

Re: Math errors in book Secret Life of Numbers

Source: <http://sci.tech--archive.net/Archive/sci.math.research/2006-05/msg00101.html>

- *From:* israel@xxxxxxxxxxx (Robert Israel)
 - *Date:* 16 May 2006 07:49:41 -0400
-

In article <e4aesc\$17o\$1@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>, <carolyn.meinel@xxxxxxxxxxxxxxxxxx> wrote:

Have any of you read "Secret Life"? I found major errors in two chapters, but I'm not sufficiently competent in areas touched upon in other chapters to know whether they might also be off base. If anyone has discovered other errors, I would be delighted to cite you in the planned book review

I haven't read it, but I'll comment on your comments.

Szpiro's explanation of the set NP quickly collapses into self-contradiction. It is true, as Szpiro writes, that nobody has proved that the class NP-Complete is not equal to the class P, meaning problems that are "easy" to solve. However, Szpiro states incorrectly that "if only one NP problem can be solved in polynomial time, all NP problems can be solved in polynomial time.... Numerous scientists have wrestled with it, not least because the Clay Foundation has offered a \$1 million prize for a correct solution."

The problem here is that the set P is a subset of NP, and by definition, all problems in P already have been proved to be solvable in a number of steps bounded by a polynomial function of the size of the problem. For example, the spanning tree problem, meaning how to build a tree that connects a given number of points with the shortest total length of branches, has been shown to be a member of P.

You're right. Szpiro's statement should be "if only one NP-complete problem ..." I don't know if this is just a typo, or a symptom of a more significant lack of understanding.

The second chapter that set off my alarm bells is "How Can One Be Sure it's Prime?" Szpiro correctly reports that Manindra Agrawal and two of

Re: Math errors in book Secret Life of Numbers

his students have proven that primes can be found in polynomial time. However, he erroneously writes that "...this unexpected result created no small sensation among colleagues in the field" because "... three mathematicians had hit on a beautiful and fundamentally new idea. For practical purposes the algorithm is, admittedly, still too time consuming. But now that the ice has been broken, experts are confident that more efficient ways of calculation are imminent."

It did create somewhat of a stir at the time.

Agrawal's finding was not "unexpected." Furthermore, it did not raise hopes of finding faster ways to find primes. Fast ways to find primes (but not to solve the problem of factoring a composite number down to its primes) have been known since the 1970s, and the fastest of them scale as the fourth power of the size of the numbers tested.

What these techniques lacked was a proof that the amount of time required could be guaranteed to be bounded by a polynomial without introducing even a small probability of error, and while running the same algorithm every time (no random choices). In practice this didn't make a difference — the time was fast enough, and a vanishingly small probability of error could be achieved.

Experience has shown that whenever calculations turn out to be fast on a practical basis, a proof that it belongs to P is highly likely to be found. An example is the linear programming program. It was long known that in practice, it always was solved in polynomial time using the simplex method. However, it wasn't proved to belong to P until 1980 [L. G. Khachiyan, "Polynomial algorithm in linear programming," U.S.S.R. Comput. Math. and Math. Phys., 20 (1980), 53—72.]

Correction: the simplex method is not a polynomial-time algorithm. It performs well in typical cases, but is known to take exponential time on certain classes of problems (e.g. the Klee–Minty examples). Khachiyan's algorithm, Karmarkar's algorithm, and more recently developed polynomial-time algorithms are not based on the simplex method.

Furthermore, in the case of the primes problem, in 1975 Vaughn R. Pratt proved that primes was a member of the class NP, and almost certainly solvable in polynomial time. ["Every prime has a succinct certificate," Vaughn R. Pratt, SIAM Journal on Computing, Vol. 4, 1975, pp. 214–220.] Therefore any mathematician with an interest in primes knew before Agrawal's publication that a proof was hardly unexpected.

It's not just that "primes" is in NP, but that it's in both NP and

co-NP (i.e. not only does every prime have a succinct certificate of primeness, but every composite has a succinct certificate of compositeness, namely a factor), as well as the fact that the best available complexity bound was like $d^{(c \log \log d)}$ where d is the number of digits. But still, there's a big gap between guessing that a polynomial-time algorithm exists and actually finding and proving one.

This is not meant to denigrate Agrawal's feat. It was the brilliance of his proof, not unexpectedness or practical application, that caused a "sensation."

According to Andrew Granville ["It is easy to determine whether a given integer is prime", Bull. Amer. Math. Soc 42 (2005) 3–38]: "Most shocking was the simplicity and originality of their test ... whereas the ?experts? had made complicated modifications on existing tests to gain improvements (often involving great ingenuity), these authors rethought the direction in which to push the usual ideas with stunning success."

Also contributing to the "sensation" was the fact that Kayal and Saxena were undergraduates. As Granville says, "There can have been few undergraduate research experiences with such a successful outcome!".

The closing statement of "How Do You Know it's Prime" is misleading: "The discovered method [Agrawal's proof] cannot be applied to breaking encryption." True, nobody could possibly use Agrawal's proof to crack RSA public key encryption, which uses the easy primes problem to create keys but the hard integer factoring problem to make cracking impossible by any known technique. Integer factoring is (somewhat informally) considered to be a member of the set NP and conjectured to be a member of the set NP-Incomplete (problems conjectured to be outside the sets of both P and NP-Complete). [Computers and Intractability: A Guide to the Theory of NP-Completeness, Michael R. Garey and David S. Johnson (W. H. Freeman and Company, New York, 23rd printing, 2002) pg. 228] According to a leading researcher in this field, Dr. Burt Kaliski, as of today, integer factoring still has not been proved to be a member of P.

The issue here is that just before Szpiro states that Agrawal's proof "cannot be applied to breaking encryption," he writes that it is too cumbersome to be practical because its computational time is bounded by a polynomial of too high an order. Abruptly changing the topic from the practical usage of a proof to the issue of encryption and by implication its link to a related problem Szpiro does not even mention – integer factoring – is confusing at best. If Szpiro had

Re: Math errors in book Secret Life of Numbers

looked into the relationship between the primes and integer factoring problems, he would have realized that NP does not equal NP-Complete and he would have been able to fix all the errors in these two chapters.

You're right, this is a completely different issue. Meanwhile the AKS algorithm has been significantly improved, and there is the reasonable possibility that further work could lead to an algorithm that might be practical.

Robert Israel israel@xxxxxxxxxxxx

Department of Mathematics <http://www.math.ubc.ca/~israel>

University of British Columbia Vancouver, BC, Canada

.