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

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

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 solution of (4) if (1) holds and if (3) has been established as far as $m=p_n$. Hence if $\phi_n(x)$ denotes the number of A_n numbers not exceeding x, then

$$\phi_n(p^2/2) \leqq (p-1)/2, \tag{5}$$

a condition which cannot hold for small p's if the A_n numbers are sufficiently dense.

Other inequalities of this kind can be derived by separating the solutions of (4) into classes. We shall do this here only in the case in which the solutions are distinguished by their parity. For every positive odd solution $\omega<p^2/3$ of (4) there exists also a solution $(p^2-\omega)/2$ (using Wieferich's criterion) which lies between $p^2/3$ and $p^2/2$, and hence differs from ω. The number $(p-1)/2$ of solutions of (4) not exceeding $p^2/2$ is then at least the number of even A_n numbers less than $p^2/3$ plus twice the number of odd A_n numbers less than $p^2/3$. This can be written as

$$\phi_n(p^2/3) + \phi_n^*(p^2/3) \leqq (p-1)/2 \tag{6}$$

where $\phi_n^*(x)$ denotes the number of odd A_n numbers less than x.

If one is to apply an inequality such as (5) or (6) outside the limit of existing tables [**13**] of A_n numbers, it is necessary to find lower bounds for ϕ_n and ϕ_n^*. Rosser [**12**] has given a lower bound for $\phi_n(10^x)$ in the form of a polynomial $f_n(x)$ of the nth degree.

By an improved method [**14**] which makes use of Bernoulli polynomials we have constructed polynomials $P_n(x)$ and $Q_n(x)$ of degree n giving lower and upper bounds for $\phi_n(10^x)$, and also a polynomial $P_{n-1}^*(x)$ of degree $n-1$ giving a lower bound for $\phi_n{}^*(10^x)$. As we shall actually need not P_{n-1}^* but the sum $P_n+P_{n-1}^*$, we tabulate the following polynomials for $n=13$:

$P_{13}(x)$		$P_{13}(x)+\overset{*}{P}_{12}(x)$		$Q_{13}(x)$	
$.0^{9}1380608198$	x^{13}	$.0^{9}1380608198$	x^{13}	$.0^{9}1380608198$	x^{13}
$.0^{7}1272704088$	x^{12}	$.0^{7}1326732670$	x^{12}	$.0^{7}1326732670$	x^{12}
$.0^{6}5247670000$	x^{11}	$.0^{6}5691949617$	x^{11}	$.0^{6}5729012056$	x^{11}
$.0^{4}1277269076$	x^{10}	$.0^{4}1439087748$	x^{10}	$.0^{4}1469359894$	x^{10}
$.0^{3}2039391192$	x^{9}	$.0^{3}2383232393$	x^{9}	$.0^{3}2493297644$	x^{9}
$.0^{2}2244543403$	x^{8}	$.0^{2}2716892889$	x^{8}	$.0^{2}2952478417$	x^{8}
$.01740607057$	x^{7}	$.02179700460$	x^{7}	$.02510548659$	x^{7}
$.09545572654$	x^{6}	$.1235281024$	x^{6}	$.1557243217$	x^{6}
$.3654889719$	x^{5}	$.4882665632$	x^{5}	$.7120647453$	x^{5}
$.9452666752$	x^{4}	1.302427247	x^{4}	2.432810990	x^{4}
1.542870198	x^{3}	2.191273599	x^{3}	6.376807029	x^{3}
1.361483164	x^{2}	1.996360212	x^{2}	13.24421612	x^{2}
$.3459458265$	x	$.5410860433$	x	21.15029718	x
$-.2049399029$		$-.2911608671$		19.69764203	

If we now replace (5) by

$$P_{13}(\log p^2/2) \leqq (p-1)/2,$$

we find, by actual substitution into P_{13}, that this inequality holds only for $p \geqq 93,785,629$, and hence (1) has no solution[1] for $p < 93,785,629$.

Since

$$Q_{13}(\log p^2/2) \leqq (p-1)/2$$

holds only for $p > 141,000,000$, it follows that the inequality (5), even if we knew the exact value of $\phi_n(x)$, could not be used beyond this limit for $n = 13$.

The inequality (6) becomes

$$P_{13}(\log p^2/3) + \overset{*}{P}_{12}(\log p^2/3) \leqq (p-1)/2.$$

This holds only for $p > 102,108,200$.

Hence the first case of Fermat's last theorem is now proved for $p < 102,108,200$.

Further criteria of type (3), when established, may be used to extend this limit by calculating approximating polynomials of higher degree from the ones given above by the method described in [**14**].

Note added March 1. Since writing the above, Dr. Rosser has kindly sent us the manuscript of his forthcoming paper [**15**] in which he completes Morishima's proof that the prime 43 gives also a criterion of the form (3). We have therefore calculated $P_{14}(x)$ and $P_{13}^*(x)$ from the P_{13} and P_{12}^* given above. These polynomials are as follows:

$P_{14}(x)$		$\overset{*}{P}_{13}(x)$		$P_{14}(x)+\overset{*}{P}_{13}(x)$	
$.0^{11}6037145739$	x^{14}			$.0^{11}6037145739$	x^{14}
$.0^{9}6683705079$	x^{13}	$.0^{10}2544306733$	x^{13}	$.0^{9}6938135752$	x^{13}
$.0^{7}3337944336$	x^{12}	$.0^{8}2536688143$	x^{12}	$.0^{7}3591613150$	x^{12}
$.0^{6}9940243443$	x^{11}	$.0^{6}1131551216$	x^{11}	$.0^{5}1107179466$	x^{11}
$.0^{4}1965570473$	x^{10}	$.0^{5}2980593461$	x^{10}	$.0^{4}2263629819$	x^{10}
$.0^{3}2719317505$	x^{9}	$.0^{4}5152041706$	x^{9}	$.0^{3}3234521676$	x^{9}
$.0^{2}2700968174$	x^{8}	$.0^{3}6140455952$	x^{8}	$.0^{2}3315013769$	x^{8}
$.01944029859$	x^{7}	$.0^{2}5157919367$	x^{7}	$.02459821796$	x^{7}
$.1009940169$	x^{6}	$.03064345185$	x^{6}	$.1316374687$	x^{6}
$.3720257684$	x^{5}	$.1271048263$	x^{5}	$.4991305947$	x^{5}
$.9365601794$	x^{4}	$.3559975936$	x^{4}	1.292557773	x^{4}
1.500217863	x^{3}	$.6290315435$	x^{3}	2.129249406	x^{3}
1.299882088	x^{2}	$.6014604442$	x^{2}	1.901342532	x^{2}
$.3050249350$	x	$.1730336327$	x	$.4780585677$	x
$-.2081092173$		$-.08700841024$		$-.2951176274$	

[1] The corresponding result obtained by Rosser is about 41,000,000.

We find that (5) is satisfied only if $p>230$ millions, while (6) gives the better inequality $p\geqq 253{,}747{,}889$.

The first case of Fermat's last theorem is therefore now established for all $p<253{,}747{,}889$.

Bibliography

1. A. Wieferich, Journal für die reine und angewandte Mathematik, vol. 136 (1909), pp. 293–302.

2. D. Mirimanoff, Comptes Rendus de l'Académie des Sciences, Paris, vol. 150 (1910), pp. 204–206.

3. H. S. Vandiver, Journal für die reine und angewandte Mathematik, vol. 144 (1914), pp. 314–318.

4. G. Frobenius, Sitzungsberichte der Akademie der Wissenschaften, Berlin, 1914, pp. 653–681.

5. F. Pollaczek, Sitzungsberichte der Akademie der Wissenschaften, Vienna, IIa, vol. 126 (1917), pp. 25–59.

6. T. Morishima, Japanese Journal of Mathematics, vol. 8 (1931), pp. 159–173.

7. J. B. Rosser, this Bulletin, vol. 46 (1940), pp. 299–304.

8. W. Meissner, Sitzungsberichte der Akademie der Wissenschaften, Berlin, 1913, pp. 663–667.

9. N. G. W. H. Beeger, Messenger of Mathematics, vol. 51 (1922), pp. 149–150; Nieuw Archief voor Wiskunde, (2), vol. 20 (1939), pp. 51–54.

10. This is a special case of a theorem due to Landau, l'Intermédiaire des Mathematiciens, vol. 20 (1913), p. 206. See also E. Gottschalk, Mathematische Annalen, vol. 115 (1938), pp. 157–158.

11. A. E. Western, unpublished manuscript.

12. J. B. Rosser, this Bulletin, vol. 45 (1939), pp. 636–640.

13. There is only one such table in print, namely: A. J. C. Cunningham, *Quadratic and Linear Tables*, London, 1927, pp. 162–170 (for $n=5$). Extensive manuscript tables have been prepared by Dr. A. E. Western.

14. D. H. Lehmer, *The lattice points of an n-dimensional tetrahedron*, Duke Mathematical Journal, vol. 7 (1940), pp. 341–353.

15. J. B. Rosser, *An additional criterion for the first case of Fermat's last theorem*, this Bulletin, vol. 47 (1941), pp. 109–110.

Lehigh University