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,

\[ x^p + y^p + z^p = 0 \]

is satisfied in integers of \( x, y, \) and \( z \) prime to each other, \( z \equiv 0 \pmod{p} \), then in another paper† I gave the relation

\[ \prod_{i=1}^{k-1} \prod_{r=1}^{k} \left( x + \alpha^{(1: r)} y \right) = \alpha^{-k\psi/k}/(z^p) \omega_p, \]

where \( k \) is an integer, \( 1 < k < p \);

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

\([s]\) is the greatest integer in \( s \); \( \omega \) is an integer in the field \( \Omega(\alpha) \), \( \alpha = e^{2\pi i/p} \); \( [1 : r] \) 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 \( \Omega(e^{2\pi i/h}) \), \( h \) prime to \( p \), in connection with (2).

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

\[ x^{n-1} - y^{n-1} = 0 \pmod{n}. \]

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

\[ (n) = q_1q_2 \cdots q_{\varphi(n-1)} \]

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

\[ q = (\beta - r, n) \]

* Presented to the Society, September 11, 1925; received by the editors in December, 1925.
where \( r \) is a primitive root of \( n \). Then (3) gives
\[
\prod_{s=0}^{n-2} (x + \beta^s y) \equiv 0 \pmod{q};
\]
hence there is an integer \( a \) in the set \( 1, 2, \ldots, n-2 \), such that
\[
(4) \quad x + \beta^a y \equiv 0 \pmod{q}
\]
if we note that \( x+y \not\equiv 0 \pmod{q} \) since \( x \not\equiv 0 \pmod{n} \). 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 \( p \), with \( p \) also prime to \( (p) \), if \( c = N(p) - 1 \),
\[
\theta^c \equiv 1 \pmod{p},
\]
\( N(p) \) being the norm of \( p \), by Fermat’s generalized theorem, and consequently there is an integer \( s \) such that
\[
\theta^{s^p} \equiv \alpha^s \pmod{p}
\]
since \( N(p) \equiv 1 \pmod{p} \). Set
\[
\left\{ \begin{array}{c} \theta \\ p \end{array} \right\} = \alpha^s.
\]
It follows that \( \theta \) is congruent to the \( p \)th power of an integer in \( \Omega(\alpha\beta) \) if and only if
\[
\left\{ \begin{array}{c} \theta \\ p \end{array} \right\} = 1.
\]
If the ideal \( \Psi = p_1'p_2' \cdots p_s' \) then we use as definition
\[
\left\{ \begin{array}{c} \theta \\ \Psi \end{array} \right\} = \left\{ \begin{array}{c} \theta \\ p_1' \end{array} \right\} \left\{ \begin{array}{c} \theta \\ p_2' \end{array} \right\} \cdots \left\{ \begin{array}{c} \theta \\ p_s' \end{array} \right\},
\]
the \( p \)'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 \( n-1 \not\equiv 0 \pmod{p} \),
\[
(4a) \quad \left\{ \begin{array}{c} \psi \\ \Omega \end{array} \right\} = 1,
\]
\( \Omega \) being an ideal in \( \Omega(\beta) \), and if \( \xi \) is an integer in \( \Omega(\alpha\beta) \) and \( \xi \) denotes the integer obtained by the substitution \( (\alpha/\alpha^i) \), \( i \) prime to \( p \), then
\[
(4b) \quad \left\{ \begin{array}{c} \xi \\
\Omega \end{array} \right\} = \left\{ \begin{array}{c} \xi \\ \Omega \end{array} \right\}^i.
\]
Let
\[
q = p_1p_2 \cdots p_d,
\]
the \( p \)'s being prime ideals in \( \Omega(\alpha\beta) \).

We shall now show that

\[
\left( \frac{\alpha}{q} \right) = \alpha^{q(n)}.
\]

\text{(4c)}

Let

\[
N(p_1) = 1 + w_1 p,
\]
\[
N(p_2) = 1 + w_2 p,
\]
\[
\ldots \quad \ldots \quad \ldots
\]
\[
N(p_d) = 1 + w_d p;
\]

multiplication gives

\[
N(q) = 1 + p \sum w \quad \text{(mod } p^2), \quad \frac{N(q) - 1}{p} = \sum w \quad \text{(mod } p).
\]

But \( w_s = (N(p_s) - 1)/p \), so that

\[
\frac{N(q) - 1}{p} = \sum_{s=1}^{d} \frac{N(p_s) - 1}{p} \quad \text{(mod } p),
\]

and \( \text{(4c)} \) follows immediately from

\[
\left\{ \frac{\alpha}{q} \right\} = \prod_{s=1}^{d} \left\{ \frac{\alpha}{p_s} \right\},
\]

since

\[
\left\{ \frac{\alpha}{q} \right\} = \alpha^{q/p};
\]

and

\[
N(q) = n^{p-1}.
\]

Now take power characters of each member of \( \text{(2)} \) with respect to \( q \), and since \( q \) is prime to \( \phi \) and \( \sigma \) and therefore to \( (x+\alpha^s y) \), we have

\[
\prod_{r=1}^{k-1} \prod_{s=1}^{[p/k]} \left\{ \frac{x+\alpha^{[1: r]} y}{q} \right\} = \left\{ \frac{\alpha}{q} \right\}^{b y q (k)/(x^e + \beta^s)}
\]

\text{(5)}

Now also by \( \text{(4)} \)

\[
\left\{ (x + \alpha^s y)/q \right\} = \left\{ (x + \beta^s y + y(\alpha^s - \beta^s))/q \right\} = \left\{ y/q \right\} \left\{ (\alpha^s - \beta^s)/q \right\}.
\]

By \( \text{(4a)} \)

\[
\left\{ \frac{y}{q} \right\} = 1,
\]
so that
\[ \left\{ \frac{x + \alpha^a y}{q} \right\} = \left\{ \frac{\alpha^a - \beta^a}{q} \right\}. \]

We also have by (4b)
\[ \left\{ \frac{\alpha^a - \beta^a}{q} \right\} = \left\{ \frac{\alpha - \beta}{q} \right\}^a. \]

Applying these relations to (5) we obtain with (4c)
\[ \left\{ \frac{\alpha - \beta}{q} \right\}^2 \equiv \frac{1}{\alpha^{q^a - q^a}} = \alpha^{-kq(k)q(n)/(x+y)}, \]
and since
\[ - kq(k) = \sum [1:r] \quad \text{(mod } p), \]
we have
\[ \left\{ \frac{\alpha - \beta}{q} \right\}^{-kq(k)} = \alpha^{-kq(k)q(n)/(x+y)}. \]

For \( k = p-1 \) we have \( q(k) \neq 0 \) (mod \( p \)) so that
\[ \left\{ \frac{\alpha - \beta}{q} \right\} = \alpha^{q^a/(x+y)}, \]
or since
\[ \left\{ \frac{\beta^a}{q} \right\} = 1, \]
then
\[ \left\{ \frac{\alpha^{q^a} - 1}{q} \right\} = \alpha^{q^a/(x+y)}. \]

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

If we write
\[ \left\{ \frac{\alpha^{q^a} - 1}{q} \right\} = \alpha^i \]
and \( i = \text{ind} (\alpha^{q^a} - 1) \), then (6) shows that for some value of \( a \) included in the set \( 1, 2, \cdots, n-2, \)
\[ \text{ind}(\alpha^{q^a} - 1) - \frac{yq(n)}{x+y} \equiv 0 \quad \text{(mod } p). \]

* Vandiver, loc. cit., p. 77, relations 17.
This is equivalent to the relation

\[ \prod_{a=1}^{n-2} (1 - v) \text{ind} (\alpha^a - 1) - q(n) \equiv 0 \pmod{p}. \]  

(7a)

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

\[ \prod_{a=1}^{n-2} ((1 - v) \text{ind} (\alpha^a - 1) - q(n)) \equiv 0 \pmod{p}. \]

(8)

holds if \(v\) has any of the six values

\[ t, 1 - t, \frac{1}{t}, \frac{1}{1 - t}, \frac{t}{t - 1}, \frac{t - 1}{t}. \]

(9)

This criterion for (1) when \(xyz \neq 0 \pmod{p}\) 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 \(\alpha = e^{2i\pi/n}\), \(\beta = e^{2i\pi/(n-1)}\)

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

where \(q = (\beta - r, n), r\) is a primitive root of \(n\),

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

\(i = \text{ind} (\alpha^a - 1),\) and \(n\) is a prime \(\equiv 0\) or \(1 \pmod{p}\).

The relation (7) is equivalent to

\[ (1 - t) \text{ind} (\alpha^a - 1) - q(n) \equiv 0 \pmod{p}. \]

(10)

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

\[ t \text{ind} (\alpha^b - 1) - q(n) \equiv 0 \pmod{p}. \]

(11)

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

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

This gives

\[ * \text{Wiener Berichte, Ia, 1912, 589-92.} \]
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

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

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

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

For $n=3$, $q=(3)$, and

$$\left\{ \begin{array}{c} \alpha^1 - 1 \\ 3 \end{array} \right\} = \left\{ \begin{array}{c} -\alpha - 1 \\ 3 \end{array} \right\} = \left\{ \begin{array}{c} \alpha + 1 \\ 3 \end{array} \right\} = \left\{ \begin{array}{c} \alpha^1 + \alpha^{-1} \\ 3 \end{array} \right\} = \left\{ \begin{array}{c} \alpha^4 \\ 3 \end{array} \right\} = \alpha^{q(3)/2}.$$

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 $q=(2-i)$. 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

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

Theorem I also gives

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

As in the case $n=3$ we find

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

Hence if we write

$$\text{ind} (\alpha^a - 1) = I_a,$$

we have from (13)

$$q(5)(t + 1)((1 - t)I_1 - q(5))((1 - t)I_2 - q(5)) \equiv 0 \pmod{p}.$$
Now also
\[ I_1 + I_3 = \text{ind} (\alpha^2 + 1) = q(5) \pmod{\psi}, \]
so that
\[ I_3 = q(5) - I_1 \pmod{\psi}. \]
Comparing (12) and (14) it follows that
\[ q(5)((1 - t)I_1 - q(5))(1 - t)I_3 - q(5) \equiv 0 \pmod{\psi} \]
for \( t = 2 \) and \( t = \frac{1}{2} \), and these values give in each case, using (14a),
\[ q(5)(I_1 + q(5))((I_1 - 2q(5)) = 0 \pmod{\psi}. \]

3. We shall now consider the second case of the Last Theorem. In
(7a) assume \( y \equiv 0 \pmod{\psi} \); then we obtain
\[ \prod_{a=1}^{n-2} \text{ind} (\alpha^a - 1) \equiv 0 \pmod{\psi}, \]
under the assumption that \( x, y \) and \( z \) are each prime to \( n \). If \( x \) or \( z \) is divisible
by \( n \) then \( q(n) \equiv 0 \pmod{\psi} \), but this does not necessarily hold when \( y \equiv 0 \)
\( \pmod{\psi} \). Hence

**Theorem III.** If \( p \) is an odd prime and \( x^p + y^p + z^p = 0 \) is satisfied in integers, none zero, \( y \equiv 0 \pmod{\psi} \), with \( x \neq 0 \pmod{\psi} \), then either \( y \equiv 0 \pmod{n} \) or
\[ q(n) \prod_{a=1}^{n-2} \text{ind} (\alpha^a - 1) \equiv 0 \pmod{\psi}, \]
the symbols being defined as in Theorem I.

**University of Texas,**
**Austin, Tex.**