A FALLACIOUS PRINCIPLE IN THE THEORY OF NUMBERS

BY D. H. LEHMER

Since the beginning of the history of mathematics much effort has been spent on the problem of identifying prime numbers. There have thus resulted, among other things, a number of methods and a rapidly increasing assortment of large primes, well above the scope of existing factor tables. It is desirable that such a list of numbers be absolutely accurate. Doubtless a few entries that are actually composite have crept in as a result of miscalculations. There is a greater danger, however, of an invasion of this hard won list by a horde of composite numbers on account of an erroneous method. It would seem worth while therefore to point out a fallacious principle which can be traced back to Seelhoff in 1886* and which is remarkable in that it has evoked no criticism, but on the contrary has been endorsed by no less a mathematician than F. N. Cole. The recent appearance of a book devoted to the principle prompts us to write the present criticism.

We are indebted to Legendre for one of the most powerful tools for attacking the problem complementary to the one mentioned above, namely that of factoring composite numbers. Legendre's method is based upon the fact that the knowledge of one quadratic residue of the given number N, eliminates approximately half of its trial divisors. Thus if there are n primes $\leqq \sqrt{N}$, and if $2^{r-1} \leqq n \leqq 2^r$, then a knowledge of r independent quadratic residues of N would reduce the number of trial divisors to a mere handful. But the task of combining the separate bits of information offered by each residue, and thus excluding nearly all (if not all) the trial divisors, is often the most difficult part of the procedure. It was Seelhoff's idea to eliminate this part of the work by formulating the following principle.

If at least r primes can be found which, when taken with the proper sign, are quadratic residues of N, then N is a prime, the number r being defined above.

* Zeitschrift für Mathematik und Physik, vol. 31, p. 307.

As one example Seelhoff chooses a factor of $2^{43}-1$, namely $N=20408568497$ and shows that the following 16 primes, 1, 2, 7, 11, 17, 19, 23, 31, 43, 53, 61, 67, 83, 97, 113, 131, are quadratic residues of N. The number of primes $<\sqrt{N}$ is 13253 (instead of "about 1600" according to Seelhoff), while the number of trial divisors of N is reduced to one case in $2^{16}=65536$. Hence Seelhoff concludes that N is a prime. However Landry had found seventeen years earlier that $N=9719\cdot 2099863$.

In terms of the factor stencils of D. N. Lehmer, Seelhoff's principle assures us that after we have selected the appropriate stencil sheets, it is unnecessary to use them at all.

Seelhoff makes no explicit statement about the magnitudes of the prime quadratic residues, although in the example just quoted the residues are actually the smallest available ones (except for the last). Cole's interpretation* of Seelhoff's principle added to it the requirement that the prime quadratic residues should constitute an unbroken sequence of the smallest possible primes. As to the number of primes required to establish the primality of N, Cole states that for N a 22 digit number about 70 primes are enough and "in fact a much smaller sequence would suffice." Although Cole refers to Seelhoff's paper and also to an article in which the factors of Seelhoff's "prime" occur, he not only fails to draw a moral from Seelhoff's example (which presumably satisfies all the requirements of his interpretation of the principle), but proceeds to apply the method to prove that $2^{61}-1$ is a prime.

Another application of the principle was made by Hoppe in the investigation of $(10^{19}-1)/9$. Two proofs of the primality of this number were submitted by him to the London Mathematical Society.† The first proof consisted in isolating an unbroken sequence of the 73 smallest prime residues, in fact all those $\leqq 761$. He submitted this proof to Cole, who did not consider it sufficient. This seems to indicate that Cole had some doubt as to the rigor of his own method. It was probably Cole's reply that prompted Hoppe to give an independent proof of the

* This Bulletin, vol. 10, p. 134.

† Proceedings of the London Mathematical Society, Records of Meetings of Dec. 6, 1917 and Feb. 14, 1918.

primality of his number, as described in his second communication to the Society.*

The latest and most elaborate application of Seelhoff's principle is to be found in Kraitchik's *Recherches sur la Théorie des Nombres*, vol. 2 (Paris, 1929). He bases his method on the following theorem.

If every prime p of which N is a residue is, when taken with the proper sign, a residue of N, then N is a prime.

This theorem (of which no proof is given) cannot be applied directly to a given N since it involves infinitely many operations, not to mention the knowledge of an infinitude of primes. The author surmounts this difficulty by exhibiting a limited number of such primes p, the implication being, that after having obtained these residues, the fate of all the other primes of which N is a residue, is determined. It is natural to inquire what finite number of such residues is sufficient to establish the primality of N. This pressing question is not answered.

Consider for example Kraitchik's proof of the primality of $N=(2^{96}+1)/(2^{32}+1)=18446744069414584321$. Reducing the proof to its essentials, we have exactly 76 primes $p<1000$ of which N is a residue. Of these, 56 are shown to be residues. The characters of the other 20 primes are not determined. But according to the author "Il n'est pas nécessaire d'insister sur ce point." This he considers sufficient evidence for the primality of N.† As we have just presented it, the evidence seems to be rather weak. As presented by Kraitchik it accumulates with increasing rapidity in an almost dramatic way. Thus in the case of $N=(2^{120}+1)(2^{8}+1)/(2^{24}+1)(2^{40}+1)=18518800563924107521$,‡ all but 10 of a certain set of 52 primes <1000 are shown to be residues of N by an ingenious combination of no less than 60 carefully selected quadratic partitions of N. Just as we begin to fear that these outstanding primes are actually non-residues of N, we are brought face to face with the fact that

* The facts of the above paragraph were kindly supplied by Mr. R. E. Powers, who was in correspondence with Hoppe during the latter's investigation.

† Fortunately N is actually a prime, as we have shown by the converse of Fermat's theorem.

‡ No satisfactory proof of the the primality of this number has as yet been given.

(61) $N = 8583172679^2 - 3851^2 \cdot 2^4 \cdot 3^2 \cdot 13 \cdot 5 \cdot 661 \cdot 743 \cdot 809.$

This one fact added to our previous knowledge proves that the 10 remaining primes are actually residues. Hence Kraitchik concludes that N is a prime.

It is difficult to see how a rigorous and practical test for primality could be obtained by modifying Seelhoff's principle. In fact, for a given finite set of primes, there exist composite as well as prime numbers which have this set as residues. Consequently some other evidence more characteristic of the given number is required. It is inevitable, in dealing with very large numbers that the size and number of the residues depend more on the method of their discovery than on the number itself. But a "large" residue is just as much a residue as a "small" one. In considering the 56 residues offered by Kraitchik in evidence of the primality of $(2^{96}+1)/(2^{32}+1)$ one should not forget the 9223372034707292104 other residues which were not consulted in the matter. If the mere exhibition of quadratic residues is insufficient proof, what significance has it? In the final paragraph of the appendix of his book Kraitchik discusses briefly the "moral certainty" of his method. Instead of concluding, as he does, that the proof is sufficient, one may use the evidence (as Hoppe did) in deciding which legitimate method is best suited to the number in question. Whether this guide will prove reliable or not, is a matter for experiment, and is a question of technique rather than theory.

California Institute of Technology