

Congruence properties of certain polynomial sequences

bу

L. CARLITZ (Durham, North Carolina)

1. Introduction. Consider the recurrence

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

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

$$(1.2) u_0 = 1, u_1 = f(0), g(0) = 0.$$

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

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

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

for all $n \ge 0$, where

$$(1.4) r_1 = [(r+1)/2],$$

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 congruences

(1.5)
$$\sum_{s=0}^{r} (-1)^{s} {r \choose s} u_{n+sm} u_{m}^{r-s} \equiv 0 \pmod{m^{r_{1}}},$$

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

(1.6)
$$\sum_{s=0}^{r} (-1)^{s \binom{r}{s}} u_{n+sm} u_{k+(r-s)m} \equiv 0 \; (\bmod \, m^{r_1})$$

for all $n \ge 0$, $k \ge 0$; for k = 0, (1.6) evidently reduces to (1.3). For a more general result see Theorem 2 below.

Congruence properties

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

(1.7)
$$\sum_{s=0}^{r} (-1)^{s} {r \choose s} (2x)^{(r-s)m} H_{n+sm}(x) \equiv 0 \pmod{m^{r_1}},$$

(1.8)
$$\sum_{s=0}^{r} (-1)^{s} {r \choose s} (-x)^{(r-s)m} A_{n+sm}^{(s)}(x) \equiv 0 \pmod{m^{r_1}},$$

where

$$A_n^{(\lambda)}(x) = n! L_n^{(\lambda)}(x)$$

and $L_n^{(\lambda)}(x)$ is the Laguerre polynomial in the usual notation ([4], Chapter 5); the parameter λ is a rational number that is integral (mod 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.

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

$$(2.1) u_{n+1}(x) = (x+f(n))u_n(x)+g(n)u_{n-1}(x),$$

$$(2.2) u_0(x) = 1, u_1(x) = x + f(0), g(0) = 0;$$

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

Since (2.1) implies

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

it is clear that

$$x^m u_n(x) = \sum_{s=-m}^m A_{ms}(n) u_{n+s}(x) \quad (m, n = 0, 1, 2, ...),$$

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

(2.3)
$$u_m(x)u_n(x) = \sum_{s=-m}^m B_{ms}(n)u_{n+s}(x),$$



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

$$B_{ms}(n) = 0 \quad (s < -n).$$

We now rewrite (2.3) as

(2.4)
$$u_m(x)u_n(x) - u_{m+n}(x) = \sum_{s=-m}^{m-1} B_{ms}(n)u_{n+s}(x)$$

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

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

Then (2.4) becomes

(2.5)
$$\sum_{s=m}^{m-1} B_{ms}(n) u_{n+s}(x) \equiv 0 \; (\text{mod } m).$$

We shall require the following

LEMMA. Let $u_0(x)$, $u_1(x)$, ..., $u_n(x)$ denote a set of polynomials in x with integral coefficients and highest coefficients = 1; also let

$$\deg u_s(x) = s \quad (0 \leqslant s \leqslant n).$$

Assume that A_0, A_1, \ldots, A_n are integers such that

(2.6)
$$\sum_{s=0}^{n} A_s u_s(x) \equiv 0 \pmod{m};$$

then

$$(2.7) A_s \equiv 0 \pmod{m} (0 \leqslant s \leqslant n).$$

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

$$u_s(x)=\sum_{j=0}^s a_{sj}x^j \quad (a_{ss}=1,\ 0\leqslant s\leqslant n),$$

(2.6) becomes

$$\sum_{s=0}^n A_s \sum_{j=0}^s a_{sj} x^j \equiv 0 \pmod{m},$$

so that

$$\sum_{j=0}^n A x^j \sum_{s=j}^n A_s a_{sj} \equiv 0 \pmod{m}.$$

Consequently, by the above remark,

(2.8)
$$\sum_{s=i}^{n} A_s a_{si} \equiv 0 \pmod{m} \quad (0 \leqslant s \leqslant n).$$

Since the matrix (a_{sj}) is triangular and $a_{ss} = 1$ for $0 \le s \le 1$, 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

$$(2.9) B_{ms}(n) \equiv 0 \pmod{m} (-m \leqslant s \leqslant m-1).$$

In the next place we define the operator Δ by means of

$$\Delta \varphi_n = u_m(x)\varphi_n - \varphi_{n+m}$$

and generally

$$(2.11) \Delta^{\mathbf{r}} \varphi_n = u_m(x) \Delta^{\mathbf{r}-1} \varphi_n - \Delta^{\mathbf{r}-1} \varphi_{n+m},$$

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

Applying Δ^{r-1} to both members of (2.4) we get

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

(2.14)
$$\delta^{r}\varphi_{n} = \sum_{s=0}^{r} (-1)^{s} {r \choose s} \varphi_{n+sm}.$$

Since (2.14) is equivalent to

(2.15)
$$\varphi_{n+km} = \sum_{j=0}^{k} (-1)^{j} {k \choose j} \delta^{j} \varphi_{n},$$

we get

$$\begin{split} \varDelta^{r-1}\{B_{ms}(n)\,u_{n+s}(x)\} &= \sum_{k=0}^{r-1} (-1)^k \binom{r-1}{k} u_m^{r-1-k}(x) B_{ms}(n+km)\,u_{n+km}(x) \\ &= \sum_{k=0}^{r-1} (-1)^k \binom{r-1}{k} u_m^{r-1-k}(x)\,u_{n+km}(x) \sum_{j=0}^k (-1)^j \binom{k}{j} \,\delta^j B_{ms}(n) \\ &= \sum_{j=0}^{r-1} \binom{r-1}{j} \delta^j B_{ms}(n) \sum_{k=j}^{r-1} (-1)^{k-j} \binom{r-1-j}{k-j} u_m^{r-1-k}(x)\,u_{n+km}(x) \\ &= \sum_{j=0}^{r-1} \binom{r-1}{j} \delta^j B_{ms}(n) \sum_{k=0}^{r-1-j} (-1)^k \binom{r-1-j}{k} u_m^{r-1-j-k}(x)\,u_{n+jm+km}(x) \\ &= \sum_{j=0}^{r-1} \binom{r-1}{j} \,\delta^j B_{ms}(n) \cdot \varDelta^{r-1-j} u_{n+jm}(x) \,. \end{split}$$

Thus (2.13) becomes

(2.16)
$$\Delta^{\mathbf{r}} u_n(x) = \sum_{s=-m}^{m-1} \sum_{j=0}^{r-1} \delta^j B_{ms}(n) \Delta^{r-1-j} u_{n+jm}(x).$$

We shall now prove (1.5) by an induction with respect to r. For r=1, the result is the case r=1 of (1.3). We accordingly assume that (1.5) holds up to and including the value r-1. Also since $B_{ms}(n)$ is a polynomial in n with integral coefficients, it follows from (2.14) that

$$\delta^{j}B_{ms}(n) \equiv 0 \pmod{m^{j}}.$$

Consider a typical term

$$A_{js} = \delta^{j} B_{ms}(n) \Delta^{r-1-j} u_{n+jm}(x)$$

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

$$(2.18) A_{08} \equiv 0 \; (\bmod \, m^{1+[r/2]}),$$

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

(2.19)
$$A_{js} \equiv 0 \; (\text{mod } m^{j+[(r-j)/2]}).$$

Since

$$1+[\frac{1}{2}r] \geqslant [\frac{1}{2}(r+1)], \quad j+[\frac{1}{2}(r-j)] \geqslant [\frac{1}{2}(r+1)] \quad (1 \leqslant j \leqslant r),$$

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

This completes the proof of (1.5).

Congruence properties

We may state

THEOREM 1. Let f(n), g(n) denote polynomials in n with coefficients that are integral $(\bmod m)$, where m is a fixed integer $\geqslant 1$. 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 $n \geqslant 0$, $r \geqslant 1$, where

$$\Delta^{r} u_{n}(x) = \sum_{s=0}^{r} (-1)^{s} {r \choose s} u_{m}^{r-s}(x) u_{n+sm}(x)$$
 and $r_{1} = [(r+1)/2].$

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

(3.1)
$$U_{nk}^{(r)}(x) = \sum_{s=0}^{r} (-1)^{s} {r \choose s} u_{n+sm}(x) u_{k+(r-s)m}(x).$$

Then we have

(3.2)
$$U_{nk}^{(r)}(x) = \sum_{s=0}^{r} (-1)^{r-j} \binom{r}{s} \Delta^{s} u_{n}(x) \cdot \Delta^{r-s} u_{k}(x).$$

Indeed it follows easily from the definition of $\Delta^s u_n(x)$ that

(3.3)
$$u_{n+rm}(x) = \sum_{s=0}^{r} (-1)^{s} {r \choose s} u_{m}^{r-s}(x) \Delta^{s} u_{n}(x).$$

Then (3.1) becomes

$$\begin{split} U_{nk}^{(r)}(x) &= \sum_{s=0}^{r} (-1)^{s} {r \choose s} \sum_{j=0}^{s} (-1)^{j} {s \choose j} u_{m}^{s-j}(x) \varDelta^{j} u_{n}(x) \cdot u_{k+(r-s)m}(x) \\ &= \sum_{j=0}^{s} {r \choose j} \varDelta^{j} u_{n}(x) \sum_{s=j}^{r} (-1)^{s-j} {r-j \choose s-j} u_{m}^{s-j}(x) u_{k+(r-s)m}(x) \\ &= \sum_{j=0}^{s} {r \choose j} \varDelta^{j} u_{n}(x) \sum_{s=0}^{r-j} (-1)^{s} {r-j \choose s} u_{m}^{s}(x) u_{k+(r-j-s)m}(x) \\ &= \sum_{j=0}^{s} (-1)^{r-j} {r \choose j} \varDelta^{j} u_{n}(x) \cdot \varDelta^{r-j} u_{k}(x). \end{split}$$

This evidently proves (3.2).

Now by Theorem 1, we have

(3.4)
$$\Delta^{s} u_{n}(x) \equiv 0 \; (\text{mod } m^{[(s+1)/2]}),$$

(3.5)
$$\Delta^{r-s} u_k(x) \equiv 0 \; (\text{mod } m^{[(r-s+1)/2]})$$

for all $n \ge 0$, $k \ge 0$, $0 \le s \le r$. Since

$$[\frac{1}{2}(s+1)] + [\frac{1}{2}(r-s+1)] \geqslant [\frac{1}{2}(r+1)],$$

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

$$(3.6) U_{rk}^{(r)}(x) \equiv 0 \pmod{m^{r_1}}$$

for all $n \ge 0$, $k \ge 0$. 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

$$(3.7) \quad U_k^{(r)} = U_{n_1...n_k}^{(r)}(x) = \sum_{s_1 + ... + s_k = r} \frac{r!}{s_1! ... s_k!} \lambda_1^{s_1} ... \lambda_k^{s_k} \prod_{j=1}^k u_{n_j + s_j m}(x).$$

This can be written more compactly in the symbolic form

$$(3.8) U_k^{(r)} = u_1^{n_1} \dots u_k^{n_k} (\lambda_1 u_1^m + \dots + \lambda_k u_k^m)^n,$$

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

Using (3.2), we get

$$\begin{split} U_k^{(r)} &= \sum_{s_1 + \ldots + s_k = r} \frac{r!}{s_1! \ldots s_k!} \lambda_1^{s_1} \ldots \lambda_k^{s_k} \times \\ &\times \prod_{j=1}^k \sum_{t_j = 0}^{s_j} (-1)^{t_j} {s_j \choose t_j} u_m^{s_j - t_j} \Delta^{t_j} u_{n_j} \\ &= \sum_{t_1 + \ldots + t_k \leq r} (-1)^t \frac{r!}{t_1! \ldots t_k! (r - t)!} \lambda_1^{t_1} \ldots \lambda_k^{t_k} \Delta^{t_1} u_{n_1} \ldots \Delta^{t_k} u_{n_k} \times \\ &\times \sum_{s_1, \ldots, s_k} \frac{(r - t)!}{(s_1 - t_1)! \ldots (s_k - t_k)!} (\lambda_1 u_m)^{s_1 - t_1} \ldots (\lambda_k u_m)^{s_k - t_k}, \end{split}$$

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

(3.9)
$$U_{k}^{(r)} = \sum_{t_{1}+\dots t_{k} \leqslant r} (-1)^{t} \frac{r!}{t_{1}!\dots t_{k}!(r-t)!} \lambda_{1}^{t_{1}}\dots \lambda_{k}^{t_{k}} \times (\lambda_{1}+\dots+\lambda_{k})^{r-t} u_{m}^{r-t} \Delta^{t_{1}} u_{n_{1}}\dots \Delta^{t_{k}} u_{n_{k}}$$

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

$$(3.10) \lambda_1 + \ldots + \lambda_k \equiv 0 \pmod{m}.$$

Applying Theorem 1 we get

$$\Delta^{t_1}u_{n_1}\ldots\Delta^{t_k}u_{n_k}\equiv 0\ (\mathrm{mod}\, m^e),$$

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)

$$\equiv 0 \, (\operatorname{mod} m^{r-(t_1+\ldots+t_k)+e}).$$

Since

$$t_i - \lceil \frac{1}{2}(t_i + 1) \rceil \leq \frac{1}{2}t_i \quad (i = 1, ..., k).$$

it is clear that

$$r - (t_1 + \ldots + t_k) + e \geqslant r - \frac{1}{2}(t_1 + \ldots + t_k) \geqslant \frac{1}{2}r$$

It follows that

$$(3.11) U_k^{(r)} \equiv 0 \pmod{m^{r_1}}.$$

We may now state

THEOREM 2. Let the sequence $\{u_n(x)\}$ be defined as in Theorem 1. Define

$$U_k^{(r)} = U_{n_1...n_k}^{(r)}(x)$$

by means of (3.7), where n_1, \ldots, n_k are arbitrary integers ≥ 0 and $\lambda_1, \ldots, \lambda_k$ are integral (mod m) and in addition satisfy (3.10). Then $U_k^{(r)}$ satisfies (3.11) with $r_1 = \lceil (r+1)/2 \rceil$.

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]:

$$(3.12) h_1^{n_1} \dots h_k^{n_k} (\lambda_1 h_1^{p-1} + \dots + \lambda_k h_k^{p-1})^r \equiv 0 \pmod{(p^r, p^{n_1 - 1}, \dots, p^{n_k - 1})}$$
$$(n_i \not\equiv 0 \pmod{p - 1}, i = 1, \dots, k),$$

where the left member is expended by the multinomial theorem and B_n/n substituted for h_i^n in the result; B_m is the Bernoulli number in the even suffix notation, the λ_j are rational integers such that

$$\lambda_1 + \ldots + \lambda_k \equiv 0 \pmod{p}$$

and p is an odd prime. For example, when r=2, (3.12) implies in particular

$$\sum_{s=0}^{r} (-1)^{s} {r \choose s} \frac{B_{m+(r-s)(p-1)}}{m+(r-s)(p-1)} \frac{B_{n+s(p-1)}}{n+s(p-1)} \equiv 0 \; (\bmod \, p^{r})$$

provided $p-1 \nmid m, p-1 \nmid n, m > r, n > r$. 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 λ_j may contain indeterminates, or again may be algebraic numbers; all that is required is that each λ_i is integral (mod m) and that (3.10) is satisfied.

We also remark if some sequences $\{u_n(x)\}$ satisfies

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

then exactly as in the proof of Theorem 2, we get

$$(3.14) U_k^{(r)} = 0 \pmod{m^r};$$

observe that in both (3.13) and (3.14) the modulus is m^r rather than m^{r_1} .

4. As remarked in the Introduction, Theorem 1 and 2 apply to the Hermite polynomial $H_n(x)$ and the modified Laguerre polynomial $\Lambda_n^{(2)}(x)$ as defined by (1.9). Since

$$H_m(x) \equiv (2x)^m, \quad \Lambda_m^{(\lambda)}(x) \equiv (-x)^m \pmod{m},$$

we get (1.7) and (1.8).

Another interesting example is furnished by the polynomial $f_n(x)$ defined as follows. Put

$$\frac{(1+t)^u}{(1-t)^{u+1}} = \sum_{n=0}^n A_n(u)t^n, \quad f_n(x) = n!A_n(u) \quad (x = 2u+1).$$

Then $f_n(x)$ satisfies the recurrence

$$f_{n+1}(x) = x f_n(x) + n^2 f_{n-1}(x);$$

also $f_0(x) = 1$, $f_1(x) = x$. Thus (2.1) and (2.2) are satisfied. It is proved in [3] that

(4.1)
$$\sum_{s=0}^{r} (-1)^{s} {r \choose s} f_{n+sm}(x) f_{(r-s)m}(x) \equiv 0 \pmod{m^{r}}.$$

It is also proved that

$$f_m(x) \equiv (x-1)(x-3)...(x-2m+1) \pmod{m}$$
.

Consequently Theorem 1 yields

$$(4.2) \sum_{s=0}^{r} (-1)^{s} {r \choose s} \{(x-1)(x-3) \dots (x-2m+1)\}^{r-s} f_{n+sm}(x) \equiv 0 \pmod{m^{r_1}}.$$

L. Carlitz

158

Note that in (4.1) the modulus is m^r while in (4.2) it is only m^{r_1} . As remarked at the end of § 3, the hypothesis (3.13) implies in particular

$$U_2^{(r)} \equiv 0 \; (\bmod \, m^r),$$

but the converse is apparently not true.

References

- [1] L. Carlitz, Congruence properties of the polynomials of Hermite, Laguerre and Legendre, Mathematische Zeitscrift 59 (1954), p. 474-483.
- [2] Congruence properties of the Hermite and Laguerre polynomials, Archiv der Mathematik 10 (1959), p. 460-465.
- [3] Some congruences of Vandiver, American Journal of Mathematics 75 (1953), p. 707-1712.
- [4] A special functional equation, Rivista di Mathematica della Università di Parma 7 (1956), p. 211-233.
 - [5] G. Szegö, Orthogonal polynomials, New York 1939.
- [6] H. S. Vandiver, Note on a certain ring congruence, Bulletin of the American Mathematical Society 43 (1937), p. 418-423.

DUKE UNIVERSITY

Reçu par la Rédaction le 7. 12. 1959



On the average number of direct factors of a finite abelian group

by

E. COHEN (Knoxville, Tenn.)

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 $x \ge 2$.

$$D(x) \equiv \sum_{n \leq x} \tau(n) = x(\log x + 2\gamma - 1) + O(\sqrt{x}),$$

γ denoting Euler's constant, and Mertens's estimate [8],

(1.2)
$$D^*(x) = \sum_{n \le x} t(n) = ax(\log x + 2\gamma - 1) + 2bx + O(\sqrt{x}\log x),$$

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. 282-283, 289, [7], p. 665-666.

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_0 the identity of X, we say that G and H are relatively prime if $(G, H) = E_0$. A direct factor D of G will be called unitary if $D \times E = G$, $(D, E) = E_0$.

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 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