On Fermat's Last Theorem
Author(s): Louis Long
Source: *The Mathematical Gazette*, Vol. 45, No. 354 (Dec., 1961), pp. 319-321
Published by: The Mathematical Association
Stable URL: http://www.jstor.org/stable/3614095
Accessed: 24/03/2010 21:20

ON FERMAT'S LAST THEOREM

By Louis Long

In my note in the December 1960 Gazette I proved that if there is an odd prime p and numbers a, b, c prime to p such that

$$a^{2p} + b^{2p} = c^{2p} \tag{1}$$

then p necessarily has one of the forms $120k+1$, $120k+49$.

In the present note I extend the range of values of p for which equation (1) has no solution with a, b, c prime to p. My method is to find values of p for which one of the numbers a, b, c in equation (1) is necessarily divisible by 11.

Any odd prime p has one of the forms

$$10k \pm 1, \quad 10k \pm 3$$

(for numbers of the form $10k \pm 5$ are not prime). I showed in my previous note that (1) has no solution prime to p when p has the forms $5k \pm 2$, and so there remains to consider only values of p of the form $10k \pm 1$. I have obtained no results in the case $10k+1$ and I shall now consider the case $10k-1$. With $p = 10k-1$ equation (1) takes the form

$$(a^2)^{10k-1} + (b^2)^{10k-1} = (c^2)^{10k-1}$$

and since, by Fermat's little theorem, $x^{10} \equiv 1 \pmod{11}$, for any x, we have

$$a^{-2} + b^{-2} \equiv c^{-2} \pmod{11}$$

that is

$$b^2c^2 + c^2a^2 - a^2b^2 \equiv 0 \pmod{11} \tag{1.1}$$

The quadratic residues of 11 are

$$+1, \ -2, \ +3, \ +4, \ +5 \tag{1.2}$$

Because none of a, b, c is divisible by p, it follows as in my previous note that $c^2 - a^2$, $c^2 - b^2$, $a^2 + b^2$ are all squares so that we may write

$$c^2 - a^2 = A^2 \tag{2}$$
$$c^2 - b^2 = B^2 \tag{3}$$
$$a^2 + b^2 = D^2 \tag{4}$$

Considering the quadratic residues to modulus 11, listed in (1.2), and writing h_r^2 for the remainder when h^2 is divided by 11, we see that to any value of c^2 correspond only two possible values of a_r^2. Let s, t be the two values of a_r^2 for a given c^2; it follows that the two values of b_r^2 are all s and t. If a_r^2 and b_r^2 have the same value, then by (4) we have $2a^2 \equiv D^2 \pmod{11}$, which is impossible since 2 is not a quadratic residue of 11. Therefore $a_r^2 = s$ and $b_r^2 = t$ (or *vice-versa*) and so

$$a^2 + b^2 = c^2 \pmod{11} \tag{5}$$

Writing (1.1) in the form

$$c^2(a^2 + b^2) = a^2b^2 \pmod{11} \tag{6}$$

it follows that

$$c^4 = a^2b^2 \pmod{11} \tag{7}$$

Similarly

$$b^4 = -a^2c^2 \pmod{11}, \tag{8}$$
$$a^4 = -b^2c^2 \pmod{11} \tag{9}$$

From (7), (8), (9) we obtain

$$c^4 = a^4 + b^4 \pmod{11} \tag{10}$$

and from (5)

$$c^4 = a^4 + b^4 + 2a^2b^2 \pmod{11} \tag{10.1}$$

whence

$$2a^2b^2 = 0 \pmod{11}$$

contradicting the hypothesis that neither a nor b is divisible by 11. Thus we may suppose that b is divisible by 11.

Hence the equation (1)

$$a^2 = b^2 \pmod{11}$$

that is, $c^2 - a^2$ is divisible by 11.

But

$$c^{2p} - a^{2p} = (c^2 - a^2)R$$

since $(c^2)^p - (a^2)^p$ is divisible by $c^2 - a^2$, and

$$\begin{aligned} R &= c^{2(p-1)} + c^{2(p-2)}a^2 + \dots + a^{2(p-1)} \\ &= c^{2(p-1)} - a^{2(p-1)} + a^2(a^{2(p-2)} - a^{2(p-2)}) + \dots + p \,.\, a^{2(p-1)} \\ &= 11s + p \,.\, a^{2(p-1)} \end{aligned}$$

Since R is a square, $p \,.\, a^{2(p-1)}$ is a quadratic residue of 11 and therefore p itself is a quadratic residue of 11.

Thus we have arrived at the following conclusion.

If p is a prime of the form $10k - 1$ then equation (1) has no solution a, b, c prime to p if p is a quadratic non-residue of 11.

From my previous note we know that there is no solution of (1) prime to p unless p has one of the forms

$$120l+1, \quad 120l+49,$$

only the second of which is of the form $10k-1$. It remains only to see which of the numbers $120l+49$ is a quadratic non-residue of 11. Since $120l+49=121l+44-l+5$, and since the non-residues of 11 are

$$-1, \ +2, \ -3, \ -4, \ -5,$$

we have

$$l-5=1, \ -2, 3, 4, 5 \quad (\text{mod } 11)$$

and so for the following values of p

$$\begin{aligned} 120(11m+6)+49 &= 1320n-551, & (n=m+1) \\ 120(11m+3)+49 &= 1320n+409, & (n=m) \\ 120(11m+8)+49 &= 1320n-311, & (n=m+1) \\ 120(11m+9)+49 &= 1320n-191, & (n=m+1) \\ 120(11m+10)+49 &= 1320n+71\ , & (n=m+1) \end{aligned}$$

equation (1) has no solution with a, b, c prime to p.

These values are all different from those already found in my previous note.

The method we have used for the prime 11 may be used successfully for any other prime, although we do not always obtain new values of p in this way. It is perhaps worth remarking, too, that the proof in my previous note which showed that the equation

$$a^{2p}+b^{2p}=c^{2p}$$

has no solution in integers prime to p when p has either of the forms $5m\pm2$, is valid whether p is prime or not and so the equation

$$a^n+b^n=c^n$$

has no solution with a, b, c prime to n when the terminal digit of n is 4 or 6.

Fair-View House L.L.
Stratton-on-the-Fosse, Near Bath