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

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

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

$$(1') \qquad (s+1)^p \equiv s^p + 1 \mod p^3,$$

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

$$(2) \qquad (s+1)^p = s^p + 1 + (\lambda - \mu)p.$$

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

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

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