Parabola Volume 57, Issue 1 (2021)

The Overselling of Mathematics

Alon Amit[1]

Based on your personal understanding, off the top of your head: what would a proof of the Riemann Hypothesis do to internet security? Don't look it up. Just consider how you would generally answer this based on what you may have read or heard. Is it "nothing"? "Something"? "We're toast"?

All right, now do look it up. No, really, go on, Google "Riemann hypothesis security". I just did, and up came a bunch of relevant articles, including one dubbed *The Unexpected Connection Between Internet Security and the Riemann Hypothesis*. Therein, we find:

> *However, this application [to quantum physics – AA] pales in comparison to the effect that the Riemann hypothesis could have on a field of global importance: Internet security and encryption. [...] it is possible that a proof for the Riemann hypothesis could lead to quicker and easier methods of finding large primes. This could in turn lead to the breakdown of modern encryption methods because choosing numbers to use as potential factors of the encryption key would be more efficient. Basically, if we already know where the primes are, we only have to pick those as factors instead of picking every number.*

This is from the website of the University of Alabama in Birmingham, a perfectly respectable academic institute. Specifically, it's from UAB's Undergraduate Research Journal. But I don't wish to pick on them in particular, because this sentiment is ubiquitous. It is also, as you might have guessed by now, sheer nonsense.

Nobody knows what a proof of the Riemann Hypothesis looks like, so we are free to speculate that such a proof would provide a way of powering nuclear submarines with potatoes. But merely by virtue of it being a proof of the Riemann Hypothesis, there is absolutely no reason to expect that it would do anything to our ability to find large primes. In fact, our ability to find large primes is already in fantastically good shape, which is precisely why encryption methods based on the hardness of integer factorization are possible in the first place. Being able to generate large primes quickly is a necessary step, and it's not in the least helpful for factorization. And no, a proof of the Riemann Hypothesis is not expected to offer any insight into factoring integers, nor any novel algorithm for doing so quickly. (And even if it did, we have a plethora of other encryption algorithms which do not rely on integer factorization).

[1] Alon Amit is a San Francisco Bay Area-based entrepreneur, executive, and enthusiastic math educator and evangelist, and holds a Ph.D. in mathematics from the Hebrew University, Jerusalem, Israel.

Like most pervasive memes, it's impossible to trace where and when, exactly, did the notion emerge that the future of eCommerce and the world's economy hang on the balance of the zeroes of the Riemann zeta function. It may seem like a simple misunderstanding of higher mathematics, but I believe there is an additional contributing factor: the eagerness of many expositors and popularizers of math to mildly overstate, or wildly over-blow, the significance and utility of pure mathematics to "the Real World".

Quanta Magazine recently published a fantastic video, "The Riemann Hypothesis, Explained", narrated by Rutgers University's Alex Kontorovich. There is much to admire about the content and quality of that video, but a couple of times it falls into slight hyperbole. At 0:50, we learn that

> "If the hypothesis is true, it would solve a mystery as old as math itself. That is, the mystery of the prime numbers. Countless theorems in fields as far apart as Cryptography and Quantum Physics assume that the Riemann Hypothesis is true, which means that we have a lot riding on this single unproven statement."

Would a solution to the Riemann Hypothesis "solve the mystery of the prime numbers"? It's hard to justify this oft-repeated claim. There are many unsolved problems about primes, ancient and new, elementary and advanced, and the vast majority of them would not be affected by a proof or refutation of the Riemann Hypothesis. Once it is solved, in all likelihood we still won't know if the Twin Prime Conjecture is true, or if there are infinitely many Fermat or Mersenne primes. Even something like whether there's a prime between n^2 and $(n+1)^2$ for every n, which is closely related to the density of primes, is not known to depend on the Riemann Hypothesis: it is far too weak to prove something so delicate. There really isn't "*the*" mystery of the prime numbers, and if there is, RH doesn't solve it.

The Riemann Hypothesis is beautiful, profound and deep as it stands, without unnecessary marketing hype. There do exist many theorems which are only currently known to be true assuming its truth (and more often, that of its generalized and extended versions), but its connections to cryptography and quantum physics are somewhere between tenuous and non-existent. Many mathematicians would be thrilled beyond words to see the RH resolved, but neither cryptographers nor physicists are holding their breath.

The overselling isn't limited to the Riemann Hypothesis, of course. Among the worst offenders is the tiresome Golden Ratio, which was sold to the general public with such zealous vigor that it is now believed by some to virtually run the world. "Nature uses this ratio to maintain balance" informs us Investopedia, mentioning atoms and galaxies before admonishing would-be investors that they need to concern themselves

with "Fibonacci arcs" and "Fibonacci fans" as they attempt to monetarily gain from the movement of stocks. If you're not a day-trader, it may be your dentist who chooses to apply the positive real root of $x^2 - x = 1$ to the proportions of your face. There's nothing wrong with 8:5 in various bodily or artistic ratios, of course, but it would work just as nicely without the bogus belief that the golden ratio was used by Greek architects (it wasn't), by da Vinci (nope), or by Mother Nature itself, like, *everywhere*. There are a few pleasant occurrences of the ratio in nature, arising from simple mechanisms of growth (Conway and Guy address this nicely in *The Book of Numbers*). Those are as rare as they are minor.

Algebraic Geometry is a tough sell for the general public. People who have studied it, or even just got a glimpse of it in grad school, are aware of its beauty and depth, but it's hard to convey that to laypeople. In a 2014 obituary of Alexander Grothendieck, the New York Times was moved to say:

> *Algebraic geometry is a field of pure mathematics that studies the relationships between equations and geometric spaces. Mr. Grothendieck was able to answer concrete questions about these relationships by finding universal mathematical principles that could shed unexpected light on them. Applications of his work are evident in fields as diverse as genetics, cryptography and robotics.*

This, honestly, is just plain false. Nothing in Grothendieck's work informed the fields of genetics, cryptography or robotics. Some on the MathOverflow community attempted to identify the source of those exaggerations, and the results are the expected speculative, though sometimes interesting, experiments with identifying algebraic varieties in certain contexts. None of them have anything to do with Grothendieck's transformation of the field.

It is not hard to understand why this happens. Mathematicians wish to share their genuine love of the field with the world, and that's hard. Whenever possible, we have a desire to connect the abstract mathematical world with more mundane, seemingly more "impactful" concepts.

When researchers in mathematics write grant requests, they are compelled to justify their work to taxpayers and speculate on possible future applications of their research. In the traditional dance of researchers and grant givers, this is well understood: the mathematicians know they are allowed some wishful leeway, and the reviewers generally expect and accept that. Besides, math research is dirt cheap.

But when we talk to the general public, I feel that this overselling is damaging. It misrepresents many of the reasons behind the mathematical endeavor: curiosity, a search of beauty, and a sense of awe which are wholly decoupled from applications. At the same time, much of the evolution of mathematics *did* stem from questions of science and engineering, or found such applications long after the original theories were built,

and that's wonderful. Let us honestly represent those profound connections when they do exist, rather than invent them when they don't.

The Riemann Hypothesis is one of the best questions humanity has ever asked, and studying it is a worthy, noble pursuit, but it doesn't have anything to do with cryptography. The theory of continued fractions and quadratic irrationalities, of which the golden ratio is one, are genuinely connected to hyperbolic geometry and arithmetic in deep and beautiful ways; there's no reason to overhype it with ill-informed connections to finance or physics.

And I'm quite sure Grothendieck, who left the IHÉS once he learned that it is partially funded by the military, would not be excited to see his work tied to robotics, especially when it truly isn't. Please, let's keep it straight.

Stop overselling mathematics.