NOTE ON FERMAT'S LAST THEOREM*

BY

H. S. VANDIVER

1. If x, y and z are integers prime to each other, and

$$x^p + y^p + z^p = 0, \tag{1}$$

where p is a prime, and

$$q(r) = \frac{r^{p-1} - 1}{p},$$

Furtwängler † has shown that

$$q(r) \equiv 0 \pmod{p}$$

for each factor r of x, in case $x \not\equiv 0 \pmod{p}$, and for each factor r of $x^2 - y^2$, in case $x^2 - y^2$ is prime to p.

By applying this theorem, Furtwängler deduces the criterion of Wieferich $q(2) \equiv 0 \pmod{p}$ and the criterion of Mirimanoff $q(3) \equiv 0 \pmod{p}$ for the solution of (1) in integers prime to p. I shall here extend these results and show that in addition we have, provided that $q(2) \not\equiv 0 \pmod{p^3}$, the criteria $q(5) \equiv 0 \pmod{p}$ for $p \equiv 1 \pmod{3}$ and $q(5) \equiv q(7) \equiv 0 \pmod{p}$ for $p \equiv 2 \pmod{3}$.

2. Assume that x, y and z are prime to each other and to p and that $p > 5$. If one of the integers x, y, z is divisible by 5, then $q(5) \equiv 0 \pmod{p}$ by Furtwängler's theorem. If none of them is so divisible, then, modulo 5, x^p, y^p, z^p have the residues ± 2, ± 2, ± 1 or ± 1, ± 1, ∓ 2 in some order. We may therefore take $x^p \equiv y^p \pmod{5}$. Then $x \equiv y \pmod{5}$, since every integer has a unique cube root modulo 5. Thus 5 is a divisor of $x^2 - y^2$. Hence (§ 1) $q(5) \equiv 0 \pmod{p}$, unless $x^2 \equiv y^2 \pmod{p}$, i. e., unless $x \equiv y \pmod{p}$, since $x \equiv -y$ and $x + y + z \equiv 0 \pmod{p}$ would imply $z \equiv 0 \pmod{p}$, contrary to hypothesis. Using $x + y + z \equiv 0$, we may state the result:

If (1) *is satisfied by integers prime to* p, *then the congruence*

$$q(5)(t-1)(t+2)(t+1/2) \equiv 0 \pmod{p} \tag{2}$$

is satisfied by each of the following values of t:

$$\frac{x}{y}, \frac{y}{x}, \frac{x}{z}, \frac{z}{x}, \frac{y}{z}, \frac{z}{y}. \tag{3}$$

* Presented to the Society, February 28, 1914.

† Sitzungsberichte K. Akademie der Wissenschaften, Wien, vol. 121 (1912), p. 589.

3. From (1) we have

$$\frac{x^p + y^p}{x + y} = v^p,$$

when v is an integer, since the quotient is relatively prime to $x + y$ and hence is a pth power. Since v is a factor of z, it is not divisible by p, and is of the form $1 + kp$, since the fraction is congruent to $-z^p/(-z)$ modulo p. Furthermore,

$$(1 + kp)^{p-1} \equiv 1 \pmod{p^2}$$

by Furtwängler's theorem. Multiply the members by $1 + kp$ and apply $(1 + kp)^p \equiv 1 \pmod{p^2}$. Hence $k \equiv 0 \pmod{p}$, and $v^p \equiv 1 \pmod{p^3}$. Hence

$$x^p + y^p \equiv x + y,$$

$$x^p + z^p \equiv x + z, \pmod{p^3}, \tag{4}$$

$$y^p + z^p \equiv y + z$$

$$x^p \equiv x, \qquad y^p \equiv y, \qquad z^p \equiv z \pmod{p^3}. \tag{5}$$

Hence by (1),

$$x + y + z \equiv 0 \pmod{p^3}. \tag{6}$$

4. Suppose that $y = x + p\mu$. Substituting in the first relation (4), we have

$$x^p + (x + p\mu)^p \equiv 2x + p\mu \pmod{p^3},$$

$$2x^p + p^2 \mu x^{p-1} \equiv 2x + p\mu \pmod{p^3}.$$

Hence, by (5),

$$p\mu\,(px^{p-1} - 1) \equiv 0 \pmod{p^3}, \qquad \mu \equiv 0 \pmod{p^2}.$$

We may therefore set $y = x + p^3\mu$. Then, from (6), $z = -2x + p^3\nu$. Hence, from (1),

$$x^p + (x + p^3\mu)^p + (-2x + p^3\nu)^p = 0,$$

$$2x^p - 2^p x^p \equiv 0 \pmod{p^4},$$

$$q\,(2) \equiv 0 \pmod{p^3}.$$

5. Now consider the criteria given by Mirimanoff* for the solution of (1). He showed that if (1) is satisfied by integers prime to p, then the ratios (3) satisfy

$$F(t) = \prod_{i=1}^{m-1} (t + \alpha^i) \sum_{i=1}^{m-1} \frac{R_i}{t + \alpha^i} \equiv 0 \pmod{p} \tag{7}$$

when $m = 2, 3, \cdots, p - 1$ and

$$R_i = \frac{\varphi_{p-1}(-\alpha^i)}{(1 - \alpha^i)^{p-1}}, \qquad \alpha = e^{2\pi\sqrt{-1}/m},$$

*Journal für Mathematik, vol. 139 (1911), p. 309 et seq.

$$\varphi_i(t) = t - 2^{i-1}t^2 + 3^{i-1}t^3 - \cdots - (p-1)^{i-1}t^{p-1}.$$

He also showed that

$$F(-1) \equiv (-1)^m m q(m) \pmod{p}. \tag{8}$$

Let $m = 7$ in (7). Assume $p > 7$. The resulting congruence is of degree 5 in t. The ratios (3) have 6 incongruent values unless one of them is a root of

$$(t-1)(t+2)(t+1/2) \equiv 0 \text{ or } t^2 + t + 1 \equiv 0 \pmod{p}.$$

If $p \equiv 2 \pmod{3}$, the latter is not possible for t rational. Hence $t \equiv 1$, -2 or $-1/2$ and therefore, by § 4, $q(2) \equiv 0 \pmod{p^3}$ unless (7) is an identity. In the latter case we may set $t \equiv -1$ and obtain $q(7) \equiv 0 \pmod{p}$ by reason of (8). Hence the criteria:

If (1) *is satisfied by integers prime to* p, *then either*

$$q(2) \equiv 0 \pmod{p^3}, \qquad q(3) \equiv 0 \pmod{p},$$

or else

$$q(2) \equiv q(3) \equiv q(5) \equiv 0 \pmod{p};$$

and if $p \equiv 2 \pmod{3}$,

$$q(7) \equiv 0 \pmod{p}.$$

6. There are no primes p at present known such that $q(2) \equiv 0 \pmod{p^3}$. Meissner* observes that $q(2) \equiv 0 \pmod{1{,}093}$, but finds $q(2) \not\equiv 0 \pmod{1{,}093^2}$. He also states that $q(2) \not\equiv 0 \pmod{p}$ for every $p < 2{,}000$ excepting 1,093.

7. If any one of the forms

$$2^\alpha 3^\beta \pm 1, \qquad 2^\alpha \pm 3^\beta,$$

where α and β are positive integers or zero, is divisible by a prime p but is not divisible by p^2, then p is excluded as an exponent in (1), if x, y and z are prime to each other and to p.† For, if p is admissible in (1), then $q(2) \equiv q(3) \equiv 0 \pmod{p}$, and

$$(2^\alpha)^{p-1} \equiv (3^\beta)^{p-1} \equiv 1, \qquad (2^\alpha 3^\beta)^{p-1} \equiv 1 \pmod{p^2}. \tag{9}$$

But if $2^\alpha 3^\beta \pm 1 \equiv 0$ or $2^\alpha \pm 3^\beta \equiv 0 \pmod{p}$ but $\not\equiv 0 \pmod{p^2}$, then

$$(2^\alpha 3^\beta)^{p-1} \not\equiv 1 \pmod{p^2}, \qquad (2^\alpha)^{p-1} \not\equiv (3^\beta)^{p-1} \pmod{p^2},$$

which contradict (9). As an example, the integer $p = 2^{61} - 1$ is known to be prime, hence it is excluded as an exponent in (1).

*Sitzungsberichte der Preuss. Akademie der Wissenschaften, 1913, no. 35, p. 663.

†See also Mirimanoff, Paris Comptes Rendus, vol. 150 (1910), p. 206.