

THE NEW YORKER

- « Crowdsourcing the Stars
- Main
- Faraway: The Making of a Universe »

May 2, 2013

A Most Profound Math Problem

Posted by *Alexander Nazaryan*

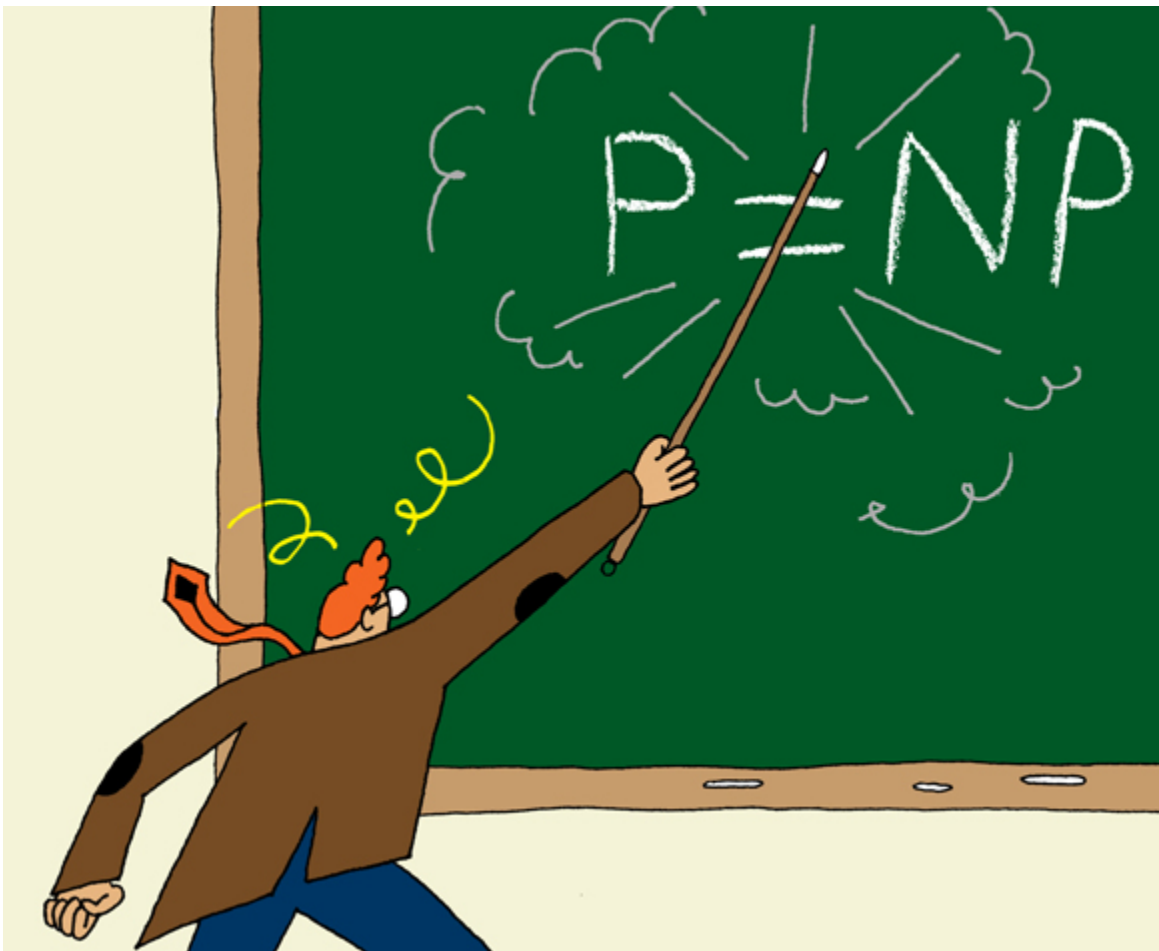
- Print
- More

Share

Close

-
- [Reddit](#)
- [Linked In](#)
- [Email](#)

•





On August 6, 2010, a computer scientist named Vinay Deolalikar published a paper with a name as concise as it was audacious: “ $P \neq NP$.” If Deolalikar was right, he had cut one of mathematics’ most tightly tied Gordian knots. In 2000, the $P = NP$ problem was designated by the Clay Mathematics Institute as one of seven Millennium Problems—“important classic questions that have resisted solution for many years”—only one of which has been solved since. (The Poincaré Conjecture was vanquished in 2003 by the reclusive Russian mathematician Grigory Perelman, who refused the attached million-dollar prize.)

A few of the Clay problems are long-standing head-scratchers. The Riemann hypothesis, for example, made its debut in 1859. By contrast, P versus NP is relatively young, having been introduced by the University of Toronto mathematical theorist Stephen Cook in 1971, in a paper titled “The complexity of theorem-proving procedures,” though it had been touched upon two decades earlier in a letter by Kurt Gödel, whom David Foster Wallace branded “modern math’s absolute Prince of Darkness.” The question inherent in those three letters is a devilish one: Does P (problems that we can easily solve) equal NP (problems that we can easily check)?

Take your e-mail password as an analogy. Its veracity is checked within a nanosecond of your hitting the return key. But for someone to *solve* your password would probably be a fruitless pursuit, involving a near-infinite number of letter-number permutations—a trial and error lasting centuries upon centuries. Deolalikar was saying, in essence, that there will always be some problems for which we can recognize an answer without being able to quickly find one—intractable problems that lie beyond the grasp of even our most powerful microprocessors, that consign us to a world that will never be quite as easy as some futurists would have us believe. There always will be problems unsolved, answers unknown.

If Deolalikar’s audacious proof were to hold, he could not only quit his day job as a researcher for Hewlett-Packard but rightly expect to enter the pantheon as one of the day’s great mathematicians. But such glory was not forthcoming. Computer scientists and mathematicians went at Deolalikar’s proof—which runs to dozens of pages of fixed-point logistics and k -SAT structures and other such goodies—with the ferocity of sharks in the presence of blood. The M.I.T. computational theorist Scott Aaronson (with whom I consulted on this essay’s factual assertions) wrote on his blog, “If Vinay Deolalikar is awarded the \$1,000,000 Clay Millennium Prize for his proof of $P \neq NP$, then I, Scott Aaronson, will personally supplement his prize by the amount of \$200,000.” It wasn’t long before Deolalikar’s paper was thoroughly discredited, with Dr. Moshe Vardi, a computer-science professor at Rice University, telling the *Times*, “I think Deolalikar got his 15 minutes of fame.”

As Lance Fortnow describes in his new book, “The Golden Ticket: P , NP and the Search for the Impossible,” P versus NP is “one of the great open problems in all of mathematics” not only because it is extremely difficult to solve but because it has such obvious practical applications. It is the dream of total ease, of the confidence that there is an efficient way to calculate nearly everything, “from cures to deadly diseases to the nature of the universe,” even “an algorithmic process to recognize greatness.” So while a solution for the Birch and Swinnerton-Dyer conjecture, another of the Clay Millennium Prize problems, would be an impressive feat, it would have less practical application than definitive proof that anything we are able to quickly check (NP), we can also quickly solve (P).

Fortnow’s book—which, yes, takes its name from “Willy Wonka & the Chocolate Factory”—bills itself as a primer for the general reader, though you will likely regret not having paid slightly more attention during calculus class. Reading “The Golden Ticket” is sort of like watching a movie in a foreign language without captions. You will miss some things, but not everything. There is some math humor, which is at once amusing, cheesy, and endearing exactly in the way that you think a mathematician’s humor might be amusing, cheesy, and endearing.

What Fortnow calls “ P ” stands for polynomial time, meaning the size of the input raised to a fixed number like two or three. Conversely, exponential time is some number raised to the size of the input. Though polynomial time can be long (say, 50^2), it is nothing compared to its exponential opposite (2^{50}). If the first is the Adirondacks, the second is the Himalayas. When

solving things, we want to keep them in polynomial time if we still want to have time for lunch.

“NP” (nondeterministic polynomial time) is a set of problems we want to solve, of varying degrees of difficulty. Many everyday activities rely on NP problems: modern computer encryption, for example, which involves the prime factors of extremely large numbers. Some forty years ago, Richard Karp, the Berkeley theoretician, first identified twenty-one problems as being “NP-complete,” meaning that they are at least as hard as any other NP problem. The NP-complete problems are a sort of inner sanctum of computational difficulty; solve one and you’ve solved them all, not to mention all the lesser NP problems lurking in the rear. Karp’s foreboding bunch of problems have names like “directed Hamiltonian cycle” and “vertex cover.” Though they are extremely hard to solve, solutions are easy to check. A human may be able to solve a variation of one of these problems through what Soviet mathematicians called “*perebor*,” which Fortnow translates as “brute-force search.” The question of P versus NP is whether a much faster way exists.

So far, the answer is no. Take one of these NP-complete problems, called “*k*-clique,” which Fortnow explains as follows: “What is the largest clique on Facebook [such that] all of [them] are friends with each other?” Obviously, the more users there are on Facebook, the more difficult it is to find the biggest self-enclosed clique. And thus far, no algorithm to efficiently solve the clique problem has been discovered. Or, for that matter, to solve any of its NP-complete siblings, which is why most people do think that $P \neq NP$.

There are considerations here, too, beyond math. Aaronson, the M.I.T. scientist, wrote a blog post about why he thinks $P \neq NP$, providing ten reasons for why this is so. The ninth of these he called “the philosophical argument.” It runs, in part, as follows: “If $P = NP$, then the world would be a profoundly different place than we usually assume it to be. There would be no special value in ‘creative leaps,’ no fundamental gap between solving a problem and recognizing the solution once it’s found. Everyone who could appreciate a symphony would be Mozart; everyone who could follow a step-by-step argument would be Gauss; everyone who could recognize a good investment strategy would be Warren Buffett.”

We already check novels for literary qualities; most critics could easily enough put together a list of categories that make a novel great. Imagine, now, if you could write an algorithm to efficiently create verifiably great fiction. It isn’t quite as outlandish as you think: back in 2008, the Russian writer Alexander Prokopovich “wrote” the novel “True Love” by taking seventeen classics that were recombined via computer in seventy-two hours into an entirely new work. As Prokopovich told the St. Petersburg *Times*, “Today publishing houses use different methods of the fastest possible book creation in this or that style meant for this or that readers’ audience. Our program can help with that work.” He then added a note of caution: “However, the program can never become an author, like Photoshop can never be Raphael.” But if $P = NP$, then it could only be a matter of time before someone figured out how to create verifiably “great” novels and paintings with mathematical efficiency.

Much of Fortnow’s book is spent depicting a world in which P is proven to equal NP, a world of easily computed bliss. He imagines, for example, an oncologist no longer having to struggle with the trial and error of chemotherapy because “we can now examine a person’s DNA as well as the mutated DNA of the cancer cells and develop proteins that will fold in just the right way to effectively starve the cancer cells without causing any problems for the normal cells.” He also whips up a political scandal in which a campaign manager “hired a computer programmer, who downloaded tens of thousands of well-received speeches throughout the decades. The programmer then used [an] algorithm to develop a new speech based on current events”—one that the unwitting public predictably loves.

To postulate that $P \neq NP$, as Fortnow does, is to allow for a world of mystery, difficulty, and frustration—but also of discovery and inquiry, of pleasures pleasingly delayed. Fortnow concedes the possibility that “it will forever remain one of the true great mysteries of mathematics and science.” Yet Vinay Deolalikar is unlikely the last to attempt a proof, for all of mathematics rests on a fundamental hubris, a belief that we can order what Wallace Stevens calls “a slovenly wilderness.” It is a necessary confidence, yet we are not always rewarded for it.

Alexander Nazaryan is on the editorial board of the New York Daily News, where he edits the Page Views book blog.

Illustration by Jordan Awan.

Correction: It is the Riemann Hypothesis, not the Reimann Hypothesis.

Keywords

- elements;
- math;
- techpages
- Print
- More

Share

Close

-
- Reddit
- Linked In
- Email



Elements

- All posts
- RSS

2 hours ago

The Scuffle and the Vine

17 hours ago

Faraway: The Making of a Universe

18 hours ago

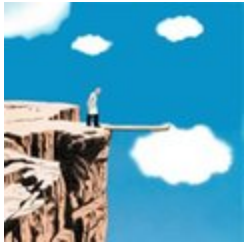
A Most Profound Math Problem

- @Elements
- Follow
- Our Newsletters

You might like

Most shared

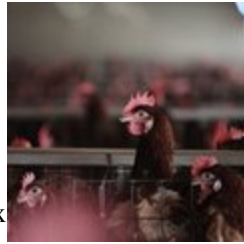




Can Science Lead to Faith?
BY GARY MARCUS



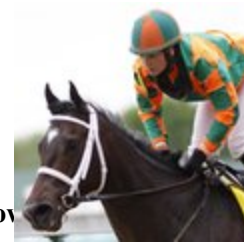
How to Provoke National Unrest with a Facebook Photo
BY EMILY GREENHOUSE



How Much Should We Fear H7N9?
BY PATRICK DI JUSTO



The Crisis in Social Psychology That Isn't
BY GARY MARCUS



A Storied Kentucky Derby
BY CAITLIN KELLY

