ON SOME SPECIAL FACTORIZATIONS OF $(1 - x^n)/(1 - x)$

L. Carlitz and L. Moser

(received May 1, 1966)

Let A: $a_1 < a_2 < \ldots < a_k$ be a set of non-negative integers. We call the corresponding polynomial $A(x) = x^{a_1} + x^{a_2} + \ldots + x^{a_k}$ the characteristic polynomial, or briefly, the c-polynomial of A. Any polynomial of such a form we call a c-polynomial and any factorization of a c-polynomial into others of the kind we call a c-factorization. If a c-polynomial cannot be factored in this way we call it c-irreducible. In this note we will determine all c-factorizations of the polynomial $1 + x + x^2 + \ldots + x^{n-1}$, and will find under what circumstances the c-irreducible factors are also irreducible in the usual sense, i.e., irreducible over the field of rationals.

The motivation for these problems stems from the following considerations: If we have three sets of integers A, B, C, with corresponding c-polynomials $A(x)$, $B(x)$ and $C(x)$, then $A(x) = B(x)\,C(x)$ if and only if each element of A is uniquely expressible, apart from order, as a sum of one element from B and one from C. In characterizing the c-factorizations of $1 + x + x^2 + \ldots + x^{n-1}$ we are therefore, in effect, characterizing all sets of sets $A_1, A_2, \ldots, A_r$, such that each of the numbers $0, 1, 2, \ldots, n-1$ has a unique representation in the form $a_1 + a_2 + \ldots a_r$ with $a_i \in A_i$, $i = 1, 2, \ldots, r$. For the set $0, 1, 2, \ldots, n-1$ replaced by the set of all non-negative integers this last problem was solved by De Bruijn [1]. De Bruijn's argument operates directly with the integers, i.e., does not consider c-polynomials, and though quite elementary is still a little subtle.

Canad. Math. Bull. vol. 9, no. 4, 1966

1. Let $F_n(x) = \prod_{r \cdot s=n} (x^r - 1)^{\mu(s)}$,

where $\mu(n)$ is the Möbius function, denote the cyclotomic polynomial. We shall prove the following

THEOREM 1. *Put* $n = p_1 p_2 \cdots p_r$, *where the* p_j *are primes (not necessarily distinct):* Then we have the factorization

$$(1) \quad \frac{x^n - 1}{x-1} = F_{p_1}(x) F_{p_2}(x^{p_1}) F_{p_3}(x^{p_1 p_2}) \ldots F_{p_r}(x^{p_1 p_2 \cdots p_{r-1}})$$

where on the right each factor is c-irreducible. Moreover, all factorizations of $1 + x + \ldots + x^{n-1}$ *into c-irreducible factors are obtained in this way.*

For example we have the factorizations

$$\frac{x^6 - 1}{x-1} = (x^2 + x + 1)(x^3 + 1) = (x + 1)(x^4 + x^2 + 1),$$

$$\frac{x^{12} - 1}{x-1} = (x + 1)(x^2 + 1)(x^8 + x^4 + 1)$$

$$= (x + 1)(x^4 + x^2 + 1)(x^6 + 1)$$

$$= (x^2 + x + 1)(x^3 + 1)(x^6 + 1).$$

Generally it is clear from the theorem that if

$$n = p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r},$$

where now the p_j are distinct primes, then the number of factorizations of the form (1) is equal to

$$\frac{(e_1 + e_2 + \ldots + e_r)!}{e_1! \, e_2! \ldots e_r!}$$

The theorem is an easy consequence of the following lemmas.

https://doi.org/10.4153/CMB-1966-050-1 Published online by Cambridge University Press

LEMMA 1. *Let*

$$(2) \qquad \frac{x^n - 1}{x-1} = A(x)\,B(x)$$

where $A(x)$ *and* $B(x)$ *are c-polynomials. Then either* $A(x)$ *or* $B(x)$ *is of the form* $(x^r - 1)/(x-1)$ *where* r *is a divisor of* n.

Proof. If the lemma is false we may assume that

$$A(x) = 1 + x + \ldots + x^{j-1} + x^{k+1} + \ldots \qquad (k \geq j),$$

so that

$$B(x) = 1 + x^j + x^{j+1} + \ldots + x^k + \ldots \quad .$$

Then the coefficient of x^{k+1} in $A(x)\,B(x)$ is at least 2. This evidently contradicts (2).

LEMMA 2. *Let*

$$(3) \qquad \frac{x^{nr} - 1}{x^r - 1} = A(x)\,B(x)$$

where $A(x)$ *and* $B(x)$ *are c-polynomials. Then the exponents of all powers of* x *occuring in* $A(x)$ *and* $B(x)$ *are multiples of* r.

Proof. If the lemma is false we may suppose that $A(x)$ contains a term x^k where k is not a multiple of r. Then the product $A(x)\,B(x)$ contains the term x^k, which contradicts (3).

LEMMA 3. *If* p *is a prime and* r *is an arbitrary integer* ≥ 1, *the polynomial* $F_p(x^r)$ *is c-irreducible.*

Proof. The lemma follows from Lemma 2 and the fact that $F_p(x)$ is irreducible over the rationals.

2. We shall now prove

THEOREM 2. *In the factorization (1) the factors on the right are irreducible over the rationals if and only if*

$$p_1 = p_2 = \ldots = p_r = p .$$

https://doi.org/10.4153/CMB-1966-050-1 Published online by Cambridge University Press

Proof. The sufficiency follows from the observation that

$$F_{p^r}(x) = \frac{x^{p^r} - 1}{x^{p^{r-1}} - 1} = F_p(x^{p^{r-1}})$$

together with the irreducibility of $F_{p^r}(x)$ over the rationals.

To prove the necessity we observe that if $r \nmid p^n$ then $F_p(x^r)$ is reducible over the rationals. Indeed if

$$r = p^k m \qquad (p \nmid m),$$

then

$$F_p(x^r) = \frac{x^{pr} - 1}{x^r - 1} = \prod_{d \mid m} F_{p^{k+1} d}(x).$$

Since $m > 1$ it is evident that $F_p(x^r)$ is reducible.

3. Let $f(n)$ denote the number of factorizations

(4) $$\frac{x^n - 1}{x - 1} = A(x)\, B(x),$$

where $A(x)$, $B(x)$ are c-polynomials and the orders of the factors are disregarded. To determine $f(n)$ we put

$$R_k(x) = (x^k - 1)/(x - 1)$$

and

$$A(x) = R_{k_1}(x)\, R_{k_3}(x^{k_1 k_2}) \ldots ,$$

$$B(x) = R_{k_2}(x^{k_1})\, R_{k_4}(x^{k_1 k_2 k_3}) \ldots ,$$

where $n = k_1 k_2 \ldots k_r$ and every $k_t > 1$. It follows from Theorem 1 that

$$f(n) = \sum_{\substack{k_1 k_2 \cdots k_r = n \\ k_t > 1}} 1 = \sum_{r=0} T'_r(n),$$

where

$$(\zeta(s) - 1)^r = \sum_{n=1}^{\infty} \frac{T'_r(n)}{n^s}.$$

This evidently implies (with $f(1) = 1$)

$$(5) \qquad \sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \sum_{r=0}^{\infty} (\zeta(s) - 1)^r = \frac{1}{2 - \zeta(s)},$$

so that

$$(6) \qquad 2f(n) = \sum_{d \mid n} f(d).$$

By means of (5) or (6) we may calculate $f(n)$. For $n = p^\alpha$, where p is a prime and $\alpha \geq 1$, (6) reduces to

$$f(p^\alpha) = \sum_{j=0}^{\alpha-1} f(p^j).$$

This implies

$$(7) \qquad f(p^\alpha) = 2^{\alpha-1} \qquad (\alpha \geq 1).$$

To compute $f(n)$, where n is squarefree, put

$$u_r = f(p_1 p_2 \cdots p_r) \qquad (p_i \neq p_j).$$

Then by (6)

$$2u_r = \sum_{j=0}^{r} \binom{r}{j} u_j,$$

which implies

https://doi.org/10.4153/CMB-1966-050-1 Published online by Cambridge University Press

$$\sum_{r=0}^{\infty} \frac{u_r x^r}{r!} = \frac{1}{2 - e^x} .$$

If we recall [2] the definition of the Eulerian number $H_n(\lambda)$:

$$\frac{\lambda - 1}{\lambda - e^x} = \sum_{n=0}^{\infty} H_n(\lambda) \frac{x^n}{n!} ,$$

we see that

(8) $$u_r = H_r(2) .$$

REFERENCES

1. N.G. De Bruijn, On number systems. Nieuw Archief voor Wiskunde (3), 4, (1956), pages 15-17.

2. L. Carlitz, Eulerian numbers and polynomials. Mathematics Magazine, 32, (1958), pages 247-258.

Duke University, Durham, North Carolina
and
University of Alberta, Edmonton, Alberta

https://doi.org/10.4153/CMB-1966-050-1 Published online by Cambridge University Press