CONGRUENCES CONNECTED WITH THE SOLUTION OF A CERTAIN DIOPHANTINE EQUATION

HAROLD F. S. JONAH

Introduction. In this paper we shall show that, with the application of certain parts of the theory of functions, it is possible to derive some congruences connected with the solution of a certain diophantine equation. The use of analysis to derive certain arithmetical facts is not new, a typical such paper is that of Rademacher,[1] on the derivation of the Dedekind reciprocal formula. The methods of analysis have been used repeatedly in analytic number theory. Rademacher in an invitation address said:[2] "It would, however, be a misplacement of emphasis if we were to look upon analysis, which here means function theory, only as a tool applied to investigation of number theory. It is more the inner harmony of a system which we wish to depict, $\cdots$." Here, by analysis, we shall derive general congruences from which the previously known congruences will appear as special cases. Heretofore these special congruences have been developed not as a single entity, but by a gradual sharpening of the methods used, which were primarily algebraic in character.

1. **Historical résumé.** The solution of the diophantine equation

$$x^p + y^p + z^p = 0, \qquad p = \text{odd prime}, \tag{1.1}$$

in terms of the integers x, y, z prime to p, is connected with the congruences

$$B_n f_{p-2n}(t) \equiv 0 \pmod{p}, \qquad f_{p-1}(t) \equiv 0 \pmod{p}, \tag{1.2}$$

where $-t$ may be any of the quantities

$$x/y,\ y/x,\ x/z,\ z/x,\ y/z,\ z/y \pmod{p},$$

and where

$$f_r(t) = \sum_{i=0}^{p-1} i^{r-1} t^i \qquad (r > 1,\ n = 1, 2, \cdots, (p-3)/2),$$

and $B_1 = 1/6$, $B_2 = 1/30$, $B_3 = 1/42$, and so on, are the Bernoulli num-

Presented to the Society, April 17, 1942; received by the editors April 21, 1944.

[1] *Über a Reziprozitäts formel aus der Theorie der Modulfunktionen*, Matematikai es Physikai Lapok vol. 40 (1933) pp. 24–31 (in German), Zusammenfassung, pp. 32–34 (Hungarian).

[2] *Fourier expansions of modular forms and problems of partition*, Bull. Amer. Math. Soc. vol. 46 (1940) pp. 59–73.