A NEW LOWER BOUND FOR THE EXPONENT IN THE FIRST CASE OF FERMAT'S LAST THEOREM[1]

BARKLEY ROSSER

1. **Introduction.** In this paper is proved the theorem: If p is an odd prime and

$$a^p + b^p + c^p = 0 \tag{1}$$

has a solution in integers prime to p, then $p > 41{,}000{,}000$.

It seems certain that still higher lower bounds for p can be deduced by the methods of this paper. However an argument is given which makes it seem unlikely that an indefinitely high lower bound can be so deduced.

2. **Preliminary results.** Unless otherwise specified, we shall assume that p is an odd prime for which (1) can be satisfied by integers prime to p. Hence[2] $p > 8{,}000{,}000$. Also $x \equiv y$ shall denote $x \equiv y \pmod{p}$. Also any statement regarding factorization of a polynomial is to be understood modulo p.

Morishima has proved[3] that for each odd prime $m \leqq 43$, there is a t ($t \not\equiv 0$, $\not\equiv 1$) such that each of the values

$$t, \quad \frac{1}{t}, \quad 1 - t, \quad \frac{1}{1 - t}, \quad \frac{t - 1}{t}, \quad \frac{t}{t - 1} \tag{2}$$

satisfies each of the following relations when substituted for x:

$$\{(m^{p-1} - 1)/p\}(x^{m-1} - 1) \equiv 0, \tag{3}$$

$$x^4 \not\equiv 1, \tag{4}$$

$$x^6 \not\equiv 1. \tag{5}$$

Morishima further proved that for each odd prime $m \leqq 31$, there is no t such that the values in (2) satisfy (4), (5), and

$$x^{m-1} \equiv 1. \tag{6}$$

Hence for such m's, $(m^{p-1} - 1)/p \equiv 0$. That is

$$m^{p-1} \equiv 1 \pmod{p^2}. \tag{7}$$

---

[1] Presented to the Society, September 8, 1939.

[2] Barkley Rosser, *On the first case of Fermat's last theorem*, this Bulletin, vol. 45 (1939), pp. 636–640. This paper will be referred to as I.

[3] Taro Morishima, *Über den Fermatschen Quotienten*, Japanese Journal of Mathematics, vol. 8 (1931), pp. 159–173.