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

(SECOND PAPER)

BY

H. S. VANDIVER

In my first paper under the present title I gave criteria in connection with both cases of the Last Theorem. Here by extensions of the methods previously employed, I shall obtain more general criteria. If

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

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

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

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

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

$[s]$ is the greatest integer in s; ω is an integer in the field $\Omega(\alpha)$; $\alpha = e^{2i\pi/p}$; $[1:r]$ is the integer i in the relation $ri \equiv 1 \pmod{p}$. Also, throughout the paper, if a fraction a/b appears as the exponent of α, it stands for an integer u which satisfies $a \equiv bu \pmod{p}$.

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

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

If β is a primitive $(n-1)$th root of unity then in the field $\Omega(\alpha\beta)$ we have, since $n-1$ is prime to p,

$$(n) = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_e,$$

where

$$\phi((n-1)p) = ef, \quad n^f \equiv 1 \pmod{(n-1)p}$$

---

* Presented to the Society, January 1, 1926; received by the editors February 6, 1926.

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

the $\mathfrak{p}$'s being prime ideals in the field $\Omega(\alpha\beta)$, of degree f. The relation (3) gives

$$\sum_{s=0}^{n-2}(x+\beta^s y) \equiv 0 \pmod{(n)}$$

$$\equiv 0 \pmod{\mathfrak{p}}$$

hence there is an integer in the set $0, 1, \cdots, n-2$, such that

$$x+\beta^a y \equiv 0 \pmod{\mathfrak{p}}. \tag{4}$$

It is known that if (θ) is an ideal in $\Omega(\alpha\beta)$ prime to (p) and $\mathfrak{p}$, θ an integer in $\Omega(\alpha\beta)$, then there is an integer s such that, if $w = N(\mathfrak{p})-1$,

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

where $N(\mathfrak{p})=n^f$, the norm of $\mathfrak{p}$. Also θ is congruent to the pth power of an integer $\Omega(\alpha\beta)$ if and only if

$$\left\{\frac{\theta}{\mathfrak{p}}\right\} = 1, \text{ where } \left\{\frac{\theta}{\mathfrak{p}}\right\} = \alpha^s, \text{ in general.}$$

Since (n) is prime to (p) then $\mathfrak{p}$ is prime to (p) and $\mathfrak{p}$ is also prime to $(x+\alpha^c y)$, $c \not\equiv 0 \pmod{p}$, since the norm of $x+\alpha^c y$ has all its factors of the form $1+wp$. Consequently we may set α^m for α in (2), m any integer $\not\equiv 0 \pmod{p}$, and take pth power characters of each member of (2) with respect to $\mathfrak{p}$, which gives

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

We may write

$$\left\{\frac{x+\alpha^c y}{\mathfrak{p}}\right\} = \left\{\frac{x+\beta^a y + y(\alpha^c-\beta^a)}{\mathfrak{p}}\right\}$$

and by (4) the right hand member reduces to

$$\left\{\frac{y(\alpha^c-\beta^a)}{\mathfrak{p}}\right\} = \left\{\frac{y}{\mathfrak{p}}\right\}\left\{\frac{\alpha^c-\beta^a}{\mathfrak{p}}\right\}.$$

Now

$$y^{w/p} = y^{(n-1)d} \equiv 1 \pmod{n},$$

since $N(\mathfrak{p})-1$ is divisible by $n-1$ but $n-1$ is prime to p. Hence

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

and therefore

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

Applying this to (5) and using the notation

$$\left\{\frac{\theta}{\mathfrak{p}}\right\} = \alpha^{I(\theta)},$$

we have, if we set

$$\sum \text{ for } \sum_{r=1}^{k-1} \sum_{r=1}^{[rp/k]},$$

$$\sum I(\alpha^{m[1:r]} - \beta^a) \equiv -\frac{mkyq(k)}{x+y} I(\alpha) \pmod{p}. \tag{6}$$

Set

$$D_s = \sum_{d=1}^{p-1} d^s I(\alpha^d - \beta^a).$$

To determine $I(\alpha^c-\beta^a)$ in terms of the D's, let d_1 be any of the integers $1, 2, \cdots, p-1$ and consider the sum

$$\sum_{s=0}^{p-2} \sum_{d=1}^{p-1} d_1^{p-1-s} d^s I(\alpha^d - \beta^a),$$

which may be put in the form

$$(p-1)\, I(\alpha^{d_1} - \beta^a) + \sum_{d_1 \neq d} d_1 \frac{d_1^{p-1} - d^{p-1}}{d_1 - d} I(\alpha^d - \beta^a) \pmod{p},$$

whence

$$-I(\alpha^d - \beta^a) \equiv D_0 + d^{p-2}D_1 + d^{p-3}D_2 + \cdots + dD_{p-2},$$

modulo p. Applying this to (6) we may write, if $\mu = (p-1)/2$,

$$\begin{aligned} &\mu(k-1)D_0 m^{p-1} + \sum (m[1:r])^{p-2} D_1 \\ &+ \sum (m[1:r])^{p-3} D_2 + \cdots + m\left(\sum [1:r] D_{p-2} - \frac{kyq(k)}{x+y} I(\alpha)\right) \equiv 0, \end{aligned} \tag{7}$$

modulo p. Let m range over the integers $1, 2, \cdots, p-1$. We obtain, from (7), $(p-1)$ congruences and since the determinant

$$\begin{vmatrix} 1 & 1 & 1 & \cdots & 1 \\ 2 & 2^2 & 2^3 & \cdots & 2^{p-1} \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ p-1 & (p-1)^2 & (p-1)^3 & \cdots & (p-1)^{p-1} \end{vmatrix} = \prod_{i,j}^{1\cdots p-1} (i-j)(p-1)!, \qquad i > j,$$

is not divisible by p, we have, modulo p,

$$D_0 \equiv \sum [1:r]^{p-s} D_{s-1} \equiv 0 \pmod{p}$$

$$(s = 2,3, \cdots, p-2); \tag{8}$$

$$\sum [1:r] D_{p-2} - \frac{kyq(k)}{x+y} I(\alpha) \equiv 0 \pmod{p}.$$

But we also have*

$$\frac{(1-k^i)b_i}{k^{i-1}i} \equiv \sum [1:r]^{p-i} \pmod{p},$$

where $b_1 = -\frac{1}{2}$, $b_{2a} = (-1)^{a+1} B_a$, $b_{2a+1} = 0$ $(a>0)$, the B's being the numbers of Bernoulli, $B_1 = 1/6$, $B_2 = 1/30$, etc. Let k be a primitive root of p; then $k^l - 1 \not\equiv 0 \pmod{p}$, $l < p-1$, and also†

$$-kq(k) \equiv \sum [1:r] \pmod{p};$$

and since we may take another value of k to be $p-1$, we have $q(p-1) \not\equiv 0 \pmod{p}$, so that (8) becomes, modulo p, after division by $k^l - 1$ and $q(k)$,

$$D_0 \equiv b_{s+1} D_s \equiv 0 \qquad (s = 1,2, \cdots, p-3), \tag{8a}$$

$$D_{p-2} \equiv -\frac{y}{x+y} I(\alpha).$$

2. Now assume that in (1), y is divisible by p; then it is known that

$$\left(\frac{z + \alpha^l x}{1 - \alpha^l}\right) = \mathfrak{q}_l^p$$

where $\mathfrak{q}_l$ is an ideal in $\Omega(\alpha)$, $l \not\equiv 0 \pmod{p}$, and we also have‡

$$\prod \mathfrak{q}_{[1:h]} \sim 1,$$

* Annals of Mathematics, (2), vol. 18, p. 114, relation 11.

† Annals of Mathematics, (2), vol. 18, p. 114, relation 12.

‡ Annals of Mathematics, (2), vol. 21 (1919), p. 74.

where h ranges over the positive integers $h<p$ which satisfy $h+|rh|>p$, or, what is the same thing, the integers h such that, for $q=1, 2, \cdots, r$,

$$\frac{qp}{r+1} < h < \frac{qp}{r}, \quad 0 < r < p-1.$$

Here $|rh|$ is the least positive residue of rh, modulo p and $[1 : h]$ stands for the integer i in $hi \equiv 1 \pmod{p}$. Then following the same method employed in the article just cited in deriving (2) of the present paper we find with ω an integer in $\Omega(\alpha)$

$$\prod_h \left(\frac{z+\alpha^{[1:h]}x}{1-\alpha^{[1:h]}}\right)^{p-1} = \alpha^g \omega^{p(p-1)} \tag{9}$$

where g is some integer. Let the ideal $(\rho)=(1-\alpha)$ and reduce each side of (9) modulo (ρ^2). On the left we have

$$\frac{z+\alpha^{[1:h]}x}{1-\alpha^{[1:h]}} = \frac{z+x}{1-\alpha^{[1:h]}} - x \equiv -x \pmod{(\rho^2)},$$

since $z+x$ is divisible by p and $(p)=(\rho)^{p-1}$. Also

$$\alpha^g = (1-\rho)^g \equiv 1 - g\rho \pmod{(\rho^2)}.$$

Then (9) gives, since $\omega^{p(p-1)} \equiv 1 \pmod{(\rho^2)}$,

$$(-x)^{(p-1)\mu} \equiv 1 - g\rho \pmod{(\rho^2)};$$

or

$$g \equiv 0 \pmod{(\rho)},$$

and since g is rational,

$$g \equiv 0 \pmod{p},$$

so that (9) may be written in the form

$$\prod_h (z+\alpha^{[1:h]}x)^{p-1} = \prod_h (1-\alpha^{[1:h]})^{p-1}\omega_1^p, \tag{10}$$

$$\omega_1 = \omega^{p-1}.$$

Now if s is one of the h's then $p-s$ is not. Also

$$(1-\alpha^l) = \alpha^l(\alpha^{-l}-1)$$

so that

$$\prod_h (1-\alpha^{[1:h]}) = \alpha^{\Sigma[1:h]} \prod_h (\alpha^{-[1:h]}-1).$$

But

$$\prod_h (1-\alpha^{[1:h]})(\alpha^{-[1:h]}-1) = (-1)^\mu p,$$

and therefore

$$\prod_h (1 - \alpha^{[1:h]})^{p-1} = (-1)^{\mu^2} p^\mu \alpha^{\mu\Sigma[1:h]}.$$

Then (10) gives

$$\prod_h (z + \alpha^{[1:h]}x)^{p-1} = (-1)^{\mu^2} p^\mu \alpha^{\mu\Sigma[1:h]}\omega_1{}^p. \tag{11}$$

Now employ the same process on (11) as was used to derive (8a) from (2). Use the same ideal $\mathfrak{p}$ and take pth power characters in (11), noting that $\mathfrak{p}$ is prime to $(z+\alpha^c x)$, $c \not\equiv 0 \pmod p$. We have

$$\left\{\frac{p}{\mathfrak{p}}\right\} = 1,$$

since

$$p^{w/p} \equiv p^{(n-1)d} \equiv 1 \pmod n$$
$$\equiv 1 \pmod{\mathfrak{p}}$$

where d is an integer because $n-1 \not\equiv 0 \pmod p$. Also

$$\left\{\frac{-1}{\mathfrak{p}}\right\} = 1$$

since $N(\mathfrak{p})-1$ is even for n odd. Hence (11) gives

$$\prod_h \left\{\frac{z + \alpha^{[1:h]}x}{\mathfrak{p}}\right\}^2 = \left\{\frac{\alpha}{\mathfrak{p}}\right\}^{\Sigma[1:h]}. \tag{12}$$

Now as in (4) if $zy \not\equiv 0 \pmod n$ there is an integer b in the set $0, 1, \cdots, n-2$, such that $z+\beta^b y \equiv 0 \pmod{\mathfrak{p}}$, and (12) gives

$$\prod_h \left\{\frac{\alpha^{[1:h]} - \beta^b}{\mathfrak{p}}\right\}^2 = \left\{\frac{\alpha}{\mathfrak{p}}\right\}^{\Sigma[1:h]},$$

or putting α^m for α in (11)

$$2\sum I(\alpha^{m[1:h]} - \beta^b) \equiv m\sum [1:h] I(\alpha) \pmod p.$$

In the same way that (7) was obtained we find if

$$D_s' = \sum_{d=1}^{p-1} d^s I(\alpha^d - \beta^b),$$

$$\mu D_0' m^{p-1} + \sum_h (m[1:h])^{p-2} D_1' + \sum_h (m[1:h])^{p-3} D_2' + \cdots$$
$$+ m\left(\sum_h [1:h] D_{p-2}' + \frac{\sum[1:h] I(\alpha)}{2}\right) \equiv 0 \pmod p, \tag{13}$$

and in the same way that (8) was derived we have

$$D_0' \equiv \sum[1:h]^{p-s}D_{s-1}' \equiv 0 \pmod{p}$$

(13a) $$(s = 2,3,\cdots,p-2),$$

$$\sum[1:h]D_{p-2}' + \frac{\sum[1:h]I(\alpha)}{2} \equiv 0 \pmod{p}.$$

But also*

(13b) $$\sum[1:h]^{p-s} \equiv \frac{b_s(r^{p-s} - (r+1)^{p-s} + 1)}{s} \pmod{p},$$

(13c) $$\sum[1:h] \equiv -rq(r) + (r+1)q(r+1) \pmod{p}.$$

Hence, selecting r so that $r^{p-s}-(r+1)^{p-s}+1 \not\equiv 0 \pmod{p}$, and proceeding in a similar way with (13c) we obtain

$$D_0' \equiv 0,\ b_{s+1}D_s' \equiv 0 \pmod{p}$$

(14) $$(s = 1,2,\cdots,p-3);$$

$$2D_{p-2}' \equiv -I(\alpha) \pmod{p}.$$

3. Consider now the first case of the Last Theorem. The relations (8a) were derived under the assumption that xy was prime to n. By assumption x, y, and z are prime to each other. If one of these is divisible by n then $q(n)\equiv 0 \pmod{p}$ by Furtwängler's theorem. If $a=0$, or $(n-1)/2$, then the congruences $D_0 \equiv b_{s+1}D_s \equiv 0 \pmod{p}$ all vanish identically, that is, if $x \pm y \equiv 0 \pmod{n}$. Of the numbers x^2-y^2, x^2-z^2, and y^2-z^2 select one not divisible by p, which is always possible. Let x^2-y^2 be such a number, when, if n divides x^2-y^2, we have $q(n)\equiv 0 \pmod{p}$ by Furtwängler's theorem. Hence the

THEOREM I. *If*

$$x^p + y^p + z^p = 0$$

is satisfied in integers none zero and each prime to the odd prime p, then

$$q(n)D_0 \equiv 0,\ q(n)B_{(s+1)/2}D_s \equiv 0 \pmod{p}$$

$$(s = 1,3,\cdots,p-4);$$

where

$$D_s = \sum_{d=1}^{p-1} d^s I(\alpha^d - \beta^a), \qquad \left\{\frac{\theta}{\mathfrak{p}}\right\} = \alpha^{I(\theta)},$$

* Vandiver, Annals of Mathematics, (2), vol. 18 (1917), p. 114, relation (13) and the one immediately preceding.

$\mathfrak{p}$ is a prime ideal divisor of (n) in the field $\Omega(\alpha\beta)$, n being a rational odd prime, $\not\equiv 0$ or 1 (mod p),

$$\alpha = e^{2i\pi/p}\ ;\quad \beta = e^{2i\pi/(n-1)}\ ;$$

θ is any integer in the field $\Omega(\alpha\beta)$, such that (θ) is prime to $\mathfrak{p}$, a is some integer in the set $1, \cdots, n-2$, *other than* $(n-1)/2$; *the B's being the numbers of Bernoulli,* $B_1 = 1/6$, $B_2 = 1/30$, *etc.*

Note that the above criteria are independent of x, y and z.

Now consider again the relation (8a). If $z \equiv 0 \pmod{p}$ then $q(n) \equiv 0 \pmod{p}$, since $z \not\equiv 0 \pmod{p}$ by Furtwängler's theorem,* and we have

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

$$q(n) \sum_{a=1}^{n-2} ((1 - v)D_{p-2} + I(\alpha)) \equiv 0 \pmod{p},$$

where v has any one of the six values t, $1/t$, $1-t$, $1/(1-t)$, $(t-1)/t$, $t/(t-1)$; $-x/y = t$, the other symbols being defined as in Theorem I.

4. We now will treat the second case of the Last Theorem. Assume in (1) that y is divisible by p and that $xyz \not\equiv 0 \pmod{n}$; then (8a) holds with $D_{p-2} \equiv 0 \pmod{p}$. If xy is prime to n and $z \equiv 0 \pmod{n}$ then (8a) also holds. Suppose, however, that y is divisible by n; then (14) holds. If $x \equiv 0 \pmod{n}$ then a set of relations similar to (8a) hold. The relations (8a) and (14) vanish identically, however, if $a = 0$ or $(n-1)/2$; that is, if $x^2 - y^2$, $z^2 - y^2$ or $x^2 - z^2 \equiv 0 \pmod{n}$. Now suppose that $x + z \not\equiv 0 \pmod{n}$. If $x - z \equiv 0 \pmod{n}$ we may employ (8a) instead of (14), since if $x \pm y \equiv 0 \pmod{n}$ we have $q(n) \equiv 0 \pmod{p}$. Whence we have

THEOREM III. *If p is an odd prime and $x^p + y^p + z^p = 0$ with $y \equiv 0 \pmod{p}$ and $xz \not\equiv 0 \pmod{p}$, then either $x + z \equiv 0 \pmod{n}$ or*

$$q(n)D_0 \equiv 0,\ q(n)B_{(s+1)/2}D_s \equiv 0 \pmod{p} \qquad (s = 1, 3, \cdots, p-4),$$

and in addition one of the two relations

$$q(n)D_{p-2} \equiv 0,\ q(n)(D_{p-2} + I(\alpha)/2) \equiv 0 \pmod{p},$$

is satisfied, the other symbols being defined as in Theorem I.

---

* Wiener Sitzungsberichte, IIa, vol. 121 (1912), pp. 589–92.

In Theorems I and III, D_s may be shown to be divisible by p for particular values of s and n. For example, if n is a primitive root of p, it is easy to show that $D_s \equiv 0 \pmod{p}$, $s = 1, 3, \cdots, p-4$.

From Theorem II of this article it is possible to deduce Theorem I of the first paper under the present title,* but the proof is obviously much more complicated than that given in the first paper.

5. In all the theorems given here and in the first paper it was assumed that $n \not\equiv 1 \pmod{p}$. However it is also possible to give analogous results involving integers n which are of the form $1+wp$. In this case the field $\Omega(\beta)$ includes $\Omega(\alpha)$, and if we go through the same type of argument that was employed to obtain (8a) and (14) we note that $\{y/\mathfrak{p}\}$ is not necessarily unity. But we have

$$x+y=v^p,$$

where v is an integer, whence $y(1-\beta^a) \equiv v^p \pmod{\mathfrak{p}}$ and therefore

$$\left\{\frac{y}{\mathfrak{p}}\right\} = \left\{\frac{1-\beta^a}{\mathfrak{p}}\right\}^{-1}.$$

Also if β^a is a power of α then $q(n) \equiv 0 \pmod{p}$, provided $y \not\equiv 0 \pmod{p}$. We then put

$$D_s = \sum_{d=1}^{p-1} d^s I\left(\frac{\alpha^d - \beta^a}{1-\beta}\right),$$

$\alpha^d \neq \beta^a$, and proceed as in the proofs in the present paper.

---

*These Transactions, vol. 28 (1926), pp. 554-560.

UNIVERSITY OF TEXAS,
AUSTIN, TEX.