August 16, 2010

Step 1: Post Elusive Proof. Step 2: Watch Fireworks.

By JOHN MARKOFF

The potential of Internet-based collaboration was vividly demonstrated this month when complexity theorists used blogs and wikis to pounce on a claimed proof for one of the most profound and difficult problems facing mathematicians and computer scientists.

Vinay Deolalikar, a mathematician and electrical engineer at Hewlett-Packard, posted a proposed proof of what is known as the "P versus NP" problem on a Web site, and quietly notified a number of the key researchers in a field of study that focuses on problems that are solvable only with the application of immense amounts of computing power.

The researcher asserted that he had demonstrated that P (the set of problems that can be easily solved) does not equal NP (those problems for which solutions can be verified relatively quickly). As with earlier grand math challenges — for example, Fermat's last theorem — there is a lot at stake, not the least of which is a $1 million prize.

In 2000 the Clay Mathematics Institute picked seven of the greatest unsolved problems in the field, named them "Millennium Problems" and offered $1 million for the solution of each of them. P versus NP is one of those problems. (In March, the first prize was awarded to a reclusive Russian mathematician, Grigory Perelman, for the solution to the century-old Poincaré conjecture. A few months later he refused the prize.)

P versus NP has enormous practical and economic importance, because modern cryptography is based on the assumption, which is workable so far, that P does not equal NP. In other words, there are problems that are impossible for computers to solve, but for which the solutions are easily recognizable. If these problems were shown to be solvable, that could undermine modern cryptography, which could paralyze electronic commerce and digital privacy because transactions would no longer be secure.

In a note sent to a small group of researchers on Aug. 6, Dr. Deolalikar wrote: “The proof required the piecing together of principles from multiple areas within mathematics. The major effort in constructing this proof was uncovering a chain of conceptual links between various fields and viewing them through a common lens.”

An outsider to the insular field, Dr. Deolalikar set off shock waves because his work appeared to be a concerted and substantial challenge to a problem that has attracted intense scrutiny since it was first posed in 1971 by Stephen Cook, a mathematician and computer scientist who teaches at the University of Toronto.

“The reason there was such excitement is there have been many alleged proofs,” said Moshe Vardi, a professor of computer science at Rice University and the editor in chief of The Communications of the Association for Computing Machinery. “This looks like a serious paper. In particular what he has done is bring forward a new idea that is worth exploring.”

In this case, however, the significant breakthrough may not be in the science, but rather in the way science is practiced. By the middle of last week, although Dr. Deolalikar had not backed away from his claim, a consensus had emerged among complexity theorists that the proposed proof had several significant shortcomings.

“At this point the consensus is that there are large holes in the alleged proof — in fact, large enough that people do not consider the alleged proof to be a proof,” Dr. Vardi said. “I think Deolalikar got his 15 minutes of fame, but at this point the excitement has subsided and

the skepticism is turning into negative conviction."

What was highly significant, however, was the pace of discussion and analysis, carried out in real time on blogs and a wiki that had been quickly set up for the purpose of collectively analyzing the paper. This kind of collaboration has emerged only in recent years in the math and computer science communities. In the past, intense discussions like the one that surrounded the proof of the Poincaré conjecture were carried about via private e-mail and distribution lists as well as in the pages of traditional paper-based science journals.

Several of the researchers said that until now such proofs had been hashed out in colloquiums that required participants to be physically present at an appointed time. Now, with the emergence of Web-connected software programs it is possible for such collaborative undertakings to harness the brainpower of the world's best thinkers on a continuous basis.

In his recently published book "Cognitive Surplus: Creativity and Generosity in a Connected Age" (Penguin Press), Clay Shirky, a professor of interactive telecommunications at New York University, argues that the emergence of these new collaborative tools is paving the way for a second scientific revolution in the same way the printing press created a demarcation between the age of alchemy and the age of chemistry.

"The difference between the alchemists and the chemists was that the printing press was used to coordinate peer review," he said. "The printing press didn't cause the scientific revolution, but it wouldn't have been possible without it."

Now, he says, the new tools are likely to set off a similar transformation.

"It's not just, 'Hey, everybody, look at this,' " he said, "but rather a new set of norms is emerging about what it means to do mathematics, assuming coordinated participation."

The computer science community has long been an innovator in the design of science-collaboration tools. Indeed, the ARPAnet, the forerunner of the Internet, was initially created in 1969 to make one of the first computerized collaboration tools, Douglas Engelbart's oNLine System, or NLS, available from remote locations. During the 1980s physicists at the physics research center CERN near Geneva created the World Wide Web to facilitate the sharing of scientific research.

In 2009, a Cambridge mathematician, Timothy Gowers, created the Polymath Project, a blog and wiki-oriented collaboration tool that used the comments section of a blog to pursue mathematics collaboratively. Related efforts like the Web site Mathoverflow help attack unsolved mathematical problems by using new Internet tools to help stimulate collaboration.

In the case of the P versus NP paper, most of the action has taken place in several blogs maintained by researchers in the field, like a computer scientist, Richard Lipton, at Georgia Tech and a theoretical physicist, Dave Bacon, at the University of Washington, as well as in a wiki by a quantum theoretician, Michael Nielsen.

Passions have run high. A computer scientist at the Massachusetts Institute of Technology, Scott Aaronson, literally bet his house last week — $200,000 — that the Deolalikar paper would be proved incorrect: "If Vinay Deolalikar is awarded the $1,000,000 Clay Millennium Prize for his proof of P-NP, then I, Scott Aaronson, will personally supplement his prize by the amount of $200,000."

Despite his skepticism, he acknowledged that this was, to date, one of the most impressive attempts to settle the question.

"So far this is not your typical P versus NP crank solution, which I hear about once a week," he said.

This article has been revised to reflect the following correction:

Correction: August 21, 2010

An article on Tuesday about a proposed solution of a classic mathematical formula called P versus NP described NP incorrectly and misidentified the location of the CERN physics research center. NP stands for the class of problems for which solutions can be verified relatively quickly, not the class of problems that are difficult to solve but easy to verify. And the CERN laboratory is near Geneva, not in Zurich.