ON THE FIRST CASE OF FERMAT'S LAST THEOREM

D. H. AND EMMA LEHMER

In 1909 Wieferich [1] proved his celebrated criterion for the first case of Fermat's last theorem, namely:

The equation

$$x^p + y^p = z^p, \qquad x, y, z \text{ prime to } p, \tag{1}$$

has no solutions unless

$$2^{p-1} \equiv 1 \pmod{p^2}. \tag{2}$$

Since that time numerous other criteria of the form

$$m^{p-1} \equiv 1 \pmod{p^2} \tag{3}$$

have been proved by Mirimanoff [2] (for $m=3$), Vandiver [3] (for $m=5$), Frobenius [4], Pollaczek [5], Morishima [6], and Rosser [7] for all prime values of $m \leqq 41$.

Wieferich's criterion alone has been applied by Meissner [8] and Beeger [9] for $p<16{,}000$ and was found to be satisfied only for $p=1{,}093$ and $3{,}511$, both of which cases failed to satisfy Mirimanoff's criterion.

Until recently no effort has been made to combine these various criteria in a practical way. Mirimanoff observed, however, in 1910 that his criterion and that of Wieferich could be combined to state that equation (1) has no solutions for all primes p of the form $2^\alpha 3^\beta \pm 1$ or $|2^\alpha \pm 3^\beta|$.

In the presence of more criteria this statement can be extended thus: We call a number an "A_n number" (after Western) if it is divisible by no prime exceeding the nth prime p_n. If the criterion (3) has been established for all $m \leqq p_n$, then equation (1) does not hold if p is the sum or difference of two A_n numbers [10]. Since all the numbers less than p_{n+1} are A_n numbers, we may state that equation (1) has no solution for any prime in a region where the A_n numbers are so dense that they do not differ by more than $2p_{n+1}-1$. This method was used in 1938 by A. E. Western [11] to show that (1) is impossible for $16{,}000<p<100{,}000$.

A more powerful method of combining the criteria was suggested recently by Rosser [12], who observes that while the congruence

$$x^{p-1} \equiv 1 \pmod{p^2} \tag{4}$$

has only $(p-1)/2$ solutions less than $p^2/2$, every A_n number is a