This, (4.3) and (4.6) give

$$|S| \geqslant \frac{e^{1/2\,A\nu}}{30^{\nu}} \cdot e^{-\log^{1/3}\cdot\frac{1}{\delta}} e^{-24}$$

$$> \left(\frac{1}{\delta}\right)^{1/2} \exp\left\{-\log^{1/3}\frac{1}{\delta} - 2\log 30 \cdot \frac{\log\frac{1}{\delta}}{\log\log\frac{1}{\delta}} - \frac{1}{6}\left(\log\frac{1}{\delta}\right)^{1/3} - 24\right\}$$

$$> 2\left(\frac{1}{\delta}\right)^{1/2} \exp\left(-8\,\frac{\log\frac{1}{\delta}}{\log\log\frac{1}{\delta}}\right).$$

Using now (3.14) and (4.2) we obtain

$$\frac{\omega^{\nu}}{\nu!} \max_{e^{-\omega} \leqslant y \leqslant 1} |F(y)| \geqslant \left(\frac{1}{\delta}\right)^{1/2} \exp\left(-8\,\frac{\log\frac{1}{\delta}}{\log\log\frac{1}{\delta}}\right) - c_8 \sum_{j=1}^{\nu} \frac{\omega^{\nu-j}}{(\nu-j)!}. \tag{4.7}$$

But

$$\frac{\omega^{\nu}}{\nu!} \leqslant \left(\frac{e\log\frac{1}{\delta}}{\nu}\right)^{\nu} < e^{8\frac{\log 1/\delta}{\log\log 1/\delta}\log\log\log 1/\delta}$$

and also

$$\sum_{j=1}^{\nu} \frac{\omega^{\nu-j}}{(\nu-j)!} \leqslant \nu\,\frac{\omega^{\nu}}{\nu!},$$

whence by (4.7)

$$\max_{\delta \leqslant y \leqslant 1} |F(y)| > \left(\frac{1}{\delta}\right)^{1/2} \exp\left(-4\,\frac{\log\frac{1}{\delta}}{\log\log\frac{1}{\delta}}\log\log\log\frac{1}{\delta}\right),$$

Q.E.D.

References

[1] Cahen, *Thèse*, Paris 1894.

[2] А. О. Гельфонд, *Исчисление конечных разностей*, Москва 1952.

[3] G. H. Hardy and J. E. Littlewood, *Contributions to theory of the Riemann zeta-function and the theory of the distribution of primes*, Acta Math. 41 (1918), pp. 119-196.

[4] S. Knapowski, *Contributions to the theory of the distribution of prime numbers in arithmetical progressions* I, Acta Arithm. 6 (1961), pp. 415-434.

[5] Mellin, Acta Soc. Fennicae 20 (1895), pp. 1-39.

[6] N. Nielsen, *Handbuch der Theorie der Gammafunktion*, Leipzig 1906.

[7] E. C. Titchmarsh, *The theory of the Riemann zeta-function*, Oxford 1951.

[8] P. Turán, *Eine neue Methode in der Analysis und deren Anwendungen*, Budapest 1953.

Reçu par la Rédaction le 23. 2. 1961

ACTA ARITHMETICA
VII (1962)

A theorem on "ordered" polynomials in a finite field

by

L. Carlitz (Durham, North Carolina)

Let F denote the finite field $GF(q)$ of order q, where $q = p^n$ is odd. Put $\psi(a) = +1, -1$ or 0 according as a is a non-zero square, a non-square or zero in F. Then we have

$$\psi(a) = a^m, \tag{1}$$

where $q = 2m+1$. The writer has proved the following theorem.

Theorem A. *Let $f(x)$ be a permutation polynomial such that*

$$f(0) = 0, \quad f(1) = 1 \tag{2}$$

and

$$\psi\big(f(x)-f(y)\big) = \psi(x-y) \tag{3}$$

for all $x, y \in F$. Then we have

$$f(x) = x^{p^j} \tag{4}$$

for some j in the range $0 \leqslant j < n$.

We recall that a polynomial $f(x)$ with coefficients in F is a permutation polynomial if the numbers $f(a)$, $a \in F$, are distinct. Also two polynomials $f(x)$, $g(x)$ are defined as equal if $f(a) = g(a)$ for all $a \in F$; this is equivalent to the statement

$$f(x) \equiv g(x) \pmod{x^q - x}.$$

Now it is evident that the hypothesis (3) implies that $f(x)$ is a permutation polynomial. Also we may drop the hypothesis (2) and replace Theorem A by the following slightly more general theorem.

Theorem B. *Let $f(x)$ be a polynomial with coefficients $\in F$ such that*

$$\psi\big(f(x)-f(y)\big) = \lambda\psi(x-y)$$

for all $x, y \in F$, where $\lambda = \pm 1$ is fixed. Then we have

$$f(x) = ax^{p^j} + b \tag{5}$$

for some j in the range $0 \leqslant j < n$ and where $a, b \in F$, $\psi(a) = \lambda$.

We now consider polynomials $f(x, y)$ with coefficients ϵF such that

(6) $$\psi\big(f(x,y)-f(z,y)\big) = \lambda\psi(x-z),$$

(7) $$\psi\big(f(x,y)-f(x,z)\big) = \mu\psi(y-z)$$

for all $x, y, z \epsilon F$, where $\lambda = \pm 1$ are fixed.

By Theorem B it follows from (6) that for each $y \epsilon F$

(8) $$f(x,y) = a(y)x^{p^{j(y)}} + c(y),$$

where $0 \leqslant j(y) < n$ and

(9) $$\psi\big(a(y)\big) = \lambda$$

for all $y \epsilon F$. Similarly from (7) we get

(10) $$f(x,y) = b(x)y^{p^{k(x)}} + d(x),$$

where $0 \leqslant k(x) < n$ and

(11) $$\psi\big(b(x)\big) = \mu$$

for all $x \epsilon F$. We may evidently assume that $a(y)$, $b(y)$, $c(x)$, $d(x)$ are polynomials in the respective variables.

The case $q = p$ is particularly simple. In this case (8) and (10) become

$$f(x,y) = a(y)x + c(y) = b(x)y + d(x),$$

from which it is clear that

(12) $$f(x,y) = axy + bx + cy + d \qquad (a, b, c, d \epsilon F).$$

By (6) we get

$$\psi\big((ay+b)(x-z)\big) = \lambda\psi(x-z),$$

for all $x, y, z \epsilon F$. In particular for $x-z = 1$ this becomes

$$\psi(ay+b) = \lambda$$

for all $y \epsilon F$. Consequently $a = 0$ and (12) reduces to

(13) $$f(x,y) = bx + cy + d,$$

where $\psi(b) = \lambda$, $\psi(c) = \mu$, while d is arbitrary.

The general case is not quite so easy. Let M_r denote the set of $y \epsilon F$ such that the exponent $j(y)$ in (8) satisfies $j(y) = r$. Let $g_r(u)$ be the unique polynomial of degree $< q$ such that

$$g_r(y) = \begin{cases} 1 & (y \epsilon M_r), \\ 0 & (y \notin M_r); \end{cases}$$

if M_r is vacuous it is clear that $g_r(u) = 0$. Then (8) becomes

$$f(x,y) = a(y)\sum_{r=0}^{n-1} g_r(y)x^{p^r} + c(y).$$

Changing the notation, we may write

(14) $$f(x,y) = \sum_{r=0}^{n-1} a_r(y)x^{p^r} + c(y),$$

where the $a_r(y)$ are polynomials $\epsilon F[y]$. Similarly it follows from (10) that

(15) $$f(x,y) = \sum_{s=0}^{n-1} b_s(x)y^{p^s} + d(x),$$

where the $b_s(x)$ are polynomials $\epsilon F[x]$.

Comparing (15) with (14) it follows that

(16) $$f(x,y) = \sum_{r,s=0}^{n-1} a_{rs}x^{p^r}y^{p^s} + \sum_{r=0}^{n-1} b_r x^{p^r} + \sum_{s=0}^{n-1} c_s y^{p^s} + d \qquad (a_{rs}, b_r, c_s, d \epsilon F).$$

If we apply (6) to (16) we get

(17) $$\psi\Big\{\sum_{r,s} a_{rs}(x-z)^{p^r}y^{p^s} + \sum_r b_r(x-z)^{p^r}\Big\} = \lambda\psi(x-z)$$

for all $x, y, z \epsilon F$. In particular, for $y = 0$, (17) reduces to

$$\psi\Big(\sum_r b_r(x-z)^{p^r}\Big) = \lambda\psi(x-z).$$

Applying Theorem B to the polynomial

$$f(x) = \sum_{r=0}^{n-1} b_r x^{p^r}$$

it follows that all $b_r = 0$ except b_{r_0}, say, where $\psi(b_{r_0}) = \lambda$. A similar argument applies to the coefficients c_s. Hence (16) reduces to

(18) $$f(x,y) = \sum_{r,s=0}^{n-1} a_{rs}x^{p^r}y^{p^s} + bx^{p^{r_0}} + cy^{p^{s_0}} + d,$$

where $\psi(b) = \lambda$, $\psi(c) = \mu$.

Applying (6) to (18) we get

(19) $$\psi\Big\{\sum_{r,s} a_{rs}(x-z)^{p^r}y^{p^s} + b(x-z)^{p^{r_0}}\Big\} = \lambda\psi(x-z).$$

For fixed y define

$$f(x) = f_y(x) = \sum_{r=0}^{n-1} x^{p^r}\sum_{s=0}^{n-1} a_{rs}y^{p^s} + bx^{p^{r_0}}.$$

In view of (19) we have

$$\psi\big(f(x)-f(z)\big) = \lambda\psi(x-z)\,.$$

By Theorem B, $f_y(x)$ must be a monomial in x for each y. Assume that not all the coefficients $a_{rs}=0$. If for some r_1 not all $a_{r_1 s}=0$, then the equation

$$\sum_{s=0}^{n-1} a_{r_1 s} y^{p^s} + b\delta_{r_0 r_1} = 0$$

has at most p^{n-1} solutions y. If $r_1 \neq r_0$ then not all $a_{r_0 s}=0$. But by the above remark it is evidently impossible to have two non-vanishing rows.

Thus in the matrix (a_{rs}) all elements except possibly those in the r_0-th row vanish. In like fashion we can show that all elements except possibly those in the s_0-th column vanish. Consequently (18) becomes

(20) $$f(x,y) = ax^{p^{r_0}}y^{p^{s_0}} + bx^{p^{r_0}} + cy^{p^{s_0}} + d\,,$$

where $a = a_{r_0 s_0}$.

Applying (6) once more we get

$$\psi\big((ay^{p^{s_0}}+b)(x-z)^{p^{r_0}}\big) = \lambda\psi(x-z)$$

for all $x, y, z \in F$. For $x-z=1$ this reduces to

(21) $$\psi(ay^{p^{s_0}}+b) = \lambda\,.$$

If $a \neq 0$, we take

$$y = -(b/a)^{p^{n-s_0}}$$

to get a contradiction.

We have therefore proved the following result.

Theorem C. *Let $f(x,y)$ be a polynomial with coefficients $\in F$ such that* (6) *and* (7) *hold for all $x, y, z \in F$, where $\lambda = \pm 1$, $\mu = \pm 1$ are fixed. Then*

$$f(x,y) = bx^{p^r} + cy^{p^s} + d\,,$$

where $0 \leqslant r < n$, $0 \leqslant s < n$ and

$$\psi(b) = \lambda\,, \qquad \psi(c) = \mu\,.$$

The general case is covered by the following theorem.

Theorem D. *Let $f(x_1, \dots, x_k)$ be a polynomial with coefficients $\in F$ such that*

(22) $$\psi\big(f(x_1,\dots,x_{r-1},x_r,x_{r+1},\dots,x_k) - f(x_1,\dots,x_{r-1},y_r,x_{r+1},\dots,x_k)\big) = \lambda_r\psi(x_r-y_r) \qquad (r=1,2,\dots,k)$$

for all $x_j, y_j \in F$, where the λ_j are fixed, $\lambda_j = \pm 1$. Then

(23) $$f(x_1,\dots,x_k) = \sum_{j=1}^{k} b_j x_j^{p^{r_j}} + d\,,$$

where

$$\psi(b_j) = \lambda_j \qquad (j = 1, 2, \dots, k)\,.$$

It will suffice to sketch briefly the proof of the theorem. We assume the truth of the theorem for k variables. Then for fixed $x = x_{k+1}$, it follows from the inductive hypothesis and (22) with k replaced by $k+1$ that

$$f(x_1,\dots,x_k,x) = \sum_{j=1}^{k} b_j(x) x_j^{p^{r_j(x)}} + d(x)\,.$$

Then, exactly as in the proof of (14), we get

(24) $$f(x_1,\dots,x_k,x) = \sum_{r=0}^{n-1}\sum_{j=1}^{k} b_{rj}(x) x_j^{p^r} + d(x)\,.$$

On the other hand, for fixed $x_1, \dots, x_k$, we have

(25) $$f(x_1,\dots,x_k,x) = a(x_1,\dots,x_k)x^{p^t} + c(x_1,\dots,x_k)$$

for some t. Comparison of (25) with (24) yields

(26) $$f(x_1,\dots,x_k,x) = \sum_{j=1}^{k}\sum_{r,s=0}^{n-1} a_{jrs}x_j^{p^r}x^{p^s} + \sum_{j=1}^{k}\sum_{r=0}^{n-1} b_{jr}x_j^{p^r} + \sum_{s=0}^{n-1} c_s x^{p^s} + d\,.$$

For $x=0$ the inductive hypothesis requires that for each j all $b_{jr}=0$ except b_{jr_j}, say; similarly, for $x_1 = \dots = x_k = 0$, all $c_s = 0$ except c_{s_0}, say. We then show first that all $a_{jrs}=0$ except possibly $a_{jr_js_0}$. Thus (26) reduces to

(27) $$f(x_1,\dots,x_k,x) = \sum_{j=1}^{k} a_j x_j^{p^{r_j}} x^{p^{s_0}} + \sum_{j=1}^{k} b_j x_j^{p^{r_j}} + c_{s_0}x^{p^{s_0}} + d\,,$$

where $a_j = a_{jr_js_0}$, $b_j = b_{jr_j}$.

Now by (27) and the hypothesis of the theorem

$$\psi\Big(\sum_{j=1}^{k} a_j x_j^{p^{r_j}} + c_{s_0}\Big) = \lambda_{k+1}$$

for all $x_1, \dots, x_k \in F$. If any $a_j \neq 0$ this is impossible since the equation

$$\sum_{j=1}^{k} a_j x_j^{p^{r_j}} + c_{s_0} = 0$$

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 $(\bmod\, m)$.

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

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