SINGLE VARIABLE BELL POLYNOMIALS

by

L. Carlitz

To Professor José M.ª Orts

1. Let

$$S(n,\,k) = \frac{1}{k!}\sum_{r=0}^{k} (-1)^{k-r}\binom{k}{r} r^n \tag{1.1}$$

denote the Stirling number of the second kind. The polynomial

$$A_n(x) = \sum_{k=0}^{n} S(n,\,k)\, x^k \tag{1.2}$$

is of considerable combinatorial interest [4, p. 76]. The first few values are

$$A_0 = 1,\ A_1 = x,\ A_2 = x + x^2,\ A_3 = x + 3x^2 + x^3$$
$$A_4 = x + 7x^2 + 6x^3 + x^4,\ A_5 = x + 15x^2 + 25x^3 + 10x^4 + x^5,$$
$$A_6 = x + 13\,x^2 + 90x^3 + 65x^4 + 15x^5 + x^6.$$

Removing the factor x, it is easily checked that the complementary factors in A_2, A_3, A_4, A_5, A_6 are irreducible over the rational field R. For A_2 and A_3 this is obvious. For A_4 we have

$$x^{-1} A_4(x) \equiv x^3 + x + 1 \qquad (\text{mod } 2);$$

since $x^3 + x + 1$ is irreducible (mod 2) it follows that $x^{-1}A_4(x)$ is irreducible over R. As for A_5 we have

$$x^{-1}A_5(x) \equiv x^4 + x^2 + x + 1 \equiv (x+1)(x^3 + x^2 + 1) \qquad (\text{mod } 2),$$
$$x^{-1}A_5(x) \equiv x^4 + 1 \equiv (x^2 + 2)(x^2 - 2) \qquad (\text{mod } 5);$$

it follows that $x^{-1} A_5(x)$ is irreducible over R. Finally for A_6 we have

$$x^{1-}A_6 \equiv x^5 + x^4 + x^3 + x + 1 \qquad (\text{mod } 2);$$

since $x^5 + x^4 + x^3 + x + 1$ is divisible by neither $x + 1$ nor $x^2 + x + 1$

Supported in part by National Science Foundation grant G 16485.

(mod 2) it must be irreducible (mod 2) and therefore $x^{1-}A_6$ is irreducible over R.

If $n = p$, a prime greater than 2 it follows from (1.1) that

$$S(p, k) \equiv \frac{1}{k!} \sum_{r=0}^{k} (-1)^{k-r} \binom{k}{r} r \equiv 0 \pmod{p}$$

for $1 < k < p$. As for the excluded values we have

$$S(p, 1) = 1, \quad S(p, p) = 1.$$

Thus

$$x^{-1} A_p \equiv x^{p-1} + 1 \qquad \text{(mod p)}.$$

It is known that $x^{p-1} + 1$ is the product (mod p) of $(p - 1)/2$ irreducible quadratics, indeed

$$x^{p-1} + 1 \equiv \prod_{\beta} (x^2 1 - \beta) \qquad \text{(mod p)}, \tag{1.3}$$

where the product is extended over the quadratic non-residues of p.

Touchard [5] has obtained the congruence

$$A_{n+p} = A_{n+1} + x^p A_n \qquad \text{(mod p)}, \tag{1.4}$$

where p is an arbitrary prime ; see also [4, p. 81]. In particular, for $p = 2$, (1.4) reduces to

$$A_{n+2} = A_{n+1} + x^2 A_n \qquad \text{(mod 2)}, \tag{1.5}$$

a recurrence of the second order.

The chief object of the present paper is to determine the factorization (mod 2) of the polynomial $A_n(x)$. This is described in Theorem 1 below and depends in particular upon the factorization (mod 2) of the cyclotomic polynomial. We incidentally determine the residue (mod 2) of the Stirling number (1.1).

It seems plausible that the polynomial $x^{-1}A_n(x)$ is irreducible in R for all $n > 1$. However we are unable to prove such a result except in the special case covered by Theorem 4 below.

For a discussion of arithmetic properties of general Bell and Stirling polynomials see [1] and [2].

2. It will be convenient to make a change of notation. Put

$$C_n = C_n(x) = x^{n+1} A_{n+1}\left(\frac{1}{x}\right) \qquad (n = 0, 1, 2, \ldots). \tag{2.1}$$

Then C_n is of degree n and satisfies

$$C_{n+2} \equiv x\, C_{n+1} + C_n \qquad \text{(mod 2)} \quad (\text{n} = 0, 1, 2, \ldots). \tag{2.2}$$

The first few values reduced (mod 2) are

$C_0=1,\ C_1=x+1,\ C_2=x^2+x+1,\ C_3=x^3+x^2+1,\ C_4=x^4+x^3+x^2+1,$
$C_5=x^5+x^4+x^2+x+1,\quad C_6=x^6+x^5+x^4+x+1,\quad C_7=x^7+x^6+x^4+1,$

$$C_8=x^8+x^7+x^6+x^4+1.$$

It follows from (2.2) that

$$C_{n+3} \equiv (x^2+1)\ C_{n+1} + xC_n \qquad (\text{mod } 2). \tag{2.3}$$

Since $C_1 = x + 1$ we infer that $C_{3n+1}(x)$ is divisible (mod 2) by $x + 1$; on the other hand $C_{3n}(x)$ and $C_{3n+2}(x)$ are prime to $x+1$.

If we put

$$C_n(x) = \sum_{r=0}^{n} c_{n,r}\ x^{n-r},$$

so that by (1.2) and (2.1)

$$c_{nr} = S(n+1,\ r+1), \tag{2.4}$$

it is evident that

$$c_{n+1,r} = c_{n,r-1} + (r+1)\ c_{n,r}. \tag{2.5}$$

It follows that

$$c_{n+1,2s} \equiv c_{n,2s-1} + c_{n,2s} \qquad \text{mod } 2), \tag{2.6}$$

$$c_{n+1,\,2s+1} \equiv c_{n,2s} \qquad (\text{mod } 2). \tag{2.7}$$

The congruences (2.6), (2.7) imply

$$c_{n+1,2s} \equiv c_{n-1,2s-2} + c_{n,2s} \qquad (\text{mod } 2). \tag{2.8}$$

We adjoin a table of the residues (mod 2) of c_{nr} for $o \le r \le n \le 10$.

n \ r	0	1	2	3	4	5	6	7	8	9	10
0	1										
1	1	1									
2	1	1	1								
3	1	1	0	1							
4	1	1	1	0	1						
5	1	1	0	1	1	1					
6	1	1	1	0	0	1	1				
7	1	1	0	1	0	0	0	1			
8	1	1	1	0	1	0	0	0	1		
9	1	1	0	1	1	1	0	0	1	1	
10	1	1	1	0	0	1	1	0	1	1	1

It is evident that

$$c_{n0} = 1 \quad (n \geq 0), \quad c_{n1} = 1 \quad (n \geq 1)$$

and it is easily proved that

$$c_{n2} \equiv n + 1 \qquad (\text{mod } 2) \qquad (n \geq 2).$$

Then by (2.7)

$$c_{n3} \equiv n \qquad (\text{mod } 2) \qquad (n \geq 3).$$

Making use of (2.6) we can show that

$$c_{n4} \equiv 1 + \binom{n}{2} \qquad (\text{mod } 2) \qquad (n \geq 4).$$

Similarly we find that

$$c_{n6} \equiv \binom{n-1}{1} + \binom{n-1}{3} \qquad (\text{mod } 2) \qquad (n \geq 6),$$

$$c_{n8} \equiv 1 + \binom{n-1}{2} + \binom{n-2}{4} \qquad (\text{mod } 2) \qquad (n \geq 8).$$

These special results suggest the general consequence :

$$(2.9) \qquad c_{n,2s} \equiv \sum_j \binom{n-s+2}{s-2j} \qquad (\text{mod } 2) \qquad (n \geq 2s),$$

which is easily proved by induction. In view of (2.7) we have also

$$(2.10) \qquad c_{ns2s+1} \equiv \sum_j \binom{n-s+1}{s-2j} \quad (\text{mod } 2) \qquad (n \geq 2s+1).$$

The congruences (2.9) and (2.10) are not very satisfactory for large values of s. Now it is evident that

$$c_{nn} = 1, \; c_{n,n-1} = \tfrac{1}{2}\, n\,(n+1).$$

Making use of (2.5) it is not difficult to show that

$$c_{n,n-2} \equiv \binom{n+1}{4} + \binom{n+1}{3}, \; c_{n,n-3} \equiv \binom{n+1}{6} + \binom{n+1}{4} \; (\text{mod } 2).$$

These special results suggest the following general congruence

$$(2.11) \qquad c_{n,n-s} \equiv \sum_{j=0}^{s-1} \binom{s-1}{j} \binom{n+1}{2s-j} \; (\text{mod } 2) \quad (n \geq s \geq 1),$$

which can be proved by induction without much trouble. However since

$$\sum_{j=0}^{s-1} \binom{s-1}{j} \binom{n+1}{2s-j} = \binom{n+s}{2s},$$

(2.11) may be replaced by the simpler formula

(2.12) $$c_{n,n-s} \equiv \binom{n+s}{2s} \pmod 2 \qquad (n \geq s \geq 0).$$

Replacing s by $n - s$, (2.12) becomes

(2.13) $$c_{ns} \equiv \binom{2n-s}{s} \pmod 2 \qquad (n \geq s \geq 0).$$

In particular, since

$$\binom{2n-2s}{2s} \equiv \binom{n}{s} \pmod 2,$$

(2.13) implies

(2.14) $$c_{n,2s} \equiv \binom{n-s}{s} \pmod 2 \qquad (n \geq 2s \geq 0).$$

By (2.7) we have also

(2.15) $$c_{n,2s+1} \equiv \binom{n-s-1}{s} \pmod 2 \qquad (n \geq 2s+1).$$

Comparison of (2.14) and (2.15) with (2.9) and (2.10) leads to a rather curious result.

It is not difficult to give a direct proof of (2.13). The formula is obviously true for $n = 0$. Then by (2.5)

$$\begin{aligned} c_{n+1,s} &= c_{n,s-1} + (s+1)\, c_{ns} \\ &\equiv \binom{2n-s+1}{s-1} + (s+1) \binom{2n-s}{s} \\ &\equiv \binom{2n-s+1}{s-1} + (2n-2s+1) \binom{2n-s+1}{s} \\ &\equiv \binom{2n-s+1}{s-1} + \binom{2n-s+1}{s} \\ &\equiv \binom{2n-s+2}{s}. \end{aligned}$$

This evidently completes the induction.

The right member of (2.14) suggests a connection with the Chebyshev polynomial $U_n(t)$ defined by [4, p. 222]

$$U_n(x) = \frac{\sin (n+1)\Theta}{\sin \Theta} \qquad (x = \cos \Theta) \tag{2.16}$$

$$= \sum_{2r \leq n} (-1)^r \binom{n-r}{r} (2x)^{n-2r}.$$

We may replace (2.16) by

$$W_n(t+t^{-1}) = \frac{t^{n+1} - t^{-n-1}}{t - t^{-1}} = \sum_{2r \leq n} (-1)^r \binom{n-r}{r} (t+t^{-1})^{n-2r}, \tag{2.17}$$

where $W_n(x) = U_n(x/2)$, so that $W_n(x)$ is a polynomial with integral coefficients. It follows from (2.13) and (2.17) that

$$C_n(x^2) \equiv W_{2n}(x) \pmod 2. \tag{2.18}$$

Also, making use of (2.14) and (2.15), we get

$$C_n(x) \equiv W_n(x) + W_{n-1}(x) \pmod 2. \tag{2.19}$$

Since the Stirling number $S(n, r)$ satisfies

$$x^n = \sum_{r=1}^{n} S(n, r)\, x(x-1)\ldots(x-r+1) \qquad (n \geq 1)$$

and

$$x(x-1)\ldots(x-2r+1) \equiv (x(x-1))^r, \quad x(x-1)\ldots(x-2r) \equiv x(x-1))^r,$$

it follows from (2.4), (2.14) and (2.15) that

$$x^{n-1} \equiv \sum_r \binom{n-r}{r-1} (x(x-1))^r + x \sum_r \binom{n-r}{r} (x(x-1))^r. \tag{2.20}$$

It is of some interest to determine the number of odd coefficients in the polynomial $C_n(x)$. For fixed n, let $\Theta_0(n)$ denote the number of odd coefficients $c_{n,2s}$ and $\Theta_1(n)$ the number of odd coefficients $c_{n,2s+1}$. It is clear from (2.7) that

$$\Theta_1(n+1) = \Theta_0(n). \tag{2.21}$$

In the next place since

$$\binom{2n+1-s}{s} \equiv 0 \pmod 2$$

unless s is even and

$$\binom{2n+1-2s}{2s} \equiv \binom{2n-2s}{2s} \equiv \binom{n-s}{s},$$

it follows from (2.14) that (2.15) that

$$\Theta_0(2n+1) = \Theta_0(n). \tag{2.22}$$

Similarly since

$$\binom{2n-2s}{2s} \equiv \binom{n-s}{s}, \quad \binom{2n-2s-1}{2s+1} \equiv \binom{2n-2s-2}{2s} \equiv \binom{n-s-1}{s},$$

we have also

$$\Theta_0(2n) = \Theta_0(n) + \Theta_0(n-1). \tag{2.23}$$

If $\Theta(n)$ denotes the number of odd c_{ns}, $o \leq s \leq n$, we have by (2.21) and (2.23)

$$\Theta(n) = \Theta_0(n) + \Theta_1(n) = \Theta_0(2n). \tag{2.24}$$

It follows from (2.22) and (2.23) that the generating function

$$G(x) = \sum_{n=0}^{\infty} \Theta_0(n)\, x^n$$

satisfies

$$G(x) = (1 + x + x^2)\ G(x^2),$$

so that

$$G(x) = (1 + x + x^2)\ (1 + x^2 + x^4)\,(1 + x^4 + x^8)\ldots \tag{2.25}$$

By means of (2.22) and (2.23) it is easy to show that for example

$$\Theta_0(2^r) = r+1,\ \Theta_0(2^r - 1) = 1 \tag{2.26}$$

and

$$\Theta_0(2^r + 2^{r-s}) = r + s + rs \qquad (s > 0)\ ; \tag{2.27}$$

however the general formula for $\Theta_0(n)$ with

$$n = 2^{r_0} + 2^{r_0 - r_1} + \ldots + 2^{r_0 + r_1 + \cdots + r_k} \tag{2.28}$$

seems to be complicated. We reamrk that if we put

$$n_j = 2^{r_j} + 2^{r_j + r_{j+1}} + \ldots + 2^{r_j + \cdots + r_k},$$

$$m_j = 2^{r_0} + 2^{r_0 + r_1} + \ldots + 2^{r_0 + r_1 + \cdots + r_j},\ m_{-1} = 0,$$

then

$$\Theta_0(n) = \Theta_0(m_j)\ \Theta_0(n_{j+1}) - \Theta_0(m_{j-1})\ \Theta_0(n_{j+2}) \quad (o \leq j \leq k). \tag{2.29}$$

In particular (2.29) implies

$$\Theta_0(n_0) = (1 + r_0)\ \Theta_0(n_1) - \Theta_0(n_2), \tag{2.30}$$

(2.31) $$\Theta_0(m_k) = (1 + r_k)\, \Theta_0(m_{k-1}) - \Theta_0(m_{k-2}).$$

3. If we put

(3.1) $$x = t + t^{-1},$$

(2.18) becomes

$$\begin{aligned} C_n(t^2 + t^{-2} &\equiv W_{2n}(t + t^{-1}) \\ &\equiv \frac{t^{2n+1} - t^{-2n-1}}{t - t^{-1}} \\ &\equiv t^{-2n}\, \frac{t^{2n+2} - 1}{t^2 - 1} \qquad \pmod 2. \end{aligned}$$

Replacing t^2 by t, this reduces to

(3.2) $$t^n\, C_n(t + t^{-1}) \equiv \frac{t^{2n+1} - 1}{t - 1} \qquad \pmod 2.$$

We remark that (3.2) can be proved directly using only (2.2).

We recall next that the cyclotomic polynomial defined by means of

(3.3) $$t^n - 1 = \prod_{d|n} F_d\,(t)$$

has the following factorization property. Let n be odd and let 2 belong to the exponent e (mod n). Then if $\phi\,(n) =$ ef, where $\phi\,(n)$ is the Euler function, we have the factorization

(3.4) $$F_n(t) \equiv P_1(t) \ldots P_f(t) \qquad \pmod 2,$$

where the P_j are distinct irreducible polynomials (mod 2) of degree e.

Thus the factorization (mod 2) of the polynomial

(3.5) $$t^n\, C_n\,(t + t^{-1})$$

is determined by means of (3.4). However to get the factorization of $C_n\,(x)$ we need something more.

We remark first that if the a_j are arbitrary integers then integers b_j can be determined so that

(3.6) $$\sum_{j=0}^{n} a_j\,(t^j + t^{-j}) = \sum_{j=0}^{n} b_j(t + t^{-1})^j;$$

a like statement holds (mod 2). Now if $A\,(x)$ is an arbitrary polynomial with integral coefficients it is evident that we may apply (3.6) to obtain

(3.7) $$A\,(t)\;A\,(t^{-1}) = B(t + t^{-1}),$$

where $B(x)$ is a polynomial with integral coefficients.

We assume that $A(x)$ is irreducible (mod 2) and moreover that

$$(3.8) \qquad A(x) \neq x^n A(x^{-1}) \qquad (\deg A = n);$$

we shall show that $B(x)$ is also irreducible (mod 2). For if we assume that

$$B(x) \equiv R(x)\ S(x) \pmod 2$$

then (3.7) becomes

$$(3.9) \qquad A(t)\ \overline{A}(t) \equiv t^n R(t+t^{-1})\ S(t+t^{-1}),$$

where $\overline{A}(t) = t^n A(t^{-1})$. If $\deg R(x) = k$, it follows from (3.9) that

$$t^k R(t+t^{-1}) \equiv A(t),\ t^{n-k} S(t+t^{-1}) \equiv \overline{A}(t).$$

But from the last of these relations we have

$$t^k S(t+t^{-1}) \equiv A(t),$$

so that $R = S$, $A = \overline{A}$, which contradicts (3.8). Therefore $B(x)$ as defined by (3.6) is irreducible (mod 2).

If in place of (3.8) we have

$$(3.10) \qquad A(x) = \overline{A}(x) = x^n A(x^{-1})$$

and $A(x)$ is irreducible (mod 2) of degree $n > 1$, then, to begin with, n is even. For otherwise $A(x)$ contains an even number of terms, which implies divisibility (mod 2) by $x + 1$. If we put $n = 2k$ we may apply (3.6) to get

$$t^{-k} A(t) = B(t - t^{-1}).$$

It follows at once that $B(x)$ is also irreducible (mod 2).

We can now describe the factorization (mod 2) of $C(n)$. We state the following

THEOREM 1. *To obtain the factorization* (mod 2) *of* $C_n(x)$ *we first factor the polynomial in* t

$$(3.11) \qquad (t^{2n+1} - 1)/(t\ 1)$$

by means of (3.3) *and* (3.4). *Let* $P(t)$ *be an irreducible factor of* (3.11) *of degree* $m < 2$. *Then if*

$$(3.12) \qquad P(t) = t^m P(t^{-1})$$

it follows that $m = 2k$ *and*

$$t^{-k} P(t) = Q(x)$$

furnishes an irreducible factor of $C_n(x)$ *of degree* k. *If* (3.12) *is not satisfied then*

$$P(t)\ P(t^{-1}) = Q(x) \tag{3.13}$$

furnishes an irreducible factor of $C_n(x)$ *of degree* m. *The polynomial* (3.11) *has the quadratic factor* $t^2 + t + 1$ *if and only if* $3/2n + 1$; *to this factor corresponds the linear factor* $x + 1$ *of* $C_n(x)$. *In this way all irreducible factors of* $C_n(x)$ *are obtained. Morevoer* $C_n(x)$ *has no repeated factors.*

The only ambiguity in the theorem is that we have no way of deciding in advance when (3.12) is satisfied. We are therefore unable to predict the number of irreducible factors of $C_n(x)$ of a given degree.

We remark that in the factorization (mod 2) of the cyclotomic polynomial $F_n(t)$ irreducible factors occur that may or may not satisfy (3.21). For example we have

$$t^{-2}F_5\ (t) \equiv t^2 + t + 1 + t^{-1} + t^{-2} \equiv x^2 + x + 1,$$

$$t^{-3}F_7\ (t) \equiv (t^3 + t + 1)\ (t^{-3} + t^{-1} + 1) \equiv x^3 + x^2 + 1,$$

$$t^{-3}F_9\ (t) \equiv t^3 + 1 + t^{-3} \equiv x^3 + x + 1,$$

$$t^{-5}F_{11}(t) \equiv t^5 + \ldots + t^{-5} \equiv x^5 + x^4 + x^2 + x + 1,$$

$$t^{-6}F_{13}(t) \equiv t^6 + \ldots + t^{-6} \equiv x^6 + x^5 + x^4 + x + 1,$$

$$t^{-4}F_{15}(t) \equiv (t^4 + t + 1)\ (t^{-4} + t^{-1} + 1) \equiv x^4 + x^3 + 1,$$

$$t^{-8}F_{17}(t) \equiv (t^4 + t^3 + t^2 + 1 + t^{-2} + t^{-3} + t^{-4}).\ (t^4 + t + 1 + t^{-1} + t^{-4})$$
$$\equiv (x^4 + x^3 + x^2 + x + 1)\ (x^4 + x + 1),$$

$$t^{-6}F_{21}(t) \equiv (t^6 + t^5 + t^4 + t^2 + 1)\ (t^6 + t^4 + t^2 + 1) \equiv x^6 - x^5 - 1.$$

4. The following additional properties of $C_n(x)$ follow easily from (3.2).

THEOREM 2. *If* $2m + 1/2n + 1$, *then* $C_m(x)$ *is a factor* (mod 2) *of* $C_n(x)$.

THEOREM 3. *If* $(2m + 1,\ 2n + 1) = 2r + 1$, *then* $C_r(x)$ *is the greatest common divisor* (mod 2) *of* $C_m(x)$ *and* $C_n(x)$. *In particular if* $(2m + 1, 2n + 1) = 1$, *then* $C_m(x)$ *and* $C_n(x)$ *are relatively prime* (mod 2).

As a corollary of Theorem 1 we state

THEOREM 4. *If* $p = 2n + 1$ *is prime and* 2 *is a primitive root* (mod p) *then* $C_n(x)$ *is irreducible* (mod 2) *and therefore irreducible in* R.

If 2 belongs to an odd exponent (mod n) it is clear from the discussion following (3.10) that if $P(t)$ is an irreducible factor (mod 2) of $F_n(t)$ then $P(t)$ does not satisfy (3.12). Therefore the irreducible factor of $C_n(x)$ corresponding to $P(t)$ is given by (3.13). Note that in this case the degree of $Q(x)$ is necessarily odd. However the converse is not true as is evident for example from the factorization of $t^{-3}F_7(t)$ or $t^{-5}F_{11}(t)$ given above.

In the present connection the following theorem is of some interest.

THEOREM 5. *Let*

$$Q(x) = x^n + c_1x^{n-1} + \dots + c_{n-1}x + c_n \tag{4.1}$$

be an irreductible polynomial (mod 2) *of degree* $n \geq 1$. *Then* $Q(x)$ *admits the factorization*

$$t^n Q(t + t^{-1}) = P(t)\ \bar{P}(t), \tag{4.2}$$

vhere $P(t)$ *and* $\bar{P}(t)$ *are distinct irreducibles of degree* n, *if and only if* $c_{n-1} = 0$.

Proof. If (4.2) holds it is evident that $\bar{P}(t) = t^nP(t^{-1})$. Thus if α is a root of $P(t)$ then α^{-1} is a root of $\bar{P}(t)$. It follows that

$$\beta = \alpha + \alpha^{-1} \tag{4.3}$$

is a root of $Q(x)$. Moreover from (4.2)

$$\left(\frac{\alpha}{\beta}\right)^2 = \frac{\alpha}{\beta} + \frac{1}{\beta 2},$$

which implies

$$\left(\frac{\alpha}{\beta}\right)^{2^n} = \frac{\alpha}{\beta} + \sum_{j=1}^{n} \beta^{-2^j}.$$

Since α, $\beta \ \varepsilon\ GF(2^n)$ we get

$$\sum_{j=1}^{n} \beta^{-2^j} = 0.$$

But since $\beta^{-2}, \beta^{-2^2}, \dots, \beta^{-2^n}$ are the roots of $Q(x)$ we have also

$$c_{n-1} = \sum_{j=1}^{n} \beta^{-2^j}.$$

Hence the necessity of the condition

$$c_{n-1} = 0. \tag{4.4}$$

Conversely when (4.4) holds the equation

$$\xi^2 = \xi + \frac{1}{\beta^2}$$

is solvable in $GF(2^n)$; in other words for given β there exists $\alpha \varepsilon GF(2^n)$ satisfying (4.3). Moreover since $Q(x)$ is irreducible the least positive integer t such that

$$\beta^{2^t} = \beta$$

is $t = n$. If we assume that $\alpha^{2^t} = \alpha$, where $o < t < n$, (4.3) implies $\beta^{2^t} = \beta$, which is impossible. Therefore the polynomial

$$P\ (t) = \prod_{j=0}^{n-1} (t - \beta^{2^j})$$

is irreducible in $GF\ [2,\ t]$. This evidently completes the proof of the theorem.

Theorem 5 may be compared with the known result [3, p. 34] that the irreducible polynomial (4.1) satisfies

$$Q(t^2 + t) = R(t)\ R(t+1),$$

where $R(t)$ is also irreducible, if and only if $c_1 = 0$.

We conclude with a few additional factorizations (mod 2) of $C_n(x)$. We have already noted that C_1, C_2, C_3, C_5 are irreducible while $C_4 = (x+1)\ (x^3 + x + 1)$.

$$\begin{aligned}
C_6 &= x^6 + x^5 + x^4 + x + 1, \\
C_7 &= (x+1)\ (x^6 + x^3 + x^2 + x + 1), \\
C_8 &= (x^4 + x^3 + x^2 + x + 1)\ (x^4 + x + 1), \\
C_9 &= x^9 + x^8 + x^6 + x^5 + x^4 + x + 1. \\
C_{10} &= (x+1)\ (x^3 + x + 1)\ (x^6 + x^5 + 1), \\
C_{11} &= x^{11} + x^{10} + x^9 + x^4 + x^3 + x^2 + 1, \\
C_{12} &= (x^2 + x + 1)\ (x^{10} + x^6 + x^5 + x^3 + x^2 + x + 1).
\end{aligned}$$

We remark that the irreducibility of C_6, C_9, C_{11} is implied by Theorem 1 while the factorizations of C_7, C_8, C_{10}, and C_{12} depend upon the factorization of F_{15}, F_{17}, F_{21} and F_{25}, respectively.

REFERENCES

1. H. W. BECKER and J. RIORDAN, *The arithemetic of Bell and Stirling numbers*, *American Journal of Mathematics*, vol. 70 (1948), pp. 385-394.

2. L. CARLITZ, *Congruences for generalized Bell and Stirling numbers*, Duke Mathematical Journal, vol. 22 (1955), pp. 193-205.

3. L. E. DICKSON, *Linear groups*, Dover Publications, New York, 1958.

4. J. RIORDAN, *Combinatorial analysis*, John Wiley, New York, 1958.

5. J. TOUCHARD, *Propriétés arithmétiques de certains nombres recurrents*, Ann. Soc. Sci. Bruxelles, vol. A53 (1933), pp. 21-31.