AN ADDITIONAL CRITERION FOR THE FIRST CASE OF FERMAT'S LAST THEOREM[1]

BARKLEY ROSSER

In an earlier paper[2] it was shown that if p is an odd prime and

$$a^p + b^p + c^p = 0$$

has a solution in integers prime to p, then

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

for each prime $m \leqq 41$. In this paper the result is extended to $m \leqq 43$.

We will use the notations and conventions of I throughout, and a reference to a numbered equation will refer to the equation of that number in I. With p assumed to be an odd prime such that (1) has a solution in integers prime to p, we assume that a t exists such that the values of (2) satisfy (4), (5), and (6) with $m = 43$. Put $g(x) = f(x)f(-x)$ and

$$h(x) = (x^{42} - 1)/(x^6 - 1).$$

Then $g(x)$ divides $h(x)$, and $g(x)$ can be completely factored modulo p.

Case 1. Assume that a root of $g(x)$ is a root of

$$h(x)/(x^{12} + x^{10} + x^8 + x^6 + x^4 + x^2 + 1).$$

Then this root belongs to either the exponent 21 or the exponent 42 modulo p. Hence $p \equiv 1 \pmod{42}$. So there is an ω such that

$$\omega^2 + \omega + 1 \equiv 0.$$

Then $g(x)$, $g(\omega x)$, and $g(\omega^2 x)$ all divide $h(x)$. Moreover, the only cases in which two of $g(x)$, $g(\omega x)$, and $g(\omega^2 x)$ have a common factor are

I. $a^6 + 1 \equiv 0$,

II. $a^6 + a^3 + 3a^2 + 3a + 1 \equiv 0$,

III. $a^6 - a^3 - 3a^2 - 3a - 1 \equiv 0$,

or cases derived from these by replacing a by one of the other roots of $f(x)$. So if we show that $h(x)$ has no factor in common with any of $x^6 + 1$, $x^6 + x^3 + 3x^2 + 3x + 1$, or $x^6 - x^3 - 3x^2 - 3x - 1$, then we can conclude that $g(x)g(\omega x)g(\omega^2 x)$ must divide $h(x)$.

Clearly $h(x)$ has no factor in common with $x^6 + 1$.

---

[1] Presented to the Society, April 27, 1940.

[2] *A new lower bound for the exponent in the first case of Fermat's last theorem*, this Bulletin, vol. 46 (1940), pp. 299–304. This paper will be referred to as I.