SECOND NOTE ON FERMAT'S LAST THEOREM.

BY PROFESSOR R. D. CARMICHAEL.

In a note printed on pages 233–236 of the present volume of the Bulletin I have proved the following theorem:

If p is an odd prime and the equation

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

has a solution in integers x, y, z each of which is prime to p, then there exists a positive integer s, less than $\frac{1}{2}(p - 1)$, such that

$$(s + 1)^{p^2} \equiv s^{p^2} + 1 \mod p^3. \tag{1}$$

Professor Birkhoff has called my attention to the fact that condition (1) may be replaced by the simpler condition

$$(s + 1)^p \equiv s^p + 1 \mod p^3, \tag{1'}$$

these two conditions being equivalent. Let us define the integers λ and μ by the relations

$$(s + 1)^p = s + 1 + \lambda p, \quad s^p = s + \mu p.$$

Then

$$(s + 1)^p = s^p + 1 + (\lambda - \mu)p. \tag{2}$$

We have also

$$\begin{aligned}(s + 1)^{p^2} &\equiv (s + 1)^p + \lambda p^2(s + 1)^{p-1} \mod p^3\\ &\equiv s + 1 + \lambda p + \lambda p^2 \mod p^3\\ &\equiv s + 1 + \lambda(p + p^2) \mod p^3.\end{aligned}$$

Likewise

$$s^{p^2} \equiv s + \mu(p + p^2) \mod p^3.$$

From the last two congruences we have

$$(s + 1)^{p^2} \equiv s^{p^2} + 1 + (\lambda - \mu)(p + p^2) \mod p^3. \tag{3}$$

From (2) and (3) we see that a necessary and sufficient condition for either (1) or (1′) is that $\lambda - \mu \equiv 0 \mod p^2$. Therefore (1) and (1′) are equivalent.

The simpler relation (1′) can be derived more readily than the relation (1). For from the congruence $x + y + z \equiv 0 \mod p^2$, obtained in my previous paper, we have immediately $(x + y)^p \equiv - z^p \mod p^3$. Hence

$$(x + y)^p \equiv x^p + y^p \mod p^3,$$

from which (1′) is readily deduced.

Professor Birkhoff points out further that the test fails to be effective for all primes p of the form $6n + 1$. For if $p = 6n + 1$ it follows from the theory of primitive roots modulo p^3 that the congruence

$$t^3 \equiv 1 \mod p^3$$

has a solution t for which $t - 1$ is prime to p. Hence also

$$t^2 + t + 1 \equiv 0 \mod p^3.$$

Then we have

$$(t + 1)^p = (t + 1)(t + 1)^{6n} \equiv (t + 1)(- t^2)^{6n} \equiv t + 1 \mod p^3,$$

$$(t + 1)^{p^2} \equiv (t + 1)^p \equiv t + 1 \mod p^3,$$

and

$$t^p \equiv t \cdot t^{6n} \equiv t \mod p^3, \qquad {}^{p^2} \equiv t^p \equiv t \mod p^3.$$

Therefore

$$(t + 1)^{p^2} \equiv t^{p^2} + 1 \mod p^3.$$

Now put

$$t = \sigma + vp, \qquad (0 < \sigma < p - 1).$$

Then

$$t^{p^2} \equiv \sigma^{p^2}, \quad (t + 1)^{p^2} \equiv (\sigma + 1)^{p^2} \mod p^3.$$

Therefore

$$(\sigma + 1)^{p^2} \equiv \sigma^{p^2} + 1 \mod p^3, \quad (0 < \sigma < p - 1).$$

This is relation (7) of my previous note; from this follows (1) as in the earlier treatment. Hence (1) is satisfied by all primes of the form $6n + 1$. Therefore the test can be useful only when the exponent p is 3 or is of the form $6n - 1$.

INDIANA UNIVERSITY,
March, 1913.

AN EXTENSION OF A THEOREM OF PAINLEVÉ.

BY DR. E. H. TAYLOR.

(Read before the American Mathematical Society, October 26, 1912.)

THEOREM: Let $f(z)$ be a function which is single-valued and analytic throughout the interior of a region S of the z-plane, $z = x + yi$. If $f(z)$ vanishes at every point of a