a graduate student at Queen Mary College, University of London.

It may be that deterministically simulating each level of a Boolean circuit simply must bump you one step along a composition series, which in a solvable group G is a finite, non-renewable resource.

However, we also have other ideas. Perhaps we can get mileage out of choosing different solvable groups G for different input sizes n. This relates complexity questions to ones about the possible lengths of composition series in groups of certain sizes—although what we know about such sizes is not so promising. But perhaps a randomized simulation can possibly avoid these limitations.

11.5 Complexity Theory

I think we have good intuition here, but I have seen many surprises in my career:

- Linear programming is in polynomial time.
- Nondeterministic space is closed under complement.
- Polynomial-size bounded-width branching programs are powerful.
- Permanent has random self-reduction.
- Quantum polynomial time can factor integers.
- Random walks for undirected graphs can be de-randomized.
- Proofs can be checked in constant time.
- Zero-knowledge protocols exist for natural problems.
- . . .

I have reasonable intuition, yet all of these were surprising to me—even some that I worked on and contributed to their development.

11.6 Open Problems

Is intuition simply built up by learning more and more about an area? Or is intuition something that is separate from just being an expert in an area? Can you be quite strong in an area and still have weak intuition, or is that impossible?

11.7 Notes and Links

Original post:
http://rjlipton.wordpress.com/2010/10/01/mathematical-intuition-what-is-it/
Twin primes:
http://en.wikipedia.org/wiki/Twin_prime
Blog item on higher-dimensional geometry:
http://ontopo.wordpress.com/2009/03/03/reasoning-in-higher-dimensions-hyperspheres/
Colin Reid's homepage:
http://qmul.academia.edu/ColinReid