ACTA ARITHMETICA
XIII (1967)

Reducibility of polynomials and covering systems of congruences

by

A. Schinzel (Warszawa)

The following problem has been proposed by Professor P. Turán in an oral communication:

Does there exist a constant C such that for every polynomial $f(x) = \sum_{i=0}^{n} a_i x^{n-i}$ (a_i integers, $a_0 \neq 0$), there is a polynomial $g(x) = \sum_{i=0}^{n} b_i x^{n-i}$ (b_i integers) irreducible over the rationals and satisfying $\sum_{i=0}^{n} |b_i - a_i| \leqslant C$?

This problem, apparently very difficult becomes simpler if one removes the condition that the degree of g should not exceed the degree of f. Then it seems plausible that for polynomials $f(x)$ with $f(0) \neq 0$ the value of C can be taken 1, i.e. for a suitable n and a suitable sign the polynomial $\pm x^n + f(x)$ is irreducible.

I have treated the irreducibility of $x^n + f(x)$ in [3] and I have proved (Theorem 5) that for every polynomial $f(x)$ with rational coefficients such that $f(0) \neq 0$, $f(1) \neq -1$ and $f(x) \not\equiv 1$, there exist infinitely many n's for which $x^n + f(x)$ has exactly one irreducible factor that is not a cyclotomic polynomial (the precise formulation of the theorem says a little more). The example

$$f_0(x) = \tfrac{1}{12}(3x^9 + 8x^8 + 6x^7 + 9x^6 + 8x^4 + 3x^3 + 6x + 5)$$

shows that $x^n + f(x)$ may have cyclotomic factors for any n. In this example, however, the coefficients of $f(x)$ are not integers. The aim of the present paper is to investigate the irreducibility of $x^n + f(x)$, where $f(x)$ has integer coefficients and to show its connection with the so called covering systems of congruences.

A system of congruences $a_i \bmod m_i$ is called *covering* if every integer satisfies one of the congruences (cf. [1] and the papers quoted there). The precise formulation of the results is given below, but their most striking consequence is that if there are no covering systems with distinct odd moduli > 1 (the conjecture of Selfridge), then for every polynomial $f(x)$ with integer coefficients such that $f(0) \neq 0$, $f(1) \neq -1$, $x^n+f(x)$ is irreducible for infinitely many n.

THEOREM 1. *The following two propositions are equivalent.*

A. *For every polynomial $f(x)$ with integer coefficients such that $f(0) \neq 0, f(1) \neq -1$ and $f(x) \not\equiv 1$, there exists an arithmetical progression N such that if $\nu \in N$ then $x^{\nu} + f(x)$ is irreducible over the rationals.*

B. *In every finite covering system of congruences $a_i \bmod m_i$ $(m_i > 1)$ at least one of the quotients m_j/m_i equals q^{α} (q prime, $\alpha \geqslant 0$), $a_j \not\equiv a_i \bmod m_i$ and either $q > 2$ or $m_i \equiv 1 \bmod 2$ or $a_j \not\equiv a_i \bmod (m_i/2)$.*

THEOREM 2. *There is an implication* C → B → D, *where* C *and* D *are the following propositions.*

C. *In every finite covering system of congruences $a_i \bmod m_i$ $(m_i > 1)$ either there are two equal moduli or there is a modulus even.*

D. *In every finite covering system of congruences $a_i \bmod m_i$ $(m_i > 1)$ at least one modulus divides another one.*

Notation. Z is the ring of integers, Q the field of rationals, a monic polynomial means a polynomial with the highest coefficient ± 1.

$X_n(x)$ is the nth cyclotomic polynomial, ζ_n is a primitive nth root of unity. For any polynomial $f(x)$, $Kf(x)$ is the factor of $f(x)$ of the greatest possible degree whose no root is 0 or a root of unity and whose leading coefficient is equal to that of $f(x)$.

LEMMA 1. *Let $F_i(x), a_i(x) \in Z[x]$ $(i = 1, 2, \ldots, r)$. If the polynomials $F_i(x)$ $(i = 1, 2, \ldots, r)$ are monic and relatively prime in pairs modulo every prime, then there exists a polynomial $f(x) \in Z[x]$ such that*

$$f(x) \equiv a_i(x) \bmod F_i(x), \tag{1}$$

$$\textit{degree } f(x) < \textit{degree} \prod_{i=1}^{r} F_i(x). \tag{2}$$

Proof. For each $i \leqslant r$ consider the polynomials

$$F_i(x) \quad \text{and} \quad G_i(x) = F_i(x)^{-1} \prod_{i=1}^{r} F_i(x).$$

Since they are monic and relatively prime mod 2 they are relatively prime over Q and there exist polynomials $U_i(x)$, $V_i(x) \in Z[x]$ such that

$$\text{degree } U_i < \text{ degree } G_i, \qquad \text{degree } V_i < \text{degree } F_i$$

and

$$F_i(x)\,U_i(x) + G_i(x)\,V_i(x) = R_i \neq 0.$$

Let $U_i(x) = u_i U_i^*(x)$, $V_i(x) = v_i V_i^*(x)$, where u_i, v_i are integers and $U_i^*(x)$, $V_i^*(x)$ are primitive polynomials.

If $R_i/(u_i, v_i)$ has any prime factor p, we have either

$$p \nmid \frac{u_i}{(u_i, v_i)} \quad \text{or} \quad p \nmid \frac{v_i}{(u_i, v_i)}.$$

Without loss of generality we may assume the former. Since $F_i(x)$ and $G_i(x)$ are relatively prime mod p, it follows from

$$F_i(x)\frac{u_i}{(u_i, v_i)}\, U_i^*(x) + G_i(x)\frac{v_i}{(u_i, v_i)}\, V_i^*(x) = \frac{R_i}{(u_i, v_i)} \tag{3}$$

that

$$\frac{u_i}{(u_i, v_i)}\, U_i^*(x) \equiv 0 \big(\text{mod } p, G_i(x)\big).$$

Since $u_i \neq 0$ and $G_i(x)$ is monic, the degree of $U_i^*(x)$ is less than the degree of $G_i(x)$ also mod p, thus we get a contradiction.

Therefore, $R_i/(u_i, v_i)$ has no prime factors; equals $\varepsilon_i = \pm 1$ and it follows from (3) that

$$\varepsilon_i \frac{v_i}{(u_i, v_i)}\, G_i(x)\, V_i^*(x) \equiv \begin{cases} 1 \bmod F_i(x), \\ 0 \bmod G_i(x). \end{cases} \tag{4}$$

Now, put

$$\sum_{i=1}^{r} \varepsilon_i \frac{v_i}{(u_i, v_i)}\, a_i(x) G_i(x)\, V_i^*(x) = q(x) \prod_{i=1}^{r} F_i(x) + f(x), \tag{5}$$

where $q(x) \in Q[x]$ and

$$\text{degree } f(x) < \text{degree} \prod_{i=1}^{r} F_i(x).$$

Since $\prod_{i=1}^{r} F_i(x)$ is monic, $f(x) \in Z[x]$. By (4) and (5) (1) holds.

Remark. Without the condition (2) the lemma is true also if polynomials $F_i(x)$ are not monic, but the proof is much more complicated.

LEMMA 2. *If q is a prime, then $X_m(x)$, $X_n(x)$ $(m \leqslant n)$ are relatively prime* mod q *except if $n/m = q^{\alpha}$ $(\alpha \geqslant 0)$, in which case*

$$X_n(x) \equiv X_m(x)^{\varphi(n)/\varphi(m)} \pmod q. \tag{6}$$

Proof. Let $m = q^{\mu} m_1, n = q^{\nu} n_1$, where $q \nmid m_1 n_1$.

We have by the properties of cyclotomic polynomials

$$X_m(x) = \frac{X_{m_1}(x^{q^{\mu}})}{X_{m_1}(x^{q^{\mu-1}})} \equiv X_{m_1}(x)^{q^{\mu} - q^{\mu-1}} \pmod q \qquad (\mu \geqslant 1) \tag{7}$$

and similarly

$$X_n(x) = \frac{X_{n_1}(x^{q^{\nu}})}{X_{n_1}(x^{q^{\nu-1}})} \equiv X_{n_1}(x)^{q^{\nu} - q^{\nu-1}} \pmod q \qquad (\nu \geqslant 1). \tag{8}$$

If $n_1 \neq m_1$, the polynomials $X_{m_1}(x)$, $X_{n_1}(x)$ are relatively prime over Q, and both divide $x^{n_1 m_1}-1$. Thus their resultant R divides the discriminant of $x^{n_1 m_1}-1$ and since $n_1 m_1 \not\equiv 0 \bmod q$ we get $R \not\equiv 0 \bmod q$. Hence $X_{m_1}(x)$ and $X_{n_1}(x)$ are relatively prime mod q and by (7) and (8) the same is true about $X_m(x)$ and $X_n(x)$. If $n_1 = m_1$, (6) follows from (7) and (8) after taking into account the case $\mu = 0$.

LEMMA 3. *For every odd $c \geqslant 1$ and integer $a \geqslant 1$ the polynomial*

$$D_{2^a c}(x) = \tfrac{1}{2}[X_{2^a c}(x) - X_c(x^{2^{a-1}})] \tag{9}$$

belongs to $Z[x]$, is monic and relatively prime mod every prime to $X_{2^\beta c}(x)$, where $\beta < a$.

Proof. We have

$$X_{2^a c}(x) = X_c(-x^{2^{a-1}}), \tag{10}$$

thus $D_{2^a c}(x) \in Z[x]$. If $c = 1$, $D_{2^a c}(x) = 1$, thus the lemma is true. If $c > 1$ and c^* is the product of all distinct prime factors of c, we have

$$X_c(x) = X_{c^*}(x^{c/c^*}) = x^{\varphi(c)} - \mu(c^*)x^{\varphi(c)-c/c^*} + \ldots,$$

whence

$$D_{2^a c}(x) = \mu(c^*)x^{2^{a-1}(\varphi(c)-c/c^*)} + \ldots$$

and $D_{2^a c}(x)$ is monic. Since

$$X_c(x^{2^{a-1}}) = \prod_{\beta=0}^{a-1} X_{2^\beta c}(x),$$

it follows from Lemma 2 that $D_{2^a c}(x)$ and $X_{2^\beta c}(x)$ $(\beta < a)$ are relatively prime modulo every odd prime. In order to prove that they are relatively prime mod 2 consider their resultant R. We have

$$R = \prod D_{2^a c}(\zeta),$$

where ζ runs through all primitive roots of unity of degree $2^\beta c$. By (9) and (10)

$$R = 2^{-\varphi(2^\beta c)} \prod X_c(-\zeta^{2^{a-1}}).$$

When ζ runs through all primitive roots of unity of degree $2^\beta c$, $\zeta^{2^{a-1}}$ runs $\varphi(2^\beta)$ times through all primitive roots of degree c. Therefore,

$$R = 2^{-\varphi(2^\beta c)} \Big(\prod_{(\gamma,c)=1} X_c(-\zeta_c^\gamma)\Big)^{\varphi(2^\beta)}.$$

Since

$$X_c(x) = \prod_{(\delta,c)=1} (x - \zeta_c^\delta),$$

we have

$$\prod_{(\gamma,c)=1} X_c(-\zeta_c^\gamma) = \prod_{(\gamma\delta,c)=1} (\zeta_c^\gamma + \zeta_c^\delta) = 2^{\varphi(c)} \prod_{\substack{(\gamma\delta,c)=1\\ \gamma\neq\delta}} (\zeta_c^\gamma + \zeta_c^\delta).$$

Thus

$$R = \prod_{(\gamma\delta,c)=1} (\zeta_c^\gamma + \zeta_c^\delta)^{\varphi(2^\beta)} \equiv \prod_{\substack{(\gamma\delta,c)=1\\ \gamma\neq\delta}} (\zeta_c^\gamma - \zeta_c^\delta)^{\varphi(2^\beta)} \equiv d^{\varphi(2^\beta)} \bmod 2,$$

where d is the discriminant of $X_c(x)$. Since d is odd, R is also odd and the proof is complete.

LEMMA 4. *Let $f(x)$ be a polynomial satisfying the assumptions of Proposition* B. *Let e_0 be the greatest integer e such that $-f(x) = g(x)^e$, $g(x) \in Z[x]$.*

There exists a constant $D_0(f)$ such that if $n > D_0(f)$, $(\nu, e_0) = 1$ and $\nu \not\equiv 0 \bmod 4$ in the case $f(x) = 4h(x)^4$, $h(x) \in Z[x]$, then $K\big(x^\nu + f(x)\big)$ is irreducible over Q.

Proof. Put in Theorem 2 of [2]: $F(y,z) = y + f(z)$, $n = \nu$, $m = 1$. By that theorem there exists an integral matrix $M = \begin{bmatrix} \nu_1 & \mu_1 \\ \nu_2 & \mu_2 \end{bmatrix}$ with the following properties:

$$0 \leqslant \nu_i \leqslant C_1(F), \quad 0 \leqslant \mu_i \leqslant C_1(F) \quad (i = 1, 2), \tag{11}$$

$$[\nu, 1] = [u, v]M \quad (u, v \text{ integers} \geqslant 0), \tag{12}$$

(13) if $y^{\nu_1}z^{\nu_2} + f(y^{\mu_1}z^{\mu_2}) = \text{const}\, F_1(y,z)^{e_1} F_2(y,z)^{e_2} \ldots F_r(y,z)^{e_r}$ is a decomposition of $y^{\nu_1}z^{\nu_2} + f(y^{\mu_1}z^{\mu_2})$ into factors irreducible over Q, then either

$$K\big(x^\nu + f(x)\big) = \text{const}\ KF_1(x^u, x^v)^{e_1} KF_2(x^u, x^v)^{e_2} \ldots KF_r(x^u, x^v)^{e_r}$$

is a decomposition of $K\big(x^\nu + f(x)\big)$ into factors irreducible over Q or

$$\nu \leqslant C_0(F).$$

$C_0(F)$ and $C_1(F)$ are constants independent of ν.

We take $D_0(f) = \max\{C_0(F), C_1(F)\}$ and assume $\nu > D_0(f)$, $(\nu, e_0) = 1$ and $\nu \not\equiv 0 \bmod 4$ if $f(x) = 4h(x)^4$, $h(x) \in Z[x]$.

It follows from (12) that

$$\nu = \nu_1 u + \nu_2 v, \quad 1 = \mu_1 u + \mu_2 v, \tag{14}$$

thus by (11)

$$\mu_1 u = 1, \ \mu_2 v = 0 \quad \text{or} \quad \mu_1 u = 0, \ \mu_2 v = 1.$$

In view of the symmetry we may assume the former. Thus $\mu_1 = u = 1$ and either $v = 0$ or $\mu_2 = 0$. If $v = 0$, then $\nu = \nu_1 \leqslant D_0(f)$ against the assumption. If $\mu_2 = 0$,

$$y^{\nu_1}z^{\nu_2} + f(y^{\mu_1}z^{\mu_2}) = y^{\nu_1}z^{\nu_2} + f(z).$$

By the theorem of Capelli (cf. [3], p. 6), the last polynomial can be reducible over Q only if

$$-f(z)z^{-\nu_2} = k(z)^p, \quad \text{where} \quad p\,|\,\nu_1 \text{ and } k(z)\,\epsilon\, Q(z) \tag{15}$$

or

$$f(z)z^{-\nu_2} = 4k(z)^4, \quad \text{where} \quad 4\,|\,\nu_1 \text{ and } k(z)\,\epsilon\, Q(z). \tag{16}$$

Since $f(0) \neq 0$, (15) implies that $p\,|\,e_0$ and $p\,|\,\nu_2$, thus by (14) $(\nu, e_0) \neq 1$ against the assumption. Similarly (16) implies that $f(z) = 4h(z)^4$, $h(z)\,\epsilon\, Z[z]$ and $\nu \equiv 0 \bmod 4$, again contrary to the assumption. Thus $y^{\nu_1}z^{\nu_2}+f(y^{\mu_1}z^{\mu_2})$ is irreducible over Q and by (13) $K\big(x^{\nu}+f(x)\big)$ is also irreducible, q.e.d.

Proof of Theorem 1. Implication A ->B. Assume B is false, thus there exists a finite set S of integral pairs (m, a) with $m > 1$ and with the following properties.

(17) For every integer ν there exists a pair $(m, a)\,\epsilon\, S$ such that $\nu \equiv a \bmod m$ (the system $a \bmod m$, $(m, a)\,\epsilon\, S$ is covering).

(18) If $(m, a)\,\epsilon\, S$, $(n, b)\,\epsilon\, S$ and $n/m = q^a$ (q prime, $a \geqslant 0$), then either $b \equiv a \bmod m$ or $q = 2$, $m \equiv 0 \bmod 2$ and $b \equiv a \bmod \dfrac{m}{2}$.

Let S_0 be a subset of S irreducible with respect to property (17). If $(m, a)\,\epsilon\, S_0$, $(n, b)\,\epsilon\, S_0$, $(m, a) \neq (n, b)$ and $m\,|\,n$, then $b \not\equiv a \bmod m$; otherwise, $S_0\setminus\{(n, b)\}$ would also have property (17). Property (18) is hereditary, but in view of the last remark it takes for S_0 the following simpler form.

If $(m, a)\,\epsilon\, S_0$, $(n, b)\,\epsilon\, S_0$, $(m, a) \neq (n, b)$ and $n/m = q^a$ (q prime, $a \geqslant 0$), then $q = 2$, $a > 0$, $m \equiv 0 \bmod 2$, $b \equiv a \bmod \dfrac{m}{2}$ and $b \not\equiv a \bmod m$.

Divide the set S_0 into classes assigning two pairs (m, a) and (n, b) to the same class if $n/m = 2^a$ ($a \geqslant 0$ or < 0). We obtain the decomposition of S_0

$$S_0 = \bigcup_{i=1}^{r} C_i, \tag{19}$$

and the pairs in any class C_i can be represented in the form $(2^{a_{ij}}c_i, a_{ij})$ ($j = 1, 2, \ldots, k_i$), where c_i is odd and $k_i = 1, 2^{a_{i1}}c_i > 1$ or

$$\begin{gathered} 0 < a_{i1} < a_{i2} < \ldots < a_{ik_i} = a_i, \\ a_{ij} \equiv a_{ik_i} \bmod 2^{a_{ij}-1}c_i, \qquad a_{ij} \not\equiv a_{ik_i} \bmod 2^{a_{ij}}c_i \qquad (1 \leqslant j < k_i). \end{gathered} \tag{20}$$

For each i such that $k_i > 1$ consider the system of congruences

$$g(x) \equiv 0 \bmod \prod_{j=1}^{k_i-1} X_{2^{a_{ij}}c_i}(x), \qquad g(x) \equiv -x^{a_{ik_i}} \bmod D_{2^{a_i}c_i}(x). \tag{21}$$

By Lemma 3 for each $j < k_i$, $X_{2^{a_{ij}}c_i}(x)$ is relatively prime to $D_{2^{a_i}c_i}(x)$ mod every prime, thus the same is true about $\prod\limits_{j=1}^{k_i-1} X_{2^{a_{ij}}c_i}(x)$. By Lemma 1 for each i such that $k_i > 1$, there exists a polynomial $g_i(x)\,\epsilon\, Z[x]$ satisfying the system (21).

Now, put for each $i \leqslant r$:

$$f_i(x) = \begin{cases} \dfrac{g_i(x)+x^{a_{ik_i}}}{D_{2^{a_i}c_i}(x)}X_{2^{a_i}c_i}(x) - x^{a_{ik_i}}, & \text{if} \quad k_i > 1, \\ -x^{a_{i1}}, & \text{if} \quad k_i = 1, \end{cases} \tag{22}$$

and consider the system of congruences

$$f(x) \equiv f_i(x) \bmod \prod_{j=1}^{k_i} X_{2^{a_{ij}}c_i}(x) \qquad (i = 1, 2, \ldots, r). \tag{23}$$

By Lemma 2 the moduli are relatively prime in pairs mod every prime, thus by Lemma 1 there exists a polynomial $f_{r+1}(x)\,\epsilon\, Z[x]$ satisfying (23) and such that

$$\text{degree } f_{r+1}(x) < \text{degree} \prod_{i=1}^{r}\prod_{j=1}^{k_i} X_{2^{a_{ij}}c_i}(x). \tag{24}$$

We claim that

$$f_{r+1}(x) \equiv -x^{a_{ij}} \bmod X_{2^{a_{ij}}c_i}(x) \qquad (1 \leqslant i \leqslant r,\ 1 \leqslant j \leqslant k_i). \tag{25}$$

This is clear by (22), if $k_i = 1$. On the other hand, if $k_i > 1$,

$$X_{c_i}(x^{2^{a_i-1}}) = \prod_{\beta=0}^{a_i-1} X_{2^{\beta}c_i}(x),$$

thus

$$2D_{2^{a_i}c_i}(x) \equiv X_{2^{a_i}c_i}(x) \bmod \prod_{j=1}^{k_i-1} X_{2^{a_{ij}}c_i}(x)$$

and it follows from (21) (with g replaced by g_i), (22) and (23) (with f replaced by f_{r+1}) that

$$\begin{gathered} f_{r+1}(x) \equiv x^{a_{ik_i}} \bmod \prod_{j=1}^{k_i-1} X_{2^{a_{ij}}c_i}(x), \\ f_{r+1}(x) \equiv -x^{a_{ik_i}} \bmod X_{2^{a_i}c_i}(x). \end{gathered} \tag{26}$$

By (20) $a_{ik_i} \equiv a_{ij} \bmod 2^{a_{ij}-1}c_i$ but $a_{ik_i} \not\equiv a_{ij} \bmod 2^{a_{ij}}c_i$, hence $x^{2a_{ik_i}} \equiv x^{2a_{ij}} \bmod X_{2^{a_{ij}}c_i}(x)$, $x^{a_{ik_i}} \not\equiv x^{a_{ij}} \bmod X_{2^{a_{ij}}c_i}(x)$, thus

$$x^{a_{ik_i}} \equiv -x^{a_{ij}} \bmod X_{2^{a_{ij}}c_i}(x) \qquad (1 \leqslant j < k_i). \tag{27}$$

Now (25) follows from (26) and (27). Put

$$t = \max\{1, 2-f_{r+1}(0), -f_{r+1}(1)\}\tag{28}$$

and consider the polynomial

$$f_0(x) = f_{r+1}(x)+t\prod_{i=1}^{r}\prod_{j=1}^{k_i} X_{2^{a_{ij}}c_i}(x).\tag{29}$$

By (20) $2^{a_{ij}}c_i > 1$, thus we have

$$f_0(0) = f_{r+1}(0)+t \geqslant 2, \qquad f_0(1) \geqslant f_{r+1}(1)+t \geqslant 0$$

and the polynomial $f_0(x)$ satisfies the assumptions of Proposition A. On the other hand, by the choice of S_0 and (19) for every integer $\nu \geqslant 0$ there exists $i \leqslant r$ and $j \leqslant k_i$ such that

$$\nu \equiv a_{ij} \bmod 2^{a_{ij}}c_i.$$

Hence

$$x^{\nu} \equiv x^{a_{ij}} \bmod X_{2^{a_{ij}}c_i}(x)$$

and by (25) and (29)

$$x^{\nu}+f_0(x) \equiv 0 \bmod X_{2^{a_{ij}}c_i}(x).\tag{30}$$

However, by (24) and (28) $f_0(x)$ has the degree equal to that of $\prod_{i=1}^{r}\prod_{j=1}^{k_i} X_{2^{a_{ij}}c_i}(x)$ and the leading coefficient positive. Since $\sum_{i=1}^{r} k_i > 1$, the degree of $x^{\nu}+f_0(x)$ is greater than that of $X_{2^{a_{ij}}c_i}(x)$ and it follows from (30) that $x^{\nu}+f_0(x)$ is reducible. Thus we have proved more than was necessary, namely the existence of a polynomial $f(x)$ satisfying the assumptions of Proposition A and such that $x^{\nu}+f(x)$ is reducible for all $\nu \geqslant 0$.

Implication B $\to$ A. Let $f(x)$ be a polynomial satisfying the assumptions of A and let e_0 be the greatest integer e such that

$$-f(x) = g(x)^e, \qquad g(x)\in Z[x].$$

Consider first the case, where $f(x) = 4h(x)^4$, $h(x)\in Z[x]$. Then let r_0 be the least number r such that $(r, 2e) = 1$ and $r > D_0(f)$. The arithmetical progression N: $2et+r_0$ $(t = 0, 1, \ldots)$ has the property asserted in A. Indeed, if $\nu\in N$ then $\nu > D_0(f)$, $(\nu, e) = 1$ and $\nu \not\equiv 0 \bmod 4$, thus, by Lemma 4, $K\big(x^{\nu}+f(x)\big)$ is irreducible. But no root of unity, ζ_m say, can be a zero of $x^{\nu}+f(x)$, since it would follow that

$$\zeta_m^{\nu}+4h(\zeta_m)^4 = 0, \qquad \zeta_m^{\nu} \equiv 0 \bmod 4,$$

which is impossible.

Assume now that $f(x) \neq 4h(x)^4$, $h(x)\in Z[x]$. Let P be the set of all pairs $(p, 0)$, where p is a prime and $p\,|\,e_0$. Let M be the set of all pairs (μ, a), where $0 \leqslant a < \mu$ and

$$\zeta_\mu^{a}+f(\zeta_\mu) = 0.\tag{31}$$

M is finite. Indeed, it follows from (31) that $f(\zeta_\mu)f(\zeta_\mu^{-1}) = 1$, thus ζ_μ is a root of the equation $x^d f(x)f(x^{-1})-x^d = 0$, where d is the degree of $f(x)$, and we get $\varphi(\mu) \leqslant 2d$. Since $f(1) \neq -1$ we have $\mu > 1$ for all $(\mu, a)\in M$.

We claim that the system of congruences $a \bmod m$, where $(m, a)\in P\cup M$ does not satisfy the condition for covering system asserted in B. Indeed, suppose that

$$(m, a)\in P\cup M, \qquad (n, b)\in P\cup M,$$

$$\frac{n}{m} = q^{\alpha} \quad (q \text{ prime}, \ \alpha \geqslant 0), \qquad b \not\equiv a \bmod m,\tag{32}$$

$$q > 2 \quad \text{or} \quad m \equiv 1 \bmod 2 \quad \text{or} \quad b \not\equiv a \bmod \frac{m}{2}.\tag{33}$$

$(m, a)\in P$, $(n, b)\in P$ is impossible in view of (32).

Consider first the case $(m, a)\in P$, $(n, b)\in M$. By the definition of P, m is a prime and

$$-f(x) = k(x)^m, \qquad k(x)\in Z[x].$$

On the other hand, by the definition of M

$$\zeta_n^{b}+f(\zeta_n) \equiv 0.$$

Thus, we get $k(\zeta_n)^m = \zeta_n^b$ and

$$k(\zeta_n) = \zeta_{mn}^{\beta}, \qquad \text{where} \qquad (\beta, n) = (b, n).\tag{34}$$

$k(\zeta_n)$ is a primitive root of unity of degree $mn/(\beta, mn)$, but $k(\zeta_n)\in Q(\zeta_n)$, thus by a known theorem (cf. e.g. [2], p. 536)

$$\frac{mn}{(\beta, mn)}\,\Big|\,\frac{2n}{(2, n)}; \qquad m\,\Big|\,\frac{2(\beta, mn)}{(2, n)}$$

and

$$m\,\Big|\,\frac{2\beta}{(2, n)}.\tag{35}$$

Since by the first part of (32) $m\,|\,n$, it follows from (34) and (35) that $b \equiv 0 \bmod m$, which contradicts the second part of (32).

Consider next the case $(m, a)\in M$, $(n, b)\in P$. Then since n is a prime and $m > 1$, it follows from (32) that $n = m$, thus we can interchange the roles of m and n and apply the preceding case.

Consider finally the case $(m, a)\epsilon M$, $(n, b)\epsilon M$. We have

$$(36)\qquad \begin{aligned} x^a+f(x) &\equiv 0 \bmod X_m(x),\\ x^b+f(x) &\equiv 0 \bmod X_n(x). \end{aligned}$$

Since by Lemma 2, $X_n(x)\equiv X_m(x)^{\varphi(n)/\varphi(m)} \bmod q$, we get from (36)

$$x^b-x^a\equiv 0\ \big(\bmod q,\, X_m(x)\big).$$

Since x and $X_m(x)$ are relatively prime $\bmod q$, it follows that

$$(37)\qquad x^{|b-a|}-1\equiv 0\ \big(\bmod q,\, X_m(x)\big).$$

Put $\Delta=|b-a|=q^{\delta}\Delta_1$, where $q\nmid \Delta_1$. We have

$$(38)\qquad x^{\Delta}-1\equiv (x^{\Delta_1}-1)^{q^{\delta}}\equiv \prod_{d|\Delta_1} X_d(x)^{q^{\delta}} \bmod q.$$

It follows from (37), (38) and Lemma 2 that for some $d_1|\Delta_1$ and some $\beta\geqslant 0$,

$$\frac{m}{d_1}=q^{\beta},\qquad X_m(x)\equiv X_{d_1}(x)^{\varphi(m)/\varphi(d_1)} \bmod q,$$

and

$$X_{d_1}(x)^{q^{\delta}}\equiv 0\big(\bmod q,\, X_{d_1}(x)^{\varphi(m)/\varphi(d_1)}\big).$$

The last congruence implies

$$(39)\qquad q^{\delta}\geqslant \frac{\varphi(m)}{\varphi(d_1)}=\varphi(q^{\beta}).$$

If $\beta=0$ or $q>2$, it follows from (39) that $\delta\geqslant\beta$, thus $\Delta\equiv 0 \bmod m$ and $b\equiv a \bmod m$ contrary to (32). If $\beta>0$ and $q=2$ we get from (39) that $\delta\geqslant\beta-1$, thus $\Delta\equiv 0 \bmod \frac{m}{2}$ and $b\equiv a \bmod \frac{m}{2}$ contrary to (33).

By the proposition B, the system $a \bmod m$, where $(m, a)\epsilon P\cup M$ is not covering, thus there exist numbers D_1 and r_1 such that if $\nu\equiv r_1 \bmod D_1$ then $\nu\not\equiv a \bmod m$ for any $(m, a)\epsilon P\cup M$.

Let r_0 be the least integer r such that $r\equiv r_1 \bmod D_1$ and $r>D_0(f)$. The arithmetical progression $N: D_1t+r_0$ $(t=0, 1, \ldots)$ has the property asserted in A. Indeed, if $\nu\epsilon N$ then $\nu>D_0(f)$ and $(\nu, e)=1$, hence by Lemma 4 $K\big(x^{\nu}+f(x)\big)$ is irreducible. On the other hand, no root of unity can be a zero of $x^{\nu}+f(x)$, since this would imply $\left(m, \nu-m\left[\frac{\nu}{m}\right]\right)\epsilon M$ for a suitable m.

Proof of Theorem 2. The implication B → D being obvious, it is enough to prove C → B. Assume B is false, thus (compare the proof of Theorem 1, implication A → B) there exists a covering system $a_{ij} \bmod 2^{\alpha_{ij}}c_i$ $(1\leqslant i\leqslant r, 1\leqslant j\leqslant k_i)$, where c_i are odd and distinct and for $k_i>1$ (20) holds.

Consider the system of congruences

$$(40)\qquad a_{ik_i} \bmod c_i \quad (1\leqslant i\leqslant r,\ c_i>1),$$

$$(41)\qquad a_{i_0j} \bmod 2^{\alpha_{i_0j}} \quad (1\leqslant j\leqslant k_{i_0}),\quad \text{where } c_{i_0}=1.$$

If C is true, system (40) is not covering, thus there exists an integer ν_1 such that

$$\nu_1\not\equiv a_{ik_i} \bmod c_i,\quad \text{for any } i\leqslant r \text{ with } c_i>1.$$

On the other hand, system (41) is not covering, since by (20) a_{i_0j} $(1\leqslant j\leqslant k_{i_0})$ are distinct and $\sum_j \frac{1}{2^{\alpha_{i_0j}}}<1$. Thus there exists an integer ν_2 such that

$$\nu_2\not\equiv a_{i_0j} \bmod 2^{\alpha_{i_0j}}\quad \text{for any } j\leqslant k_{i_0}.$$

By the Chinese Remainder Theorem there exists

$$\nu_0\equiv\begin{cases}\nu_1 \bmod \prod_{i=1}^{r} c_i,\\ \nu_2 \bmod 2^{\alpha_{i_0}}.\end{cases}$$

By the choice of ν_1 and ν_2, ν_0 does not satisfy any of the congruences (40) and (41), thus system (40), (41) and *a fortiori* the system $a_{ij} \bmod 2^{\alpha_{ij}}c_i$ is not covering and we get a contradiction.

Remark. The implication C → D was first proved in a similar way by J. L. Selfridge.

References

[1] P. Erdös, *Some recent advances and current problems in number theory*, Lectures on modern mathematics 3 (1965), pp. 196-244.

[2] H. Hasse, *Zahlentheorie*, Berlin 1963.

[3] A. Schinzel, *On the reducibility of polynomials and in particular of trinomials*, Acta Arith. 11 (1965), pp. 1-34. *Errata*, ibid. p. 491.

Reçu par la Rédaction le 11. 10. 1966