KONINKL. NEDERL. AKADEMIE VAN WETENSCHAPPEN – AMSTERDAM
Reprinted from Proceedings, Series A, **56**, No. 4 and Indag. Math., **15**, No. 4, 1953

MATHEMATICS

ON THE FACTORIZATION OF CYCLIC GROUPS

BY

N. G. DE BRUIJN

(*University of Amsterdam*)

(Communicated by Prof. H. D. KLOOSTERMAN at the meeting of June 27, 1953)

§ 1. *Introduction*

Recently G. HAJÓS [4] discovered that there exist cyclic groups which admit a non-trivial factorization. Here $G = AB$ is called a factorization of the cyclic group G, if A and B are subsets of G such that every element $g \in G$ can be represented uniquely as $g = ab$, $a \in A$, $b \in B$ (the group operation is multiplication). A subset A is called periodic whenever there is an element $g \in G$, $g \neq e$ such that $Ag = A$ (e stands for the unit element).

A factorization $G = AB$ will be called *trivial* if at least one of the factors A, B is periodic. If every factorization of G is trivial, G is called "good"; if non-trivial factorizations exist, G is called "bad".

HAJÓS [4] gave a method for constructing non-trivial factorizations of certain cyclic groups; his simplest example was one in the group of order 180. In a previous paper [2] we gave a slight extension of HAJÓS' method. Theorem 1 of that paper, applied to cyclic groups, shows the following fact: If $n = d_1 d_2 d_3$, $(d_1, d_2) = 1$, $d_3 > 1$, and if both d_1 and d_2 are composite numbers, then the cyclic group of order n is "bad".

The cyclic groups which are not covered by this result are those of orders p^λ ($\lambda \geqslant 1$), $p^\lambda q$ ($\lambda \geqslant 1$), p^2q^2, $p^\lambda qr$ ($\lambda = 1,2$), $pqrs$; here p, q, r, s, denote different primes.

REDÉI [5] proved that the cyclic groups of orders p^λ ($\lambda \geqslant 1$), pq, pqr are "good". In the present paper we shall show, among other things, that the cyclic groups of order $p^\lambda q$ ($\lambda \geqslant 1$) are "good" (theorem 4). So at present, the only undecided cases are the orders p^2q^2, p^2qr, $pqrs$.

The simplest non-trivial factorization known at present is in the group of order 72. Using the method of theorem 1 of [2], the following example can be constructed [1] ($g^{72} = e$):

A: g^0, g^8, g^{16}, g^{18}, g^{26}, g^{34};

B: g^{18}, g^{54}, g^{24}, g^{60}, g^{48}, g^{12}, g^{17}, g^{41}, g^{65}, g^{45}, g^{69}, g^{21}.

In a "good" group every factorization is trivial; therefore all factorizations can be found if all factorizations of all proper subgroups are

[1] With the notations of the proof of that theorem, take $H_1^* = (g^0, g^{36})$, $H_2^* = (g^0, g^{24}, g^{48})$; $a_1 = g^0$, $a_2 = g^{18}$, $b_1 = g^0$, $b_2 = g^8$, $b_3 = g^{16}$, $c_1 = g^0$, $c_2 = g^9$, $u = g^{18}$, $v = g^8$.

known. As these subgroups are also "good", the reduction can be continued. Hence it is easy to construct all factorizations of any "good" group. (cf. HAJÓS [3]). In "bad" groups, however, we are still very far from the solution of that problem. What can be said in general about the structure of non-trivial factorizations?

HAJÓS [3] proposed the question whether every factorization is quasi-periodic. A factorization $G = AB$ is called *quasiperiodic* if either A or B, B say, can be split into a number of parts $B = B_1 + \ldots + B_m$ $(m > 1)$, such that $AB_i = g_i AB_1$ $(i = 1, \ldots, m)$, where the elements $g_1, \ldots, g_m$ form a subgroup of G.

In theorem 5 below we prove something in this direction. If in that theorem, under the extra assumption that the coefficients of both $A(x)$ and $B(x)$ are nonnegative, we would be able to prove that the coefficients of all $B_j(x)$ are nonnegative, we would have an affirmative answer to HAJÓS' question for cyclic groups of squarefree order.

Another matter to be touched upon in this paper is the following:

Conjecture 1. If $G = AB$ is a factorization of a cyclic group G, and if A has p elements, where p is a prime, then the factorization is trivial.

In theorem 3 we show the truth of this conjecture for the case that n has two different prime factors; if $n = p^\lambda$ it simply follows from the fact that the group is "good".

It can be shown that conjecture 1 is equivalent to the following one, already stated in [1]:

Conjecture 2. Let R denote the set of all integers, and let R be the direct sum [2]) of two subsets A and B: $R = A + B$. Assume $0 \in A$, $0 \in B$, whereas the g.c.d. of the elements of A is 1. Then A consists of a complete set of residues mod p [3]), and B consists of all multiples of p.

The equivalence of these conjectures follows from the following fact: If R is a direct sum $R = A + B$, and if A is finite, then B is periodic (see [3]).

As in REDÉI's paper [5], we shall proceed by translating the group problems in terms of polynomials. This is done in the following way: Every factorization $G = AB$ of the cyclic group of order n corresponds to a congruence

$$1 + x + x^2 + \ldots + x^{n-1} \equiv A(x)\, B(x) \pmod{x^n - 1} \tag{1.1}$$

in the ring of polynomials with integer coefficients. Here $A(x) = \Sigma x^k$, where k runs through all numbers which are such that $g^k \in A$, $0 \leqslant k < n$ (g is a fixed generating element of G). The same applies to $B(x)$ and B. Therefore, all coefficients of $A(x)$ and $B(x)$ are either 0 or 1. However, the only thing we shall need in the sequel is, that those coefficients are non-negative integers.

[2]) This denotes the same thing as factorization, but for the fact that in the present case the group operation is addition.

[3]) This part of the statement was actually proved in [1].

Notations. Throughout the paper, $F_n(x)$ denotes the n-th cyclotomic polynomial

$$F_n(x) = \prod_{d/n} (1 - x^{n/d})^{\mu(d)} .$$

We shall frequently use the fact that the F_n's are irreducible and relatively prime.

The polynomial $G_{n,d}$ is, if d/n, defined by

$$G_{n,d}(x) = (x^n - 1)/(x^{n/d} - 1) = 1 + x^{n/d} + x^{2n/d} + \ldots + x^{(d-1)n/d}.$$

The set of all integers is denoted by R, and $R[x]$ stands for the ring of all polynomials with integer coefficients. The set of all polynomials with non-negative integer coefficients will be denoted by $R_P[x]$.

All notions concerning divisibility, congruence and ideals have to be interpreted with respect to $R[x]$. If $f, \varphi_1, \ldots, \varphi_k$ are elements of $R[x]$, then both

$$f \equiv 0 \pmod{(\varphi_1, \ldots, \varphi_k)} \quad \text{and} \quad f \in (\varphi_1, \ldots, \varphi_k)$$

denote that f belongs to the ideal generated by $\varphi_1, \ldots, \varphi_k$, that is, f is of the form $f_1 \varphi_1 + \ldots + f_k \varphi_k$ (all $f_i \in R[x]$). We write f/g (f divides g) whenever $g \in (f)$. $f \equiv g$ means the same as $f - g \equiv 0$. If convenient, the ideal $(\varphi_1, \ldots, \varphi_k)$ will be written as $\cup_{i=1}^{k} (\varphi_i)$.

§ 2. *A theorem of* Redéi

We first consider a special case, which is sufficient for our purposes in § 3 and § 4. Let n be of the form $n = p^\lambda q^\mu$ ($\lambda \geqslant 1$, $\mu \geqslant 1$), where p and q are different primes. Then we have

$$F_n(x) = P(x)\, G_{n,p}(x) + Q(x)\, G_{n,q}(x) \qquad (P(x) \in R[x],\ Q(x) \in R[x]). \tag{2.1}$$

In order to show this, we write

$$F_n(x) = (x^n - 1)\,(x^{n/pq} - 1)\,(x^{n/p} - 1)^{-1}\,(x^{n/q} - 1)^{-1},$$

and so we have to prove

$$x^{n/pq} - 1 = P(x)\,(x^{n/q} - 1) + Q(x)\,(x^{n/p} - 1).$$

This follows from the following well known fact: if a, b are positive integers, and $c = (a, b)$ is their g.c.d., then $x^c - 1 \in (x^a - 1,\ x^b - 1)$. For, there are integers s, t with $s > 0$, $t > 0$, $as = c + bt$, whence

$$x^c - 1 = (x^{as} - 1) - x^c (x^{bt} - 1),\ x^{as} - 1 \in (x^a - 1),\ x^{bs} - 1 \in (x^b - 1). \tag{2.2}$$

In § 5 we shall also need the following more general theorem of Redéi ([5], Hilffssatz 4), which asserts the analogue of (2.1) for general values of n:

Theorem 1. We have $F_n(x)/f(x)$, if and only if $f(x)$ is of the form

$$f(x) = \sum_{p/n} G_{n,p}(x)\, f_p(x) \qquad (f_p(x) \in R[x]).$$

In other words, we have,

$$(F_n(x)) = \cup_{p/n} (G_{n,p}(x)).$$

Proof [4]). We shall prove the following formulas simultaneously by induction with respect to the number of different prime divisors of n:

$$F_n(x) \in \{\cup_{p,n} G_{nt,p}, x^n-1\} \qquad ((t,n) = 1). \tag{2.3}$$

$$(x^n-1)/F_n(x) \in \{\prod_{p/n} (x^{tn/p}-1),\ x^n-1\} \qquad ((t,n) = 1). \tag{2.4}$$

If k is the number of different prime divisors of n, we shall denote (2.3) by $\mathbf{A}_k$, and (2.4) by $\mathbf{B}_k$. The special cases $t = 1$ will be denoted by $\mathbf{A}_k^*$, $\mathbf{B}_k^*$, respectively. As $x^n - 1 \in G_{n,p}$ for each p/n, $\mathbf{A}_k^*$ can be written as

$$F_n(x) \in \cup_{p/n} G_{n,p}. \tag{2.5}$$

As, on the other hand, F_n divides all $G_{n,p}$, the theorem follows from (2.5).

Our induction runs as follows: $\mathbf{A}_0$ and $\mathbf{B}_0$ are trivial. We shall prove

$$\mathbf{A}_k^* \Rightarrow \mathbf{A}_k,\ \mathbf{B}_k^* \Rightarrow \mathbf{B}_k,\ \mathbf{A}_k^* + \mathbf{B}_k \Rightarrow \mathbf{A}_{k+1}^*,\ \mathbf{A}_k + \mathbf{B}_k^* \Rightarrow \mathbf{B}_{k+1}^*.$$

$\mathbf{A}_k^* \Rightarrow \mathbf{A}_k$ is easy, as $G_{n,p} \equiv G_{nt,p} \pmod{x^n-1}$ $((t,n) = 1)$.

$\mathbf{B}_k^* \Rightarrow \mathbf{B}_k$ follows from $x^{n/p}-1 \in (x^n-1,\ x^{tn/p}-1)$ (cf. (2.2)).

$\mathbf{A}_k^* + \mathbf{B}_k \Rightarrow \mathbf{A}_{k+1}^*$. Let n have k different prime factors, and let q be a prime not dividing n. Put $q^\lambda = v$, $q^{\lambda-1} = w$ $(\lambda \geqslant 1)$, then nv is a number with $k+1$ different prime factors. We have the identity

$$F_{nv}(x)\, F_n(x^w) = F_n(x^v). \tag{2.6}$$

Therefore, by $\mathbf{A}_k^*$ and $\mathbf{B}_k$ (with $t = q$), we have

$$(x^{nw}-1)\, F_{nv}(x) = F_n(x^v) \cdot \{(x^{nw}-1)/F_n(x^w)\} \in$$

$$\in \{\cup_{p/n} G_{n,p}(x^v)\} \cdot \{\prod_{p/n} ((x^w)^{qn/p}-1), (x^w)^n-1\} \subset \{x^{nv}-1, (x^{nw}-1) \cup_{p/n} G_{nv,p}(x)\}.$$

As $x^{nv} - 1 = (x^{nw} - 1)\, G_{nv,q}$, the latter ideal equals $(x^{nw} - 1) \cdot \cup_{p/nv} G_{nv,p}(x)$, and $\mathbf{A}_{k+1}$ follows.

$\mathbf{A}_k + \mathbf{B}_k^* \Rightarrow \mathbf{B}_{k+1}^*$. Using the same notation as in the previous case, we have, by (2.6) and by $\mathbf{B}_k^*$ and $\mathbf{A}_k$ (with $t = q$),

$$(x^{nv}-1)/F_{nv}(x) = \{((x^v)^n-1)/F_n(x^v)\} \cdot F_n(x^w) \in$$

$$\in \{x^{nv}-1,\ \prod_{p/n} (x^{nv/p}-1)\} \cdot \{\cup_{p/n} G_{nq,p}(x^w),\ x^{nw}-1\} \subset$$

$$\subset \{x^{nv}-1,\ (x^{nw}-1) \prod_{p/n} (x^{nv/p}-1)\} = \{x^{nv}-1,\ \prod_{p/nv} (x^{nv/p}-1)\}.$$

So we have proved $\mathbf{B}_{k+1}^*$.

---

[4]) Redéi states that the theorem follows from the fact that $F_n(x)$ is the g.c.d. of the polynomials $G_{n,p}(x)$ (p/n). This argument, however, seems to be insufficient; as $R[x]$ is not a principal ideal ring it only leads to the existence of a representation $f = \Sigma G_{n,p} f_p$ in terms of polynomials $f_p(x)$ with rational coefficients. Therefore, a complete proof will be presented here.

§ 3. *The case* $n = p^\lambda q^\mu$

We shall show that if n has at most 2 different prime factors, a stronger form of theorem 1 holds: if the coefficients of $f(x)$ are nonnegative, and the degree of $f(x)$ is less than n, the polynomials $f_p(x)$ can be chosen such that they have nonnegative coefficients. If n has more than two different prime factors, this is no longer generally true. If n has only one prime factor, $n = p^\lambda$, it is almost trivial. For, we have $F_n = G_{n,p}$ in that case; moreover, if the degree of $f(x)$ is $< (a+1)\,b$, then $f \in R_P[x]$, $(1 + x^b + x^{2b} + \ldots + x^{ab})/f(x)$ imply $f = g \cdot (1 + x^b + x^{2b} + \ldots + x^{ab})$, $g \in R_P[x]$. This follows from the fact that the degree of g is less than b, so that the coefficients of g repeatedly occur as coefficients of $f(x)$.

Theorem 2. $n = p^\lambda q^\mu$, $\lambda \geqq 1$, $\mu \geqq 1$, p and q are different primes. Assume $A(x) \in R_P[x]$, $F_n(x)/A(x)$, and that the degree of $A(x)$ is less than n. Then there are polynomials $P(x) \in R_P[x]$, $Q(x) \in R_P[x]$, such that

$$A(x) = P(x)\,\frac{x^n-1}{x^{n/p}-1} + Q(x)\,\frac{x^n-1}{x^{n/q}-1}. \tag{3.1}$$

Proof. Since $F_n(x)/A(x)$, we have a representation (3.1) with $P \in R[x]$, $Q \in R[x]$ (see (2.1)). Abbreviating $n/pq = p^{\lambda-1} q^{\mu-1} = v$, we have

$$(1 + x^v + x^{2v} + \ldots + x^{(q-1)v})\,G_{n,p}(x) = (1 + x^v + x^{2v} + \ldots + x^{(p-1)v})\,G_{n,q}(x).$$

This shows that P and Q are not uniquely determined by (3.1). In fact, we can and do impose the following conditions on $P(x)$: (i) the degree of $P(x)$ is less than qv; (ii) $P(x) \in R_P[x]$; (iii) under the conditions (i) and (ii) $P(x)$ is minimal in the following sense: for no value of j $(0 \leqq j < v)$ the polynomial $P(x) - x^j(1 + x^v + x^{2v} + \ldots + x^{(q-1)v})$ lies in $R_P[x]$. We can now prove that $Q(x) \in R_P[x]$. As the degree of $A(x)$ is $< n$, (3.1) shows that the degree of $Q(x)$ is less than pv. Write

$$A(x) = \sum_0^{pqv-1} a_\mu x^\mu, \quad P(x) = \sum_0^{qv-1} b_\mu x^\mu, \quad Q(x) = \sum_0^{pv-1} c_\mu x^\mu.$$

Let m be an integer $(0 \leqq m < pv)$; we shall prove that $c_m \geqq 0$. By (iii), there is a number k $(0 \leqq k < qv)$, such that $k \equiv m \pmod v$, $b_k = 0$. Furthermore, we can determine integers s, t such that

$$k + sqv = m + tpv, \quad 0 \leqq s < p, \quad 0 \leqq t < q.$$

It follows that $a_{k+sqv} = b_k + c_m = c_m$. As $A(x) \in R_P[x]$, we infer $c_m \geqq 0$. This proves the theorem.

Theorem 3. $n = p^\lambda q^\mu$, $\lambda \geqq 1$, $\mu \geqq 1$, p and q are different primes. Assume that

$$A(x) \in R_P[x], \quad B(x) \in R_P[x], \quad A(1) = p,$$
$$A(x)\,B(x) \equiv 1 + x + x^2 + \ldots + x^{n-1} \pmod{x^n - 1},$$

then at least one of the following relations holds:

$$A(x) = \varphi_1(x)\,G_{n,p}(x), \quad B(x) = \varphi_2(x)\,G_{n,p}(x), \quad B(x) = \varphi_3(x)\,G_{n,q}(x),$$

where the φ's are elements of $R_P[x]$.

Proof. Let $\mathfrak{M}$ be the set of integers m with the properties $m > 0$, m/n, $F_m(x)/A(x)$. Clearly 1 is not in $\mathfrak{M}$, as $F_1(1) = 0$. We shall show that

(3.2) $\quad p^\alpha q^\beta \in \mathfrak{M}$ implies $\alpha > 0$ and $p^\alpha q^\gamma \in \mathfrak{M} \quad (0 \leqslant \gamma \leqslant \beta)$.

Put $m = p^\alpha q^\beta$ and assume $0 \leqslant \alpha \leqslant \lambda$, $0 \leqslant \beta \leqslant \mu$, $\alpha + \beta > 0$, $F_m(x)/A(x)$. It follows that $\alpha > 0$, for otherwise $F_m(1) = q$, which does not divide $A(1)$. We also assume $\beta > 0$, for otherwise we have nothing to prove. Let $A^*(x)$ be the polynomial of degree $< m$, which satisfies $A^* \equiv A \pmod{x^m - 1}$. Applying theorem 2 to $A^*(x)$ and $F_m(x)$, we obtain

$$(3.3) \qquad A(x) \equiv P(x) \frac{x^m-1}{x^{m/p}-1} + Q(x) \frac{x^m-1}{x^{m/q}-1} \pmod{x^m-1},$$

where $P(x)$ and $Q(x)$ are in $R_P[x]$. On substituting $x = 1$ we find that $p = P(1)p + Q(1)q$. As $P(1) \geqslant 0$, $Q(1) \geqslant 0$ we infer $Q(1) = 0$, whence $Q(x) = 0$ for all x. Now we take a number d of the form $p^\alpha q^\gamma$ $(0 \leqslant \gamma \leqslant \beta)$. Then F_d divides both $G_{m,p}$ and $x^m - 1$, and so (3.3) leads to F_d/A. This proves (3.2).

Further, we have $p^\alpha \in \mathfrak{M}$ for at most one α, as $F_m(1) = p$ if $m = p^\alpha$. From (3.2) we now infer that all elements of $\mathfrak{M}$ have the same number of factors p.

Now we can show that at least one of the following cases occurs:

$$\begin{aligned} &\text{(i)} && F_m/B \text{ for } m = q^\mu,\ pq^\mu, \dots, p^\lambda q^\mu, \\ &\text{(ii)} && F_m/B \text{ for } m = p^\lambda,\ p^\lambda q, \dots, p^\lambda q^\mu, \\ &\text{(iii)} && F_m/A \text{ for } m = p^\lambda,\ p^\lambda q, \dots, p^\lambda q^\mu. \end{aligned}$$

For every m/n, $m > 1$ we have F_m/AB. So if m is not in $\mathfrak{M}$, F_m divides B. If $\mathfrak{M}$ would be empty (which actually does not happen) both (i) and (ii) hold. If the maximal element of $\mathfrak{M}$ is $p^\alpha q^\beta$, and $\alpha < \lambda$, then (ii) occurs. If $\beta < \mu$, then (i) occurs. If $\alpha = \lambda$, $\beta = \mu$, then (iii) occurs.

Forming the products of the cyclotomic polynomials in each case, we infer $G_{n,q}/B$ in case (i), $G_{n,p}/B$ in case (ii), $G_{n,p}/A$ in case (iii).

In each case, mere divisibility implies that the quotient is in $R_P[x]$. (see the remark just above theorem 2).

§ 4. *The case* $n = p^\lambda q$ $(\lambda \geqslant 1)$

We again put $n = pqv$, hence $v = p^{\lambda-1}$. We have the following relations:

$$(4.1) \qquad G_{n,p}(x) = F_n(x)\, F_{pv}(x),$$

$$(4.2) \qquad G_{n,pq}(x) = G_{n,q}(x)\, F_{pv}(x).$$

Consider a polynomial $T(x)$ of degree $< n$, whose coefficients are all $\geqslant 0$ and $< p$, and which is a multiple of $G_{n,pq}(x)$. In other words, $T(x)$ has the form

$$(4.3) \qquad T(x) = \sum_{k=0}^{pq-1} x^{kv} \sum_{j=0}^{v-1} t_j x^j, \quad 0 \leqslant t_j < p \quad (0 \leqslant j < pv).$$

The most important special case is $T(x) = 1 + x + x^2 + \ldots + x^{n-1}$.

Theorem 4. Assume $n = p^\lambda q$, and $A(x) \in R_P(x)$, $B(x) \in R_P(x)$, $A(x)\,B(x) \equiv T(x) \pmod{x^n - 1}$, where $T(x)$ is of the form (4.3). Then at least one of the factors $A(x)$, $B(x)$ is divisible either by $G_{n,p}(x)$ or by $G_{n,q}(x)$.

Proof. We have $F_n/G_{n,q}$, $G_{n,q}/G_{n,pq}$, and therefore F_n/AB. We may and do assume F_n/A. Furthermore, $F_{pv}/G_{n,pq}$, whence it follows that F_{pv} divides either A or B. If F_{pv}/A we are ready, for then, by (4.1), we have $G_{n,p}/A$. We henceforth assume F_{pv}/B.

Applying theorem 2, we obtain

$$A(x) = P(x)\,G_{n,p}(x) + Q(x)\,G_{n,q}(x) \qquad (P \in R_P[x],\ Q \in R_P[x]). \tag{4.4}$$

For, we may assume that the degree of $A(x)$ is less than n, as we do not loose anything by reduction mod $x^n - 1$.

Multiplying (4.4) by $B(x)$, we observe that $BPG_{n,p}$ is divisible by $G_{n,q}$, since $G_{n,q}$ divides T (see (4.2)). Furthermore, both B and $G_{n,p}$ are multiples of F_{pv}. Consequently $BPG_{n,p}$ is a multiple of $G_{n,q}F_{pv}^2$.

We have

$$G_{n,q} = (x^{pqv}-1)/(x^{pv}-1)\,, \quad F_{pv} = (x^{pv}-1)/(x^v-1).$$

Therefore

$$G_{n,q}\,F_{pv}^2 = G_{n,pq}\,F_{pv} \equiv p(1 + x^v + x^{2v} + \ldots + x^{(pq-1)v}) \pmod{x^n-1}.$$

It follows that $BPG_{n,p} \in (p, x^n - 1)$. In the equations $AB = BPG_{n,p} + BQG_{n,q}$ we now reduce everything mod $x^n - 1$ such that the resulting polynomials have degrees $< n$. We obtain $T = \varphi + \psi$, where both φ and ψ are in $R_P[x]$. The coefficients of φ are multiples of p, those of T are $< p$. It follows that φ vanishes identically. This means, apart from the trivial case that B vanishes identically, that P vanishes identically. Now (4.4) gives $G_{n,q}/A$.

§ 5. *A theorem connected with a problem of* Hajós

Theorem 5. Let n be the product of a number of different primes. Assume $A(x) \in R[x]$, $B(x) \in R[x]$, $A(x)\,B(x) \equiv 1 + x + \ldots + x^{n-1} \pmod{x^n - 1}$, $F_n(x)/B(x)$ (F_n obviously divides at least one of the factors A and B), $B(1) > 1$. Then there exists a prime divisor p of n, such that $B(x)$ can be written as $B(x) = B_0(x) + \ldots + B_{p-1}(x)$, where $B_j \in R[x]$ $(j = 0, \ldots, p-1)$, and

$$A(x)\,B_j(x) \equiv x^{jn/p}\,A(x)\,B_0(x) \pmod{x^n-1} \qquad (j = 0, \ldots, p-1).$$

Proof. We have $A(1)\,B(1) = n$, $B(1) > 1$. Therefore, there is a prime p which divides $B(1)$ but not $A(1)$ (otherwise p^2/n). Obviously F_p/AB, $F_p(1) = p$, and therefore $F_p(x)$ divides $B(x)$ but not $A(x)$. It follows that

$$B(x) = C(x)\,F_p(x)\,F_n(x) \qquad (C(x) \in R[x]). \tag{5.1}$$

If $n = p$, this conclusion is false, for then F_p and F_n are no longer relatively prime. However, in that case the theorem is trivial.

By theorem 1 we have

$$F_n(x) = G_{n,p}(x)\, f_p(x) + \sum_{q/n,\ q \neq p} G_{n,q}(x)\, f_q(x). \tag{5.2}$$

As p^2 does not divide n, the numbers $0, n/p, 2n/p, \ldots, (p-1)n/p$ form a complete set of residues mod p. Let $k(j)$ denote the solution of $0 \leqslant k(j) < p$, $k(j) \equiv jn/p \pmod{p}$. Then we have

$$F_p(x) = \sum_{j=0}^{p-1} x^{k(j)}.$$

Writing $(j = 0, \ldots, p-1)$

$$B_j(x) = x^{jn/p}\, f_p\, C F_p + x^{k(j)} \sum_{q/n,\ q \neq p} G_{n,q}\, f_q\, C,$$

we have $B(x) = B_0(x) + \ldots + B_{p-1}(x)$. And, it is easily verified that

$$A\{B_j - x^{jn/p} B_0\} = (x^{k(j)} - x^{jn/p}) \sum_{q/n,\ q \neq p} A G_{n,q}\, f_q C.$$

The polynomial on the right is divisible by $(x^p - 1) A F_n C = (x-1) A B$; therefore it is $\equiv 0 \pmod{x^n - 1}$. This proves the theorem.

REFERENCES

1. Bruijn, N. G. de, On bases for the set of integers. Publicationes Mathematicae (Debrecen) **1**, 232–242 (1950).
2. ————, On the factorization of finite abelian groups. Indag. Math. Kon. Ned. Akad. Wetensch. Amsterdam **15** [= Proceedings **56**, Series A] 258–264 (1953).
3. Hajós, G., Sur la factorisation des groupes abéliens. Časopis Pěst. Mat. Fys. **74**, 157–162 (1950).
4. ————, Sur le problème de factorisation des groupes cycliques. Acta Math. Acad. Sci. Hungar. **1**, 189–195 (1950).
5. Redéi, L., Ein Beitrag zum Problem der Faktorisation von endlichen Abelschen Gruppen. Acta Math. Acad. Sci. Hungar. **1**, 197–207 (1950).