NEW CRITERIA ASSOCIATED WITH FERMAT'S LAST THEOREM*

BY JOHN MCDONNELL

Furtwängler has obtained* by means of Eisenstein's law of reciprocity for residues of pth powers, p an odd prime, certain criteria in connection with the solution of the equation

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

where x, y, z are relatively prime rational integers, and these criteria involve the rational factors of x, y, z, $y-z$, $z-x$, $x-y$.

It is the object of the present article to employ the same method to derive similar criteria for the factors of

$$x^2 - yz,\ y^2 - zx,\ z^2 - xy,\ x^2 + yz,\ y^2 + zx,\ z^2 + xy.$$

THEOREM 1. *If x, y, z satisfy equation* (1), *$yz+zx+xy$ is prime to p, and r is any factor of x^2-yz, then $r^{p-1}\equiv 1 \pmod{p^2}$.*

PROOF. Let α be a pth root of unity. We have from the identity

$$x(x + y\alpha) - y(z + x\alpha) = x^2 - yz,$$

the equation in pth power characters

$$\left\{\frac{x(x + y\alpha)}{r}\right\} = \left\{\frac{y(z + x\alpha)}{r}\right\}$$

or, since

$$\left\{\frac{x}{r}\right\} = \left\{\frac{y}{r}\right\} = 1,$$

x and y being rational, we have

$$\left\{\frac{x + y\alpha}{r}\right\} = \left\{\frac{z + x\alpha}{r}\right\}. \tag{2}$$

---

* Presented to the Society, August 29, 1929.

† Wiener Sitzungsberichte, vol. 121, IIa (1912), pp. 589–592.

We shall now obtain further relations between the above characters from the theory developed in connection with Fermat's theorem. One, at least, of the numbers y, z must be prime to p. Assuming, first, that z is prime to p, we have from equation (1) the following well known result

$$x + y + z \equiv 0 \pmod{p}.$$

Moreover, the ideal $(x+y\alpha)$ is the pth power of an ideal factor of z: the number $x+y\alpha$ is prime to $1+\alpha$, and is, consequently, associated with a semi-primary number of the form $\alpha^n(x+y\alpha)$, where n is determined by the congruence

$$nz \equiv y \pmod{p}.$$

By Eisenstein's reciprocity theorem, we have*

$$\left\{\frac{\alpha^n(x + y\alpha)}{r}\right\} = \left\{\frac{r}{\alpha^n(x + y\alpha)}\right\} = 1. \tag{3}$$

Again if y be prime to p we obtain similarly

$$\left\{\frac{\alpha^m(z + x\alpha)}{r}\right\} = 1 \tag{4}$$

with $my \equiv x \pmod{p}$.

If, now, yz be prime to p both equations (3) and (4) are satisfied and together with (2) yield the result

$$\left\{\frac{\alpha}{r}\right\}^n = \left\{\frac{\alpha}{r}\right\}^m,$$

or

$$\left\{\frac{\alpha}{r}\right\}^{m-n} = 1. \tag{5}$$

From the congruences $nz \equiv y$ and $my \equiv x \pmod{p}$, we have

$$(m - n)yz \equiv zx - y^2.$$

Now

$$zx - y^2 = (yz + zx + xy) - y(x + y + z),$$

$$x + y + z \equiv 0 \pmod{p}.$$

$$yz + zx + xy \not\equiv 0.$$

* Furtwängler, loc. cit.

Hence $m-n \not\equiv 0$ and, therefore, from (5) we have*

$$\left\{\frac{\alpha}{r}\right\} = 1, \quad \text{and} \quad r^{p-1} \equiv 1 \pmod{p^2}. \tag{6}$$

On the other hand, if yz be not prime to p, either y or z is divisible by p. Assuming first that z is divisible, we have, from equation (1), the following results:

$$x + y \equiv 0 \pmod{p^2},$$

$$x + y\alpha \text{ is divisible by } 1 - \alpha.$$

Denoting the quotient $(x+y\alpha)/(1-\alpha)$ by ω, we see that the principal ideal (ω) is the p h power of an ideal factor of z and, consequently,

$$\left\{\frac{r}{\omega}\right\} = 1.$$

Furthermore

$$\omega = -y + (x + y)/(1 - \alpha),$$

and $x+y\equiv 0 \pmod{p^2}$; hence ω is a primary integer, and by Eisenstein's theorem,

$$\left\{\frac{\omega}{r}\right\} = \left\{\frac{r}{\omega}\right\} = 1.$$

Since $x+y\alpha = (1-\alpha)\omega$, it follows that

$$\left\{\frac{x + y\alpha}{r}\right\} = \left\{\frac{1 - \alpha}{r}\right\}.$$

Again y is prime to p; consequently, from (4),

$$\left\{\frac{\alpha^{-1}(z + x\alpha)}{r}\right\} = 1, \quad m \equiv -1, \pmod{p},$$

or

$$\left\{\frac{z + x\alpha}{r}\right\} = \left\{\frac{\alpha}{r}\right\}.$$

* Furtwängler, loc. cit

Substituting in (2), we have

$$\left\{\frac{1-\alpha}{r}\right\} = \left\{\frac{\alpha}{r}\right\} \tag{7}$$

or, squaring,

$$\left\{\frac{1-2\alpha+\alpha^2}{r}\right\} = \left\{\frac{\alpha}{r}\right\}^2,$$

or

$$\left\{\frac{\alpha}{r}\right\}\left\{\frac{\alpha^{-1}-2+\alpha}{r}\right\} = \left\{\frac{\alpha}{r}\right\}^2.$$

Dividing both sides by $\{\alpha/r\}$, and noting that

$$\left\{\frac{\alpha^{-1}-2+\alpha}{r}\right\} = 1,$$

since $\alpha^{-1}-2+\alpha$ is a real number, we obtain,

$$\left\{\frac{\alpha}{r}\right\} = 1,$$

and hence from (6)

$$r^{p-1} \equiv 1 \pmod{p^2}.$$

A similar proof obviously holds when y is divisible by p.

THEOREM 2. *If x, y, z satisfy equation* (1), *$x(y-z)$ (x^2+yz) is prime to p, and r is any factor of x^2+yz, then*

$$r^{p-1} \equiv 1 \pmod{p^2}.$$

PROOF. From the identity

$$(x+y\alpha)(x+z\alpha^{-1}) = x^2+yz+x(y\alpha+z\alpha^{-1}),$$

we readily obtain the equation

$$\left\{\frac{x+y\alpha}{r}\right\}\left\{\frac{x+z\alpha^{-1}}{r}\right\} = \left\{\frac{y\alpha+z\alpha^{-1}}{r}\right\}. \tag{8}$$

Assuming, first, that yz is prime to p and remembering that x is so by hypothesis, we see that $y\alpha+z\alpha^{-1}$, $x+z\alpha^{-1}$, $x+y\alpha$

are all prime to $1-\alpha$ and are, consequently, associated with semi-primary integers of the form $\alpha^l(y\alpha+z\alpha^{-1})$, $\alpha^m(x+z\alpha^{-1})$, $\alpha^n(x+y\alpha)$ respectively. From the reasoning developed in the previous theorem it is easily seen that

$$\left\{\frac{\alpha^l(y\alpha+z\alpha^{-1})}{r}\right\} = \left\{\frac{\alpha^m(x+z\alpha^{-1})}{r}\right\} = \left\{\frac{\alpha^n(x+y\alpha)}{r}\right\} = 1;$$

hence, from (8), we have

$$\left\{\frac{\alpha}{r}\right\}^{m+n-l} = 1.$$

Now the congruences satisfied by l, m, n, namely

$$lx \equiv y - z, \quad my \equiv -z, \quad nz \equiv y \pmod{p},$$

yield the congruence

$$\begin{aligned}(m+n-l)xyz &\equiv -z^2x + xy^2 - yz(y-z),\\ &\equiv (y-z)[x(y+z) - yz] \pmod{p}\\ &\equiv -(y-z)(x^2+yz),\\ &\not\equiv 0, \text{ by hypothesis.}\end{aligned}$$

Hence

$$\left\{\frac{\alpha}{r}\right\} = 1,$$

and from (6)

$$r^{p-1} \equiv 1 \pmod{p^2}.$$

On the other hand if yz is not prime to p, either y or z must be divisible by p. Assuming z to be divisible and recalling the arguments in the corresponding case in Theorem I, we have immediately the following relations:

$$\left\{\frac{x+y\alpha}{r}\right\} = \left\{\frac{1-\alpha}{r}\right\}, \quad \left\{\frac{x+z\alpha^{-1}}{r}\right\} = 1,$$

and

$$\left\{\frac{y\alpha+z\alpha^{-1}}{r}\right\} = \left\{\frac{\alpha}{r}\right\}\left\{\frac{y+z\alpha^{-2}}{r}\right\} = \left\{\frac{\alpha}{r}\right\}.$$

From the above and from (8), we obtain

$$\left\{\frac{1-\alpha}{r}\right\} = \left\{\frac{\alpha}{r}\right\},$$

and from (7) it follows that

$$r^{p-1} \equiv 1 \pmod{p^2}.$$

As before, a similar proof obtains when y is divisible by p.

OTTAWA, CANADA

ON THE SOLUTION OF THE EULER EQUATIONS FOR THEIR HIGHEST DERIVATIVES*

BY H. V. CRAIG

1. *Introduction.* J. H. Taylor† has given two elegant methods of solving for their highest derivatives the Euler equations associated with the integral $\int F(x, \dot{x})dt$. In this paper these two methods are modified so as to apply to the more general case in which the Euler equations contain derivatives of order higher than the second.

2. *Notation.* Throughout this paper we shall employ vector notation and shall use dots and enclosed superscripts to indicate differentiation with respect to the parameter. Thus x, $\dot{x}$, $x^{(m)}$ will stand for the sets

$$x^1, x^2, \cdots, x^n; \quad \frac{dx^1}{dt}, \frac{dx^2}{dt}, \cdots, \frac{dx^n}{dt}; \quad \frac{d^m x^1}{dt^m}, \frac{d^m x^2}{dt^m}, \cdots, \frac{d^m x^n}{dt^m},$$

respectively. Partial derivatives will be denoted by means of subscripts, thus

---

* Presented to the Society, September 7, 1928. This paper is a part of a thesis written at the University of Wisconsin under the direction of Professor J. H. Taylor.

† J. H. Taylor, *The reduction of Euler's equations to a canonical form*, this Bulletin, vol. 31 (1925) p. 257.