MATHEMATICS OF COMPUTATION, VOLUME 31, NUMBER 138
APRIL 1977, PAGES 519–526

On Congruences Related to the First Case of Fermat's Last Theorem

By Wells Johnson*

Abstract. Solutions to the congruences $(1 + a)^{p^n} \equiv 1 + a^{p^n} \pmod{p^{n+2}}$ and $(1 + s)^p \equiv 1 + s^p \pmod{p^n}$ are discussed. Congruences of this type arise in the study of the first case of Fermat's Last Theorem. Solutions to these congruences always exist for primes $p \equiv 1 \pmod 6$. They are derived from the existence of a primitive cube root of unity $\pmod p$. Constructive techniques for finding numerical examples are presented. The results are obtained by examining the p-adic expansions of the p-adic $(p - 1)$st roots of unity.

1. Introduction. Let $p \geqslant 5$ be a prime. Carmichael [2] proved that if the Fermat equation $x^p + y^p = z^p$ has a nonzero integral solution in the first case $(p \nmid xyz)$, then there exists an a, $0 < a < p$, satisfying

$$(1) \qquad (1 + a)^{p^2} \equiv 1 + a^{p^2} \pmod{p^3}.$$

Dickson [3, p. 772] writes that it was G. D. Birkhoff who noted that this congruence is equivalent to

$$(2) \qquad (1 + a)^p \equiv 1 + a^p \pmod{p^3}.$$

Meissner [9] gives the same result.

Using a theorem of Furtwängler, Vandiver [12] proved that a solution (x, y, z) of the Fermat equation in the first case must also satisfy the congruence $x + y \equiv z \pmod{p^3}$. Gandhi [7] has noted that this implies that the congruence

$$(3) \qquad (1 + s)^p \equiv 1 + s^p \pmod{p^4}$$

must hold for some integer s, $p \nmid s$.

Trypanis [11] and Ferentinou-Nikolakopoulou [5] have reported that a solution to the Fermat equation in the first case requires that for some a, $0 < a < p$,

$$(4) \qquad (1 + a)^{p^2} \equiv 1 + a^{p^2} \pmod{p^4}.$$

If a is a solution to Eq. (4), then Eqs. (1) and (2) hold, so that $s = a^p$ is a solution to Eq. (3).

It was known classically (essentially to Cauchy) that, if $a^2 + a + 1 \equiv 0 \pmod p$ (implying that $p \equiv 1 \pmod 6$), then Eq. (2) is satisfied by a. Meissner [9] and

Received April 26, 1976.
AMS (MOS) subject classifications (1970). Primary 10A10; Secondary 10B15, 10B40.
Key words and phrases. Congruences, Fermat's Last Theorem, p-adic roots of unity.
*Supported by a grant from the Vaughn Foundation Fund.

Pollaczek [10] have noted, however, that such a's do not give rise to a solution of the Fermat equation in the first case. We are thus led to the question of whether or not Eq. (2) can have a solution a which does not satisfy $a^2 + a + 1 \equiv 0 \pmod{p}$. It has been known for some time (cf. Arwin [1]) that there exist solutions to the congruence $(1 + a)^p \equiv 1 + a^p \pmod{p^2}$ with $a^2 + a + 1 \not\equiv 0 \pmod{p}$. S. S. Wagstaff, Jr., at the University of Illinois, has verified computationally, however, that for all primes $p < 100{,}000$ the only solutions to Eq. (2) are those also satisfying $a^2 + a + 1 \equiv 0 \pmod{p}$. In particular, no solution to Eq. (2) is known to exist for $p \equiv 5 \pmod{6}$.

In the next section, we give a proof of the fact that for $0 < a < p$ the condition $a^2 + a + 1 \equiv 0 \pmod{p}$ is equivalent to the infinite set of congruences

$$(5) \qquad (1 + a)^{p^n} \equiv 1 + a^{p^n} \pmod{p^{n+2}}, \qquad n \geqslant 1.$$

For $n = 1, 2$, Eq. (5) reduces to Eqs. (2) and (4), respectively. This equivalence places some perspective on any attempts to demonstrate the first case of Fermat's Last Theorem by means of congruences of this type (cf. Gandhi [6]).

We also present some solutions to the congruences $(1 + s)^p \equiv 1 + s^p \pmod{p^n}$ for exponents $n \geqslant 3$. It is shown that solutions always exist for $n \geqslant 3$ if $p \equiv 1 \pmod{6}$; and of course, these known solutions all satisfy $s^2 + s + 1 \equiv 0 \pmod{p}$. The solutions of this type are completely characterized $(\bmod\ p^{[n/2]})$. They occur in pairs, with sum congruent to $-1 \pmod{p^{[n/2]}}$. A simple construction is presented to compute the values of the solutions in the case $n = 5$. We also establish a general congruence for the difference $(1 + s)^p - 1 - s^p \pmod{p^4}$ for all integers s satisfying $s^2 + s + 1 \equiv 0 \pmod{p}$.

The results of this paper all follow from the existence of the $(p - 1)$st roots of unity in the ring of p-adic integers, $\mathbf{Z}_p$, and the numerical determination of their p-adic expansions. The author [8] has proved previously some well-known properties of the Bernoulli numbers from similar considerations.

2. Main Theorems.

For $0 < a < p$, let $v(a)$ denote the unique p-adic $(p - 1)$st root of 1 in $\mathbf{Z}_p$ which satisfies $v(a) \equiv a \pmod{p}$. If $a^2 + a + 1 \equiv 0 \pmod{p}$, then $p \equiv 1 \pmod{6}$ and a is a primitive cube root of $1 \pmod{p}$. From $a^3 \equiv 1 \pmod{p}$ and $a \not\equiv 1 \pmod{p}$, we deduce $v(a)^3 = 1$ and $v(a) \neq 1$ in $\mathbf{Z}_p$, so that $v(a)$ is a primitive cube root of 1 in $\mathbf{Z}_p$, and $1 + v(a) + v(a)^2 = 0$. But then $1 + v(a) = -v(a)^2$, so that $1 + v(a)$ is the $(p - 1)$st root of 1 congruent to $1 + a \pmod{p}$. By uniqueness, we obtain

$$(6) \qquad 1 + v(a) = v(1 + a).$$

All the results of this paper are a consequence of this basic fact. Everett and Metropolis [4] have shown that if Eq. (6) holds, then $a^2 + a + 1 \equiv 0 \pmod{p}$. For the sake of completeness, we include a direct proof of this fact in the following theorem.

THEOREM 1. *Let $p \equiv 1 \pmod{6}$ be a prime, and let $0 < a < p$. Then the following properties on a are equivalent*:

(1) $a^2 + a + 1 \equiv 0 \pmod{p}$ (*i.e., a is a primitive cube root of* 1 (mod p)),

(2) $1 + \upsilon(a) = \upsilon(1 + a)$,

(3) $(1 + a)^{p^n} \equiv 1 + a^{p^n} \pmod{p^{n+2}}$ *for all* $n \geqslant 1$.

Proof. We have seen that (1) ⇒ (2). To prove the converse, let V denote the cyclic subgroup of $\mathbf{Z}_p$ containing the $(p - 1)$st roots of unity. Let $F = \mathbf{Q}(V)$ be the subfield of the p-adic numbers $\mathbf{Q}_p$ generated by V over the prime subfield $\mathbf{Q}$. Let $\sigma\colon F \longrightarrow F$ be the automorphism defined by $\sigma(v) = v^{-1}$ for $v \in V$. Then, applying σ to (2), we obtain $\upsilon(1 + a)^{-1} = 1 + \upsilon(a)^{-1}$. But this implies that $1 + \upsilon(a) + \upsilon(a)^2 = 0$, which gives us (1).

Now write $\upsilon(a) = a + r_a p$ for r_a in $\mathbf{Z}_p$, uniquely defined by a. Since $\upsilon(a)^p = \upsilon(a)$, it is easy to prove by induction on $n \geqslant 0$, that $\upsilon(a) \equiv a^{p^n} + r_a p^{n+1} \pmod{p^{n+2}}$. A similar result holds for $\upsilon(1 + a)$.

If (2) holds, then $r_a = r_{1+a}$ and (3) follows immediately from (2) and the congruences above. Conversely, if (3) holds, then the congruences above imply that

$$1 + \upsilon(a) \equiv \upsilon(1 + a) \pmod{p^{n+1}}$$

for all $n \geqslant 1$, which is sufficient for (2).

We see as a corollary that, if $a^2 + a + 1 \equiv 0 \pmod{p}$, then a is a solution to Eqs. (2) and (4) and $s = a^p$ is a solution to Eq. (3). The implication (3) ⇒ (1) has been reported without proof by Trypanis [11].

We next turn to the general problem of finding solutions to the congruence $(1 + s)^p \equiv 1 + s^p \pmod{p^n}$ for exponents $n \geqslant 3$. If $a^2 + a + 1 \equiv 0 \pmod{p}$, then Eq. (6) implies that $1 + \upsilon(a)^p = \upsilon(1 + a)^p$. Thus, if we simply take a rational integer s, $s \equiv \upsilon(a) \pmod{p^n}$, then $1 + s \equiv \upsilon(1 + a) \pmod{p^n}$ by Eq. (6), so that the existence of solutions to our congruence is always assured for primes $p \equiv 1 \pmod{6}$. A slightly stronger result is true, however:

THEOREM 2. *Let* $p \equiv 1 \pmod{6}$ *be a prime, and suppose that* $a^2 + a + 1 \equiv 0 \pmod{p}$, *where* $0 < a < p$. *If* $s \equiv \upsilon(a) \pmod{p^n}$ *for* $n \geqslant 1$, *then*

$$(1 + s)^p \equiv 1 + s^p \pmod{p^{2n+1}}.$$

Proof. Write $s = \upsilon(a) + rp^n$, for some $r \in \mathbf{Z}_p$. Then $s^p \equiv \upsilon(a)^p + rp^{n+1}\upsilon(a)^{p-1} = \upsilon(a) + rp^{n+1} \pmod{p^{2n+1}}$. Also, $1 + s = \upsilon(1 + a) + rp^n$ by Eq. (6). Hence, we also have

$$(1 + s)^p \equiv \upsilon(1 + a) + rp^{n+1} \pmod{p^{2n+1}}.$$

The result now follows from Eq. (6).

Since the primitive cube roots of 1 (either (mod p) or in $\mathbf{Z}_p$) come in pairs (either a and a^2, or $\upsilon(a)$ and $\upsilon(a)^2$), we always obtain a pair of solutions (mod p^n) to the congruence in Theorem 2. Moreover, if s and s' are solutions, with $s \equiv \upsilon(a) \pmod{p^n}$ and $s' \equiv \upsilon(a)^2 \pmod{p^n}$, then $s + s' \equiv -1 \pmod{p^n}$, so that a second solution can be obtained easily from a first.

We next prove a converse to Theorem 2:

THEOREM 3. *Let* $p \equiv 1 \pmod 6$ *be a prime, and suppose* $s^2 + s + 1 \equiv 0 \pmod p$ *and* $(1+s)^p \equiv 1 + s^p \pmod{p^{2n}}$ *for some rational integer s. Then* $s \equiv \upsilon(a) \pmod{p^n}$, *where a is the smallest positive residue of s* $\pmod p$.

Proof. By induction on $n \geqslant 1$. The case $n = 1$ is trivial, since $s \equiv a \equiv \upsilon(a) \pmod p$ by the definitions of a and $\upsilon(a)$.

Next assume that $n \geqslant 2$ and that the theorem is true for $n - 1$. By the induction hypothesis, we can write $s = \upsilon(a) + rp^{n-1}$ for some $r \in \mathbf{Z}_p$. But then

$$s^p \equiv \upsilon(a)^p + rp^n \upsilon(a)^{p-1} + \binom{p}{2}\upsilon(a)^{p-2}r^2p^{2n-2} \pmod{p^{2n}}$$

or

$$s^p \equiv \upsilon(a) + rp^n + \binom{p}{2}\upsilon(a)^{-1}r^2p^{2n-2} \pmod{p^{2n}}.$$

Similarly, $1 + s = \upsilon(1+a) + rp^{n-1}$ by Eq. (6), so that

$$(1+s)^p \equiv \upsilon(1+a) + rp^n + \binom{p}{2}\upsilon(1+a)^{-1}r^2p^{2n-2} \pmod{p^{2n}}.$$

By the hypothesis and Eq. (6), we deduce

$$\binom{p}{2}\upsilon(a)^{-1}r^2p^{2n-2} \equiv \binom{p}{2}\upsilon(1+a)^{-1}r^2p^{2n-2} \pmod{p^{2n}},$$

or

$$\upsilon(1+a)r^2 \equiv \upsilon(a)r^2 \pmod p.$$

Equation (6) now implies that $p \mid r$, so that $s \equiv \upsilon(a) \pmod{p^n}$, as desired.

It should be remarked that the proofs of Theorems 2 and 3 generalize slightly. With the same hypotheses, if $s \equiv \upsilon(a) \pmod{p^n}$, then $(1+s)^{p^k} \equiv 1 + s^{p^k} \pmod{p^{2n+k}}$, and conversely, if $(1+s)^{p^k} \equiv 1 + s^{p^k} \pmod{p^{2n+k-1}}$, then $s \equiv \upsilon(a) \pmod{p^n}$.

3. A Construction and Some Examples. In this section we show how examples of solutions to the congruence $(1+s)^p \equiv 1 + s^p \pmod{p^5}$ may be constructed easily in the case that $p \equiv 1 \pmod 6$. To use Theorem 2, it is merely necessary to compute $\upsilon(a) \pmod{p^2}$ for $a^2 + a + 1 \equiv 0 \pmod p$. We write $\upsilon(a) \equiv a + \upsilon(a)_1 p \pmod{p^2}$, where $0 \leqslant \upsilon(a)_1 < p$. From the relation $\upsilon(a)^p = \upsilon(a)$, it follows that $\upsilon(a)_1 \equiv aq_a \pmod p$, where $q_a = (a^{p-1} - 1)/p$, the so-called *Fermat quotient.*

Define $b \geqslant 1$ by the equation $a^2 + a + 1 = bp$. Then $a^3 - 1 = b(a-1)p$, so that

$$a^{p-1} = (1 + b(a-1)p)^{(p-1)/3} \equiv 1 + (p-1)b(a-1)p/3 \pmod{p^2}.$$

Thus $q_a \equiv (p-1)b(a-1)/3 \pmod p$, or

$$aq_a \equiv (p-1)b(a^2 - a)/3 \equiv b(2a+1)/3 \pmod p,$$

and $\upsilon(a)_1$ is the least nonnegative residue of $b(2a+1)/3 \pmod p$. Also, $0 < a < p$ implies that $p \nmid b$, and $p \geqslant 5$ implies that $p \nmid (2a+1)$. Hence, $\upsilon(a)_1 > 0$ always, and we have

THEOREM 4. *Let p be a prime, $p \equiv 1 \pmod 6$, and let a be a solution to the congruence $a^2 + a + 1 \equiv 0 \pmod p$, $0 < a < p$. If $b \geqslant 1$ is defined by $a^2 + a + 1 = bp$, then $v(a)_1$ is the least nonnegative residue of $b(2a + 1)/3 \pmod p$, and $v(a)_1 > 0$. Hence, $s = a + v(a)_1 p$ is a rational integer solution to the congruence $(1 + s)^p \equiv 1 + s^p \pmod{p^5}$, and $p < s < p^2$.*

The simplest examples, for $p = 7$, 13, and 19 and $a = 2$, 3, and 7, respectively, yield the congruences

$$\begin{aligned} 31^7 &\equiv 1 + 30^7 \quad (\text{mod } 7^5 = 16807),\\ 147^{13} &\equiv 1 + 146^{13} \quad (\text{mod } 13^5 = 371293),\\ 293^{19} &\equiv 1 + 292^{19} \quad (\text{mod } 19^5 = 2476099). \end{aligned}$$

By the remark just before Theorem 3, we also have the congruences

$$\begin{aligned} 19^7 &\equiv 1 + 18^7 \quad (\text{mod } 7^5),\\ 23^{13} &\equiv 1 + 22^{13} \quad (\text{mod } 13^5),\\ 69^{19} &\equiv 1 + 68^{19} \quad (\text{mod } 19^5). \end{aligned}$$

The latter solutions can also be obtained from Theorem 4, by choosing $a = 4$, 9, and 11 for $p = 7$, 13, and 19, respectively.

Theorems 3 and 4 combine to give the following:

COROLLARY. *If p is an odd prime, there are no rational integer solutions a in the interval $0 < a < p$ to the simultaneous congruences*

$$a^2 + a + 1 \equiv 0 \pmod p,$$

$$(1 + a)^p \equiv 1 + a^p \pmod{p^4}.$$

This contrasts with the classical result that, for $p \equiv 1 \pmod 6$, the congruence $a^2 + a + 1 \equiv 0 \pmod p$ always has two solutions a, $0 < a < p$, both of which also satisfy Eq. (2).

4. More General Congruences.

In this section we establish general congruences for the differences $(1 + a)^{p^n} - 1 - a^{p^n} \pmod{p^{n+3}}$ and $(1 + s)^p - 1 - s^p \pmod{p^4}$, when a and s satisfy $x^2 + x + 1 \equiv 0 \pmod p$.

THEOREM 5. *If p is a prime, $p \equiv 1 \pmod 6$ and $a^2 + a + 1 \equiv 0 \pmod p$ for some a, $0 < a < p$, then for $n \geqslant 1$,*

$$(1 + a)^{p^n} \equiv 1 + a^{p^n} + (q_a q_{1+a}/2)p^{n+2} \pmod{p^{n+3}}.$$

Proof. As in the proof of Theorem 1, write $v(a) = a + r_a p$. Then $v(a) = v(a)^{p^n} \equiv a^{p^n} + r_a p^{n+1} + (aq_a^2/2)p^{n+2} \pmod{p^{n+3}}$, since $r_a \equiv aq_a \pmod p$, as we noted at the beginning of Section 3. A similar result holds for $v(1 + a)$. By Eq. (6), $r_a = r_{1+a}$ and

$$(1 + a)^{p^n} - 1 - a^{p^n} \equiv [(aq_a^2 - (1 + a)q_{1+a}^2)/2]p^{n+2} \pmod{p^{n+3}}.$$

But $r_a = r_{1+a}$ implies that $(1 + a)q_{1+a} \equiv aq_a \pmod{p}$, and the result follows.

Theorem 5 also follows from Theorem 1 and the second result of Trypanis [11]. If we choose $n = 1$ in Theorem 5, we have proved a special case (namely $0 < s < p$) of the following:

THEOREM 6. *If p is a prime, $p \equiv 1 \pmod{6}$, and $s^2 + s + 1 \equiv 0 \pmod{p}$ for some rational integer $s \geqslant 2$, $p \nmid s$, then*

$$(1 + s)^p \equiv 1 + s^p + (q_s q_{1+s}/2)p^3 \pmod{p^4}.$$

Proof. To finish the proof, it suffices to show that if the congruence holds for s, then it also holds for $s + p$. To see this, note that

$$q_{s+p} \equiv q_s - s^{-1} \pmod{p}. \tag{7}$$

This in turn implies that the congruence

$$sq_s \equiv (1 + s)q_{1+s} \pmod{p}, \tag{8}$$

proved for $0 < s < p$ above, depends only on the residue class of $s \pmod{p}$. The rest of the verification is an easy algebraic computation.

Note that if $s^2 + s + 1 \equiv 0 \pmod{p}$, then by Theorem 6 we have that $(1 + s)^p \equiv 1 + s^p \pmod{p^4}$ if and only if $q_s \equiv 0 \pmod{p}$. If we write $s = a + cp$, with $0 < a < p$ and $c \geqslant 1$, then by Eq. (7), this condition is equivalent to $q_a \equiv c/a \pmod{p}$, or $c \equiv aq_a \equiv v(a)_1 \pmod{p}$. But this means that $s \equiv v(a) \pmod{p^2}$, which is nothing more than the case $n = 2$ of Theorem 3.

5. More Examples.

It is not difficult, using Theorem 2, to construct specific solutions to the congruences $(1 + s)^p \equiv 1 + s^p \pmod{p^7}$ and $(\text{mod } p^9)$, much as we did $(\text{mod } p^5)$ in Section 3. It merely requires the computation of $v(a) \pmod{p^4}$, where $a^2 + a + 1 \equiv 0 \pmod{p}$.

For notation, expand $v(a)$ out p-adically in the form

$$v(a) = a + v(a)_1 p + v(a)_2 p^2 + \cdots + v(a)_n p^n + \cdots,$$

where the p-adic coefficients $v(a)_n$ satisfy $0 \leqslant v(a)_n < p$ for all $n \geqslant 1$. Now Eq. (6) implies the rather remarkable fact that all the p-adic coefficients for $v(a)$ and $v(1 + a)$ are equal:

$$v(a)_n = v(1 + a)_n, \qquad n \geqslant 1. \tag{9}$$

In Section 3 we saw that the relation $v(a)^p = v(a)$ implies that

$$v(a)_1 \equiv aq_a \pmod{p}. \tag{10}$$

Similarly, from $v(a)^p = v(a)$ we can compute that

$$v(a)_2 p \equiv v(a)_1 p + (aq_a - v(a)_1) \pmod{p^2}, \tag{11}$$

and

$$(12)\quad v(a)_3p^2 \equiv [v(a)_1 - v(a)_2]\,p + (aq_a - v(a)_1) + v(a)_2p^2 + (aq_a^2/2)p^2 \pmod{p^3}.$$

Equations (10)–(12) permit the computation of $v(a) \pmod{p^4}$. For example, if $p = 13$ and $a = 3$, we have already seen that $v(a) \equiv 3 + 11p \pmod{p^2}$. Now $3^3 = 1 + 2p$, and from this we can compute that

$$q_3 = 8 + 11p + 7p^2 + 5p^3 + p^4.$$

From Eqs. (10)–(12), we find that $v(3)_1 = 11$, $v(3)_2 = 6$, $v(3)_3 = 9$, so that

$$v(3) = 3 + 11p + 6p^2 + 9p^3 \pmod{p^4}.$$

From Theorem 2 and the remark before Theorem 3, we obtain the examples

$$\begin{aligned} 1161^{13} &\equiv 1 + 1160^{13} \pmod{13^7},\\ 1037^{13} &\equiv 1 + 1036^{13} \pmod{13^7},\\ 20934^{13} &\equiv 1 + 20933^{13} \pmod{13^9},\\ 7628^{13} &\equiv 1 + 7627^{13} \pmod{13^9}. \end{aligned}$$

The second congruence in each pair also follows from Theorem 2, with $a = 9$. Since $v(3) + v(9) = -1$, we can conclude that

$$v(9) \equiv 9 + p + 6p^2 + 3p^3 \pmod{p^4}.$$

The explicit formula for $v(3) \pmod{p^4}$ given above can also be deduced from the so-called Witt formula: $v(a) = \lim_{n\to\infty} a^{p^n}$ (p-adic limit). From this, one sees that if

$$a^p \equiv a + a_1p + a_2p^2 + a_3p^3 \pmod{p^4},$$

then

$$v(a) \equiv a + a_1p + (a_1 + a_2)p^2 + (a_1 + a_2 + a_3 + (a_1^2/2a))p^3 \pmod{p^4}.$$

This formula is equivalent to Eqs. (10)–(12). For $p = 13$ and $a = 3$, we find that $a_1 = 11$, $a_2 = 8$, and $a_3 = 10$, so that, as before,

$$v(3) \equiv 3 + 11p + 6p^2 + 9p^3 \pmod{p^4}.$$

From Eq. (9) with $n = 1, 2, 3$ and Eqs. (10)–(12), we obtain

$$(1 + a)q_{1+a} - aq_a \equiv (q_aq_{1+a}/2)p^2 \pmod{p^3}.$$

This congruence is in fact the case $n = 1$ of Theorem 5, so that Theorem 6 can be obtained by these more computational methods.

Department of Mathematics
Bowdoin College
Brunswick, Maine 04011

1. A. ARWIN, "Über die Lösung der Kongruenz $(\lambda + 1)^p - \lambda^p - 1 \equiv 0 \pmod{p^2}$," *Acta Math.*, v. 42, 1920, pp. 173–190.

2. R. D. CARMICHAEL, "Note on Fermat's Last Theorem," *Bull. Amer. Math. Soc.*, v. 19, 1913, pp. 233–236.

3. L. E. DICKSON, *History of the Theory of Numbers*, vol. II, Carnegie Institution of Washington, Washington, D.C., 1920.

4. C. J. EVERETT & N. METROPOLIS, "On the roots of $x^m \pm 1$ in the p-adic field Q_p," *Notices Amer. Math. Soc.*, v. 22, 1975, p. A-619. Abstract #75T-A229.

5. I. FERENTINOU-NIKOLAKOPOULOU, "A new necessary condition for the existence of a solution to the equation $x^p + y^p = z^p$ of Fermat," *Bull. Soc. Math. Grèce* (*N. S.*), v. 6I, 1965, fasc. 2, pp. 222–236; "Remarks on the article: 'A new necessary condition for the existence of a solution to the equation $x^p + y^p = z^p$ of Fermat'," *ibid.*, v. 6II, 1965, fasc. 2, pp. 356–357. (Greek) MR **34** #5738a, #5738b.

6. J. M. GANDHI, "Fermat's Last Theorem I. Some interesting observations for the first case," *Notices Amer. Math. Soc.*, v. 22, 1975, p. A-486. Abstract #725-A2.

7. J. M. GANDHI, "On the first case of Fermat's Last Theorem." (To appear.)

8. W. JOHNSON, "p-adic proofs of congruences for the Bernoulli numbers," *J. Number Theory*, v. 7, 1975, pp. 251–265. MR 51 #12687.

9. W. MEISSNER, "Über die Lösungen der Kongruenz $x^{p-1} \equiv 1 \bmod p^m$ und ihre Verwertung zur Periodenbestimmung mod p^x," *Sitzungsber. Berlin Math. Gessell.*, v. 13, 1914, pp. 96–107.

10. F. POLLACZEK, "Über den grossen Fermat'schen Satz," *Sitzungsber. Akad. Wiss. Wien* (*Math.*), v. 126 (IIa), 1917, pp. 45–59.

11. A. A. TRYPANIS, "On Fermat's last theorem," *Proc. Internat. Congr. of Mathematicians* (Cambridge, Mass., 1950), vol. 1, Amer. Math. Soc., Providence, R.I., 1952, pp. 301–302.

12. H. S. VANDIVER, "Note on Fermat's Last Theorem," *Trans. Amer. Math. Soc.*, v. 15, 1914, pp. 202–204.