Congruence properties of certain polynomial sequences

by

L. CARLITZ (Durham, North Carolina)

1. Introduction. Consider the recurrence

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

where \( f(n) \) and \( g(n) \) are polynomials in \( n \) (and possibly some additional indeterminates) with integral coefficients. Moreover we assume that

\( u_0 = 1, \quad u_1 = f(0), \quad g(0) = 0 \).

Thus the sequence \( \{u_n; n = 0, 1, 2, \ldots \} \) is uniquely determined by (1.1) and (1.2).

The writer has proved ([1], Theorem 1) that if \( m \gg 1, r \gg 1 \), then \( u_n \) satisfies the congruence

\( \sum_{k=0}^{r} (-1)^k \binom{r}{k} u_{n + km} u_{r - km} = 0 \pmod{m^2} \)

for all \( n \gg 0 \), where

\( r_1 = [(r+1)/2] \),

the greatest integer \( \leq (r+1)/2 \). The principal object of the present paper is to show that, with the same hypotheses, \( u_n \) satisfies the simpler congruence

\( \sum_{k=0}^{r} (-1)^k \binom{r}{k} u_{n + km} u_{r - km} = 0 \pmod{m^2} \),

where again \( r_1 \) is defined by (1.4). In addition we show that (1.5) implies

\( \sum_{k=0}^{r} (-1)^k \binom{r}{k} u_{n + km} u_{k + [r - km]} = 0 \pmod{m^2} \)

for all \( n \gg 0 \), \( k \gg 0 \); for \( k = 0 \), (1.6) evidently reduces to (1.3). For a more general result see Theorem 2 below.
We remark that in particular the Hermite and Laguerre polynomials satisfy (1.1) and (1.2) when \( f(n) \) and \( g(n) \) are properly specialized. Thus (1.5) applies and we obtain

\[
\sum_{k=0}^{r} (-1)^k \binom{r}{k} (2x)^{r-k} H_{r+k}(x) = 0 \pmod{m^r},
\]

(1.7)

\[
\sum_{k=0}^{r} (-1)^k \binom{r}{k} (-x)^{r-k} \Lambda_{r+k}(x) = 0 \pmod{m^r},
\]

(1.8)

where

\[
\Lambda_{r}(x) = n! L_{r}^{(n)}(x)
\]

(1.9)

and \( L_{r}^{(n)}(x) \) is the Laguerre polynomial in the usual notation ([4], Chapter 5); the parameter \( \lambda \) is a rational number that is integral \( \pmod{m} \). The writer [2] has given a simpler proof of (1.7) and (1.8) by making use of certain explicit formulas available for the Hermite and Laguerre polynomials.

It will be convenient to replace (1.1), (1.2) by

\[
u_{m+1}(x) = (x+f(n)) u_{m}(x) + g(n) u_{m-1}(x),
\]

(2.1)

\[
u_{0}(x) = 1, \quad u_{0}(x) = x + f(0), \quad g(0) = 0;
\]

(2.5)

as above it is assumed that \( f(n) \), \( g(n) \) are polynomials in \( n \) with integral coefficients. Clearly \( u_{0}(x) \) is a polynomial in \( x \) of degree \( n \) with integral coefficients; the highest coefficient is 1. Also it is evident that many sequences of orthogonal polynomials are included in the present discussion.

Since (2.1) implies

\[
u_{m}(x) = u_{m+1}(x) - f(n) u_{m}(x) - g(n) u_{m-1}(x),
\]

it is clear that

\[
u_{m}(x) = \sum_{s=0}^{m} A_{m}(n) u_{m+s}(x) \quad (m, n = 0, 1, 2, \ldots),
\]

where the \( A_{m}(n) \) are polynomials in \( n \) with integral coefficients. Consequently

\[
u_{m}(x) u_{m}(x) = \sum_{s=0}^{m} B_{m}(n) u_{m+s}(x),
\]

(2.3)

where the \( B_{m}(n) \) are polynomials in \( n \) with integral coefficients. In (2.3) we think of \( m \) as fixed while \( n = 0, 1, 2, \ldots \); also we take

\[
B_{m}(n) = 0 \quad (s < -n).
\]

We now rewrite (2.3) as

\[
u_{m}(x) u_{m}(x) - u_{m-1}(x) = \sum_{s=-m}^{-1} B_{m}(n) u_{m+s}(x)
\]

(2.4)

and apply the case \( r = 1 \) of (1.3), that is,

\[
u_{m-1}(x) = u_{m}(x) u_{0}(x) \pmod{m}.
\]

Then (2.4) becomes

\[
\sum_{s=-m}^{-1} B_{m}(n) u_{m+s}(x) = 0 \pmod{m}.
\]

(2.5)

We shall require the following

**Lemma.** Let \( u_{0}(x), u_{1}(x), \ldots, u_{s}(x) \) denote a set of polynomials in \( x \) with integral coefficients and highest coefficients \( = 1 \); also let

\[\deg u_{s}(x) = s \quad (0 \leq s \leq n).\]

**Assume** that \( A_{0}, A_{1}, \ldots, A_{s} \) are integers such that

\[
\sum_{s=0}^{n} A_{s} u_{s}(x) = 0 \pmod{m};
\]

(2.6)

then

\[A_{s} = 0 \pmod{m} \quad (0 \leq s \leq n).\]

(2.7)

We remark that if \( u(x) \) is a polynomial with integral coefficients, the statement \( u(x) = 0 \pmod{m} \) means that each coefficient of \( u(x) \) is divisible by \( m \). Then if we put

\[u_{s}(x) = \sum_{r=1}^{s} a_{sr} x^{r} \quad (a_{sr} = 1, \quad 0 \leq s \leq n),
\]

(2.6)

becomes

\[\sum_{r=0}^{s} A_{r} \sum_{r=1}^{s} a_{sr} x^{r} = 0 \pmod{m},
\]

(2.8)
so that

\[ \sum_{s=1}^{n} A_s \sum_{r=1}^{n} A_r \sigma_{sr} \equiv 0 \pmod{m}. \]

Consequently, by the above remark,

\[ \sum_{s=1}^{n} A_s \sigma_{sr} \equiv 0 \pmod{m} \quad (0 \leq s \leq n). \]  

(2.8)

Since the matrix \((a_{sr})\) is triangular and \(a_{sr} = 1\) for \(0 \leq s \leq 1\), it is clear that (2.8) implies (2.7). This completes the proof of the lemma.

Applying the lemma to (2.5) we immediately obtain

\[ B_{mn}(n) \equiv 0 \pmod{m} \quad (-m \leq s \leq m - 1). \]  

(2.9)

In the next place we define the operator \(A\) by means of

\[ A \phi_n = u_m(x) \phi_n - \varphi_{n+m}, \]  

(2.10)

and generally

\[ A \phi_n = u_m(x) A^{-1} \phi_n - A^{-1} \phi_{n+m}, \]  

(2.11)

where \(\varphi_n\) is an arbitrary function of \(n\). Clearly (2.10) and (2.11) imply

\[ A \phi_n = \sum_{s=1}^{m} (-1)^{s+1} \left( \begin{array}{c} m \\ s \end{array} \right) u_m^{s-1} \phi_{n+s}. \]  

(2.12)

Applying \(A^{-1}\) to both members of (2.4) we get

\[ A^{-1} u_n(x) = \sum_{s=0}^{m-1} A^{-1} [B_{mn}(n) u_{n+s}(x)]. \]  

(2.13)

In addition to \(A\) we also require the operator \(\delta\) defined by

\[ \delta \phi_n = \sum_{s=1}^{m} (-1)^{s+1} \left( \begin{array}{c} m \\ s \end{array} \right) \phi_{n+s}. \]  

(2.14)

Since (2.14) is equivalent to

\[ \phi_{n+m} = \sum_{s=1}^{m} (-1)^{s+1} \left( \begin{array}{c} m \\ s \end{array} \right) \delta \phi_n, \]  

(2.15)

we get

\[ A^{-1} (B_{mn}(n) u_{n+s}(x)) = \sum_{s=0}^{m} (-1)^{s+1} \left( \begin{array}{c} m \\ s \end{array} \right) u_{m+s-1} \phi_{n+s} (x) B_{mn}(n) u_{n+s}(x). \]

\[ = \sum_{s=0}^{m} (-1)^{s+1} \left( \begin{array}{c} m \\ s \end{array} \right) u_{m+s-1} \phi_{n+s} (x) u_{n+s}(x) \sum_{s=0}^{m} (-1)^{s+1} \left( \begin{array}{c} m \\ s \end{array} \right) \delta B_{mn}(n) \]

\[ = \sum_{s=0}^{m} (-1)^{s+1} \left( \begin{array}{c} m \\ s \end{array} \right) \delta B_{mn}(n) \sum_{s=0}^{m} (-1)^{s+1} \left( \begin{array}{c} m \\ s \end{array} \right) u_{m+s-1} \phi_{n+s} (x) u_{n+s}(x) \]

\[ = \sum_{s=0}^{m} (-1)^{s+1} \left( \begin{array}{c} m \\ s \end{array} \right) \delta B_{mn}(n) B_{mn}(n) \sum_{s=0}^{m} (-1)^{s+1} \left( \begin{array}{c} m \\ s \end{array} \right) u_{m+s-1} \phi_{n+s} (x) u_{n+s}(x) \]

\[ = \sum_{s=0}^{m} (-1)^{s+1} \left( \begin{array}{c} m \\ s \end{array} \right) \delta B_{mn}(n) \delta u_{n+s}(x). \]

Thus (2.13) becomes

\[ A^{-1} u_n(x) = \sum_{s=0}^{m} \sum_{j=0}^{m} \delta B_{mn}(n) A^{-1} \delta u_{n+j+s}(x). \]  

(2.16)

We shall now prove (1.5) by an induction with respect to \(r\). For \(r = 1\), the result is the case \(r = 0\) of (1.3). We accordingly assume that (1.5) holds up to and including the value \(r-1\). Also since \(B_{mn}(n)\) is a polynomial in \(n\) with integral coefficients, it follows from (2.16) that

\[ \delta B_{mn}(n) \equiv 0 \pmod{m}. \]  

(2.17)

Consider a typical term

\[ A_{\mu} = \delta B_{mn}(n) A^{-1} \delta u_{n+r}(x) \]

in the right member of (2.16). For \(j = 0\), we use (2.9) to get

\[ A_{\mu} = 0 \pmod{m^{1+p+\mu}} \]

(2.18)

by the inductive hypothesis. For \(j \geq 1\), we employ (2.17) to get

\[ A_{\mu} = 0 \pmod{m^{1+p+\mu}} \]

(2.19)

Since

\[ 1+\lfloor \frac{1}{2}(r+1) \rfloor \geq \lfloor \frac{1}{2}(r+1) \rfloor \geq \lfloor \frac{1}{2}(r+1) \rfloor \]

(\(1 \leq j \leq r\)),

it evidently follows from (2.16), (2.18) and (2.19) that

\[ A_{\mu} = 0 \pmod{m^{1+p+\mu}} \]

(2.20)

This completes the proof of (1.5).
We may state

**Theorem 1.** Let \( f(n) \), \( g(n) \) denote polynomials in \( n \) with coefficients that are integral \( (\mod m) \), where \( m \) is a fixed integer \( \geq 1 \). Define the sequence of polynomials \( \{ u_n(x) \} \) by means of (2.1) and (2.2). Then \( u_n(x) \) satisfies the congruence (2.20) for all \( n \geq 0, r \geq 1 \), where

\[
A^{f} u_n(x) = \sum_{\ell=0}^{r} (-1)^{\ell} \binom{r}{\ell} u_{n+\ell}(x) u_{n+\ell+r}(x) \quad \text{and} \quad r_1 = \lfloor (r+1)/2 \rfloor.
\]

3. The proof of (1.6) depends upon the following identity. Put

\[
U_n^k(x) = \sum_{\ell=0}^{r} (-1)^{\ell} \binom{r}{\ell} u_{n+r}(x) u_{n+\ell+r}(x).
\]

Then we have

\[
U_n^k(x) = \sum_{\ell=0}^{r} (-1)^{\ell} \binom{r}{\ell} A^{f} u_{n}(x) \cdot A^{f} u_{n+k}(x).
\]

Indeed it follows easily from the definition of \( A^{f} u_{n}(x) \) that

\[
u_{n+r}(x) = \sum_{\ell=0}^{r} (-1)^{\ell} \binom{r}{\ell} u_{n+r}(x) A^{f} u_{n}(x).
\]

Then (3.1) becomes

\[
U_n^k(x) = \sum_{\ell=0}^{r} (-1)^{\ell} \binom{r}{\ell} \sum_{\ell=0}^{r} (-1)^{\ell} \binom{r}{\ell} A^{f} u_{n}(x) \cdot u_{n+\ell+r}(x)
\]

\[
= \sum_{\ell=0}^{r} \binom{r}{\ell} A^{f} u_{n}(x) \sum_{\ell=0}^{r} (-1)^{\ell} \binom{r}{\ell} u_{n+\ell+r}(x)
\]

\[
= \sum_{\ell=0}^{r} \binom{r}{\ell} A^{f} u_{n}(x) \sum_{\ell=0}^{r} (-1)^{\ell} \binom{r}{\ell} u_{n+r+\ell}(x)
\]

\[
= \sum_{\ell=0}^{r} (-1)^{\ell} \binom{r}{\ell} A^{f} u_{n}(x) \cdot A^{f} u_{n+k}(x).
\]

This evidently proves (3.2).

Now by Theorem 1, we have

\[
A^{f} u_n(x) \equiv 0 \pmod{m^{(t+1)/2}},
\]

\[
A^{f} u_n(x) \equiv 0 \pmod{m^{(r-t)/2}},
\]

for all \( n \geq 0, k \geq 0, 0 \leq s \leq r \). Since

\[
\lfloor (s+1)/2 \rfloor + \lfloor (r-s+1)/2 \rfloor \geq \lfloor (r+1)/2 \rfloor,
\]

it follows from (3.2), (3.4) and (3.5) that

\[
U_n^k(x) \equiv 0 \pmod{m^r}
\]

for all \( n \geq 0, k \geq 0, 0 \leq s \leq r \). This completes the proof of (1.6).

A more general result can be obtained by first generalizing the identity (3.2). Let \( n_1, \ldots, n_k \) be arbitrary non-negative integers and \( \lambda_1, \ldots, \lambda_k \) arbitrary parameters. Put

\[
U_n^{\lambda}(x) = \sum_{n_1+\ldots+n_k=\lambda} \binom{\lambda}{\lambda} A^{f} u_{n_1}(x) \ldots A^{f} u_{n_k}(x).
\]

This can be written more compactly in the symbolic form

\[
U_n^{\lambda} = u_n^{\lambda_1} \ldots u_n^{\lambda_k} (\lambda_1 u_n^{\lambda_1+\ldots+\lambda_k} + \ldots + \lambda_k u_n^{\lambda_k}),
\]

where it is understood that, after expanding the right member by the multinomial theorem, each \( u_n^{\lambda_1+\ldots+\lambda_k} \) is replaced by \( u_{n+r}(x) \).

Using (3.2), we get

\[
U_n^{\lambda} = \sum_{n_1+\ldots+n_k=\lambda} \binom{\lambda}{\lambda} A^{f} u_{n_1}(x) \ldots A^{f} u_{n_k}(x)
\]

\[
\times \prod_{i=1}^{k} \sum_{n_i} (-1)^{t_i} \binom{k}{t_i} u_{n_i}^{\lambda_i-t_i} A^{f} u_{n_i}
\]

\[
= \sum_{n_1+\ldots+n_k=\lambda} \binom{\lambda}{\lambda} (-1)^{t_1} \ldots (-1)^{t_k} \times 2^{\lambda_1+\ldots+\lambda_k} u_{n_1} \ldots u_{n_k}
\]

\[
\times \prod_{i=1}^{k} \sum_{n_i} (-1)^{t_i} \binom{k}{t_i} \frac{(\lambda_i u_{n_i}^{\lambda_i-t_i} \ldots (\lambda_k u_{n_k}^{\lambda_k-t_k})}{(n_i-t_i)!(n_k-t_k)!}
\]

where \( t = t_1 + \ldots + t_k \). We therefore get the identity

\[
U_n^{\lambda} = \sum_{n_1+\ldots+n_k=\lambda} \binom{\lambda}{\lambda} (-1)^{t_1} \ldots (-1)^{t_k} \times 2^{\lambda_1+\ldots+\lambda_k} u_{n_1} \ldots u_{n_k}
\]

\[
\times \prod_{i=1}^{k} \sum_{n_i} (-1)^{t_i} \binom{k}{t_i} \frac{(\lambda_i u_{n_i}^{\lambda_i-t_i} \ldots (\lambda_k u_{n_k}^{\lambda_k-t_k})}{(n_i-t_i)!(n_k-t_k)!}
\]

In the identity (3.9) the \( \lambda_i \) are arbitrary quantities. We shall now assume that each \( \lambda_i \) is integral \( (\mod m) \) and moreover

\[
\lambda_1 + \ldots + \lambda_k = 0 \pmod{m}. \]
Applying Theorem 1 we get
\[ \Delta^t u_{n_1} \ldots \Delta^t u_{n_k} \equiv 0 \pmod{m^t}, \]
where
\[ e = [(\frac{1}{2} (t_1 + 1)] + \ldots + [(\frac{1}{2} (t_k + 1)]. \]
Therefore, using (3.10), it follows that the indicated summand in the right member of (3.8)
\[ = 0 \pmod{m^{t_1 + \ldots + t_k + t}}. \]
Since
\[ t_j - \frac{1}{2} (t_j + 1) \leq \frac{1}{2} \] (j = 1, ..., k),
it is clear that
\[ r - (t_1 + \ldots + t_k) + e \geq r - \frac{1}{2} (t_1 + \ldots + t_k) \geq \frac{1}{2} r. \]
It follows that
\[ U_i^0 = 0 \pmod{m^2}. \]
We may now state

**Theorem 2.** Let the sequence \( \{u_n(x)\} \) be defined as in Theorem 1. Define
\[ U_i^0 = u_{n_i}^0(x) \]
by means of (3.7), where \( n_1, \ldots, n_k \) are arbitrary integers \( \geq 0 \) and \( \lambda_1, \ldots, \lambda_k \) are integral \( \pmod{m} \) and in addition satisfy (3.10). Then \( U_i^0 \) satisfies (3.11) with \( r_i = (\lfloor r+1 \rfloor)/2 \).

In particular for \( r = 2 \), \( \lambda_1 = 1, \lambda_2 = -1 \), Theorem 2 reduces to (3.6).

We remark that the congruence (3.11) was suggested by the following congruence for the Bernoulli numbers proved by Vandiver [5]:
\[ h_1 \ldots h_k (\frac{1}{2} h_k^{-1} + \ldots + \frac{1}{2} h_1^{-1} \ldots - 1)^{-1} = 0 \pmod{p^t}, \]
for \( p^t \mid m^t \), where
\[ (n_i \neq 0 \pmod{p-1}, i = 1, \ldots, k), \]
and \( p \) is an odd prime. For example, when \( r = 2 \), (3.12) implies in particular
\[ \sum_{i=1}^{r} (-1)^{r-i} \frac{B_{n_1+(r-2)j-1}}{m+(r-1)p-1} = 0 \pmod{m^r}. \]

provided \( p-1 \mid p \), \( p-1 \mid m \), \( m \gg r \), \( n \gg r \). The congruence (3.12) was later generalized by the present writer [3].

While (3.11) superficially resembles (3.12), it should be noted that the congruences differ widely in certain respects.

Returning to Theorem 2, we remark that the \( \lambda_i \) may contain indeterminates, or again may be algebraic numbers; all that is required is that each \( \lambda_i \) is integral \( \pmod{m} \) and that (3.10) is satisfied.

We also remark if some sequences \( \{u_n(x)\} \) satisfies
\[ A^t u_n(x) = 0 \pmod{m^t}, \]
then exactly as in the proof of Theorem 2, we get
\[ U_i^0 = 0 \pmod{m^t}. \]

We observe that in both (3.13) and (3.14) the modulus is \( m^t \) rather than \( m^r \).

4. As remarked in the Introduction, Theorem 1 and 2 apply to the Hermite polynomial \( H_m(x) \) and the modified Laguerre polynomial \( A^m_n(z) \) as defined by (1.9). Since
\[ H_m(x) = (2x)^m, \quad A^m_n(z) = (-x)^m \pmod{m}, \]
we get (1.7) and (1.8).

Another interesting example is furnished by the polynomial \( f_n(x) \) defined as follows. Put
\[ (1+it)^r = \sum_{n=0}^{\infty} A_n(w) t^n, \quad f_n(x) = n! A_n(w) (x = 2u+1). \]
Then \( f_n(x) \) satisfies the recurrence
\[ f_{n+1}(x) = xf_n(x) + n^2 f_{n-1}(x); \]
also \( f_1(x) = 1, f_1(x) = x \). Thus (2.1) and (2.2) are satisfied. It is proved in [3] that
\[ \sum_{i=1}^{r} (-1)^{r-i} \frac{f_{n-2m}(x)}{m+(r-1)p-1} = 0 \pmod{m^n}. \]
It is also proved that
\[ f_{n-2m}(x) = (x-1)(x-3)\ldots(x-2m+1) \pmod{m}. \]
Consequently Theorem 1 yields
\[ \sum_{i=1}^{r} (-1)^{r-i} \frac{f_{n-2m}(x)}{m+(r-1)p-1} = 0 \pmod{m^{r+1}}. \]
Note that in (4.1) the modulus is \( m' \) while in (4.2) it is only \( m^n \). As remarked at the end of § 3, the hypothesis (3.13) implies in particular
\[
U^0 \equiv 0 \pmod{m^n},
\]
but the converse is apparently not true.

\section*{References}


\section*{DUKE UNIVERSITY}

\section*{On the average number of direct factors of a finite abelian group}

by

E. COHEN (Knoxville, Tenn.)

\section*{1. Introduction.}

For positive integers \( n \), let \( \tau(n) \) denote the number of divisors of \( n \), and let \( t(n) \) denote the number of decompositions of \( n \) into two relatively prime factors. In this paper we prove analogues for the finite abelian groups of the classical results of Dirichlet and Mertens on the average order of \( \tau(n) \) and \( t(n) \). We recall Dirichlet's formula [4], with \( x \geq 2 \),
\[
D(x) = \sum_{n \leq x} \tau(n) = x \log x + 2y - 1 + O(\sqrt{x}),
\]
y denoting Euler's constant, and Mertens' estimate [8],
\[
D^*(x) = \sum_{n \leq x} t(n) = ax \log x + 2y - 1 + 2b + O(\sqrt{x} \log x),
\]
where \( a = \eta(2) \), \( b = \eta'(2) \), \( \eta(s) = 1/\zeta(s) \), \( \zeta(s) \) denoting the Riemann zeta-function, \( s > 1 \). For proofs and discussions of (1.1) and (1.2) we mention [1], §§ 13.2, 13.5, 13.9, [3], p. 282-285, 289, [7], p. 663-666.

The functions \( \tau(n) \) and \( t(n) \) can be generalized from the (multiplicative) semigroup \( J^* \) of the integers \( n \) to the semigroup \( X \) of the finite abelian groups with respect to the direct product. A general discussion of functions defined in \( X \) appears in [2]. For groups \( G, H \) contained in \( X \), denote by \( (G, H) \) the group of maximal order in \( X \) which is simultaneously a direct factor of \( G \) and \( H \). Denoting by \( E \) the identity of \( X \), we say that \( G \) and \( H \) are \textit{relatively prime} if \( (G, H) = E \). A direct factor \( D \) of \( G \) will be called \textit{unitary} if \( D \times E = G \), \( (D, E) = E \).

For groups \( G \) in \( X \), let \( \tau(G) \) denote the number of direct factors of \( G \) in \( X \), or equivalently, the total number of decompositions, \( G = D \times E \), in \( X \). Analogously, let \( t(G) \) denote the number of \textit{unitary} factors of \( G \) in \( X \), that is, the total number of direct decompositions of \( G \) into two relatively prime factors of \( X \). In view of the isomorphism [2] of \( J^* \) with the