NOTE ON SOME RESULTS CONCERNING FERMAT'S LAST THEOREM

BY H. S. VANDIVER

Let us suppose that the equation

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

is satisfied in integers prime to each other and that p is an odd prime. We shall divide the discussion into two parts. We shall refer to the case where xyz is prime to p as Case I, and to the case where $xyz \equiv 0 \pmod{p}$ as Case II. The present note will be confined to statements of new results obtained by the writer for both cases, without proofs.

1. *Case* I. *Transformations of the Kummer Criteria.* If

$$f_a(t) = \sum_{r=1}^{p-1} r^{a-1}t^r,$$

then it is known that, if (1) is satisfied in Case I, we have

$$\begin{cases} f_{p-1}(t) \equiv 0 \pmod{p}, \\ B_n f_{p-2n}(t) \equiv 0 \pmod{p}, \end{cases} \tag{2}$$

$n = 1, 2, \cdots, \mu - 1$, and $-t \equiv x/y,\ y/x,\ z/x,\ x/z,\ y/z,\ z/y$, (mod p), $\mu = (p-1)/2$, where the B's are the Bernoulli numbers, $B_1 = 1/6$, $B_2 = 1/30$, etc. These congruences are known as the Kummer criteria. Transformations of them have yielded the following conditions for Case I:

$$(\sum_{r=0}^{p-1} (2r+1)^{i}t^{r})(\sum_{r=0}^{p-1} (2r+1)^{p-2-i}t^{r}) \equiv 0 \pmod{p},$$

$$(i = 1, 2, \cdots, \mu - 1),$$

$$f_p(t_1) \equiv 0 \pmod{p^2},$$

$$-t_1 \equiv x/y,\ y/x,\ x/z,\ z/x,\ y/z,\ z/y \pmod{p^2}.$$

If e is the smallest integer such that $B_e \equiv 0 \pmod{p}$, we have

$$B_c f_{2k-1}(-t) \equiv 0 \pmod{p}, \tag{3}$$

$$(c = (p - 2k + 1)/2, \quad k = 2, 3, \cdots, e - 1).$$

Kummer and Mirimanoff* have shown that if (1) is satisfied in Case I, then

$$B_{\mu-1} \equiv B_{\mu-2} \equiv B_{\mu-3} \equiv B_{\mu-4} \equiv 0 \pmod{p}.$$

The relation (3) gives material for extension of these criteria.

* Journal für Mathematik, vol. 128 (1905), pp. 45–68.

2. *Results from a New Method.* In efforts to supplement the relations (2) by independent conditions in Case I, the writer, by the use of new developments in the theory of cyclotomic fields, has derived the following criteria* for Case I:

$$(4) \qquad B_s \equiv 0 \pmod{p^2},$$

$$s = (hp + 1)/2, \qquad h = p - 4, p - 6, p - 8, p - 10.$$

If $e = a^f$, *where* a *is any prime and* f *any integer, then*

$$(5) \qquad \frac{(t^e - 1)^p - t^{ep} + 1}{p} \equiv 0 \pmod{p}.$$

This relation possibly also holds if e is any integer, but the formulas which it seems necessary to examine in the general case are very complicated. The condition (5) gives the result: *If* t *belongs to the exponent* n, *modulo* p, *and* n *is the power of a prime, then*

$$1 + \frac{1}{2} + \cdots + \frac{1}{j\nu} \equiv 0 \pmod{p},$$

$$(\nu = (p - 1)/n, \qquad j = 1, 2, \cdots, n - 1).$$

Hence

$$q(n) \equiv \frac{n^{p-1} - 1}{p} \equiv 0 \pmod{p}.$$

In addition, these methods have yielded a new derivation of the known criteria $q(2) \equiv q(3) \equiv 0 \pmod{p}$ without use of (2) or of the criterion of Furtwängler.†

3. *Criteria derived by a second method.* Using transformations of some known theorems regarding cyclotomic fields, the following conditions have been found for Case I.

Let the principal ideal $(\omega(\alpha))$ *be the pth power of any ideal in the field defined by* $\alpha = e^{2i\pi/p}$ *which is prime to* z *and* p; *then*

$$f_{p-n}(s) \left[\frac{d^n \log \omega(e^v)}{dv^n} \right]_{v=0} \equiv 0 \pmod{p},$$

where $s \equiv - x/y \pmod{p}$, $n = 1, 2, \cdots, p - 2$, *and* e *is the Napierian base.*

If we have two solutions of (1), say

$$x_1^p + y_1^p + z_1^p = 0,$$

$$x_2^p + y_2^p + z_2^p = 0,$$

* The first was previously stated in this BULLETIN, vol. 24 (1918), p. 472.

† WIENER BERICHTE, vol. 121 (1912), p. 589.

where z_1 is prime to z_2, then we have as a special case of the above,

$$f_{p-n}(S_1)f_n(S_2) \equiv 0 \pmod{p},$$

$$S_1 \equiv -x_1/y_1, \quad S_2 \equiv -x_2/y_2 \pmod{p}, \quad (n = 1, 2, \cdots, p-1),$$

which in turn includes the relations

$$f_{p-n}(t)f_n(1-t) \equiv 0 \pmod{p};$$

and we obtain also, by a modification of the theorem,

$$f_{p-n}(t)f_n(t) \equiv 0 \pmod{p},$$

n ranging as before, the latter being a known transformation of (2).

4. *Case* II. Under the following assumptions:

1. *None of the Bernoulli numbers*

$$B_k, \quad k = (sp+1)/2, \qquad (s = 1, 3, \cdots, p-4),$$

are divisible by p^2,

2. *The second factor of the class number of the field* $\Omega(\alpha)$ *is prime to* p,

I have proved that (1) is impossible in Case II. A special case of this gives the criterion that if (1) is satisfied in Case II, then the class number of $\Omega(\alpha)$ is divisible by p^2, which in turn may be shown to include the results which Kummer essayed to prove in his 1857 memoir on the last theorem. Taking into account the criteria (4) for Case I, we may cover both cases by the following statement.

Under assumptions 1 *and* 2, *the relation* (1) *is not satisfied in integers* x, y, z, *none zero, for a prime* $p > 2$.

It will be noted that this criterion may be tested for any prime in a finite number of steps.

Kummer[*] computed the value of the first factor of th eclass number of $\Omega(\alpha)$ for all primes less than 167. Assuming these computations correct, it may be shown that assumption 1 holds for all these primes. According to Kummer[†] the second assumption holds for all primes less than 100, and it has not been tested for larger primes.

CORNELL UNIVERSITY

[*] BERLINER MONATSBERICHTE, 1874.

[†] BERLINER ABHANDLUNGEN, 1857, p. 73, verification of second assumption.