ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 11, Number 4, Fall 1981

ARITHMETIC PROPERTIES OF THE MÉNAGE POLYNOMIALS

HARLAN STEVENS

1. Introduction. The ménage polynomials $U_n(t)$ are defined for $n > 1$ by

$$U_n = U_n(t) = \sum_{k=0}^{n} u_{n,k} t^k,$$

where $u_{n,k}$ is the number of ways of seating n married couples at a circular table, men and women alternating, so that exactly k husbands sit next to their own wives. The numbers $u_{n,k}$ are to be thought of as 'reduced' in that the positions of the women are taken as fixed. A comprehensive account of the *problème des ménage* is given by Riordan and Kaplansky in [3].

Riordan [4] has shown that the ménage polynomials possess a rather simple periodic property. He proved, namely, that when $U_0 = 2$, $U_1 = 2t - 1$

$$U_{n+p^2} \equiv (t^{p^2} - 1)U_n \pmod{p} \tag{1.1}$$

for all $n \geqq 0$ and odd primes p. In this note we will show that the U_n actually satisfy a much wider class of congruences. It will be demonstrated in fact that if $m = cp^e$, then

$$\sum_{s=0}^{r} (-1)^s \binom{r}{s} (t-1)^{m(r-s)} U_{n+sm} \equiv 0 \pmod{p^{(e-1)r+r_1}} \tag{1.2}$$

for $n \geqq 0$ and where $r_1 = [r/2]$ is the greatest integer $\leqq r/2$. This last notation for r_1 will be maintained throughout. The congruence (1.2) reduces to (1.1) when $m = p^2$ and $r = 1$.

In [1] Carlitz also considered congruences like (1.2). His results, however, coincide with ours only for the cases $e = 1$ or $r \leqq 2$, but are otherwise weaker. Moreover, the method of the present paper is very direct and avoids much of the computation of both [1] and [4].

It is of interest to note here that the congruences represented by (1.2) are quite reminiscent of those satisfied by Hermite and Laguerre polynomials [2]. In spite of these similarities and the fact that they all obey difference equations of the second order, it is curious that the proofs in each case are apparently unrelated.

Received by the editors on October 1, 1979.

2. Proof of (1.2) for $m = p$. All results will be considerably simplified by the introduction of operator notation. Accordingly, for a fixed positive integer m we define Δ by means of

$$\Delta g(n) = g(n + m) - (t - 1)^m g(n).$$

The operator Δ is linear and possesses all of the standard algebraic properties. Δ may also be expressed in terms of the usual shift operator E as $\Delta = E^m - (t - 1)^m$. In this notation our aim is to prove

$$\Delta^r U_n \equiv 0 \pmod{p^{r_1}}. \tag{2.1}$$

In order to prove (2.1) we employ the auxiliary polynomials $W_n = W_n(t)$ defined by

$$W_n = \sum_{k=0}^{n} \binom{2n-k+1}{k} (n - k)!(t - 1)^k, \tag{2.2}$$

which are related to the U_n by

$$U =_n nW_{n-1} + 2(t - 1)^n = W_n - (t - 1)^2 W_{n-2}. \tag{2.3}$$

The notation adopted here is that of [4], but the essential properties of the $W_n(t)$ are given in [3].

We have from (2.3)

$$W_n = nW_{n-1} + (t - 1)^2 W_{n-2} + 2(t - 1)^n. \tag{2.4}$$

Indeed, in conjunction with (2.2), W_n can now be defined for negative n. By a straightforward induction it follows that

$$W_{-n} = -(t - 1)^{-2n+2} W_{n-2}. \tag{2.5}$$

From (2.3) it is seen that (2.1) holds if

$$\Delta^r W_n \equiv 0 \pmod{p^{r_1}}. \tag{2.6}$$

To prove (2.6) we will use induction on r. For $r = 1$ there is nothing to prove. Thus its truth is to be assumed for the exponents $1, 2, \ldots, r - 1$.

An easy calculation applied to (2.4) gives

$$\Delta^r W_n = n\Delta^r W_{n-1} + rp\Delta^{r-1} W_{n+p-1} + (t - 1)^2 \Delta^r W_{n-2}.$$

Hence, according to hypothesis,

$$\Delta^r W_n \equiv n\Delta^r W_{n-1} + (t - 1)^2 \Delta^r W_{n-2} \pmod{p^{r_1}},$$

so that (2.6) is true if it is true for two consecutive values of n. We now show that it holds for $n = -r_1 p$ and $n = -r_1 p - 1$.

It is clear that only even values of r need be considered in (2.6). For $n = -r_1 p - 1$ we have by (2.5)

$$\begin{aligned}\Delta^r W_{-r_1p-1} &= \sum_{s=0}^{r} (-1)^s \binom{r}{s} (t-1)^{(r-s)p} W_{-(r_1-s)p-1} \\ &= -\sum_{s=0}^{r} (-1)^s \binom{r}{s} (t-1)^{sp} W_{(r_1-s)p-1} \\ &= -\sum_{s=0}^{r} (-1)^s \binom{r}{s} (t-1)^{(r-s)p} W_{-(r_1+s)p-1} \\ &= -\Delta^r W_{-r_1p-1};\end{aligned}$$

Thus

$$\Delta^r W_{-r_1p-1} = 0. \tag{2.7}$$

Next, for $n = -r_1p$, we get by (2.4) and (2.5)

$$\begin{aligned}\Delta^r W_{-r_1p} &= \sum_{s=0}^{r} (-1)^s \binom{r}{s} (t-1)^{(r-s)p} W_{-(r_1-s)p} \\ &= -\sum_{s=0}^{r} (-1)^s \binom{r}{s} (t-1)^{sp+2} W_{(r_1-s)p-2} \\ &= -\sum_{s=0}^{r} (-1)^s \binom{r}{s} (t-1)^{sp} \{W_{(r_1-s)p} - (r_1-s)pW_{(r_1-s)p-1} \\ &\qquad\qquad - 2(t-1)^{(r_1-s)p}\} \\ &= -\Delta^r W_{-r_1p} + r_1p\Delta^r W_{-r_1p-1} - rp(t-1)^p \Delta^{r-1} W_{-r_1p}.\end{aligned}$$

Hence, from (2.7) and the induction assumption, it follows that

$$\Delta^r W_{-r_1p} \equiv -\Delta^r W_{-r_1p} (\text{mod } p^{r_1}).$$

Since p is an odd prime, (2.6) also holds for $n = -r_1p$, which completes the proof.

A class of polynomials which, in contrast to the $W_n(t)$, does have combinatorial significance is determined by the formula

$$V_n = \sum_{k=0}^{n} v_{n,k} t^k = W_n - (t-1) W_{n-1}$$

for $n \geqq 0$. Here $v_{n,k}$ is the analog of $u_{n,k}$ for a non-circular table. It follows from (2.6) that the V_n also satisfy a congruence like (2.1).

We summarize our results in the form of the following theorem.

THEOREM 1. *Let P_n denote U_n, W_n, or V_n. Then for every odd prime p*

$$\sum_{s=0}^{r} (-1)^s \binom{r}{s} (t-1)^{(r-s)p} P_{n+sp} \equiv 0 \ (\text{mod } p^{r_1}) \tag{2.8}$$

for all $r \geqq 1$ and $n \geqq 0$, where $r_1 = [r/2]$.

3. Proof of (1.2) for arbitrary *m*. To extend Theorem 1 no specific properties of ménage polynomials are required. We may assume therefore that $\{P_n\}$ is any sequence of polynomials satisfying (2.8), which can be rewritten as

$$(3.1) \qquad (E^p - (t-1)^p)^r P_n \equiv 0 \pmod{p^{r_1}},$$

where $EP_n = P_{n+1}$.

We remark first that by the binomial expansion of $(x^p - y^p)^p$ it follows that

$$x^{p^2} - y^{p^2} = (x^p - y^p)^p + p(x^p - y^p)f(x, y)$$

for some polynomial $f(x, y)$ in x and y. More generally, it is not hard to prove by induction on e that

$$(3.2) \qquad x^{p^e} - y^{p^e} = \sum_{i=0}^{e-1} p^i (x^p - y^p)^{p^{e-i-1}} f_i(x, y),$$

where again $f_i(x, y)$ is a polynomial in x and y. We will also need the $r-th$ power of (3.2), a typical term of which is of the form $p^A(x^p - y^p)^B M(x, y)$, where $M(x, y)$ is again a polynomial,

$$A = A(\alpha_1, \alpha_2, \ldots, \alpha_e) = \alpha_2 + 2\alpha_3 + \cdots + (e-1)\alpha_e$$
$$B = B(\alpha_1, \alpha_2, \ldots, \alpha_e) = \alpha_1 p^{e-1} + \alpha_2 p^{e-2} + \cdots + \alpha_{e-1} p + \alpha_e$$

and $\alpha_1, \alpha_2, \ldots, \alpha_e$ are non-negative integers satisfying

$$(3.3) \qquad \alpha_1 + \alpha_2 + \cdots + \alpha_e = r.$$

If in (3.2) we now take $x = E$, $y = t - 1$ and apply Theorem 1, we get that

$$(E^{p^e} - (t-1)^{p^e})^r P_n \equiv 0 \pmod{p^z},$$

where z is the minimum value attained by the sum $A + [B/2]$ over all $\alpha_1, \ldots, \alpha_e$ in (3.3). This minimum is given by $\alpha_1 = \cdots = \alpha_{e-1} = 0$, $\alpha_e = r$. To see this we treat even and odd values of r separately. Since B and r have the same parity, in the even case it is enough to show that

$$\sum_{j=1}^{e} \alpha_j \left(j - 1 + \frac{1}{2} p^{e-j} \right) \geqq r(e-1) + r/2,$$

which, because of (3.3), holds if $2j + p^{e-j} \geqq 2e + 1$ for all $1 \leqq j \leqq e$. This last inequality is easily verified. The same method applies to odd values of r.

We have proven therefore that

$$(E^{p^e} - (t-1)^{p^e})^r P_n \equiv 0 \pmod{p^{(e-1)r + r_1}}$$

for all $n > 0$ and $r \geqq 1$. Since $E^{p^e} - (t-1)^{p^e}$ divides $E^m - (t-1)^m$ as a polynomial in E if p^e divides m, the following generalization of Theorem 1 can be stated.

THEOREM 2. *Let $P_n = U_n$, W_n or V_n. Then for every odd prime p*

$$\sum_{s=0}^{r} (-1)^s \binom{r}{s} (t-1)^{(r-s)m} P_{n+sm} \equiv 0 \pmod{p^{(e-1)r+r_1}} \tag{3.4}$$

for all $n \geqq 0$, $r \geqq 1$, provided that p^e divides m.

By putting $P_n = U_n(t)$ and $t = 0$ in (3.4) we obtain a similar congruence for the ménage numbers $u_n = u_{n,0}$, namely

$$\sum_{s=0}^{r} (-1)^s \binom{r}{s} u_{n+2sm} \equiv 0 \pmod{p^{(e-1)r+r_1}},$$

where it is assumed that p^e divides $2m$. The analogous result is also true for the non-circular ménage numbers $v_n = v_{n,0}$.

REFERENCES

1. L. Carlitz, *Congruence properties of the ménage polynomials*, Scripta Mathematica **20** (1954), 51–57.

2. ———, *Congruence properties of Hermite and Laguerre polynomials*, Archiv der Mathematik **10** (1959), 460–465.

3. I. Kaplansky and J. Riordan, *The problème des ménages*, **12** (1946), 113–124.

4. J. Riordan, *The arithmetic of ménage numbers*, Duke Math J. **19** (1952), 27–30.

DEPARTMENT OF MATHEMATICS, PENNSYLVANIA STATE UNIVERSITY, UNIVERSITY PARK, PA 16802.