

# 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,<sup>1</sup> 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:<sup>2</sup> "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, . . . ." 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

$$(1.1) \quad x^p + y^p + z^p = 0, \quad p = \text{odd prime},$$

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

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

where  $-t$  may be any of the quantities

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

and where

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

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.

<sup>1</sup> *Über a Reziprozitäts formel aus der Theorie der Modulfunktionen*, *Matematikai es Fizikai Lapok* vol. 40 (1933) pp. 24-31 (in German), *Zusammenfassung*, pp. 32-34 (Hungarian).

<sup>2</sup> *Fourier expansions of modular forms and problems of partition*, *Bull. Amer. Math. Soc.* vol. 46 (1940) pp. 59-73.

bers. The congruences involving the  $B$ 's are generally referred to as the Kummer criteria for the solution of (1.1).<sup>3</sup>

Vandiver<sup>4</sup> in studying the equation (1.1) has obtained certain generalizations of (1.2). For this purpose he introduced the polynomial

$$(1.3) \quad \sum_{s=0}^{p-1} (ks + l)^{n-1} x^s = h_n^{(k,l)}(x),$$

where  $p, n, k = 1, 2, \dots; l = 1, 2, \dots, k-1; x$  is arbitrary. Then, Vandiver has shown that, if (1.1) is satisfied by integers  $x, y, z$ , prime to  $p$ ,

$$(1.4) \quad \sum_{l=0}^{k-1} h_n^{(k,l)}(t) h_{p-n}^{(k,k-l)}(t) \equiv 0 \pmod{p},$$

$n = 1, 2, \dots, p-1; k$  being any positive integer and  $-t$  the ratio of any pair of  $x, y, z$  modulus  $p$ . Relation (1.4) will be referred to as the general congruences of Vandiver. For  $k = 1$ , (1.4) reduces to the form

$$(1.5) \quad f_n(t) f_{p-n}(t) \equiv 0 \pmod{p}.$$

The relation (1.5) will be referred to as the Mirimanoff congruences.<sup>5</sup>

For  $k = 2$ , after using (1.5) we have

$$(1.6) \quad h_n^{(2,1)}(t) h_{p-n}^{(2,1)}(t) \equiv 0 \pmod{p}.$$

This latter relation will be referred to as the special congruences of Vandiver.<sup>6</sup>

**2. Analytic approach.** The foundation of the analytic approach to our problem is based upon the use of a function studied by Maier<sup>7</sup> and the addition-theorems obtained by Maier for this function. The function, denoted by  $f(x, u)$ ,<sup>8</sup> was defined by the series

<sup>3</sup> See Kummer's memoir, *Abhandlungen der Akademie der Wissenschaften zu Berlin* (1857) pp. 41-77. See also the papers of Vandiver under the title *On Kummer's memoir of 1857 concerning Fermat's Last Theorem*, *Proc. Nat. Acad. Sci. U.S.A.* vol. 6 (1920) pp. 266-268; and *Bull. Amer. Math. Soc.* vol. 28 (1922) pp. 400-407. For a brief history of this problem, read Mordell, *Fermat's Last Theorem*, Cambridge Press, 1921.

<sup>4</sup> *Transformations of the Kummer criteria in connection with Fermat's Last Theorem*, *Ann. of Math.* vol. 27 (1926) pp. 171-176.

<sup>5</sup> *L'Equation indéterminée  $x^l + y^l + z^l = 0$  et le criterium de Kummer*, *J. Reine Angew. Math.* vol. 128 (1905) pp. 45-68.

<sup>6</sup> *Note on some results concerning Fermat's Last Theorem*, *Bull. Amer. Math. Soc.* vol. 28 (1922) pp. 258-260.

<sup>7</sup> *Zur Theorie der elliptischen Funktionen*, *Math. Ann.* vol. 104 (1931) pp. 745-769.

<sup>8</sup> The choice of the function  $f(x, u)$ , which can be thought of as a generating function for the Bernoulli polynomials, or a function related to it, appears reasonable when we recall the intimate connection between the Bernoulli numbers and many of the congruences connected with the attempted solutions of Fermat's Last Theorem.

$$(2.1) \quad f(x, u) = \sum_{k=-\infty}^{+\infty} \frac{e^{2\pi i x k}}{u + k},$$

for  $0 < x < 1$ , and  $u \not\equiv 0 \pmod{1}$ . Further, it has been shown, by considering a special contour integral,<sup>9</sup> that

$$(2.2) \quad f(x, u) = 2\pi i \frac{e^{-2\pi i x u}}{1 - e^{-2\pi i u}},$$

$u \not\equiv 0 \pmod{1}$ . In this form the function  $f(x, u)$  is defined for all values of  $x$ . One of the addition-laws obtained by Maier for  $f(x, u)$  is:

$$(2.3) \quad \begin{aligned} f(x, u)f(\xi, v) &= f(\xi, u + v)f(x - \xi, u) \\ &\quad - f(x, u + v)f(x - \xi, -v), \end{aligned}$$

$0 < \xi < x < 1$ ;  $u, v, (u + v) \not\equiv 0 \pmod{1}$ .

It was necessary, for this work, to introduce a new function, denoted by  $f_p(x, u)$ , and defined as

$$(2.4) \quad f_p(x, u) = f(x + p, u) - f(x, u), \quad p \equiv 0 \pmod{1}.$$

Now, on using (2.2), we obtain the following relations for the functions  $f(x, u)$  and  $f_p(x, u)$ , which will prove useful for our immediate purpose.

$$(2.5) \quad f(x, u) + f(1 - x, -u) = 0.$$

$$(2.6) \quad f(x, u) = \frac{f_p(x, u)}{e^{-2\pi i p u} - 1}.$$

$$(2.7) \quad f_p(x, u) = -2\pi i \sum_{k=0}^{p-1} e^{-2\pi i(x+k)u}.$$

$$(2.8) \quad f_p(x, u) + f_{-p}(1 - x, -u) = 0.$$

$$(2.9) \quad f_p(x + p, u) = e^{-2\pi i p u} f_p(x, u).$$

$$(2.10) \quad f_{-p}(x, u) = -f_p(x - p, u) = -e^{2\pi i p u} f_p(x, u).$$

Next, from the definition (2.4) and the above relations, we derive an addition-theorem for the function  $f_p(x, u)$ , which for our needs takes the form:

<sup>9</sup> Namely, the integral  $I_n = \int_{C_n} (e^{(2\mu-1)\pi i} / \sin \pi z) \cdot (dz / (z+u))$ , where  $0 < \mu < 1$ ,  $u \not\equiv 0 \pmod{1}$  and where  $C_n$  is a rectangle with sides  $x = \pm(2n+1/2)$  and  $y = \pm m$ , where  $m$  is an arbitrarily large positive number and  $n$  an arbitrarily large positive integer so chosen that  $z = -u$  lies in the interior of the rectangle  $C_n$ . Finally it is shown that  $\lim_{m, n \rightarrow \infty} I_n = 0$ .

$$\begin{aligned}
 & f_p(x + p, u + \alpha)f_p(\xi + p, v + \beta) - f_p(x, u + \alpha)f_p(\xi, v + \beta) \\
 & = f_p(\xi + p, u + v + \alpha + \beta)f_p(x - \xi - p, u + \alpha) \\
 (2.11) \quad & - f_p(\xi, u + v + \alpha + \beta)f_p(x - \xi, u + \alpha) \\
 & + f_p(x + p, u + v + \alpha + \beta)f_p(x - \xi, -v - \beta) \\
 & - f_p(x, u + v + \alpha + \beta)f_p(x - \xi - p, -v - \beta),
 \end{aligned}$$

where  $u + \alpha, v + \beta, u + v + \alpha + \beta \not\equiv 0 \pmod{1}$  and  $p \equiv 0 \pmod{1}$ .

Next, in the analytical development, we consider some special contour integrals involving the function  $f_p(x, u)$ . In order to illustrate our procedure, let us consider some sample integrals. First,

$$\int_C \frac{du}{u^k} f_p(x, u + \alpha).$$

Using (2.7) and the calculus of residues, this integral becomes

$$(2.12) \quad \int_C \frac{du}{u^k} f_p(x, u + \alpha) = \frac{(-1)^k (2\pi i)^{k+1}}{(k-1)!} \sum_{h=0}^{p-1} e^{-2\pi i(x+h)\alpha} (x+h)^{k-1},$$

where  $k=1, 2, \dots, p-1; p \equiv 0 \pmod{1}; (u+\alpha) \not\equiv 0 \pmod{1}$ , the path of integration  $C$  being a simple closed curve about the origin. Similarly, we obtain the expansion

$$\begin{aligned}
 & \int_C \frac{dv}{v^s} f_p(\xi + p, u + v + \alpha + \beta) \\
 (2.13) \quad & = \frac{(-1)^s (2\pi i)^{s+1}}{(s-1)!} \cdot \sum_{r=0}^{p-1} (\xi + r + p)^{s-1} \\
 & \quad \times (e^{-2\pi i\beta})^{\xi+r+p} (e^{-2\pi i(u+\alpha)})^{\xi+r+p},
 \end{aligned}$$

where  $s=1, 2, \dots, p-1; p \equiv 0 \pmod{1}; u + \alpha, v + \beta, u + v + \alpha + \beta \not\equiv 0 \pmod{1}$ , the path of integration being similar to that used in (2.12). Finally we obtain

$$\begin{aligned}
 & \int_C \int_{C'} \frac{du}{u^k} \frac{dv}{v^s} f_p(x - \xi - p, u + \alpha) f_p(\xi + p, u + v + \alpha + \beta) \\
 & = \int_C \frac{du}{u^k} f_p(x - \xi - p, u + \alpha) \int_{C'} \frac{dv}{v^s} f_p(\xi + p, u + v + \alpha + \beta) \\
 (2.14) \quad & = \frac{(-1)^{k+s} (2\pi i)^{k+s+2}}{(s-1)! (k-1)!} \cdot \sum_{r=0}^{p-1} \left\{ (\xi + r + p)^{s-1} (e^{-2\pi i\beta})^{\xi+r+p} \right. \\
 & \quad \left. \times \sum_{h=0}^{p-1} (x + r + h)^{k-1} (e^{-2\pi i\alpha})^{x+r+h} \right\},
 \end{aligned}$$

where  $k, s < p$ ;  $k, s, p \equiv 0 \pmod{1}$ ;  $(u + \alpha), (v + \beta), (u + v + \alpha + \beta) \not\equiv 0 \pmod{1}$ .

The method applied to the special contour integrals gives a device for expressing these and similar integrals as finite sums of terms involving all of the variables and parameters  $x, \xi, p, \alpha$ , and  $\beta$ . The integral (like (2.14)) of both members of the equation (2.1) can be written in the form:

$$\begin{aligned}
 & \sum_{h=0}^{p-1} (x + p + h)^{k-1} (e^{-2\pi i \alpha})^{x+p+h} \cdot \sum_{r=0}^{p-1} (\xi + p + r)^{s-1} (e^{-2\pi i \beta})^{\xi+p+r} \\
 & \quad - \sum_{h=0}^{p-1} (x + h)^{k-1} (e^{-2\pi i \alpha})^{x+h} \cdot \sum_{r=0}^{p-1} (\xi + r)^{s-1} (e^{-2\pi i \beta})^{\xi+r} \\
 (2.15) \quad & = \sum_{r=0}^{p-1} \left\{ (\xi + p + r)^{s-1} (e^{-2\pi i \beta})^{\xi+p+r} \right. \\
 & \quad \cdot \left. \sum_{h=0}^{p-1} (x + r + h)^{k-1} (e^{-2\pi i \alpha})^{x+r+h} \right\} \\
 & \quad - \sum_{r=0}^{p-1} \left\{ (\xi + r)^{s-1} (e^{-2\pi i \beta})^{\xi+r} \right. \\
 & \quad \cdot \left. \sum_{h=0}^{p-1} (x + r + h)^{k-1} (e^{-2\pi i \alpha})^{x+r+h} \right\} \\
 & \quad + \sum_{h=0}^{p-1} \left\{ (x + p + h)^{k-1} (e^{-2\pi i \alpha})^{x+p+h} \right. \\
 & \quad \cdot \left. \sum_{r=0}^{p-1} (\xi + p + h - r)^{s-1} (e^{-2\pi i \beta})^{\xi+p+h-r} \right\} \\
 & \quad - \sum_{h=0}^{p-1} \left\{ (x + h)^{k-1} (e^{-2\pi i \alpha})^{x+h} \right. \\
 & \quad \cdot \left. \sum_{r=0}^{p-1} (\xi + p + h - r)^{s-1} (e^{-2\pi i \beta})^{\xi+p+h-r} \right\}.
 \end{aligned}$$

In order to write this equation, (2.15), in a more symmetric form we shall put  $\lambda = r + h$  in the first two terms on the right side of (2.15), while in the last two terms on the right-hand side we shall put  $\mu = h - r$ . Next, we shall interchange the summation indices  $h$  and  $r$  in the first two terms on the right-hand side, and in the last two terms on the right we replace  $\mu$  by  $\lambda$ , thus obtaining the expression:

$$\begin{aligned}
 & \sum_{h=0}^{p-1} (x + p + h)^{k-1} (e^{-2\pi i \alpha})^{x+p+h} \sum_{r=0}^{p-1} (\xi + p + r)^{s-1} (e^{-2\pi i \beta})^{\xi+p+r} \\
 & \quad - \sum_{h=0}^{p-1} (x + h)^{k-1} (e^{-2\pi i \alpha})^{x+h} \sum_{r=0}^{p-1} (\xi + r)^{s-1} (e^{-2\pi i \beta})^{\xi+r} \\
 (2.16) \quad & = \sum_{h=0}^{p-1} \left[ \{ (\xi + p + h)^{s-1} (e^{-2\pi i \beta})^{\xi+p+h} (-\xi + h)^{s-1} (e^{-2\pi i \beta})^{\xi+h} \} \right. \\
 & \quad \cdot \left. \sum_{\lambda=h}^{p-1+h} (x + \lambda)^{k-1} (e^{-2\pi i \alpha})^{x+\lambda} \right] \\
 & \quad + \sum_{h=0}^{p-1} \left[ \{ (x + p + h)^{k-1} (e^{-2\pi i \alpha})^{x+p+h} - (x + h)^{k-1} (e^{-2\pi i \alpha})^{x+h} \} \right. \\
 & \quad \cdot \left. \sum_{\lambda=h}^{p-1+h} (\xi + p + \lambda)^{s-1} (e^{-2\pi i \beta})^{\xi+p+\lambda} \right]
 \end{aligned}$$

From the equation (2.16) we shall obtain congruences connected with the solution of the diophantine equation (1.1).

**3. Vandiver polynomial. A generalized polynomial.** In the previous section we developed a rather complicated equality involving finite sums. We shall now connect our work with some of the attempts that have been made to solve or extend the known range of validity of "Fermat's Last Theorem." Vandiver, in order to obtain a transformation of the Kummer criteria (1.2), introduced a polynomial, (1.3). These polynomials, (1.3), shall be referred to as the Vandiver polynomials. Then, following the successful lead of Vandiver, we shall introduce the polynomial

$$(3.1) \quad \sum_{s=-r}^{p-1-r} (s + z)^{n-1} t^{s+z} = h_n(-r; z, t),$$

for  $p, n, r \equiv 0 \pmod{1}$ ;  $r < p$ ; and any  $t$  and  $z$ . We shall refer to these as the generalized polynomials of Vandiver or for brevity as the generalized polynomials.

These new polynomials (3.1) are related to the polynomials of Vandiver (1.3) in the following manner:

$$\begin{aligned}
 (3.2) \quad h_n(0; c/d, t) & = \sum_{s=0}^{p-1} (s + c/d)^{n-1} t^{s+c/d} \\
 & = d^{-(n-1)} t^{c/d} \sum_{s=0}^{p-1} (ds + c)^{n-1} t^s \\
 & = d^{-(n-1)} t^{c/d} h_n^{(d,c)}(t),
 \end{aligned}$$

where  $p, n, c, d \equiv 0 \pmod{1}$ ;  $c < d$ ; and  $t$  arbitrary.

Before making use of the generalized polynomials we shall list some of the special forms:

$$(3.3) \quad h_n(0; 0, t) = \sum_{s=0}^{p-1} s^{n-1} t^s = f_n(t),$$

$$(3.4) \quad h_n(0; 1/2, t) = 2^{-(n-1)} t^{1/2} h_n^{(2,1)}(t),$$

$$(3.5) \quad h_n(0; (d-c)/d, t) = d^{-(n-1)} t^{(d-c)/d} h_n^{(d, d-c)}(t),$$

where  $p, n, c, d \equiv 0 \pmod{1}$ ;  $c < d$ ;  $n < p$ ;  $t$  arbitrary. The function  $f_n(t)$ , in (3.3), was used by Mirimanoff in his transformation (1.5) of the Kummer criteria. The function  $h_n^{(2,1)}(t)$  in (3.4) was used by Vandiver in obtaining a transformation of the Kummer criteria, namely (1.6). Finally the functions  $h_n^{(d, d-c)}(t)$  from (3.5) and  $h_n^{(d, c)}(t)$  from (3.2) were used by Vandiver in his general transformation, (1.4), of the Kummer criteria.

Next, let us consider the sum

$$(3.6) \quad \sum_{\lambda=h}^{h-p+1} (\xi + p + \lambda)^{n-1} \tau^{\xi+p+\lambda} = \sum_{\nu=h}^{h+p-1} (\xi + \nu + 1)^{n-1} \tau^{\xi+\nu+1} \\ = h_n(h; \xi + 1, \tau).$$

We shall develop, in the following, other properties of the generalized polynomials (2.12).

The equation (2.16), which we obtained as an expansion of certain contour integrals similar to (2.14), on replacing  $e^{-2\pi i\alpha}$  by  $t$  and  $e^{-2\pi i\beta}$  by  $\tau$ , can be written in terms of the generalized Vandiver polynomials,  $h_n(-r; z, t)$ . This equation, (2.16), after applying (3.6), can be written as

$$(3.7) \quad h_k(0; x + p, t) h_s(0; \xi + p, \tau) - h_k(0; x, t) h_s(0; \xi, \tau) \\ = \sum_{h=0}^{p-1} [h_k(h; x, t) \{ (\xi + p + h)^{s-1} \tau^{\xi+p+h} - (\xi + h)^{s-1} \tau^{\xi+h} \}] \\ + \sum_{h=0}^{p-1} [h_s(h; \xi + 1, \tau) \{ (x + p + h)^{k-1} t^{x+p+h} \\ - (x + h)^{k-1} t^{x+h} \}].$$

This equation will be used to obtain a variety of congruences connected with the solution of equation (1.1).

**4. Some special congruences.** In this section we shall derive some special congruences which are necessary for the final derivation of our general congruences.

The definition of the generalized polynomials gives us

$$\begin{aligned}
 h_n(0; a\phi, t)h_{p-n}(0; b\phi, t) &= \left( \sum_{h=0}^{p-1} (h + a\phi)^{n-1} t^{h+ap} \right) \left( \sum_{s=0}^{p-1} (s + b\phi)^{p-n-1} t^{s+b\phi} \right) \\
 &= t^{(a+b)\phi} \left( \sum_{h=0}^{p-1} (h + a\phi)^{n-1} t^{h\phi} \right) \left( \sum_{s=0}^{p-1} (s + b\phi)^{p-n-1} t^{s\phi} \right) \\
 &\equiv t^{(a+b)\phi} \left( \sum_{h=0}^{p-1} h^{n-1} t^{h\phi} \right) \left( \sum_{s=0}^{p-1} s^{p-n-1} t^{s\phi} \right) \pmod{\phi} \\
 &= t^{(a+b)\phi} h_n(0; 0, t) h_{p-n}(0; 0, t) \\
 &= t^{(a+b)\phi} f_n(t) f_{p-n}(t).
 \end{aligned}$$

Hence we obtain the following variation of the Mirimanoff congruences (1.5), namely<sup>10</sup>

$$(4.1) \quad t^{-(a+b)\phi} h_n(0; a\phi, t) h_{p-n}(0; b\phi, t) \equiv 0 \pmod{\phi},$$

where  $a, b = 0, \pm 1, \pm 2, \dots$ . A particularly simple congruence occurs when  $a = -b$ , namely

$$(4.2) \quad h_n(0; a\phi, t) h_{p-n}(0; -a\phi, t) \equiv 0 \pmod{\phi}.$$

If we put  $a=b=0$  in (4.1) this reduces to the original Mirimanoff congruences (1.5).

Let us next consider the product  $h_n(0; 1/2, t)h_{p-n}(0; 1/2, t)$  which reduces to  $t^{2-(p-2)} h_n^{(2,1)}(t) h_{p-n}^{(2,1)}(t)$ . Thus from the special congruences of Vandiver, (1.6), we have

$$(4.3) \quad t^{-1} 2^{p-2} h_n(0; 1/2, t) h_{p-n}(0; 1/2, t) \equiv 0 \pmod{\phi}.$$

In the same manner we obtain the congruences

$$(4.4) \quad 2^{p-2} t^{-1-(a+b)\phi} h_n(0; 1/2 + a\phi, t) h_{p-n}(0; 1/2 + b\phi, t) \equiv 0 \pmod{\phi},$$

where  $a, b = 0, \pm 1, \pm 2, \dots$ .

Following much the same procedure as before we shall derive some transformations of the general congruences of Vandiver, (1.4). For this purpose let us consider first

$$\sum_{c=0}^{d-1} h_n(0; c/d, t) h_{p-n}(0; (d-c)/d, t),$$

<sup>10</sup> In all the congruences given in this paper the following statements are understood. If the equation  $x^p + y^p + z^p = 0$ ,  $p = \text{odd prime}$ , is satisfied by integers  $x, y, z$  prime to  $p$ , where  $-t$  may be any of the quantities  $x/y, y/x, x/z, z/x, y/z, z/y \pmod{p}$ , then the congruences are satisfied.



where  $p, n, c, d \equiv 0 \pmod{1}$ ;  $c < d$ . This sum can be written in the form

$$\begin{aligned} & \sum_{c=0}^{d-1} \left[ \left( \sum_{h=0}^{p-1} (h + c/d)^{n-1} t^{h+c/d} \right) \left( \sum_{s=0}^{p-1} (s + (d-c)/d)^{p-n-1} t^{s+(d-c)/d} \right) \right] \\ &= t d^{-(p-2)} \sum_{c=0}^{d-1} \left[ \left( \sum_{h=0}^{p-1} (hd + c)^{n-1} t^h \right) \left( \sum_{s=0}^{p-1} (sd + d - c)^{p-n-1} t^s \right) \right] \\ &= t d^{-(p-2)} \sum_{c=0}^{d-1} h_n^{(d,c)}(t) h_{p-n}^{(d,d-c)}(t). \end{aligned}$$

Hence the general congruences of Vandiver, (1.4), are replaced by the relation

$$(4.5) \quad d^{(p-2)} t^{-1} \sum_{c=0}^{d-1} h_n(0; c/d, t) h_{p-n}(0; (d-c)/d, t) \equiv 0 \pmod{p}.$$

Next, if we consider the sum

$$\sum_{c=0}^{d-1} h_n(0; c/d + ap, t) h_{p-n}(0; (d-c)/d + bp, t)$$

we obtain another transformation of (1.4), namely

$$(4.6) \quad d^{(p-2)} t^{-1-(a+b)p} \sum_{c=0}^{d-1} h_n(0; c/d + ap, t) h_{p-n}(0; (d-c)/d + bp, t) \equiv 0 \pmod{p},$$

where  $p, n, c, d \equiv 0 \pmod{1}$ ;  $c < d$ ; and  $a, b = 0, \pm 1, \pm 2, \dots$

**5. Some general congruences.** In §3 we derived an addition-theorem (3.7) for the generalized polynomials of Vandiver, (3.1). Since (3.7) is an identity in  $x, \xi, t, \tau, k$ , and  $s$  we can substitute particular values for the variables and parameters without destroying the equality. Among a variety of possible substitutions we shall introduce the following:

- (A)  $x = \xi = 0,$
- (B)  $x = mp, \quad \xi = qp,$
- (C)  $x = 1/2 + mp, \quad \xi = 1/2 + qp,$
- (D)  $x = c/d + mp, \quad \xi = (d-c)/d + qp,$

and in each case we put

$$\tau = t, \quad k = n, \quad s = p - n,$$

where  $p, n, c, d \equiv 0 \pmod{1}$ ;  $c < d$ ; and  $m, q = 0, \pm 1, \pm 2, \dots$

Now, on applying, successively, these substitutions to the equation (3.7) we shall obtain several different quadratic functional equations for  $h_n(-r; x, t)$ .

The congruences resulting from applying (A) to the equation (3.7) and by using a proper choice of  $a$  and  $b$  in (4.1) give us a direct transformation of the Mirimanoff congruences, (1.5).

On applying (B) to (3.7) and using (4.1) we obtain the congruence

$$\begin{aligned}
 (5.1) \quad & \sum_{h=0}^{p-1} [h_n(h; m\phi, t) \{ ((q+1)\phi + h)^{p-n-1} t^{-(m+1)p+h} \\
 & \hspace{10em} - (q\phi + h)^{p-n-1} t^{-(m+2)p+h} \} ] \\
 & + \sum_{h=0}^{p-1} [h_{p-n}(h; q\phi + 1, t) \{ ((m+1)\phi + h)^{n-1} t^{-(q+1)p+h} \\
 & \hspace{10em} - (m\phi + h)^{n-1} t^{-(q+2)p+h} \} ] \\
 & + t^{-(m+q+2)p} h_n(0; m\phi, t) h_{p-n}(0; q\phi, t) \equiv 0 \pmod{\phi}.
 \end{aligned}$$

If we put  $m=q=0$  in (5.1) we obtain the same congruence which resulted from applying (A) to (3.7).

Next on applying (C) and (D) respectively to (3.7) and using appropriate forms of (4.4), (4.5) and (4.6) we obtain the following congruences

$$\begin{aligned}
 (5.2) \quad & 2^{p-2} \sum_{h=0}^{p-1} [h_n(h; 1/2 + m\phi, t) \{ (1/2 + (q+1)\phi + h)^{p-n-1} \\
 & \hspace{10em} t^{-1/2-(m+1)p+h} - (1/2 + q\phi + h)^{p-n-1} t^{-1/2-(m+2)p+h} \} ] \\
 & + 2^{p-2} \sum_{h=0}^{p-1} [h_{p-n}(h; 3/2 + q\phi, t) \{ (1/2 + (m+1)\phi + h)^{n-1} \\
 & \hspace{10em} t^{-1/2-(q+1)p+h} - (1/2 + m\phi + h)^{n-1} t^{-1/2-(q+2)p+h} \} ] \\
 & + 2^{p-2} t^{-1-(m+q+2)p} h_n(0; 1/2 + m\phi, t) h_{p-n}(0; 1/2 + q\phi, t) \\
 & \hspace{15em} \equiv 0 \pmod{\phi}, \\
 (5.3) \quad & d^{p-2} \sum_{c=0}^{d-1} \sum_{h=0}^{p-1} [h_n(h; c/d + m\phi, t) \{ ((d-c)/d + (q+1)\phi + h)^{p-n-1} \\
 & \hspace{10em} \cdot t^{-c/d-(m+1)p+h} - ((d-c)/d + q\phi + h)^{p-n-1} t^{-c/d-(m+2)p+h} \} ] \\
 & + d^{p-2} \sum_{c=0}^{d-1} \sum_{h=0}^{p-1} [h_{p-n}(h; (2d-c)/d + q\phi, t) \{ (c/d + (m+1)\phi + h)^{n-1} \\
 & \hspace{10em} \cdot t^{-(d-c)/d-(q+1)p+h} - (c/d + m\phi + h)^{n-1} t^{-(d-c)/d-(q+2)p+h} \} ] \\
 & + d^{p-2} t^{-1-(m+q+2)p} \sum_{c=0}^{d-1} h_n(0; c/d + m\phi, t) \\
 & \hspace{10em} \cdot h_{p-n}(0; (d-c)/d + q\phi, t) \equiv 0 \pmod{\phi},
 \end{aligned}$$

where  $p, n, d \equiv 0 \pmod{1}$ ;  $n < p$ ;  $c = 0, 1, 2, \dots, d-1$ ; and  $m, q = 0, \pm 1, \pm 2, \dots$ .

Thus we have obtained transformations of the Mirimanoff and Vandiver congruences connected with the solution of equation (1.1). Other, and in some cases more symmetric, transformations of these congruences are possible by using one of the other permissible forms for the quadratic functional equation (2.11).

PURDUE UNIVERSITY

---

## DEVELOPMENT OF CERTAIN QUADRATIC FUNCTIONAL EQUATIONS

HAROLD F. S. JONAH

**1. Introduction.** In some work devoted to the derivation of certain congruences connected with the solution of Fermat's Last Theorem, it was found necessary to develop several quadratic functional equations of a particular function which we shall define later. This note will deal with the derivation of these functional equations. Maier<sup>1</sup> derived two such quadratic functional equations for a generating function of the Bernoulli polynomials. This work of Maier serves as the basis for our developments.

**2. The Maier results.** The function,  $f(x, u)$ , used by Maier was defined by the infinite series

$$(2.1) \quad \sum_{r=-\infty}^{+\infty} \frac{e^{2\pi i x r}}{u + r},$$

where  $x$  is a real variable satisfying the inequality  $0 < x < 1$ , and where  $u$  is a real variable subject to the restriction  $u \not\equiv 0 \pmod{1}$ . Maier, then, showed that if  $u, v, x, \xi$  are such that  $u, v, (u+v) \not\equiv 0 \pmod{1}$  and  $0 < \xi < x < 1$ , that the function  $f(x, u)$  is a solution of the functional equation

$$(2.2) \quad \begin{aligned} f(x, u)f(\xi, v) &= f(\xi, u + v)f(x - \xi, u) \\ &\quad - f(x, u + v)f(x - \xi, -v). \end{aligned}$$

---

Received by the editors April 21, 1944.

<sup>1</sup> W. Maier, *Zur Theorie der elliptischen Funktionen*, Math. Ann. vol. 104 (1930) pp. 745-769.