# APPLICATION OF THE THEORY OF RELATIVE CYCLIC FIELDS TO BOTH CASES OF FERMAT'S LAST THEOREM

BY

H. S. VANDIVER*

If, for $p$ an odd prime,

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

is satisfied in integers of $x$, $y$, and $z$ prime to each other, $z \not\equiv 0 \pmod{p}$, then in another paper† I gave the relation

$$\prod_{\nu=1}^{k-1} \prod_{r=1}^{[\nu p/k]} (x + \alpha^{[1:r]} y) = \alpha^{-kyq(k)/(x+y)} \omega^p, \tag{2}$$

where $k$ is an integer, $1 < k < p$;

$$q(k) = \frac{k^{p-1} - 1}{p};$$

$[s]$ is the greatest integer in $s$; $\omega$ is an integer in the field $\Omega(\alpha)$, $\alpha = e^{2i\pi/p}$; $[1 : r]$ is the integer $i$ in the relation $ri \equiv 1 \pmod{p}$, and if a fraction $f/g$ occurs as an exponent of $\alpha$, then that exponent is the integer $u$ in the relation $f \equiv gu \pmod{p}$.

In the present paper I shall develop a new line of attack on the Last Theorem by the introduction of power characters in the field $\Omega(e^{2i\pi/ph})$, $h$ prime to $p$, in connection with (2).

1. Let $n$ be a prime $\not\equiv 0$ or $1 \pmod{p}$ and suppose that $xyz \not\equiv 0 \pmod{n}$; then

$$x^{n-1} - y^{n-1} \equiv 0 \pmod{n}. \tag{3}$$

If $\beta$ is a primitive $(n-1)$th root of unity then in the field $\Omega(\beta)$ we have

$$(n) = \mathfrak{q}_1 \mathfrak{q}_2 \cdots \mathfrak{q}_{\varphi(n-1)}$$

where the $\mathfrak{q}$'s are distinct prime ideals, and $\varphi(n-1)$ is the indicator of $n-1$. We may take as one of the $\mathfrak{q}$'s the ideal

$$\mathfrak{q} = (\beta - r, n)$$

* Presented to the Society, September 11, 1925; received by the editors in December, 1925.

† Annals of Mathematics, ser. 2, vol. 21 (1919), p. 78.

where $r$ is a primitive root of $n$. Then (3) gives

$$\prod_{s=0}^{n-2} (x + \beta^s y) \equiv 0 \pmod{\mathfrak{q}} ;$$

hence there is an integer $a$ in the set 1, 2, $\cdots$, $n$–2, such that

$$x + \beta^\alpha y \equiv 0 \pmod{\mathfrak{q}} \tag{4}$$

if we note that $x+y \not\equiv 0 \pmod{\mathfrak{q}}$ since $z \not\equiv 0 \pmod{n}$. Now in the field $\Omega(\alpha\beta)$ we have, if $\theta$ is any integer such that $(\theta)$ is prime to $(p)$ and the ideal prime $\mathfrak{p}$, with $\mathfrak{p}$ also prime to $(p)$, if $c = N(\mathfrak{p}) - 1$,

$$\theta^c \equiv 1 \pmod{\mathfrak{p}},$$

$N(\mathfrak{p})$ being the norm of $\mathfrak{p}$, by Fermat's generalized theorem, and consequently there is an integer $s$ such that

$$\theta^{c/p} \equiv \alpha^s \pmod{\mathfrak{p}}$$

since $N(\mathfrak{p}) \equiv 1 \pmod{p}$. Set

$$\left\{\frac{\theta}{\mathfrak{p}}\right\} = \alpha^s.$$

It follows that $\theta$ is congruent to the $p$th power of an integer in $\Omega(\alpha\beta)$ if and only if

$$\left\{\frac{\theta}{\mathfrak{p}}\right\} = 1.$$

If the ideal $\mathfrak{P} = \mathfrak{p}_1'\mathfrak{p}_2' \cdots \mathfrak{p}_c'$ then we use as definition

$$\left\{\frac{\theta}{\mathfrak{P}}\right\} = \left\{\frac{\theta}{\mathfrak{p}_1'}\right\}\left\{\frac{\theta}{\mathfrak{p}_2'}\right\} \cdots \left\{\frac{\theta}{\mathfrak{p}_c'}\right\},$$

the $\mathfrak{p}$'s being prime ideals in $\Omega(\alpha\beta)$. It follows from the definition that if $\psi$ is an integer in the field $\Omega(\beta)$, then since $n-1 \not\equiv 0 \pmod{p}$,

$$\left\{\frac{\psi}{\mathfrak{Q}}\right\} = 1, \tag{4a}$$

$\mathfrak{Q}$ being an ideal in $\Omega(\beta)$, and if $\zeta$ is an integer in $\Omega(\alpha\beta)$ and $\zeta_i$ denotes the integer obtained by the substitution $(\alpha/\alpha^i)$, $i$ prime to $p$, then

$$\left\{\frac{\zeta_i}{\mathfrak{Q}}\right\} = \left\{\frac{\zeta}{\mathfrak{Q}}\right\}^i. \tag{4b}$$

Let

$$\mathfrak{q} = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_d,$$

the $\mathfrak{p}$'s being prime ideals in $\Omega(\alpha\beta)$.

We shall now show that

$$\left\{\frac{\alpha}{\mathfrak{q}}\right\} = \alpha^{q(n)}. \tag{4c}$$

Let

$$N(\mathfrak{p}_1) = 1 + w_1 p,$$
$$N(\mathfrak{p}_2) = 1 + w_2 p,$$
$$\cdots \qquad \cdots$$
$$N(\mathfrak{p}_d) = 1 + w_d p;$$

multiplication gives

$$N(\mathfrak{q}) \equiv 1 + p \sum w \pmod{p^2}, \quad \frac{N(\mathfrak{q}) - 1}{p} \equiv \sum w \pmod{p}.$$

But $w_s = (N(\mathfrak{p}_s) - 1)/p$, so that

$$\frac{N(\mathfrak{q}) - 1}{p} \equiv \sum_{s=1}^{d} \frac{N(\mathfrak{p}_s) - 1}{p} \pmod{p},$$

and (4c) follows immediately from

$$\left\{\frac{\alpha}{\mathfrak{q}}\right\} = \prod_{s=1}^{d} \left\{\frac{\alpha}{\mathfrak{p}_s}\right\},$$

since

$$\left\{\frac{\alpha}{\mathfrak{q}}\right\} = \alpha^{c/p};$$

and

$$N(\mathfrak{q}) = n^{p-1}.$$

Now take power characters of each member of (2) with respect to $\mathfrak{q}$, and since $\mathfrak{q}$ is prime to $(p)$ and $(z)$ and therefore to $(x+\alpha^e y)$, we have

$$\prod_{\nu=1}^{k-1} \prod_{r=1}^{[\nu p/k]} \left\{\frac{x + \alpha^{[1:r]} y}{\mathfrak{q}}\right\} = \left\{\frac{\alpha}{\mathfrak{q}}\right\}^{-k\nu q(k)/(x+y)} \tag{5}$$

Now also by (4)

$$\{(x + \alpha^e y)/\mathfrak{q}\} = \{(x + \beta^a y + y(\alpha^e - \beta^a))/\mathfrak{q}\} = \{y/\mathfrak{q}\}\{(\alpha^e - \beta^a)/\mathfrak{q}\}.$$

By (4a)

$$\left\{\frac{y}{\mathfrak{q}}\right\} = 1,$$

so that

$$\left\{\frac{x+\alpha^e y}{\mathfrak{q}}\right\} = \left\{\frac{\alpha^e - \beta^a}{\mathfrak{q}}\right\}.$$

We also have by (4b)

$$\left\{\frac{\alpha^a - \beta^a}{\mathfrak{q}}\right\} = \left\{\frac{\alpha - \beta^a}{\mathfrak{q}}\right\}^e.$$

Applying these relations to (5) we obtain with (4c)

$$\left\{\frac{\alpha - \beta^a}{\mathfrak{q}}\right\}^{\Sigma[1:r]} = \alpha^{-kyq(k)q(n)/(x+y)},$$

and since*

$$-kq(k) \equiv \sum [1:r] \qquad (\bmod p),$$

we have

$$\left\{\frac{\alpha - \beta^a}{\mathfrak{q}}\right\}^{-kq(k)} = \alpha^{-kyq(k)q(n)/(x+y)}.$$

For $k=p-1$ we have $q(k)\not\equiv 0 \pmod p$ so that

$$\left\{\frac{\alpha - \beta^a}{\mathfrak{q}}\right\} = \alpha^{yq(n)/(x+y)},$$

or since

$$\left\{\frac{\beta^{-a}}{\mathfrak{q}}\right\} = 1,$$

then

$$\left\{\frac{\alpha\beta^{-a} - 1}{\mathfrak{q}}\right\} = \alpha^{yq(n)/(x+y)}. \qquad (6)$$

Note that $(\alpha\beta^{-a}-1)$ is a unit in $\Omega(\alpha\beta)$.

If we write

$$\left\{\frac{\alpha\beta^{-a} - 1}{\mathfrak{q}}\right\} = \alpha^i$$

and $i=\operatorname{ind}(\alpha\beta^{-a}-1)$, then (6) shows that for some value of $a$ included in the set $1, 2, \cdots, n-2$,

$$\operatorname{ind}(\alpha\beta^a - 1) - \frac{yq(n)}{x+y} \equiv 0 \qquad (\bmod p). \qquad (7)$$

* Vandiver, loc. cit., p. 77, relations 17.

This is equivalent to the relation

$$(7a)\qquad \prod_{a=1}^{n-2} \left(\text{ind}\,(\alpha\beta^a - 1) - \frac{y}{x+y}\, q(n)\right) \equiv 0 \pmod{p}.$$

2. Let us now consider the first case of Fermat's Last Theorem; that is, when $xyz \not\equiv 0 \pmod{p}$. Let $-x/y = t$; then it follows from (1) that the relation

$$(8)\qquad \prod_{a=1}^{n-2} ((1 - v)\,\text{ind}\,(\alpha\beta^a - 1) - q(n)) \equiv 0 \pmod{p}$$

holds if $v$ has any of the six values

$$(9)\qquad t,\quad 1 - t,\quad \frac{1}{t},\quad \frac{1}{1-t},\quad \frac{t}{t-1},\quad \frac{t-1}{t}.$$

This criterion for (1) when $xyz \not\equiv 0 \pmod{p}$ was obtained under the assumption that $xyz$ was prime to $n$. If either $x$, $y$ or $z$ is divisible by $n$, then it follows by Furtwängler's theorem* that $q(n) \equiv 0 \pmod{p}$. We may then state

THEOREM I. *If $x^p + y^p + z^p = 0$ is satisfied in integers none zero and all prime to the odd prime $p$, $v$ is any number in the set* (9), *then for* $\alpha = e^{2i\pi/p}$, $\beta = e^{2i\pi/(n-1)}$

$$q(n) \prod_{a=1}^{n-2} ((1 - v)\,\text{ind}\,(\alpha\beta^a - 1) - q(n)) \equiv 0 \pmod{p},$$

*where* $\mathfrak{q} = (\beta - r, n)$, *$r$ is a primitive root of $n$*,

$$\left\{\frac{\alpha\beta^a - 1}{\mathfrak{q}}\right\} = \alpha^i, \quad q(n) = \frac{n^{p-1} - 1}{p},$$

$i = \text{ind}\,(\alpha\beta^a - 1)$, *and $n$ is a prime* $\not\equiv 0$ *or* $1 \pmod{p}$.

The relation (7) is equivalent to

$$(10)\qquad (1 - t)\,\text{ind}\,(\alpha\beta^a - 1) - q(n) \equiv 0 \pmod{p}.$$

Because of (9), there is also an integer $b$ in the set $1, 2, \cdots, n-2$ such that

$$(11)\qquad t\,\text{ind}\,(\alpha\beta^b - 1) - q(n) \equiv 0 \pmod{p}.$$

Eliminating $t$ from (10) and (11) gives

$$\text{ind}\,(\alpha\beta^a - 1)\,\text{ind}\,(\alpha\beta^b - 1) - q(n)(\text{ind}\,(\alpha\beta^a - 1) + \text{ind}\,(\alpha\beta^b - 1)) \equiv 0 \pmod{p}.$$

This gives

---

* Wiener Berichte, IIa, 1912, 589–92.

THEOREM II. *If $x^p+y^p+z^p=0$ is satisfied in integers none zero and all prime to the odd prime $p$, then*

$$q(n) \prod_{a,b} (\operatorname{ind}(\alpha\beta^a - 1)\operatorname{ind}(\alpha\beta^b - 1)$$
$$- q(n)(\operatorname{ind}(\alpha\beta^a - 1) + \operatorname{ind}(\alpha\beta^b - 1)) \equiv 0 \pmod{p},$$

*where $a$ and $b$ each range independently over the integers* 1, 2, $\cdots$, $n-2$, *the other symbols being defined as in Theorem* I.

It will be noted that these criteria are independent of $x$, $y$ and $z$.

For $n=3$, $\mathfrak{q}=(3)$, and

$$\left\{\frac{\alpha\beta-1}{3}\right\} = \left\{\frac{-\alpha-1}{3}\right\} = \left\{\frac{\alpha+1}{3}\right\} = \left\{\frac{\alpha^{\frac{1}{2}}}{3}\right\}\left\{\frac{\alpha^{\frac{1}{2}}+\alpha^{-\frac{1}{2}}}{3}\right\} = \left\{\frac{\alpha^{\frac{1}{2}}}{3}\right\} = \alpha^{q(3)/2}.$$

Using this in connection with the criteria of Theorem II, we have

$$q(3)\left(\frac{1}{4}(q(3))^2 - 2\cdot\frac{1}{2}(q(3))^2\right) \equiv 0 \pmod{p},$$

whence $q(3)\equiv 0 \pmod{p}$ assuming $p>3$.

Take $n=5$; then $n-1=4$ and $\Omega(\beta)$ is the field $\Omega(i)$ and we may set $\mathfrak{q}=(2-i)$. We have

$$(x-y)(x^2+y^2) \equiv 0 \pmod{5}$$

and similarly for $(x, z)$, $(z, y)$ in lieu of $(x, y)$. It then follows easily that one of the integers $x-y$, $x-z$, $y-z$ is divisible by 5. If $x-y\equiv 0 \pmod{5}$ it follows from (7) that $q(5)\equiv 0 \pmod{p}$ unless $x-y\equiv 0 \pmod{p}$. This is equivalent to the condition that the set (9) satisfies

$$q(5)(t+1)(t-2)(t-\tfrac{1}{2}) \equiv 0 \pmod{p}. \tag{12}$$

Theorem I also gives

$$q(5)\prod_{a=1}^{3}\left((1-t)\operatorname{ind}(\alpha\beta^a - 1) - q(5)\right) \equiv 0 \pmod{p}. \tag{13}$$

As in the case $n=3$ we find

$$\left\{\frac{\alpha\beta^2-1}{\mathfrak{q}}\right\} = \alpha^{q(5)/2}.$$

Hence if we write

$$\operatorname{ind}(\alpha\beta^a - 1) = I_a$$

we have from (13)

$$q(5)(t+1)\left((1-t)I_1 - q(5)\right)\left((1-t)I_3 - q(5)\right) \equiv 0 \pmod{p}. \tag{14}$$

Now also

$$I_1 + I_3 = \text{ind}\,(\alpha^2 + 1) \equiv q(5) \qquad (\text{mod } p),$$

so that

$$(14a) \qquad I_3 \equiv q(5) - I_1 \qquad (\text{mod } p).$$

Comparing (12) and (14) it follows that

$$q(5)\big((1 - t)I_1 - q(5)\big)\big((1 - t)I_3 - q(5)\big) \equiv 0 \qquad (\text{mod } p)$$

for $t=2$ and $t=\frac{1}{2}$, and these values give in each case, using (14a),

$$q(5)\big(I_1 + q(5)\big)\big((I_1 - 2q(5)\big) \equiv 0 \qquad (\text{mod } p).$$

3. We shall now consider the second case of the Last Theorem. In (7a) assume $y \equiv 0 \pmod p$; then we obtain

$$\prod_{a=1}^{n-2} \text{ind}\,(\alpha\beta^a - 1) \equiv 0 \qquad (\text{mod } p),$$

under the assumption that $x$, $y$ and $z$ are each prime to $n$. If $x$ or $z$ is divisible by $n$ then $q(n) \equiv 0 \pmod p$, but this does not necessarily hold when $y \equiv 0 \pmod n$. Hence

THEOREM III. *If $p$ is an odd prime and $x^p + y^p + z^p = 0$ is satisfied in integers, none zero, $y \equiv 0 \pmod p$, with $xz \not\equiv 0 \pmod p$, then either $y \equiv 0 \pmod n$ or*

$$q(n) \prod_{a=1}^{n-2} \text{ind}\,(\alpha\beta^a - 1) \equiv 0 \qquad (\text{mod } p),$$

*the symbols being defined as in Theorem* I.

UNIVERSITY OF TEXAS,
AUSTIN, TEX.