# 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 $\omega$ 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.

Suppose $h(x)$ has a factor in common with $x^6+x^3+3x^2+3x+1$. This latter has the factors $x^2+x+1$ and $x^4-x^3+2x+1$. The first has no factor in common with $h(x)$, since it divides $x^6-1$, which has no factor in common with $h(x)$. To test the second, we try it successively with each of the four factors of $h(x)$, getting the eliminants

$$13\cdot 19^2\cdot 127\cdot 163^2,\ 5\cdot 36913,\ 2\cdot 127,\ 5\cdot 7.$$

Suppose $h(x)$ has a factor in common with $x^6-x^3-3x^2-3x-1$. This latter has the factors $x^2-x-1$ and $x^4+x^3+2x^2+2x+1$. The first has no factor in common with $h(x)$ by Lemma 3 of I. Trying the second factor successively with each of the four factors of $h(x)$, we get the eliminants

$$7^3\cdot 43,\ 2^2\cdot 7\cdot 13\cdot 43,\ 7,\ 43.$$

So $g(x)g(\omega x)g(\omega^2 x)$ must divide $h(x)$. Since both are of degree 36, they must be equal. Putting $b=c+5$ and equating coefficients, we get

$$A+1 = 2c^3+3c^2-24c+13 \equiv 1,$$
$$B+1 = c^6+12c^5+42c^4+18c^3-9c^2-222c+173 \equiv 1,$$
$$C+1 = -2c^6+12c^5+171c^4+132c^3-666c^2+132c+201 \equiv 1.$$

Dividing $16B$ and $8C$ by $A$, we get the remainder

$$43D = 43(99c^2+192c-116) \equiv 0$$

from each. Then

$$2cE = 29A+3D = 2c(29c^2+192c-60) \equiv 0.$$

As $c\equiv 0$ would give $A\equiv 12\equiv 0$, we have

$$28cF = 15D-29E = 28c(23c-96) \equiv 0,$$
$$29cG = 8E-5F = 29c(8c-49) \equiv 0,$$
$$8F-23G = 359 \equiv 0.$$

*Case* 2. Assume that no root of $g(x)$ is a root of

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

Then, since $g(x)$ divides $h(x)$ and is of degree 12,

$$g(x) \equiv x^{12}+x^{10}+x^8+x^6+x^4+x^2+1.$$

So $2c+1\equiv 1$ and $c^2+5\equiv 1$.

PRINCETON UNIVERSITY