August 8, 2002

New Method Said to Solve Key Problem in Math

By SARA ROBINSON

Three Indian computer scientists have solved a longstanding mathematics problem by devising a way for a computer to tell quickly and definitively whether a number is prime — that is, whether it is evenly divisible only by itself and 1.

Prime numbers play a crucial role in cryptography, so devising fast ways to identify them is important. Current computer recipes, or algorithms, are fast, but have a small chance of giving either a wrong answer or no answer at all.

The new algorithm — by Manindra Agrawal, Neeraj Kayal and Nitin Saxena of the Indian Institute of Technology in Kanpur — guarantees a correct and timely answer. Though their paper has not been published yet, they have distributed it to leading mathematicians, who expressed excitement at the finding.

"This was one of the big unsolved problems in theoretical computer science and computational number theory," said Shafi Goldwasser, a professor of computer science at the Massachusetts Institute of Technology and the Weizmann Institute of Science in Israel. "It's the best result I've heard in over 10 years."

The new algorithm has no immediate applications, since existing ones are faster and their error probability can be made so small that it is practically zero. Still, for mathematicians and computer scientists, the new algorithm represents a great achievement because, they said, it simply and elegantly solves a problem that has challenged many of the best minds in the field for decades.

Asked why he had the courage to work on a problem that had stymied so many, Dr. Agrawal replied in an e-mail message: "Ours was a completely new and unexplored approach. Consequently, it gave us hope that we might succeed."

The paper is now posted on the computer science department Web page at the Indian Institute of Technology (www.cse.iitk.ac.in).

Methods of determining whether a number is prime have captivated mathematicians since ancient

times because understanding prime numbers is the key to solving many important mathematical problems. More recently, attention has focused on tests that run efficiently on a computer, because such tests are part of the underlying mathematics of several widely used systems for encrypting data on computers.

So-called primality testing plays a crucial role in the widely used RSA algorithm, whose security relies on the difficulty of finding a number's prime factors. RSA is used to secure transactions over the Internet.

On Sunday, the researchers e-mailed a draft of the paper on the result to dozens of expert mathematicians and computer scientists. Dr. Carl Pomerance, a mathematician at Bell Labs, said he received the paper on Monday morning and determined it was correct.

After discussing the draft with colleagues over lunch, Dr. Pomerance arranged an impromptu seminar on the result that afternoon.

That he could prepare and give a seminar on the paper so quickly was "a measure of how wonderfully elegant this algorithm is," Dr. Pomerance said. "This algorithm is beautiful."
