PRIMES Is in P: A Breakthrough for "Everyman"

Folkmar Bornemann

"New Method Said to Solve Key Problem in Math" was the headline of a story in the *New York Times* on August 8, 2002, meaning the proof of the statement PRIMES $\in \mathcal{P}$, hitherto a big open problem in algorithmic number theory and theoretical computer science. Manindra Agrawal, Neeraj Kayal, and Nitin Saxena of the Indian Institute of Technology accomplished the proof through a surprisingly elegant and brilliantly simple algorithm. Convinced of its validity after only a few days, the experts raved about it: "This algorithm is beautiful" (Carl Pomerance); "It's the best result I've heard in over ten years" (Shafi Goldwasser).

Four days before the headline in the *New York Times*, on a Sunday, the three authors had sent a nine-page preprint titled "PRIMES is in P" to fifteen experts. The same evening Jaikumar Radhakrishnan and Vikraman Arvind sent congratulations. Early on Monday one of the deans of the subject, Carl Pomerance, verified the result, and in his enthusiasm he organized an impromptu seminar for that afternoon and informed Sara Robinson of the *New York Times*. On Tuesday the preprint became freely available on the Internet. On Thursday a further authority, Hendrik Lenstra Jr., put an end to some brief carping in the NMBRTHRY email list with the pronouncement:

> The remarks … are unfounded and/or inconsequential. … The proofs in the paper do NOT have too many additional problems to mention. The only true mistake is …, but that is quite easy to fix. Other mistakes … are too minor to mention. The paper is in substance completely correct.

And already on Friday, Dan Bernstein posted on the Web an improved proof of the main result, shortened to one page.

This unusually brief—for mathematics—period of checking reflects both the brevity and elegance of the argument and its technical simplicity, "suited for undergraduates". Two of the authors, Kayal and Saxena, had themselves just earned their bachelor's degrees in computer science in the spring. Is it then an exception for a breakthrough to be accessible to "Everyman"?

In his speech at the 1998 Berlin International Congress of Mathematicians, Hans-Magnus Enzensberger took the position that mathematics is both "a cultural anathema" and at the same time in the midst of a golden age due to successes of a quality that he saw neither in theater nor in sports. To be sure, some of those successes have many mathematicians themselves pondering the gulf between the priesthood and the laity *within* mathematics. A nonspecialist—cross your heart: how many of us are not such "Everymen"?—can neither truly comprehend nor fully appreciate the proof of Fermat's Last Theorem by Andrew Wiles, although popularization efforts like the book of Simon Singh help one get an inkling of the connections. Probably no author could be found to help "Everyman"

Folkmar Bornemann is a professor at the Zentrum Mathematik, Technische Universität München and editor of the Mitteilungen der Deutschen Mathematiker-Vereinigung. *His email address is* bornemann@ma.tum.de.

This article is a translation by the editor of the Notices *of an article by the author that appeared in German in the* Mitteilungen der Deutschen Mathematiker-Vereinigung *4-2002, 14–21.*

comprehend all the ramifications and the significance of the successes of last year's recipients of the Fields Medals.

So it is that each one adds bricks to his parapet in the Tower of Babel named Mathematics and deems his constructions there to be fundamental. Rarely is there such a success as at the beginning of August: a foundation stone for the tower that "Everyman" can understand.

Paul Leyland expressed a view that has been in many minds: "Everyone is now wondering what else has been similarly overlooked." Can this explain Agrawal's great astonishment ("I never imagined that our result will be of much interest to traditional mathematicians"): namely, why within the first ten days the dedicated website had over two million hits and three hundred thousand downloads of the preprint?

> When a long outstanding problem is finally solved, every mathematician would like to share in the pleasure of discovery by following for himself what has been done. But too often he is stymied by the abstruseness of so much of contemporary mathematics. The recent negative solution to . . . is a happy counterexample. In this article, a complete account of this solution is given; the only knowledge a reader needs to follow the argument is a little number theory: specifically basic information about divisibility of positive integers and linear congruences.
>
> Martin Davis, Hilbert's tenth problem is unsolvable, *American Mathematical Monthly* **80** (1973), 233–69, first paragraph of the introduction.

As a specialist in numerical analysis and not in algorithmic number theory, I wanted to test my mettle as "Everyman", outside of my parapet.

The Problem

Happily the three motivated their work not by the significance of prime numbers for cryptography and e-commerce, but instead at the outset followed the historically aware Don Knuth in reproducing a quotation from the great Carl Friedrich Gauss from article 329 of the *Disquisitiones Arithmeticae* (1801), given here in the 1966 translation by Arthur A. Clarke:

> The problem of distinguishing prime numbers from composite numbers and of resolving the latter into their prime factors is known to be one of the most important and useful in arithmetic. It has engaged the industry and wisdom of ancient and modern geometers to such an extent that it would be superfluous to discuss the problem at length. … Further, the dignity of the science itself seems to require that every possible means be explored for the solution of a problem so elegant and so celebrated.

In school one becomes familiar with the sieve of Eratosthenes; unfortunately using it to prove that n is prime requires computation time essentially proportional to n itself. The input length[1] of a number, on the other hand, is proportional to the number of binary digits, thus about $\log_2 n$, so we have before us an algorithm with *exponential* running time $O(2^{\log_2 n})$. To quote Gauss again from article 329 of his *Disquisitiones*:

> Nevertheless we must confess that all methods that have been proposed thus far are either restricted to very special cases or are so laborious and prolix that … these methods do not apply at all to larger numbers.

Can the primality of very large numbers be decided efficiently *in principle*? This question is rendered mathematical in the framework of modern complexity theory by demanding a *polynomial* running time. Is there a deterministic[2] algorithm that, with a fixed exponent κ, decides for every natural number n in $O(\log^\kappa n)$ steps whether this number is prime or not; in short, the hitherto open question: is PRIMES $\in \mathcal{P}$?

The State of Things before August 2002

Ever since the time of Gauss, deciding the primality of a number has been divorced from finding a (partial) factorization in the composite case. In Article 334 of the *Disquisitiones* he wrote:

> The second [observation] is superior in that it permits faster calculation, but … it does not produce the factors of composite numbers. It does however distinguish them from prime numbers.

The starting point for many such methods is Fermat's Little Theorem. It says that for every *prime*

[1] *The difference between the* size *of a number and its* length *is seen most clearly for such unmistakable giants as the number of atoms in the universe (about* 10^{79}*) or the totality of all arithmetical operations ever carried out by man and machine (about* 10^{24}*):* 80 *(respectively* 25*) decimal digits can be written out relatively quickly.*

[2] *That is, an algorithm that does not require random numbers as opposed to a probabilistic algorithm, which does require such numbers.*

number n and every number a coprime to n one has the relation

$$a^n \equiv a \mod n.$$

Unfortunately the converse is false: the prime numbers cannot be characterized this way. On the other hand, "using the Fermat congruence is so simple that it seems a shame to give up on it just because there are a few counterexamples" (Carl Pomerance). It is no wonder, then, that refinements of this criterion are the basis of important algorithms.

An elementary *probabilistic* algorithm of Miller and Rabin from 1976 makes use of a random number generator and shows after k runs either that the number is *certainly* composite or that the number is prime *with high probability*, where the probability of error is less than 4^{-k}. The time complexity is order $O(k \log^2 n)$, where the big-O involves a relatively small constant. In practice the algorithm is very fast, and it finds application in cryptography and e-commerce for the production of "industrial-grade primes" (Henri Cohen). In the language of complexity theory, one says for short PRIMES $\in$ co-$\mathcal{RP}$.

A *deterministic* algorithm of Adleman, Pomerance, and Rumely from 1983, which uses much more theory and a generalization of Fermat's Little Theorem to integers in cyclotomic fields, completely characterizes the prime numbers. The best deterministic algorithm prior to August 2002, it has running time of superpolynomial order $(\log n)^{O(\log\log\log n)}$. The triple logarithm in the exponent grows so slowly, however, that concrete versions of the algorithm have had excellent success in the pursuit of record-breaking primality proofs for numbers with more than a thousand decimal digits.[3]

Another class of modern algorithms uses elliptic curves or abelian varieties of high genus. Thus Adleman and Huang, in a very difficult and technical 1992 monograph, were able to give a *probabilistic* algorithm with polynomial running time that after k iterations either gives a definitive answer (with no possibility of error) or gives no answer, the latter case, however, having probability less than 2^{-k}. In the language of complexity theory, one says for short PRIMES $\in \mathcal{ZPP}$.

With this background, and in view of the level of difficulty that had been reached and the absence of further successes in over ten years, it was hardly to be expected that there could be a short, elegant resolution of the question that would be understandable by "Everyman".

[3] *The hero of another story, Preda Mihăilescu, developed essential refinements of this algorithm in his dissertation at ETH Zurich, and with his implementation he was for a long time a player in the prime-number-records game. Recently he proved the Catalan Conjecture.*

Enter Manindra Agrawal

Manindra Agrawal

The computer scientist and complexity theorist Manindra Agrawal received his doctorate in 1991 from the Department of Computer Science and Engineering of the Indian Institute of Technology in Kanpur (IITK). After a stay as a Humboldt fellow at the University of Ulm in 1995–96 ("I really enjoyed the stay in Ulm. It helped me in my research and career in many ways"), he returned to Kanpur as a professor. Two years ago he gained recognition when he proved a weak form of the isomorphism conjecture in complexity theory.[4]

Around 1999 he worked with his doctoral supervisor, Somenath Biswas, on the question of deciding the identity of polynomials with a probabilistic algorithm. A new probabilistic primality test appears as a simple application in the publication "Primality and identity testing via Chinese remaindering" [1].

The starting point was a generalization of Fermat's Little Theorem to *polynomials*, an easy exercise for an introductory course on number theory or algebra. Namely, if the natural numbers a and n are relatively prime, then n is prime *if and only if*

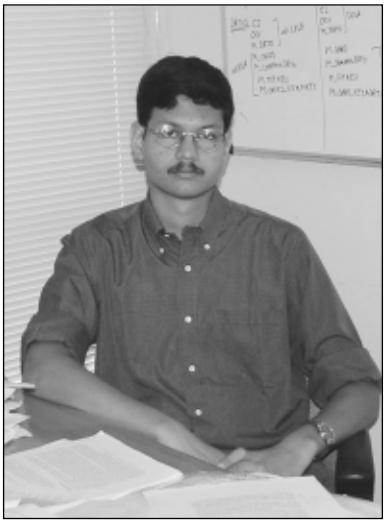
$$(x - a)^n \equiv (x^n - a) \mod n$$

in the ring of polynomials $\mathbb{Z}[x]$. Although this is a very elegant characterization of prime numbers, it is hardly useful. The calculation of $(x - a)^n$ alone requires more computation time than does the sieve of Eratosthenes. But it was precisely for polynomials of this size that Agrawal and Biswas had developed a probabilistic identity test, with bounded error probability, that completely avoided the expansion of the polynomial. Unfortunately the resulting test with polynomial running time was far from competitive with that of Miller and Rabin. A new idea was born, but initially it was interesting only as a footnote in the history of primality testing.

Two years later, with his students at IITK, Agrawal began to examine in detail the potential of the new characterization of prime numbers, in which he had great faith.

[4] *The isomorphism conjecture of Berman and Hartmanis implies that $\mathcal{P} \neq \mathcal{NP}$. A proof would therefore solve the first of the seven Millennium Prize Problems of the Clay Mathematics Institute and bring a return of one million dollars.*

Neeraj Kayal



Nitin Saxena

Two Bachelor's Projects

The admissions procedure for the Indian Institute of Technology (IIT) is rigorous and selective. There is a two-stage common procedure called the Joint Entrance Examination (JEE) for admission to one of the seven branches of the IIT and two other institutions. Last year 150,000 Indians applied for admission, and after an initial three-hour examination in mathematics, physics, and chemistry, 15,000 were invited to a second test consisting of a two-hour examination in each of the three subjects. Finally 2,900 students were awarded places, of which 45 were for computer science at the very renowned IIT in Kanpur. It is no wonder that good money is earned in India for preparing candidates for the dreaded JEE, and graduates of the IIT are eagerly hired worldwide.

It was with such highly motivated students that Agrawal now worked further on the primality test. With Rajat Bhattacharjee and Prashant Pandey, the idea arose of looking not at the excessively large polynomial power $(x-a)^n$ but instead at its remainder after division by x^r-1. If r stays logarithmic in n, then this very much smaller remainder can be directly calculated in polynomial time with suitable algorithms.

If n is prime, then certainly[5]

$$(T_{r,a}) \qquad (x-a)^n \equiv x^n - a \mod (x^r-1, n)$$

for all r and n coprime to a. Which a and r permit the converse conclusion that n is prime?

In their joint bachelor's project [5], the two students fixed $a=1$ and examined the requirements on r. Through analyzing experiments with $r \le 100$ and $n \le 10^{10}$, they arrived at the following conjecture. If r is coprime to n and

$$(T_{r,1}) \qquad (x-1)^n \equiv x^n - 1 \mod (x^r-1, n),$$

then either n is prime or $n^2 \equiv 1 \mod r$. For one of the first $\log_2 n$ prime numbers r, the latter is not the case, so one would have a proof of the primality of n in polynomial running time $O(\log^{3+\varepsilon} n)$.

Here enter the heros of our story, off stage until now, the students Neeraj Kayal and Nitin Saxena. Both were members of the Indian team in the 1997 International Mathematical Olympiad. Studying computer science instead of mathematics because of better employment prospects, they found in complexity theory a way to continue working with mathematics on a high level.

In their joint bachelor's project, they examined the relation of the test $(T_{r,1})$ to known primality tests that, like $(T_{r,1})$, in the negative case give a proof that a number is composite and in the positive case give no definitive answer. There was a rich payoff. They were able to show that under the assumption that the Riemann Hypothesis is true, the test $(T_{r,1})$ could be restricted to $r = 2, \ldots, 4\log_2^2 n$ for a primality proof. In this way one would obtain a deterministic algorithm of time complexity $O(\log^{6+\epsilon} n)$. Furthermore, they were able to show that the conjecture formulated by Bhattacharjee and Pandey would follow from a long-standing conjecture of Carl Pomerance. And in connection with one of their investigations of the class of "introspective numbers", they were led to a proof idea that later would turn out to be essential.

The work of the two, submitted in April 2002, bears the title "Towards a deterministic polynomial-time primality test" [9]. A vision, the goal is already clearly in view.

Changing the Viewpoint

That summer they did not go home first but instead directly began doctoral studies. Saxena actually had wanted to go abroad, but—irony of fates—he did not get a scholarship at his university of choice.

Only a small change of viewpoint is still needed. Both bachelor's projects studied the test $(T_{r,a})$ for fixed $a=1$ and variable r. What happens if one instead fixes r and lets a vary? The breakthrough came on the morning of July 10: through a suitable choice of parameter they obtained nothing less than a characterization of *prime powers*.

The result, as streamlined by Dan Bernstein, is the following.

Theorem. *[Agrawal-Kayal-Saxena] Suppose $n \in \mathbb{N}$ and $s \le n$. Suppose primes q and r are chosen such that $q \mid (r-1)$, $n^{(r-1)/q} \not\equiv 0, 1 \mod r$, and*

$$\binom{q+s-1}{s} \ge n^{2\lfloor\sqrt{r}\rfloor}.$$

If for all $1 \le a < s$ we have that

(i) *a is relatively prime to n, and*
(ii) *$(x-a)^n \equiv x^n - a \mod (x^r-1, n)$ in the ring of polynomials $\mathbb{Z}[x]$,*

then n is a prime power.

[5] *I follow the notation of Agrawal et al. and denote by $p(x) \equiv q(x) \mod (x^r-1, n)$ the equality of the remainders of the polynomials $p(x)$ and $q(x)$ after division by x^r-1 and division of the coefficients by n.*

The simple, short, and innovative proof of the theorem is so delightful that I could not resist sketching it in the appendix.

The theorem now leads directly to the so-called **AKS-algorithm**.[6]

1. Decide if n is a power of a natural number. If so, go to step 5.
2. Choose (q, r, s) satisfying the hypotheses of the theorem.
3. For $a = 1, \ldots, s-1$ do the following:
   (i) If a is a divisor of n, go to step 5.
   (ii) If $(x-a)^n \not\equiv x^n - a \mod (x^r - 1, n)$, go to step 5.
4. n is prime. Done.
5. n is composite. Done.

Step 1 can be accomplished in polynomial time using a variant of Newton iteration. The running time of the main step 3 using rapid FFT-based arithmetic is $\tilde{O}(sr \log^2 n)$, where the tilde over the big-O incorporates further logarithmic factors in s, r, and $\log_2 n$.

Thus to achieve our goal we must allow s and r to grow at most polynomially in $\log n$. This is the job of step 2. We first show what is possible in principle. Set $s = \theta q$ with a fixed factor θ. Stirling's formula gives the asymptotic relation

$$\log \binom{q+s-1}{s} \sim c_\theta^{-1} q.$$

Accordingly, the conditions of the theorem require the asymptotic estimate

$$q \gtrsim 2c_\theta \lfloor \sqrt{r} \rfloor \log n.$$

Essentially this can happen for large n only if there are infinitely many primes r such that $r-1$ has a prime factor $q \geq r^{1/2+\delta}$. Now this is related to a much-studied problem of analytic number theory.

Sophie Germain and Fermat's Last Theorem

The optimal cost-benefit ratio q/r is obtained for the primes named after Sophie Germain: these are the odd primes q for which $r = 2q+1$ is prime too. She had shown in 1823 that for such primes the so-called first case of Fermat's Last Theorem holds: $x^q + y^q = z^q$ has no integer solutions when $q \nmid xyz$. Therefore it became a question of burning interest whether at least there exist infinitely many such friendly primes. Unfortunately one does not know the answer even today. Heuristic considerations, however, led Hardy and Littlewood in 1922 to the following very precise conjecture on the actual density of Germain primes:

$$\#\{q \leq x : \ q \text{ and } 2q+1 \text{ are prime } \} \sim \frac{2C_2 x}{\ln^2 x},$$

where $C_2 = 0.6601618158\ldots$ is the twin-primes constant.

If this conjecture were correct, then one could find prime numbers q and $r = 2q+1$ of size $O(\log^2 n)$ satisfying the hypotheses of the theorem. The AKS-algorithm would then have polynomial running time $\tilde{O}(\log^6 n)$. Since the conjecture impressively has been confirmed up to $x = 10^{10}$, the AKS-algorithm behaves like one of complexity $\tilde{O}(\log^6 n)$ for numbers n up to 100,000 digits.

In 1985, nearly ten years before Andrew Wiles finally proved Fermat's Last Theorem, Adleman, Fouvry, and Heath-Brown proved what one had not been able to accomplish with the aid of the Germain primes: namely, that the first case of Fermat's Last Theorem holds for infinitely many primes [8]. In fact, Adleman and Heath-Brown studied, as a generalization of Germain primes, exactly those pairs (q, r) that also play a key role in the AKS-algorithm.

A Fields Medal

What they required precisely is that the estimate

$$\#\left\{r \leq x : \ q, r \text{ prime}; q \mid (r-1); q \geq x^{1/2+\delta}\right\} \geq c_\delta \frac{x}{\ln x}$$

hold for a suitable exponent $\delta > 1/6$. The hunt for the largest δ began in 1969 with Morris Goldfeld [7], who obtained $\delta \approx 1/12$, and concluded for the time being in 1985 with Étienne Fouvry [6], whose value was $\delta = 0.1687 > 1/6$. All of these works use very deep methods from analytic number theory that expand on the *large sieve* of Enrico Bombieri. He published this sieve in 1965 at the age of twenty-five, and in 1974 he received the Fields Medal. Thus a heavy task falls on "Everyman" who wishes to understand the proof of this estimate in detail. In answer to my question about whether one of the three undertook this task, Manindra Agrawal wrote:

> We tried! But Sieve theory was too dense for us—we have no background in analytical number theory. So after a while we just gave up.

Also they did not need to do it, for "the result was stated there in precisely the form we needed", and they could count on its validity by trusting in the referee and a certain interval of time—the more so since Fouvry's result related to the hot topic of Fermat's Last Theorem appeared in *Inventiones*.

Or maybe not? Fouvry forgot to take into account an additional condition in citing a lemma of Bombieri, Friedlander, and Iwaniec. This additional condition *reduced* the value of δ to $\delta = 0.1683 > 1/6$. It also might have been below the critical threshold. Fouvry later told Roger Baker about this correction, and he and Glyn Harman published it in a survey article [3] in 1996.

[6] *At* `http://www.ma.tum.de/m3/ftp/Bornemann/PARI/aks.txt` *there is an executable implementation for the freely available number-theory software package PARI-GP (*`http://www.parigp-home.de/`*).*

Incidentally, it was in an Internet search with Google that Agrawal, Kayal, and Saxena ran across Fouvry's article in the bibliography of an article by Pomerance and Shparlinski. When they inquired about the best-known value for δ, Pomerance referred them to the article of Baker and Harman.

Regardless of the optimal value, $\delta > 0$ suffices to guarantee an allowable triple (q, r, s) for the AKS-algorithm of the necessary polynomial size,

$$r = O(\log^{1/\delta} n), \qquad q, s = O(\log^{1+1/2\delta} n).$$

Thus the AKS-algorithm has, all told, a guaranteed running time of $\tilde{O}(\log^{3+3/2\delta} n)$. Hence the statement PRIMES $\in \mathcal{P}$ is proved; the breakthrough is achieved. Kudos! Fouvry's corrected value for δ gives $\tilde{O}(\log^{11.913} n)$, or, simpler to remember and also without the tilde, $O(\log^{12} n)$.[7]

The director of the IIT in Kanpur, Sanjay Dhande, was so enthusiastic about the headline in the *New York Times* that he declared Agrawal would be nominated for the highest honors in mathematics.[8] In 2006 Agrawal will be forty years old.

How Practical!?

In Internet newsgroups and in newspapers the question quickly arose of practical applications, since large prime numbers are these days an important component of cryptography and e-commerce. We firmly believe that first of all an important *theoretical* problem was solved that for several decades had eluded the experts. Agrawal himself emphasizes that the problem interested him as an intellectual challenge and that presently the AKS-algorithm is much slower than those algorithms that have raised the record in primality proofs to 5,020 decimal digits.[9] Finally, one should not forget that the definition of complexity classes like $\mathcal{P}$ is a purely theoretical question of an asymptotic statement as $n \to \infty$. In a particular case, therefore, the advantage in running time of a polynomial algorithm as opposed to a super-polynomial algorithm very possibly could become manifest only for n so large that neither of the two algorithms would produce an answer within our lifetime on current hardware. In practice the constants in the big-O in the complexity estimate also come into play.

Lower-quality "industrial-grade primes" with 512 binary digits can be produced in a fraction of a second using the Miller-Rabin test on an off-the-shelf 2GHz PC. If required, their primality can actually be *proved* in a couple of seconds with the ECPP-method of Atkin-Morain based on elliptic curves.[10] The running-time complexity of this *probabilistic* algorithm is, to be sure, a "cloudy issue" (Carl Pomerance), but heuristic considerations suggest that the likely value lies right around $\tilde{O}(\log^6 n)$.

On the other hand, because of the high cost of the polynomial congruence in the third step of the AKS-algorithm, the constant in the conjectured $\tilde{O}(\log^6 n)$ running-time bound is so large that the algorithm is estimated to take a couple of days on a 512-bit prime number, although Dan Bernstein, Hendrik Lenstra, Felipe Voloch, Bjorn Poonen, and Jeff Vaaler have already improved this constant by a factor of at least $2 \cdot 10^6$ relative to the original formulation of the algorithm—the status as of January 25, 2003; cf. [4].

Thus a factor of about 10^5 is missing to reach a competitive level. The ECPP-method too started with a completely impractical but groundbreaking new idea of Goldwasser and Kilian. Since the method that Agrawal, Kayal, and Saxena have now produced is so unexpectedly new and brilliant, we may confidently anticipate improved capabilities after further maturation of the algorithm.

The Media Pipeline

Except for an excellently researched, technically correct, very readable, and detailed report in the Indian weekly *Frontline* of August 17, the reporting in the general media was deplorable. Agrawal passed over my inquiry about his impression with a polite, "Leave aside the general public coverage."

To be sure, the previously cited *New York Times* article celebrated the result as a triumph, but opaquely by choosing to simplify to a ridiculous extent: polynomial running time became "quickly"; deterministic became "definitively". The article thus reads as follows: three Indians obtained a

[7] *On January 22, 2003, Dan Bernstein posted on the Web a new version of his draft paper [4]. There, a small variation of the Agrawal-Kayal-Saxena theorem, which he had learned from Lenstra, allows one to complete the proof of* PRIMES $\in \mathcal{P}$ *without referring to any deep analytic number theory. A well-known theorem of Chebyshev, asserting that the primes* $\leq 2k$ *have product at least* 2^k*, is enough to guarantee the existence of suitable numbers* $r, s = O(\log^5 n)$ *for which the algorithm works. This removes the last bulwark of difficult mathematics that might have prevented "Everyman" from completely understanding the result. Probably Paulo Ribenboim is right in writing me: "Our specialists should reflect about their convoluted reasoning."*

[8] *Already on October 30, 2002, he received the Clay Research Award. Previous winners were Andrew Wiles, the probabilists Smirnov and Schramm, and Fields Medalists Connes, Lafforgue, and Witten.*

[9] *Please do not confuse this with the record for the* largest known *prime number, which is at this time* $2^{13,466,917} - 1$*, a Mersenne prime with* $4,053,946$ *decimal places. These numbers have a lot of structure that allows a customized algorithm to be used.*

[10] *See* `http://www.ellipsa.net/pages/primo.html` *for the freely available program PRIMO by Marcel Martin, which for the time being holds the record.*

breakthrough because the computer could now say "quickly and definitively" if a number is prime. On the other hand, the new algorithm has no immediate application, because the already existing methods are faster and do not err in practice. "Some breakthrough," readers would say to themselves.

The Associated Press (AP) made the *New York Times* article into a wire report in which "definitively" became "accurately" and the aspect of the running time disappeared into the background. The sad end of this pipeline was the website of the *Tagesschau*. On August 12, under the heading "At last: prime numbers can be exactly calculated!" appeared such rubbish as "The joy at German schools is boundless: finally one can calculate prime numbers without tears!" The report was removed after protests from participants in the newsgroup `de.sci.mathematik`.

Aside from the article in the *New York Times*, the story went virtually unnoticed in the American press. In the UK a story in the *New Scientist* of August 17 at least used the words "polynomial time", but it went on to speak of "an algorithm that gives a definite answer to the problem in a reasonable time." A retrospective piece on November 4 in the *Wall Street Journal* bore the misleading title "One beautiful mind from India is putting the Internet on alert". A year-end column by Clive Thompson in the Sunday *New York Times* of December 15 asserted, "Ever since the time of the ancient Greeks, finding a simple way to prove a number is prime has been the holy grail of mathematics. … This year, it finally arrived. …This new algorithm could guarantee primes so massive they would afford almost perfect online security."

And the large German-language daily newspapers? The *Neue Züricher Zeitung* had its first report on August 30. The article falsely suggested that until now no absolutely certain certificate of primality could be calculated "within reasonable time" for prime numbers used in cryptography and that the three Indians had now achieved precisely this; the result was, however, not so greatly lauded by the news agencies and the media because it could not handle the largest known prime number.

In the August 9 arts section, under the heading "Polynomial gods: Resourceful Indians and their prime numbers", the *Frankfurter Allgemeine Zeitung* had a cryptic text that first made a connection between Indian mathematics and the Indian pantheon and then let four such deities hold a short discussion of the new result:

> "What is it good for?" expostulated Agni, and Lakshmi retorted: "For hacking! One needs prime numbers for encoding data for electronic transmission—there are various so-called cryptographic algorithms like RSA and the Data Encryption Standard DES; the keys are numbers with prime factorizations, and if that can now be easily done in a time that is polynomial in the input data …" "But it is already well known, for example by the Miller-Rabin test, that if one iterates enough times, one can find a primality test with as large a probability as desired of being correct even for the biggest numbers," contradicted Rudra. "And the encoding prime factorization has nothing to do with the test of whether a number is prime, which is a completely different problem; for security people what the guys have done is worthless." At dawn, the hostess Ushas finally found the magic words of reconciliation: "Let us simply take pleasure in an elegant result that the West also admires and in the continuing inspiration of our great mathematical tradition!"

What reader would get from this the reason for all the fuss?

Future Plans

The three plan to submit their work to *Annals of Mathematics* and have been in contact with Peter Sarnak about this. They want to rewrite the article "in a more 'mathematical' way as opposed to 'computer science' way, as that would be more suitable in *Annals*."

As to the emotional state and the future of the two doctoral students Kayal and Saxena, Agrawal says:

> They are happy, but at the same time quite cool about it. I would say they are very level-headed boys. As for their Ph.D., yes, I am sure that this work will qualify for their Ph.D. But I have advised them to stay back for a couple of years, since this is the best time they have for learning. They still need to pick up so many things. But they are free to make the decision—they already have an offer from TIFR [Tata Institute of Fundamental Research].

Appendix

The following is the promised sketch of the proof of the Agrawal-Kayal-Saxena theorem. I follow the streamlined presentation of Dan Bernstein [4].

Sketch of proof. We take a prime factor p of n for which already $p^{(r-1)/q} \not\equiv 0, 1 \mod r$, and we

show that if (i) and (ii) hold for all $1 \le a < s$, then the number n is a power of p.

To do this we consider—as did Agrawal on that morning of July 10 when the theorem was found—products of the form $t = n^i p^j$ with $0 \le i, j \le \lfloor \sqrt{r} \rfloor$. The pigeon-hole principle gives two distinct pairs (i_1, j_1) and (i_2, j_2) of such exponents for which $t_1 = n^{i_1} p^{j_1} \equiv n^{i_2} p^{j_2} = t_2 \mod r$. The goal is now to prove that actually $t_1 = t_2$, whence $n = p^\ell$ for some ℓ.

Via Fermat's Little Theorem, it follows from (ii) that

$$(*) \qquad (x-a)^{t_\mu} \equiv x^{t_\mu} - a \mod (x^r - 1, p)$$

for all $1 \le a \le p$ and $\mu = 1, 2$. In their bachelor's project, Kayal and Saxena called such exponents "introspective", and for these they showed that the congruence $t_1 \equiv t_2 \mod r$ lifts to a congruence $t_1 \equiv t_2 \mod \#G$ with $\#G \gg r$. For a suitable choice of parameters, $\#G$ becomes so large that $t_1 = t_2$ follows. According to Agrawal this lifting is "the nicest part of the paper."

How does one do the lifting? Since $t_1 \equiv t_2 \mod r$, we have that $x^r - 1$ divides the difference $x^{t_1} - x^{t_2}$, so from (*) it follows finally that

$$(x-a)^{t_1} \equiv (x-a)^{t_2} \mod (x^r - 1, p).$$

Therefore $g^{t_1} = g^{t_2}$ for all $g \in G$; here G denotes the multiplicative subgroup generated by the linear factors $(\zeta_r - a)$ inside the cyclotomic field over $\mathbb{Z}/p\mathbb{Z}$ generated by adjunction of the rth roots of unity ζ_r. Taking a primitive element g, that is, one of order $\#G$, shows that $\#G \mid (t_1 - t_2)$.

On the other hand, in view of (i) and because $p^{(r-1)/q} \not\equiv 0, 1 \mod n$, the group G has—by some combinatorics and elementary theory of cyclotomic polynomials—at least $\binom{q+s-1}{s}$ elements. Therefore by the hypothesis on the binomial coefficients

$$|t_1 - t_2| < n^{\lfloor \sqrt{r} \rfloor} p^{\lfloor \sqrt{r} \rfloor} \le n^{2\lfloor \sqrt{r} \rfloor} \le \binom{q+s-1}{s} \le \#G,$$

whence follows the desired equality $t_1 = t_2$.

Note Added in Proof

Early in March 2003, Agrawal, Kayal, and Saxena posted on the Web a revision of their preprint:

`http://www.cse.iitk.ac.in/news/primality_v3.pdf`

It contains the improvements by Lenstra and culminates in the new time-complexity bound $0(\log^{7.5} n)$, cf. Theorem 5.3.

Acknowledgment

My sincere thanks to Manindra Agrawal for his willingness, despite thousands of congratulatory emails, to answer my inquiries about background information graciously and thoroughly.

References

[1] Manindra Agrawal and Somenath Biswas, Primality and identity testing via Chinese remaindering, in *40th Annual Symposium on Foundations of Computer Science*, IEEE Computer Soc., Los Alamitos, CA, 1999, pp. 202–8.

[2] Manindra Agrawal, Neeraj Kayal, and Nitin Saxena, PRIMES is in P, IIT Kanpur, Preprint of August 8, 2002, `http://www.cse.iitk.ac.in/news/primality.html`.

[3] Roger C. Baker and Glyn Harman, The Brun-Titchmarsh Theorem on average, in *Proceedings of a Conference in Honor of Heini Halberstam, Vol. 1*, Birkhäuser Boston, Boston, MA, 1996, pp. 39–103.

[4] Daniel Bernstein, Proving Primality after Agrawal-Kayal-Saxena, version of January 25, 2003, `http://cr.yp.to/papers.html#aks`.

[5] Rajat Bhattacharjee and Prashant Pandey, *Primality Testing*, Bachelor of Technology Project Report, IIT Kanpur, April 2001, `http://www.cse.iitk.ac.in/research/btp2001/primality.html`.

[6] Étienne Fouvry, Théorème de Brun-Titchmarsh; application au théorème de Fermat, *Invent. Math.* **79** (1985) 383–407.

[7] Morris Goldfeld, On the number of primes p for which $p + a$ has a large prime factor, *Mathematika* **16** (1969) 23–27.

[8] D. Roger Heath-Brown, The first case of Fermat's Last Theorem, *Math. Intelligencer* 7, no. 4 (1985), 40–47, 55.

[9] Neeraj Kayal and Nitin Saxena, *Towards a Deterministic Polynomial-Time Primality Test*, Bachelor of Technology Project Report, IIT Kanpur, April 2002, `http://www.cse.iitk.ac.in/research/btp2002/primality.html`.

[10] R. Ramachandran, A prime solution, *Frontline,* India's National Magazine, **19** (August 17, 2002), `http://www.flonnet.com/fl1917/19171290.htm`.