γ being the angle between the directions θ, φ and α, β. By using the Mehler formulæ for Legendre's polynomials P_n, (18) may be transformed so as to contain elliptic sigma functions under a triple integral sign, giving a formula somewhat similar to (3).

CHICAGO, ILL.,
November 9, 1912.

NOTE ON FERMAT'S LAST THEOREM.

BY PROFESSOR R. D. CARMICHAEL.

(Read before the American Mathematical Society, December 31, 1912.)

THE object of this note is to prove the following

THEOREM. *If p is an odd prime and the equation*

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

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

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

The proof is elementary. If there exists a set of integers x, y, z satisfying (1), there exists such a set having the further property that they are prime each to each. Consequently, for the purpose of argument we may assume that x, y, z have this property.

Then from elementary considerations it is known* that integers α, β, γ exist such that

$$x + y = \gamma^p, \quad y + z = \alpha^p, \quad z + x = \beta^p.$$

Therefore

$$(x+y)^{p-1} \equiv 1, \quad (y+z)^{p-1} \equiv 1, \quad (z+x)^{p-1} \equiv 1 \bmod p^2, \tag{2}$$

since $a^{p(p-1)} \equiv 1 \bmod p^2$ when a is prime to p.

From (1) it follows that

$$x + y + z \equiv 0 \bmod p,$$

* See, for instance, Bachmann's Niedere Zahlentheorie, Zweiter Teil, p. 467.

since $x^p \equiv x$, $y^p \equiv y$, $z^p \equiv z \bmod p$ by Fermat's theorem. Writing $x + y = Ap - z$, we have readily $(x + y)^p \equiv - z^p \bmod p^2$. Replacing $- z^p$ by its value $x^p + y^p$ and writing the resulting congruence and two similar ones, we have

$$(3) \qquad (x + y)^p \equiv x^p + y^p, \quad (y + z)^p \equiv y^p + z^p,$$
$$(z + x)^p \equiv z^p + x^p \bmod p^2.$$

From (2) and (3) we see that

$$x^p + y^p \equiv x + y, \quad y^p + z^p \equiv y + z, \quad z^p + x^p \equiv z + x \bmod p^2.$$

Adding these congruences and making use of equation (1), we have

$$x + y + z \equiv 0 \bmod p^2.$$

Then we may write $x + y = Bp^2 - z$, whence $(x + y)^p \equiv - z^p \bmod p^3$. Hence, since $- z^p = x^p + y^p$, we have

$$(x + y)^p \equiv x^p + y^p, \quad (y + z)^p \equiv y^p + z^p,$$
$$(z + x)^p \equiv z^p + x^p \bmod p^3.$$

Adding these three congruences and employing (1), we have

$$(4) \qquad (x + y)^p + (y + z)^p + (z + x)^p \equiv 0 \bmod p^3.$$

Now from (2) we have $(x + y)^{p-1} = 1 + cp^2$, whence it follows that

$$(x + y)^{p(p-1)} \equiv 1 \bmod p^3; \text{ or } (x + y)^{p^2} \equiv (x + y)^p \bmod p^3,$$

with similar congruences for $y + z$ and $z + x$. From these congruences and (4) we have the following relation:

$$(5) \qquad (x + y)^{p^2} + (y + z)^{p^2} + (z + x)^{p^2} \equiv 0 \bmod p^3.$$

But $x + y = Ap - z$, and therefore $(x + y)^{p^2} \equiv - z^{p^2} \bmod p^3$, with similar congruences for $y + z$ and $z + x$. Substituting in (5), we have

$$(6) \qquad x^{p^2} + y^{p^2} + z^{p^2} \equiv 0 \bmod p^3.$$

Now let σ be the positive integer less than p such that

$$y \equiv \sigma x \bmod p.$$

Then since $x + y + z \equiv 0 \bmod p$ we have $x + \sigma x + z \equiv 0 \bmod p$ or $z \equiv -(\sigma + 1)x \bmod p$. It is then obvious that $y^{p^2} \equiv (\sigma x)^{p^2} \bmod p^3$ and $z^{p^2} \equiv \{-(\sigma + 1)x\}^{p^2} \bmod p^3$. Substituting in (6) and dividing the resulting congruence by x^{p^2}, we have

$$(7) \qquad (\sigma + 1)^{p^2} \equiv \sigma^{p^2} + 1 \bmod p^3.$$

If $\sigma < \frac{1}{2}(p - 1)$, it may be taken for the s of the theorem, and our demonstration is then complete. If $\sigma > \frac{1}{2}(p - 1)$, write

$$s = p - \sigma - 1,$$

whence $s < \frac{1}{2}(p - 1)$. From (7) we have

$$(\sigma + 1 - p)^{p^2} \equiv (\sigma - p)^{p^2} + 1 \bmod p^3;$$

or

$$(p - \sigma)^{p^2} \equiv (p - \sigma - 1)^{p^2} + 1 \bmod p^3,$$

whence

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

If $\sigma = \frac{1}{2}(p - 1)$ we have from (7), on multiplying by 2^{p^2},

$$(p + 1)^{p^2} \equiv (p - 1)^{p^2} + 2^{p^2} \bmod p^3;$$

or

$$1 \equiv -1 + 2^{p^2} \bmod p^3,$$

whence

$$2^{p^2} \equiv 2 \bmod p^3,$$

so that for the s of the theorem we may in this case take $s = 1$. This completes the demonstration of the theorem.

COROLLARY. *If any two of the numbers x, y, z are congruent modulo p, then*

$$2^{p^2-1} \equiv 1 \bmod p^3.$$

For, if x and y are congruent, σ is equal to unity and the corollary follows at once from (7). A similar proof may of course be made when y and z or z and x are congruent.

From the way in which the theorem was proved it is clear that in general there are several values of σ satisfying congruence (7). Thus if $\sigma\tau \equiv 1 \bmod p$, so that $x \equiv \tau y \bmod p$, it is obvious that we have also

$$(\tau + 1)^{p^2} \equiv \tau^{p^2} + 1 \bmod p^3.$$

But this congruence is implied by (7) alone, as one may readily verify by multiplying (7) by τ^{p^2}. Other cases may be dealt with similarly.

Indiana University,
November, 1912.

INTEGRAL EQUATIONS.

Introduction à la Théorie des Equations intégrales. By T. Lalesco. Paris, A. Hermann et Fils, 1912. 152 pp.

L'Equation de Fredholm et ses Applications à la Physique mathématique. By H. B. Heywood and M. Frechet. Paris, A. Hermann et Fils, 1912. 165 pp.

The theory of integral equations has been developed since the publication of Volterra's first paper in 1896, and most of the work has been done since Fredholm's fundamental memoir appeared in 1900. Yet, in this comparatively short time, the number of printed papers dealing with the subject has become so great that one approaching the subject for the first time is embarrassed by the wealth of material at his command. The two books mentioned above have been written for the beginner in the study of this interesting and useful branch of analysis. The authors have given a clear and concise exposition of the fundamental principles and of the most important results obtained up to the present time. While admitting freely that there is much yet to be done both on the theoretical side and the side of applications to mathematical physics and mechanics, there can be no doubt that the fundamental portions have already reached a form that will remain classic, and that it is now desirable to have them in book form for the convenience of the mathematical public. These two small volumes will be found very useful to the reader who wishes merely an acquaintance with the first principles of the subject, as well as to the reader who expects to attain a wider knowledge by studying the journal articles. While there is necessarily some repetition the two books may well be used together. The first one is devoted to the theory of integral equations and