is solvable in F. Hence (27) reduces to

$$f(x_1, \ldots, x_k, x) = \sum_{j=0}^{k} b_j x_j^{p^{r_j}} + c_{s_0} x^{p^{s_0}} + d\,,$$

where clearly

$$\psi(b_j) = \lambda_j \quad (j = 1, \ldots, k)\,, \qquad \psi(c_{s_0}) = \lambda_{k+1}\,,$$

and the induction is complete.

Reference

[1] L. Carlitz, *A theorem on permutations in a finite field*, Proc. Amer. Math. Soc. 11 (1960), pp. 456-459.

DUKE UNIVERSITY

Reçu par la Rédaction le 9. 3. 1961

ACTA ARITHMETICA
VII (1962)

Congruence properties of certain linear homogeneous difference equations

by

L. Carlitz (Durham, North Carolina)

1. Introduction. In a recent paper [1] the writer considered the recurrence

$$u_{n+1} = f(n)\,u_n + g(n)\,u_{n-1}\,, \tag{1.1}$$

where $f(n), g(n)$ are polynomials in n (and possibly some additional indeterminates) with integral coefficients. It was assumed that

$$u_0 = 1\,, \quad u_1 = f(0)\,, \quad g(0) = 0\,. \tag{1.2}$$

The main result of [1] is contained in the congruence

$$\sum_{s=0}^{r} (-1)^s \binom{r}{s} u_{n+sm} u_m^{r-s} \equiv 0 \pmod{m^{r_1}}\,, \tag{1.3}$$

for all $n \geqslant 0$, $m \geqslant 1$, $r \geqslant 1$ and where

$$r_1 = [(r+1)/2]\,, \tag{1.4}$$

the greatest integer $\leqslant (r+1)/2$. Indeed, to get (1.3) it is only necessary to assume that the coefficients of the polynomials $f(n), g(n)$ are integral $(\operatorname{mod} m)$.

A number of applications of (1.3) were given, in particular to the polynomials of Hermite and Laguerre.

It seems natural to consider the recurrence

$$u_{n+1}^{(k)} = a_0(n)\,u_n^{(k)} + a_1(n)\,u_{n-1}^{(k)} + \ldots + a_k(n)\,u_{n-k}^{(k)} \tag{1.5}$$

of order $k+1$, where the $a_j(n)$ are polynomials in n with integral coefficients. Corresponding to (1.2) we now assume that

$$a_j(s) = 0 \quad (s = 0, 1, \ldots, j-1,\ j = 1, \ldots, k); \tag{1.6}$$

also we suppose that (1.5) holds for all $n \geqslant 0$. In view of (1.6) it is not necessary to explicitly define $u_{-1}^{(k)}, \ldots, u_{-k}^{(k)}$. We take $u_0^{(k)} = 1$ and it follows that

$$u_1^{(k)} = a_0(0)\,, \quad u_2^{(k)} = a_0(1)\,u_1^{(k)} + a_1(1)\,, \quad \text{etc.}$$

We shall show that $u_n^{(k)}$ satisfies the congruence

$$\sum_{s=0}^{r} (-1)^s \binom{r}{s} u_{n+sm}^{(k)} (u_m^{(k)})^{r-s} \equiv 0 \pmod{m^{r_1}}, \tag{1.7}$$

for all $n \geqslant 0$, where r_1 is defined by (1.4). For a somewhat more general result see Theorem 4 below.

A number of applications of (1.7) are discussed. For example the sequence $\{u_n\}$ defined by

$$\exp\left\{a_0 t + a_1 \frac{t^2}{2} + \ldots + a_k \frac{t^{k+1}}{k+1}\right\} = \sum_{n=0}^{\infty} u_n \frac{t^n}{n!},$$

where the a_j are integers (or polynomials in several indeterminates with integral coefficients), is shown to satisfy a recurrence of the form (1.5). Moreover the final result is made more explicit by determining the residue of $u_m \pmod m$, when certain conditions are satisfied (see Theorems 8 and 9 below). In the second place the sequence $\{u_n\}$ defined by means of

$$(1-at)^{-x}(1-bt)^{-y}(1-ct)^{-z} = \sum_{n=0}^{\infty} u_n \frac{t^n}{n!}$$

also satisfies a recurrence of the form (1.5) of order three; the number of factors on the left side can be increased. Finally some more special applications are discussed in § 7.

2. As in [1] we consider in place of (1.5) the recurrence of order $k+1$:

$$u_{n+1}^{(k)}(x) = \big(x + a_0(n)\big) u_n^{(k)}(x) + \sum_{j=1}^{k} a_j(n) u_{n-j}^{(k)}(x), \tag{2.1}$$

where as before the $a_j(n)$ are polynomials in n with integral coefficients; the $a_j(n)$ may contain additional indeterminates but are independent of x. We assume that conditions (1.6) are satisfied and that (2.1) holds for all $n \geqslant 0$. We take $u_0^{(k)}(x) = 1$ and it follows that

$$u_1^{(k)}(x) = x + a_0(0), \quad u_2^{(k)}(x) = \big(x + a_0(1)\big) u_1^{(k)}(x) + a_1(1), \quad \text{etc.}$$

Clearly $u_n^{(k)}(x)$ is a polynomial in x of degree n with highest coefficient equal to 1.

We show first that if m is an arbitrary integer $\geqslant 1$ then

$$u_n(x) u_m(x) \equiv u_{n+m}(x) \pmod m, \tag{2.2}$$

for all $n \geqslant 0$, where for brevity we put

$$u_n(x) = u_n^{(k)}(x). \tag{2.3}$$

For $n = 0$, (2.2) is obvious. For $n = 1$ we have by (2.1) and (1.6)

$$\begin{aligned} u_{m+1}(x) &= \big(x + a_0(m)\big) u_m(x) + \sum_{j=1}^{k} a_j(m) u_{m-j}(x) \\ &\equiv \big(x + a_0(0)\big) u_m(x) + \sum_{j=1}^{k} a_j(0) u_{m-j}(x) \\ &\equiv \big(x + a_0(0)\big) u_m(x) \\ &\equiv u_1(x) u_m(x) \pmod m. \end{aligned}$$

For $n = 2$ we have

$$\begin{aligned} u_{m+2}(x) &= \big(x + a_0(m+1)\big) u_{m+1}(x) + \sum_{j=1}^{k} a_j(m+1) u_{m+1-j}(x) \\ &\equiv \big(x + a_0(1)\big) u_{m+1}(x) + \sum_{j=1}^{k} a_j(1) u_{m+1-j}(x) \\ &\equiv \big(x + a_0(1)\big) u_{m+1}(x) + a_1(1) u_m(x) \\ &\equiv \Big\{\big(x + a_0(1)\big) u_1(x) + a_1(1)\Big\} u_m(x) \\ &\equiv u_2(x) u_m(x) \pmod m. \end{aligned}$$

Assume that (2.2) holds for $n = 0, 1, \ldots, s$, where s is a fixed integer $< k$. Then (2.1) yields

$$\begin{aligned} a_{s+m+1}(x) &= \big(x + a_0(s+m)\big) u_{s+m}(x) + \sum_{j=1}^{k} a_j(s+m) u_{s+m-j}(x) \\ &\equiv \big(x + a_0(s)\big) u_{s+m}(x) + \sum_{j=1}^{s-1} a_j(s) u_{s+m-j}(x) \\ &\equiv \Big(\big(x + a_0(s)\big) u_s(x) + \sum_{j=1}^{s-1} a_j(s) u_{s-j}(x)\Big) u_m(x) \\ &\equiv u_{s+1}(x) u_m(x) \pmod m. \end{aligned}$$

Hence (2.2) holds for $s+1$ and therefore for all $n = 0, 1, \ldots, k$.

It is now easy to complete the proof of (2.2). Indeed,

$$\begin{aligned} u_{n+m+1}(x) &\equiv \big(x + a_0(n+m)\big) u_{n+m}(x) + \sum_{j=1}^{k} a_j(n+m) u_{n+m-j}(x) \\ &\equiv \Big\{x + a_0(n) u_n(x) + \sum_{j=1}^{k} a_j(n) u_n(x)\Big\} u_m(x) \\ &\equiv u_{n+1}(x) u_m(x) \pmod m. \end{aligned}$$

We may state

THEOREM 1. *Let $u_n(x)$ be the sequence of polynomials defined by* (2.1) *and* (1.6), *where the $a_j(n)$ are polynomials in n with integral coefficients. Then*

$$u_n(x)\,u_m(x) \equiv u_{n+m}(x) \pmod{m}$$

for all $n \geqslant 0$, $m \geqslant 1$.

A little more generally we have

THEOREM 2. *Let $u_n(x) = u_n^{(k)}(x)$ be the sequence of polynomials defined by* (2.1) *and* (1.6), *where the $a_j(n)$ are polynomials in n with coefficients integral* (mod m). *Then we have*

$$u_{n+tm}(x) \equiv u_n(x)\,u_{tm}(x) \equiv u_n(x)\,u_m^t(x) \pmod{m} \tag{2.4}$$

for all $n \geqslant 0$, $t \geqslant 1$, $m \geqslant 1$.

An immediate corollary is contained in

THEOREM 3. *Let $u_n = u_n^{(k)}$ be the sequence defined by* (1.5) *and* (1.6), *where the $a_j(n)$ are polynomials in n with coefficients integral* (mod m). *Then*

$$u_{n+tm} \equiv u_n u_{tm} \equiv u_n u_m^t \pmod{m} \tag{2.5}$$

for all $n \geqslant 0$, $t \geqslant 1$, $m \geqslant 1$.

3. It follows from (2.1) that

$$xu_n(x) = u_{n+1}(x) - \sum_{j=0}^{k} a_j(n)\,u_{n-j}(x)\,. \tag{3.1}$$

Repeated application of (3.1) leads to

$$x^s u_n(x) = \sum_{j=-ks}^{s} A_{sj}(n)\,u_{n+j}(x) \qquad (s, n = 0, 1, 2, \ldots)\,,$$

where in the summation we may suppose $j \geqslant -n$; the $A_{sj}(n)$ are polynomials in n with coefficients integral (mod m). It follows that

$$u_n(x)\,u_m^t(x) - u_{n+tm}(x) = \sum_{j=-ktm}^{tm} B_j(n)\,u_{n+j}(x) \qquad (s, n = 0, 1, 2, \ldots)\,, \tag{3.2}$$

where the $B_j(n) = B_j(n;\,t,\,m)$ are also polynomials in n with coefficients integral (mod m). Also we may assume that in the summation $j \geqslant -n$, or what is the same thing

$$B_j(n) = 0 \qquad (-ktm \leqslant j < -n)\,. \tag{3.3}$$

We shall require the

LEMMA. *Let $u_0(x), u_1(x), u_2(x), \ldots, u_n(x)$ denote a set of polynomials in x with coefficients integral* (mod m) *and highest coefficients equal to* 1. *Also let*

$$\deg u_s(x) = s \qquad (0 \leqslant s \leqslant N)\,.$$

Let $A_0, A_1, \ldots, A_N$ be integral (mod m) *and such that*

$$\sum_{s=0}^{N} A_s u_s(x) \equiv 0 \pmod{m}\,.$$

Then it follows that

$$A_s \equiv 0 \pmod{m} \qquad (0 \leqslant s \leqslant N)\,.$$

For the proof see [1], p. 151.

By (2.3) and (3.2) we have

$$\sum_{j=-ktm}^{tm} B_j(n)\,u_{n+j}(x) \equiv 0 \pmod{m}\,. \tag{3.4}$$

Applying the Lemma to (3.4) we get

$$B_j(n) \equiv 0 \pmod{m} \qquad (-ktm \leqslant j \leqslant tm)\,. \tag{3.5}$$

We now define the operator Δ by means of

$$\Delta\varphi_n = u_m^t(x)\,\varphi_n - \varphi_{n+tm}\,, \tag{3.6}$$

where t and m are fixed integers $\geqslant 1$. More generally we define for $r \geqslant 1$

$$\Delta^r\varphi_n = u_m^t(x)\,\Delta^{r-1}\varphi_n - \Delta^{r-1}\varphi_{n+mt}\,. \tag{3.7}$$

In (3.6) and (3.7) φ_n is an arbitrary function of n. It follows from (3.7) that

$$\Delta^r\varphi_n = \sum_{s=0}^{r} (-1)^s \binom{r}{s} u_m^{t(r-s)}(x)\,\varphi_{n+stm}\,. \tag{3.8}$$

If we apply Δ^{r-1} to (3.2) we get

$$\Delta^r u_n(x) = \sum_{j=-ktm}^{tm} \Delta^{r-1}\{B_j(n)\,u_{n+j}(x)\}\,. \tag{3.9}$$

In addition to the operator Δ we shall require also the operator δ^r defined by

$$\delta^r\varphi_n = \sum_{s=0}^{r} (-1)^s \binom{r}{s} \varphi_{n+stm}\,. \tag{3.10}$$

Cleary (3.10) is equivalent to

$$\varphi_{n+rtm} = \sum_{s=0}^{r} (-1)^s \binom{r}{s} \delta^s\varphi_n\,. \tag{3.11}$$

Returning to (3.9) we get

$$\Delta^{r-1}\{B_j(n)a_{n+j}(x)\}$$

$$=\sum_{s=0}^{r-1}(-1)^s\binom{r-1}{s}u_m^{t(r-1-s)}(x)B_j^{(n+stm)}u_{n+j+stm)}(x)$$

$$=\sum_{s=0}^{r-1}(-1)^s\binom{r-1}{s}u_m^{t(r-1-s)}(x)u_{n+j+stm}(x)\cdot\sum_{i=0}^{s}(-1)^i\binom{s}{i}\delta^iB_j(n)$$

$$=\sum_{i=0}^{r-1}\binom{r-1}{i}\delta^iB_j(n)\sum_{s=1}^{r-1}(-1)^{s-i}\binom{r-1-i}{s-i}u_m^{t(r-1-s)}(x)u_{n+j+stm}(x)$$

$$=\sum_{i=0}^{r-1}\binom{r-1}{i}\delta^iB_j(n)\sum_{s=0}^{r-1-i}(-1)^s\binom{r-1-i}{s}u_m^{t(r-1-i-s)}(x)u_{n+j+(i+s)tm}(x)$$

$$=\sum_{i=0}^{i-1}\binom{r-1}{i}\delta^iB_j(n)\cdot\Delta^{r-1-i}u_{n+j+itm}(x)\,.$$

Substituting in (3.9) we get

$$\Delta^r u_n(x)=\sum_{j=-ktm}^{tm}\sum_{i=0}^{r-1}\binom{r-1}{i}\delta^iB_j(n)\cdot\Delta^{r-1-i}u_{n+j+itm}(x)\,. \tag{3.12}$$

We shall now prove by an induction on r that

$$\Delta^r u_n(x)\equiv 0 \pmod{m^{r_1}} \tag{3.13}$$

for all $r\geqslant 1$, where r_1 is defined by (1.4). The case $r=1$ is contained in (2.4). We accordingly assume that (3.13) holds up to and including the value $r-1$. Since $B_j(n)$ is a polynomial in n with coefficients integral $(\operatorname{mod} m)$, it follows from (3.10) and the elements of finite differences that

$$\delta^iB_j(n)\equiv 0 \pmod{m^i}\,. \tag{3.14}$$

Consider the typical product

$$A_i=\delta^iB_j(n)\cdot\Delta^{r-1-i}u_{n+j+itm}(x) \tag{3.15}$$

occurring in the right member of (3.12). For $i=0$ it follows from (3.5) and the inductive hypothesis that

$$A_0\equiv 0 \pmod{m^{1+[r/2]}}\,. \tag{3.16}$$

For $i\geqslant 1$ it follows from (3.14) and the inductive hypothesis that

$$A_i\equiv 0 \pmod{m^{i+[(r-i)/2]}}\,. \tag{3.17}$$

Since

$$1+[r/2]\geqslant[(r+1)/2]\,,$$
$$i+[(r-i)/2]\geqslant[(r+1)/2]\qquad(1\leqslant i<r)\,,$$

it is evident from (3.12), (3.15), (3.16) and (3.17) that

$$\Delta^r u_n(x)\equiv 0 \pmod{m^{r_1}}\,.$$

We may now state the main result.

THEOREM 4. *Let $u_n(x)=u_n^{(k)}(x)$ be the sequence of polynomials defined by* (2.1) *and* (1.6), *where the $a_j(n)$ are polynomials in n with coefficients integral* $(\operatorname{mod} m)$. *Then we have*

$$\sum_{s=0}^{r}(-1)^s\binom{r}{s}u_m^{t(r-s)}(x)u_{n+stm}(x)\equiv 0 \pmod{m^{r_1}} \tag{3.18}$$

for all $n\geqslant 0,\ r\geqslant 1,\ t\geqslant 1,\ m\geqslant 1$.

THEOREM 5. *Let $u_n=u_n^{(k)}$ be the sequence defined by* (1.5) *and* (1.6), *where the $a_j(n)$ are polynomials in n with coefficients integral* $(\operatorname{mod} m)$. *Then*

$$\sum_{s=0}^{r}(-1)^s\binom{r}{s}u_m^{t(r-s)}(x)u_{n+stm}\equiv 0 \pmod{m^{r_1}} \tag{3.19}$$

for all $n\geqslant 0,\ r\geqslant 1,\ t\geqslant 1,\ m\geqslant 1$.

Remark. By making very slight changes in the proof we can replace (3.18) and (3.19) by

$$\sum_{s=0}^{r}(-1)^s\binom{r}{s}u_{tm}^{r-s}(x)u_{n+stm}(x)\equiv 0 \pmod{m^{r_1}}\,, \tag{3.18'}$$

$$\sum_{s=0}^{r}(-1)^s\binom{r}{s}u_{tm}^{r-s}u_{n+stm}\equiv 0 \pmod{m^{r_1}}\,, \tag{3.19'}$$

respectively.

4. We state

THEOREM 6. *If the hypothesis of Theorem 4 are satisfied then*

$$\sum_{s=0}^{r}(-1)^s\binom{r}{s}u_{n+stm}(x)u_{j+(r-s)tm}(x)\equiv 0 \pmod{m^{r_1}} \tag{4.1}$$

for all $n\geqslant 0,\ j\geqslant 0$. *In particular*

$$\sum_{s=0}^{r}(-1)^s\binom{r}{s}u_{n+stm}u_{j+(r-s)tm}\equiv 0 \pmod{m^{r_1}}\,. \tag{4.2}$$

For a more general result we put

$$U_{n_1,\ldots,n_s}^{(r)}=u_1^{n_1}\ldots u_s^{n_s}(\lambda_1u_1^{tm}+\ldots+\lambda_su_s^{tm})^r\,, \tag{4.3}$$

where it is understood that after expanding the right member by the multinomial theorem, each $u_j^{n_j+mtr_j}$ is replaced by $u_{n_j+mtr_j}(x)$.

THEOREM 7. *Let $\lambda_1, \ldots, \lambda_s$ be integral* $(\bmod m)$ *and such that*

$$\lambda_1 + \ldots + \lambda_s \equiv 0 \pmod{m}. \tag{4.4}$$

Then if the hypothesis of Theorem 4 are satisfied it follows that

$$U^{(r)}_{n_1,\ldots,n_s} \equiv 0 \pmod{m^{r_1}} \tag{4.5}$$

for all $n_1 \geqslant 0, \ldots, n_s \geqslant 0, r \geqslant 1, t \geqslant 1, m \geqslant 1$.

The proof of this result is exactly the same as the proof of Theorem 2 of [1] and will be omitted.

5. We now discuss several applications of the above results. To begin with, consider the sequence $\{u_n\}$ defined by

$$\exp\left\{a_0 t + a_1 \frac{t^2}{2} + \ldots + a_k \frac{t^{k+1}}{k+1}\right\} = \sum_{n=0}^{\infty} u_n \frac{t^n}{n!}. \tag{5.1}$$

Differentiation with respect to y yields

$$(a_0 + a_1 t + \ldots + a_k t^k) \sum_{n=0}^{\infty} u_n \frac{t^n}{n!} = \sum_{n=0}^{\infty} u_{n+1} \frac{t^n}{n!},$$

so that

$$u_{n+1} = a_0 u_n + a_1 n u_{n-1} + a_2 n(n-1) u_{n-2} + \ldots + a_k n(n-1)\ldots(n-k+1) u_{n-k}. \tag{5.2}$$

In particular when $k = 1$, (5.1) includes the familiar generating function for the Hermite polynomials $\exp\{2at - t^2\}$.

In the general case we may put

$$u_n = C_n(a_0, a_1, \ldots, a_k), \tag{5.3}$$

where C_n is the cycle indicator of the symmetric group ([8], p. 68); note however that in the general definition of C_n the number of indeterminates is not limited.

If the coefficients $a_0, a_1, \ldots, a_k$ are indeterminates or rational numbers integral $(\bmod m)$, it is clear that Theorem 5 applies and we get

$$\sum_{s=0}^{r} (-1)^s \binom{r}{s} u_m^{t(r-s)} u_{n+stm} \equiv 0 \pmod{m^{r_1}} \tag{5.4}$$

for all $n \geqslant 0$.

However in the present situation we can make (5.4) more explicit by determining the residue $(\bmod m)$ of u_m. Indeed it follows from (5.1) that

$$u_m = \sum \frac{m!\, a_0^{n_1} a_1^{n_2} \ldots a_k^{n_{k+1}}}{n_1!\, n_2! \ldots n_{k+1}!\, 1^{n_1} 2^{n_2} \ldots (k+1)^{n_{k+1}}}, \tag{5.5}$$

where the summation is extended over all non-negative n_j such that

$$n_1 + 2n_2 + \ldots + (k+1) n_{k+1} = m. \tag{5.6}$$

If

$$\big(m, (k+1)!\big) = 1 \tag{5.7}$$

it follows easily from (5.5) and (5.6) that

$$u_m \equiv a_0^m \pmod{m}. \tag{5.8}$$

Therefore (5.4) reduces to

$$\sum_{r=0}^{r} (-1)^s \binom{r}{s} a_0^{tm(r-s)} u_{n+stm} \equiv 0 \pmod{m^{r_1}}. \tag{5.9}$$

In passing from (5.4) to (5.9) we have made use of the easily proved lemma that if

$$a_m \equiv \lambda \pmod{m}$$

then (5.5) is equivalent to

$$\sum_{s=0}^{r} (-1)^s \binom{r}{s} \lambda^{tm(r-s)} u_{n+stm} \equiv 0 \pmod{m^{r_1}}.$$

We may state

THEOREM 8. *If m satisfies* (5.7) *then the sequence u_n defined by* (5.1) *satisfies* (5.9) *for all $n \geqslant 0$. The coefficients $a_0, a_1, \ldots, a_k$ are either integral* $(\bmod m)$ *or polynomials in an arbitrary number of indeterminates with coefficients integral* $(\bmod m)$.

We remark that if a_j is divisible by $j+1$ for $j = 0, 1, \ldots, k$ then Theorem 8 applies without any restriction on m. In other words the sequence $\{u_n\}$ defined by

$$u_{n+1} = b_0 u_n + 2b_1 n u_{n-1} + 3b_2 n(n-1) u_{n-2} + \ldots + (k+1) b_k n(n-1)\ldots(n-k+1) u_{n-k},$$

where the b_j are integral (or polynomials with integral coefficients), satisfies (5.9) for all $m \geqslant 1$.

When (5.7) is not satisfied we can no longer assert (5.8). However in some cases it is still possible to obtain explicit results for the residue of u_m. For example if

$$m = p = k+1, \tag{5.10}$$

where p is a prime, we find that (5.5) reduces to

$$u_p \equiv a_0^p - a_{p-1} \pmod{p}. \tag{5.11}$$

To extend this result we put

$$u_n = C_n(a_0, a_1, \ldots, a_{p-1}),$$
$$v_n = C_n(a_0, a_1, \ldots, a_{p-2}),$$

the notation being that of (5.3). Then by (5.1)

$$u_m = \sum_{sp \leqslant m} \frac{m!}{s!(m-sp)!\,p^s} a_{p-1}^s v_{m-sp}. \tag{5.12}$$

We take $m = p^e$, where $e \geqslant 1$. Let p^j being the highest power of p dividing s; then it is easily verified that the coefficient

$$A_s = \frac{m!}{s!(m-sp)!\,p^s}$$

is divisible by exactly p^{e-j-1}. Since $m-sp$ is divisible by p^{j-1}, it follows from (2.5) and (5.8) that

$$v_{m-sp} \equiv a_0^{m-sp} \pmod{p^{j+1}},$$

so that

$$A_s v_{m-sp} \equiv A_s a_0^{m-sp} \pmod{p^e}. \tag{5.13}$$

In the next place, since

$$A_s = \binom{m}{sp}\frac{(sp)!}{s!\,p^s}, \qquad \binom{p^e}{sp} \equiv \binom{p^{e-1}}{s} \pmod{p^e}$$

this follows from $(x+y)^{p^e} \equiv (x^p+y^p)^{p^{e-1}} \pmod{p^e}$),

$$\frac{(sp)!}{s!\,p^s} = \prod_{\substack{h=1\\ p\nmid h}}^{sp} h \equiv (-1)^s \pmod{p^{j-1}}$$

for $p \geqslant 2$ (by the generalized Wilson theorem), we get

$$A_s \equiv \binom{p^{e-1}}{s} \pmod{p^e}. \tag{5.14}$$

Thus by (5.12), (5.13) and (5.14) it follows that

$$u_{p^e} \equiv (a_0^p - a_{p-1})^{p^{e-1}} \pmod{p^e} \tag{5.15}$$

provided $k = p-1$, $p > 2$.

We may state

THEOREM 9. *If* $k = p-1$, $p^e | m$, $e \geqslant 1$, $p > 2$, *then*

$$\sum_{s=0}^{r} (-1)^r \binom{r}{s} (a_0^p - a_{p-1})^{(r-s)m/p} u_{n+sm} \equiv 0 \pmod{p^{er_1}} \tag{5.16}$$

for all $n \geqslant 0$. *When* $e = 1$, (5.16) *holds for all* p. *The coefficients* $a_0, a_1, \ldots, a_{p-1}$ *are either integral* $(\operatorname{mod} p)$ *or polynomials in an arbitrary number of indeterminates with coefficients integral* $(\operatorname{mod} p)$.

6. As a second application we consider the sequence defined by means of

$$(1-at)^{-x}(1-bt)^{-y}(1-ct)^{-z} = \sum_{n=0}^{\infty} u_n \frac{t^n}{n!}, \tag{6.1}$$

where

$$u_n = \varphi_n(x, y, z; a, b, c). \tag{6.2}$$

It follows easily from (6.1) that

$$u_n = \sum_{i+j+k=n} \frac{n!}{i!\,j!\,k!} a^i b^j c^k (x)_i (y)_j (z)_k, \tag{6.3}$$

where

$$(x)_i = x(x+1)\ldots(x+i-1), \qquad (x)_0 = 1$$

and the summation is over all non-negative integers i, j, k such that $i+j+k = n$. Thus u_n is a polynomial in the six variables x, y, z, a, b, c with integral coefficients.

The generating function

$$(1-at)^{-x}(1-bt)^{-y}$$

has received some attention (see for example [4] and [5], vol. 3, p. 248). For simplicity we confine ourselves to the case of three factors; the more general case can be handled without difficulty.

Differentiating (6.1) with respect to t we get

$$\sum_{n=0}^{\infty} u_{n+1} \frac{t^n}{n!} = \left(\frac{ax}{1-at} + \frac{by}{1-bt} + \frac{cz}{1-ct}\right) \sum_{0}^{\infty} u_n \frac{t^n}{n!}.$$

If we put

$$\frac{ax}{1-at} + \frac{by}{1-bt} + \frac{cz}{1-ct} = \frac{A+Bt+Ct^2}{(1-at)(1-bt)(1-ct)},$$

it follows that

$$\begin{aligned} u_{n+1} - (a+b+c)nu_n + (bc+ca+ab)n(n-1)u_{n-1} - {} \\ -abcn(n-1)(n-2)u_{n-2} = Au_n + Bnu_{n-1} + Cn(n-1)u_{n-2}. \end{aligned} \tag{6.4}$$

This is evidently of the form (1.5). Hence if the parameters x, y, z, a, b, c are integral $(\operatorname{mod} m)$ or indeterminates (or polynomials with integral coefficients) Theorem 5 applies. Moreover u_m is explicitly determined by (6.3). In certain cases (6.3) can be simplified considerably. If first x, y, z are integral $(\operatorname{mod} m)$, we have

$$u_m = m! \sum_{i+j+k=n} \frac{(x)_i (y)_j (z)_k}{i!\,j!\,k!} a^i b^j c^k,$$

so that in this case

(6.5) $$u_m \equiv 0 \pmod{m}.$$

Using (6.5), (3.19) reduces to

(6.6) $$u_n \equiv 0 \pmod{m^{r_1}} \qquad (n \geqslant rm).$$

On the other hand if x, y, z are indeterminates and $m = p$, then since

$$(x)_p \equiv x^p - x \pmod{p},$$

(6.3) implies

(6.7) $$u_p \equiv a^p(x^p - x) + b^p(y^p - y) + c^p(z^p - z) \pmod{p}.$$

For general m, if z is integral then (6.3) yields

(6.8) $$u_m \equiv \sum_{i=0}^{m} \binom{m}{i} a^i b^j (x)_i (x)_j \pmod{m},$$

while if both y and z are integral we get

(6.9) $$u_m \equiv a^m (x)_m \pmod{m}.$$

If we specialize the parameters the recurrence (6.4) simplifies considerably. For example if $a = 1, b = \omega, c = \omega^2$, where $\omega^2 + \omega + 1 = 0$ and $y = \omega^2 x$, $z = \omega x$, (6.4) reduces to

(6.10) $$u_{n+1} = 3x u_n + n(n-1)(n-2) u_{n-2}.$$

From (6.10) it follows that u_n is a polynomial in $3x$ with integral coefficients, which is not obvious from (6.3). It follows from (6.10) that

(6.11) $$u_n = \sum_{3s \leqslant s} c_{n,s} (3x)^{n-3s},$$

where the coefficients $c_{n,s}$ are integers that satisfy the mixed recurrence

6.12) $$c_{n+1,s} = c_{n,s} + n(n-1)(n-2) c_{n-2,s-1}$$

together with

$$c_{n,0} = 1 \qquad (n = 0, 1, 2, \ldots).$$

Another way of determining u_n is by means of

(6.13) $$\sum_{n=0}^{\infty} u_n \frac{t^n}{n!} = \exp\{3x F(t)\},$$

where

$$F(t) = \sum_{n=0}^{\infty} \frac{t^{3r+1}}{3r+1}.$$

It is easily verified that (6.13) and (6.10) are equivalent.

It follows from (6.10) that

(6.14) $$u_p \equiv \begin{cases} 3(x^p - x) \pmod{p} & (p \equiv 1 \pmod{3}), \\ 3x^p \pmod{p} & (\text{otherwise}). \end{cases}$$

7. Let g_n denote the number of polygons of n sides (including degenerate cases) formed by a network of n lines. Robinson [10] showed that g_n satisfies the recurrence

(7.1) $$g_{n+1} = n g_n + \tfrac{1}{2} n(n-1) g_{n-2} \qquad (n \geqslant 2),$$

where $g_1 = g_2 = 0$, $g_3 = 1$, it is convenient to define $g_0 = 1$. Thus Theorem 5 applies to (7.1) and we get

(7.2) $$\sum_{s=0}^{r} (-1)^s \binom{r}{s} g_m^{(r-s)t} g_{n+stm} \equiv 0 \pmod{m^{r_1}},$$

for all $n \geqslant 0$, provided $m \geqslant 1$ and odd. The writer [3] has given a direct proof of (7.2). Moreover

$$g_m \equiv -2^{-m} \pmod{m^{r_1}},$$

so that (7.2) becomes

(7.3) $$\sum_{s=0}^{r} (-1)^{s(t+1)} \binom{r}{s} 2^{stm} g_{n+stm} \equiv 0 \pmod{m^{r_1}}.$$

In the next place let $K_n = K(3, n)$ denote the number of reduced three-line latin rectangles. Riordan [9] (see also [8], pp. 204-210) showed that K_n satisfies

(7.4) $$K_{n+1} = (n+1)^2 K_n + n(n+1) K_{n-1} + 2n(n^2-1) K_{n-2} + k_{n+1},$$

where

(7.5) $$k_{n+1} + (n+1) k_n = -n \cdot 2^{n+1}.$$

The writer showed that K_n satisfies the congruence

(7.6) $$\sum_{s=0}^{r} (-1)^s \binom{r}{s} 2^{(r-s)m} K_{n+sm} \equiv 0 \pmod{m^r}$$

for all $n \geqslant 0$, $m \geqslant 1$. Now Kerawala [6] had earlier found that K_n satisfies a certain recurrence of the fifth order, which indeed can be obtained by eliminating k_n from (7.4) and (7.5). However this recurrence is not of the form (1.5) and therefore the general theorems of this paper are not immediately applicable even though (7.6) is of the same form as (3.19). Notice also that the modulus in (7.6) is m^r rather than m^{r_1}.

In conclusion we mention that in certain cases recurrences of the third order have been found for hypergeometric polynomials ([7], Chapter 14). For example, for the polynomial

$$f_n(x) = {}_2F_2(-n, n+1; 1, \tfrac{1}{2}; x)$$

it is found that

$$(7.7)\qquad (n+1)f_{n+1}(x) = (3n+1+4x)f_n(x)-(3n-1+4x)f_{n-1}(x)+(n-2)f_{n-2}(x)\,.$$

If we put

$$u_n = n!\,f_n(x)\,,$$

(7.7) becomes

$$(7.8)\qquad u_{n+1} = (3n+1+4x)u_n - n(3n-1+4x)u_{n-1} + n(n-1)(n-2)u_{n-2}\,.$$

In the second place for the polynomial

$$\varphi_n(x) = {}_2F_2(-n,\,1+\beta;\,1,\,1+\alpha;\,x)$$

it is shown that

$$(7.9)\qquad (n+1)(\alpha+n+1)\varphi_{n+1}(x) = \big(3n(n+1)+\alpha(2n+1)-(\beta+n+1)x\big)\varphi_n(x) - n(\alpha+3n-x)\varphi_{n-1}(x) + n(n-1)\varphi_{n-2}(x)\,.$$

If we put

$$u_n = n!\,(\alpha+1)_n\varphi_n(x)\,,$$

(7.9) becomes

$$(7.10)\qquad u_{n+1} = \big(3n(n+1)+\alpha(2n+1)-(\beta+n+1)x\big)u_n - n^2(\alpha+n)(\alpha+3n-x)u_n + n^2(n-1)^2(\alpha+n)(\alpha+n-1)u_{n-2}\,.$$

Clearly Theorem 5 is applicable to both (7.8) and (7.10).

References

[1] L. Carlitz, *Congruence properties of certain polynomial sequences*, Acta Arith. 6 (1960), pp. 149-158.

[2] — *Congruences connected with three-line latin rectangles*, Proc. Amer. Math. Soc. 4 (1953), pp. 9-11.

[3] — *Congruences for the number of n-gons formed by n lines*, Amer. Math. Monthly 67 (1960), pp. 961-966.

[4] — *A special functional equation*, Riv. Math. Univ. Parma 7 (1956), pp. 211-233.

[5] A. Erdélyi, W. Magnus, F. Oberhettinger, F. G. Tricomi, *Higher trancendental functions*, New York 1955.

[6] S. M. Kerawala, *The enumeration of the latin rectangles of depth three by means of a difference equation*, Bull. Calcutta Math. Soc. 33 (1941), pp. 119-127.

[7] E. D. Rainville, Special functions, New York 1960.

[8] J. Riordan, *An introduction to combinatorial analisis*, New York, 1958.

[9] — *A recurrence relation for three-line latin rectangles*, Amer. Math. Montly 59 (1952), pp. 159-162.

[10] R. Robinson, *A new absolute geometric constant?*, Amer. Math. Monthly 58 (1951), pp. 462-469.

Reçu par la Rédaction le 9. 3. 1961

ACTA ARITHMETICA
VII (1962)

Sur le problème de M. Werner Mnich

par

G. Sansone (Firenze) et J. W. S. Cassels (Cambridge)

Un de nous a donné récemment [2] une réponse négative au problème de M. Mnich (1): existent ils trois nombres rationnels u, v, w tels que

$$(1)\qquad u+v+w = uvw = 1\,.$$

La démonstration dans [2] utilise et la théorie quelque peu approfondie des points rationnels sur les courbes de genre un et les propriétés d'un corps de nombres algébriques de degré 3. Nous donnons ici une démonstration tout à fait élémentaire (2) qui n'utilise que les propriétés classiques du corps d'Eisenstein (c'est-à-dire du corps engendré par les racines cubiques d'unité).

Comme on vérifie sans peine (voir [1], [2]), la réponse négative au problème de M. Mnich équivaut à l'enoncé suivant:

THÉORÈME. *Les seules solutions de l'équation*

$$(2)\qquad x^3+y^3+z^3 = xyz$$

en nombres rationnels sont les solutions banales, c'est-à-dire les solutions où $xyz = 0$.

Sans nuire à la generalité, nous supposons par absurde qu'il existe des entiers (x, y, z) tels que (2) tienne, et tels que

$$(3)\qquad xyz \neq 0\,,\qquad 3\nmid z\,.$$

Nous supposons aussi que $|xyz|$ est le plus petit possible, c'est-à-dire que

$$(4)\qquad |x_1y_1z_1| \geqslant |xyz|$$

pour toute solution entière (x_1, y_1, z_1) non banale de l'equation (2).

Posons

$$(5)\qquad \begin{cases} \gamma = 3x+3y+z\,, \\ \sigma = 3\varepsilon x+3\bar\varepsilon y+z\,, \\ \bar\sigma = 3\bar\varepsilon x+3\varepsilon y+z\,, \end{cases}$$

(1) Pour l'histoire de ce problème, voir [1].

(2) M. Sansone a trouvé la démonstration et l'a soumise à la Rédaction des Acta Arithmetica au mois de novembre, 1960. M. Cassels y a rapporté quelques simplifications. Les auteurs tiennent à remercier M. A. Schinzel de ses précieuses suggestions.