ACTA ARITHMETICA
XVI (1970)

Reducibility of lacunary polynomials II

by

A. Schinzel (Warszawa)

To the memory of my teachers
Wacław Sierpiński and Harold Davenport

This paper is based on the results of [6] and the notation of that paper is retained. In particular $|f|$ is the degree of a polynomial $f(x)$ and $\|f\|$ is the sum of squares of the coefficients of f, supposed rational.

The aim of the paper is to prove the following theorem.

THEOREM. *For any nonzero integers A, B, and any polynomial $f(x)$ with integral coefficients, such that $f(0)\neq 0$* and *$f(1)\neq -A-B$, there exist infinitely many irreducible polynomials $Ax^m+Bx^n+f(x)$ with $m>n>|f|$. One of them satisfies*

$$m<\exp\big((5|f|+2\log|AB|+7)(\|f\|+A^2+B^2)\big).$$

COROLLARY. *For any polynomial $f(x)$ with integral coefficients there exist infinitely many irreducible polynomials $g(x)$ with integral coefficients such that*

$$\|f-g\|\leqslant\begin{cases}2 & \text{if } f(0)\neq 0,\\ 3 & \text{always}.\end{cases}$$

One of them, g_0, satisfies $|g_0|<\exp\big((5|f|+7)(\|f\|+3)\big)$.

The example $A=12$, $B=0$, $f(x)=3x^9+8x^8+6x^7+9x^6+8x^4+3x^3+6x+5$ taken from [4], p. 4, shows that in the theorem above it would not be enough to assume $A^2+B^2>0$. On the other hand, in the first assertion of Corollary the constant 2 can probably be replaced by 1, but this was deduced in [5] from a hypothetical property of covering systems of congruences. Corollary gives a partial answer to a problem of Turán (see [5]). The complete answer would require $|g_0|\leqslant\max\{|f|,1\}$.

LEMMA 1. *If $\sum_{\nu=1}^{k}a_\nu\zeta_l^{\alpha_\nu}=0$, where a_ν, α_ν are integers, then either the sum $\sum$ can be divided into two vanishing summands or for all $\mu\leqslant\nu\leqslant k$*

$$l\,|\,(\alpha_\mu-\alpha_\nu)\exp\vartheta(k).$$

Proof. This is the result of Mann [2] stated in a form more convenient for our applications. If $\sum$ cannot be divided into two vanishing summands, the relation $\sum = 0$ is in Mann's terminology irreducible. Then according to his Theorem 1 there are distinct primes $p_1, p_2, \ldots, p_s$ where $p_1 < p_2 < \ldots < p_s \leqslant k$ and $p_1 p_2 \ldots p_s$th roots of unity η_ν such that

$$\zeta_l^{a_\nu} = \eta_\nu \zeta, \quad \nu = 1, \ldots, k.$$

Hence we get

$$l \mid (a_\mu - a_\nu) p_1 p_2 \ldots p_s \quad (1 \leqslant \mu \leqslant \nu \leqslant k)$$

and since $p_1 p_2 \ldots p_s \mid \exp \vartheta(k)$ the lemma follows.

LEMMA 2. *Let A, B, f satisfy the assumptions of the theorem and besides $|f| > 0, f(x) \neq \varepsilon A x^q + \eta B x^r$ ($\varepsilon = \pm 1, \eta = \pm 1$). Then there exists an integer d such that*

(1) $$d < \exp \tfrac{5}{2}|f|$$

and

(2) $$A\zeta_l^m + B\zeta_l^n + f(\zeta_l) = 0$$

implies $l \mid d$.

Proof. Set

$$d = \exp\psi(|f|) \exp\vartheta(|f|+3).$$

By the inequality $\vartheta(x) \leqslant \psi(x) < 1.04x$ (see [3], Theorem 12) it follows that $d \leqslant \exp\frac{5}{2}|f|$ for $|f| > 7$ and for $|f| \leqslant 7$ the same can be verified directly. Assume now (2). Setting $f(x) = \sum_{i=0}^{|f|} a_i x^i$ we get

$$S = A\zeta_l^m + B\zeta_l^n + \sum_{i=0}^{|f|} a_i \zeta_l^i = 0.$$

The sum S can be divided into a certain number $\geqslant 1$ of vanishing summands for which further such division is impossible. If at least one summand with k terms, say, contains at least two terms from $f(\zeta_l)$, $a_q\zeta_l^q$ and $a_r\zeta_l^r$ ($q \neq r$), say, then by Lemma 1 $l \mid (q-r)\exp\vartheta(k)$ and since $q - r \mid \exp\psi(|f|)$, $k \leqslant |f|+3$ we get $l \mid d$.

If each summand contains at most one term from $f(\zeta_l)$, then since each term is contained in a certain summand the number of terms in $f(\zeta_l)$ is at most two. Since $|f| > 0, f(0) \neq 0$ the number of terms is exactly two,

$$f(x) = a_q x^q + a_r x^r \quad \text{and} \quad A\zeta_l^m + a_q\zeta_l^q = B\zeta_l^n + a_r\zeta_l^r = 0 \quad (q \neq r).$$

It follows hence $a_q = \varepsilon A$, $a_r = \eta B$, $\varepsilon = \pm 1, \eta = \pm 1$; $f(x) = \varepsilon A x^q + \eta B x^r$, contrary to the assumption.

LEMMA 3. *If A, B are integers, $0 < |A| \leqslant |B|$, $\varepsilon = \pm 1, \eta = \pm 1$ and*

(3) $$A\zeta_l^m + B\zeta_l^n + \varepsilon A\zeta_l^q + \eta B\zeta_l^r = 0,$$

hen either

(4) $$\zeta_l^m + \varepsilon\zeta_l^q = \zeta_l^n + \eta\zeta_l^r = 0$$

or

$$B = 2\theta A \quad (\theta = \pm 1),$$

(5) $$\zeta_l^m = \varepsilon\zeta_l^q, \quad \{\varepsilon\theta\zeta_l^{n-q}, \varepsilon\eta\theta\zeta_l^{r-q}\} = \{\zeta_3, \zeta_3^2\}$$

or

$$B = \theta A \quad (\theta = \pm 1),$$

(6) $$\zeta_l^n = \eta\zeta_l^r, \quad \{\zeta_l^m, \varepsilon\zeta_l^q\} = \{-\theta\zeta_l^n, -\eta\theta\zeta_l^r\}.$$

Proof. Set $A = (A, B)A_1$, $B = (A, B)B_1$. By (3)

$$A_1(\zeta_l^m + \varepsilon\zeta^q) = -B_1(\zeta_l^n + \eta\zeta_l^r)$$

and it follows on taking norms that $B_1^{\varphi(l)}$ divides the norm of $\zeta_l^m + \varepsilon\zeta_l^q$. The latter can be divisible by $\varphi(l)$th power of a prime only when it is 0 or $2^{\varphi(l)}$. Hence we get either (4) or $B_1 = \pm 1$ or $B_1 = \pm 2, \zeta_l^m = \varepsilon\zeta_l^q$.

Since $|A_1| \leqslant |B_1|$ and $(A_1, B_1) = 1$ we get besides (4) the two possibilites

$$B = 2\theta A \quad (\theta = \pm 1), \quad \zeta_l^m = \varepsilon\zeta_l^q, \quad \varepsilon\zeta_l^q + \theta\zeta_l^n + \theta\eta\zeta_l^r = 0$$

or

$$B = \theta A \quad (\theta = \pm 1), \quad \zeta_l^m + \theta\zeta_l^n + \varepsilon\zeta_l^q + \eta\theta\zeta_l^r = 0, \quad \zeta_l^m + \varepsilon\zeta_l^q \neq 0.$$

Taking the complex conjugates we get in the former case

$$\varepsilon\zeta_l^{-q} + \theta\zeta_l^{-n} + \theta\eta\zeta_l^{-r} = 0,$$

in the latter case

$$\zeta_l^{-m} + \theta\zeta_l^{-n} + \varepsilon\zeta_l^{-q} + \theta\eta\zeta_l^{-r} = 0.$$

It follows that the elements of both sets occurring in (5) or (6) have the same nonzero sum and the same sum of reciprocals, hence the sets coincide.

LEMMA 4. *Let A, B, f satisfy the assumptions of the theorem and besides $|A| \leqslant |B|$; $|f| = 0$ or $f(x) = \varepsilon A x^q + \eta B x^r$, $\varepsilon = \pm 1, \eta = \pm 1$. Then there exist integers a, b, d such that*

(7) $$d \leqslant 3|f| + 3$$

and $m > 0, n > 0, m \equiv a, n \equiv b \bmod d$ implies

(8) $$K\big(Ax^m + Bx^n + f(x)\big) = Ax^m + Bx^n + f(x).$$

Proof. Assume first that $f(x) = \varepsilon A x^q + \eta B x^r$, where $qr = 0$. Since $f(1) \neq -A - B$ it follows

$$\varepsilon = 1 \quad \text{or} \quad \eta = 1. \tag{9}$$

(8) holds unless for some l we have (3). Consider separately four cases

$$B \neq \pm A, \ \pm 2A, \tag{10}$$

$$B = 2\theta A \quad (\theta = \pm 1), \tag{11}$$

$$B = -A, \tag{12}$$

$$B = A. \tag{13}$$

In case (10) by Lemma 3, (3) implies (4) and by (9) $l \equiv 0 \bmod 2$. We set $d = 2$, $a = q+1$, $b = r + \frac{1-\eta}{2}$. If $m \equiv a \bmod d$ we infer from (4) $\varepsilon = 1$, $l \equiv 2 \bmod 4$, $n \equiv r + \frac{l}{2} \cdot \frac{1+\eta}{2} \bmod l$, $n \equiv r + \frac{1+\eta}{2} \bmod 2$, which contradicts $n \equiv b \bmod d$.

In case (11) by Lemma 3, (3) implies (4) or (5). We set $d = 6$, $a = q+1$, $b = r\frac{1-\eta}{2}$. By the argument given above, (4) is impossible. (5) is impossible also since it implies $l \equiv 0$, $m \equiv q \bmod 3$. If $q = r = 0$ it is enough to take $d = 2$, thus (7) holds.

In case (12) by Lemma 3, (3) implies (4) or (6). Since $f(1) \neq -A - B = 0$ we have $\varepsilon = -\eta$. In view of symmetry between q and r we assume $r = 0$ and set

$$d = 2, \quad a = q + \frac{1-\varepsilon}{2}, \quad b = q + \frac{1+\varepsilon}{2} \quad \text{if} \quad q \equiv 0 \bmod 2,$$

$$d = 4, \quad a = q\frac{3-\varepsilon}{2}, \quad b = q\frac{3+\varepsilon}{2} \quad \text{if} \quad q \equiv 1 \bmod 2.$$

(4) implies $l \equiv 0 \bmod 2$ and

$$m \equiv q + \frac{1+\varepsilon}{2} \cdot \frac{l}{2}, \quad n \equiv \frac{1-\varepsilon}{2} \cdot \frac{l}{2} \bmod l,$$

hence if $m \equiv a \bmod 2$, $\varepsilon = 1$, $l \equiv 0 \bmod 4$, $n \equiv 0 \bmod 4$ contrary to $n \equiv b \bmod d$. (6) implies $l \equiv 0 \bmod 2$ and either $m \equiv n \bmod 2$ or

$$m \equiv \frac{1+\varepsilon}{2} \cdot \frac{l}{2}, \quad n \equiv q + \frac{1-\varepsilon}{2} \cdot \frac{l}{2} \bmod l,$$

hence if $n \equiv b \bmod 2$ then either $m \equiv b \bmod 2$ or $\varepsilon = -1$, $l \equiv 0 \bmod 4$, $m \equiv 0 \bmod 4$ contrary to $m \equiv a \bmod d$.

In case (13) by Lemma 3, (3) implies (4) or (6). In view of symmetry between q and r we assume $r = 0$ and set

$$d = 2, \quad a = 0, \ b = q+1 \quad \text{if} \quad \varepsilon = \eta = 1,$$

$$d = 2q, \quad a = b = 1 \quad \text{if} \quad \varepsilon = 1, \eta = -1,$$

$$d = 2q, \quad a = b = q+1 \quad \text{if} \quad \varepsilon = -1, \eta = 1$$

(note that if $\varepsilon = -\eta$ we have $q > 0$ since $f(0) \neq 0$).

If $\varepsilon = \eta = 1$, (4) or (6) implies $l \equiv 0 \bmod 2$, $m+n \equiv q \bmod 2$ which is incompatible with $m \equiv 0$, $n \equiv q+1 \bmod 2$.

If $\varepsilon = 1, \eta = -1$ (4) implies $l \equiv 0 \bmod 2$, $n \equiv 0 \bmod 2$ contrary to $n \equiv b \bmod 2$; (6) implies $l \equiv 0 \bmod 2$, $m \equiv 0 \bmod 2$ or $m - n \equiv \frac{l}{2} \bmod 1$, $q \equiv 0 \bmod l$ contrary to $m \equiv a \bmod 2$, $m - n \equiv 0 \bmod q$ (q even).

If $\varepsilon = -1, \eta = 1$, (4) implies $l \equiv 0 \bmod 2$, $m \equiv q \bmod l$ contrary to $m \equiv a \bmod 2$; (6) implies $l \equiv 0 \bmod 2$, $n \equiv q \bmod 2$ or $m - n \equiv \frac{1}{2} \bmod l$, $q \equiv 0 \bmod l$ contrary to $n \equiv b \bmod 2$, $m - n \equiv 0 \bmod q$ (q even).

Assume now that $|f| = 0, f(x) \neq \varepsilon A + \eta B$. Then by Theorem 4 of [4], (8) holds unless

$$f(x) = \varepsilon A = \eta B, \quad m_1 + n_1 \equiv 0 \bmod 3, \quad \varepsilon^{n_1} = \eta^{m_1},$$

where $m_1 = m/(m, n)$, $n_1 = n/(m, n)$. We set $d = 3$, $a = b = 1$. If $m \equiv a$, $n \equiv b \bmod d$ we have $m + n \not\equiv 0 \bmod 3$ and $m_1 + n_1 \not\equiv 0 \bmod 3$.

Lemma 5. *Let* $D = \{\langle m, n\rangle\colon\ 0 \leqslant m < d,\ 0 \leqslant n < d\}$ *and let* $l_1, \ldots, l_k$ *be divisors of* d *relatively prime in pairs. Set*

$$D_{l_j} = \{\langle m, n\rangle\colon\ 0 \leqslant m < l_j,\ 0 \leqslant n < l_j\} \quad (1 \leqslant j \leqslant k)$$

and let $S(l_j)$ *be a subset of* D *such that*

$$\langle m, n\rangle \in S(l_j), \quad \langle m', n'\rangle \in D \quad \text{and} \quad \langle m, n\rangle \equiv \langle m', n'\rangle \bmod l_j \quad \text{imply} \ \langle m', n'\rangle \in S(l_j). \tag{14}$$

Then

$$d^{-2}|S(l_j)| = l_j^{-2}|S(l_j) \cap D_{l_j}|,$$

$$d^{-2}\Big|\bigcap_{j=1}^{k} S(l_j)\Big| = \prod_{j=1}^{k} d^{-2}|S(l_j)|,$$

where $|S|$ *is the cardinality of* S.

Proof. Set

$$L = l_1 l_2 \ldots l_k, \quad D_0 = \{\langle m, n\rangle\colon\ 0 \leqslant m < dL^{-1},\ 0 \leqslant n < dL^{-1}\}.$$

Choose integers a_j such that

$$a_j \equiv 1 \bmod l_j, \quad a_j \equiv 0 \bmod L l_j^{-1} \quad (1 \leqslant j \leqslant k).$$

The formula

$$\langle m, n\rangle \equiv \langle m_0, n_0\rangle L + \sum_{j=1}^{k} \langle m_j, n_j\rangle a_j \bmod d, \qquad \langle m_j, n_j\rangle \in D_{l_j}$$

settles one-to-one correspondence between D and the cartesian product $D_0 \times D_{l_1} \times \ldots \times D_{l_j}$ in such a way that

$$\langle m, n\rangle \equiv \langle m_j, n_j\rangle \bmod l_j.$$

If χ_j is the characteristic function of $S(l_j)$ then by (14)

$$\chi_j(m, n) = \chi_j(m_j, n_j).$$

Hence

$$d^{-2}|S(l_j)| = d^{-2} \sum_{\langle m,n\rangle \in D} \chi_j(m, n) = d^{-2} \sum_{\langle m_0,n_0\rangle \in D_0} \sum\nolimits_1 \ldots \sum\nolimits_k \chi_j(m_j, n_j),$$

where $\sum_i$ is taken over all $\langle m_i, n_i\rangle \in D_{l_i}$ and

$$d^{-2}|S(l_j)| = d^{-2}|D_0| \prod_{i=1, i\neq j}^{k} |D_{l_i}| \sum\nolimits_j \chi_j(m_j, n_j) = l_j^2 |S(l_j) \cap D_{l_j}|.$$

It follows further

$$d^{-2}\Big|\bigcap_{j=1}^{k} S(l_j)\Big|$$

$$= d^{-2} \sum_{\langle m,n\rangle \in D} \prod_{j=1}^{k} \chi_j(m, n) = d^{-2} \sum_{\langle m_0,n_0\rangle \in D_0} \sum\nolimits_1 \ldots \sum\nolimits_k \prod_{j=1}^{k} \chi_j(m_j, n_j)$$

$$= d^{-2}|D_0| \prod_{j=1}^{k} \sum\nolimits_j \chi_j(m_j, n_j) = L^{-2} \prod_{j=1}^{k} |S(l_j) \cap D_{l_j}| = \prod_{j=1}^{k} d^{-2}|S(l_j)|.$$

LEMMA 6. *The following inequalities hold*

$$(15)\qquad \prod_{p=3}^{\infty}\Big(1+\frac{p}{p^3-p^2-2p+1}\Big) < 1.377, \qquad \sum_{p=3}^{\infty}\frac{p}{p^3-p^2-2p+1} > 0.3445,$$

$$(16)\qquad \prod_{p=3}^{\infty}\Big(1+\frac{p}{p^3-p^2-3p+1}\Big) < 1.460, \qquad \sum_{p=3}^{\infty}\frac{p}{p^3-p^2-3p+1} > 0.4175,$$

$$(17)\qquad \prod_{p=3}^{\infty}\Big(1-\frac{2(p^2-1)}{p(p^3-p^2-3p+1)}\Big) > 0.3676,$$

$$\sum_{p=3}^{\infty}\frac{p^2-1}{p(p^3-p^2-3p+1)} > 0.3804,$$

where p runs over primes.

Proof. We have for $p \geqslant 11$ and $c = 2$ or 3

$$\frac{1}{p^2}+\frac{1}{p^3}+\frac{c+1}{p^4} < \frac{p}{p^3-p^2-cp+1} < \frac{1}{p^2}+\frac{1}{p^3}+\frac{c+2}{p^4},$$

hence

$$\sum_{p=11}^{\infty} p^{-2} + \sum_{p=11}^{\infty} p^{-3} + 3\sum_{p=11}^{\infty} p^{-4} < \sum_{p=11}^{\infty}\frac{p}{p^3-p^2-2p+1}$$

$$< \sum_{p=11}^{\infty}\log\Big(1+\frac{p}{p^3-p^2-3p+1}\Big) < \sum_{p=11}^{\infty}\frac{p}{p^3-p^2-3p+1}$$

$$< \sum_{p=11}^{\infty} p^{-2} + \sum_{p=11}^{\infty} p^{-3} + 5\sum_{p=11}^{\infty} p^{-4}.$$

Now

$$\sum_{p=11}^{\infty} p^{-2} = \sum_{p=2}^{\infty} p^{-2} - \sum_{p=2}^{7} p^{-2} = 0.452247\ldots - 0.421519\ldots = 0.030728 + \varepsilon_2,$$

$$\sum_{p=11}^{\infty} p^{-3} = \sum_{p=2}^{\infty} p^{-3} - \sum_{p=2}^{7} p^{-3} = 0.174766\ldots - 0.172952\ldots = 0.02810 + \varepsilon_3,$$

$$\sum_{p=11}^{\infty} p^{-4} = \sum_{p=2}^{\infty} p^{-4} - \sum_{p=2}^{7} p^{-4} = 0.076993\ldots - 0.076862\ldots = 0.000131 + \varepsilon_4,$$

where the values of $\sum_{p=2}^{\infty} p^{-i}$ $(i = 2, 3, 4)$ are taken from the tables [1], p. 249 and $|\varepsilon_i| < 10^{-6}$. Hence

$$\sum_{p=11}^{\infty}\log\Big(1+\frac{p}{p^3-p^2-3p+1}\Big) < 0.034193 + \varepsilon_2 + \varepsilon_3 + 5\varepsilon_4 < 0.0342,$$

$$\sum_{p=11}^{\infty}\frac{p}{p^3-p^2-2p+1} > 0.033951 + \varepsilon_2 + \varepsilon_3 + 3\varepsilon_4 > 0.0339.$$

On the other hand,

$$\sum_{p=3}^{7}\log\Big(1+\frac{p}{p^3-p^2-2p+1}\Big) < 0.2856, \qquad \sum_{p=3}^{7}\frac{p}{p^3-p^2-2p+1} > 0.3106,$$

$$\sum_{p=3}^{7}\log\Big(1+\frac{p}{p^3-p^2-3p+1}\Big) < 0.3442, \qquad \sum_{p=3}^{7}\frac{p}{p^3-p^2-3p+1} > 0.3836,$$

hence

$$\sum_{p=3}^{\infty}\log\left(1+\frac{p}{p^3-p^2-2p+1}\right)<0.3198,\qquad \sum_{p=3}^{\infty}\frac{p}{p^3-p^2-2p+1}>0.3445,$$

$$\sum_{p=3}^{\infty}\log\left(1+\frac{p}{p^3-p^2-3p+1}\right)<0.3784,\qquad \sum_{p=3}^{\infty}\frac{p}{p^3-p^2-3p+1}>0.4175,$$

which implies (15) and (16).

In order to prove (17) we notice that for $p\geqslant 11$

$$\log\left(1-\frac{2(p^2-1)}{p(p^3-p^2-3p+1)}\right)>-\frac{2(p^2-1)}{p(p^3-p^2-3p+1)}>-\frac{2}{p^2}-\frac{2}{p^3}-\frac{13}{p^4},$$

$$\frac{p^2-1}{p(p^3-p^2-3p+1)}>\frac{1}{p^2}+\frac{1}{p^3}+\frac{3}{p^4},$$

hence

$$\sum_{p=11}^{\infty}\log\left(1-\frac{2(p^2-1)}{p(p^3-p^2-3p+1)}\right)>-2\sum_{p=11}^{\infty}p^{-2}-2\sum_{p=11}^{\infty}p^{-3}-13\sum_{p=11}^{\infty}p^{-4}$$

$$=-0.068779-2\varepsilon_2-2\varepsilon_3-13\varepsilon_4>-0.0688,$$

$$\sum_{p=11}^{\infty}\frac{p^2-1}{p(p^3-p^2-3p+1)}>\sum_{p=11}^{\infty}p^{-2}+\sum_{p=11}^{\infty}p^{-3}+3\sum_{p=11}^{\infty}p^{-4}$$

$$=0.033951+2\varepsilon_2+2\varepsilon_3+3\varepsilon_4>0.0339.$$

On the other hand,

$$\sum_{p=3}^{7}\log\left(1-\frac{2(p^2-1)}{p(p^3-p^2-3p+1)}\right)>-0.9319,$$

$$\sum_{p=3}^{7}\frac{p^2-1}{p(p^3-p^2-3p+1)}>0.3465,$$

whence

$$\sum_{p=3}^{\infty}\log\left(1-\frac{2(p^2-1)}{p(p^3-p^2-3p+1)}\right)>-1.0007,$$

$$\sum_{p=3}^{\infty}\frac{p^2-1}{p(p^3-p^2-3p+1)}>0.3804,$$

which completes the proof.

LEMMA 7. *Let A, B, f satisfy the assumptions of the theorem. Then there exist integers a, b, d such that*

$$d\leqslant 3\exp\tfrac{5}{2}|f| \tag{18}$$

and $m>0$, $n>0$, $m\equiv a$, $n\equiv b \bmod d$ implies

$$K\big(Ax^m+Bx^n+f(x)\big)=Ax^m+Bx^n+f(x). \tag{19}$$

Proof. In view of symmetry we can assume $0<|A|\leqslant|B|$. In virtue of Lemma 4 we can suppose that A, B, f satisfy the assumptions of Lemma 2; set $d=2d_0$, where d_0 is an integer from that lemma. (18) follows from (1) and (19) holds unless we have (2) for some $l\,|\,d_0$.

Put

$$D=\{\langle m,n\rangle:\ 0\leqslant m<d,\ 0\leqslant n<d\},$$

$$D_l=\{\langle m,n\rangle:\ 0\leqslant m<l,\ 0\leqslant n<l\},$$

$$E_l=\{\langle m,n\rangle\in D:\ A\zeta_l^m+B\zeta_l^n+f(\zeta_l)\neq 0\}.$$

If $\langle a,b\rangle\in\bigcap_{l|d}E_l$ then $m>0$, $n>0$, $m\equiv a$, $n\equiv b \bmod d$ implies (19). Since $f(1)\neq -A-B$ we have $E_1=D$. We show that $\bigcap_{l|d}E\neq\emptyset$ separately in each of the cases (10), (11), (12), (13). In the first two cases we use the inequality

$$\Big|\bigcap_{l|d}E_l\Big|\geqslant|D|-\sum_{1<l|d}|D\setminus E_l|,$$

where in virtue of Lemma 5

$$|D\setminus E_l|=d^2l^{-2}|(D\setminus E_l)\cap D_l|.$$

In case (10) we have

$$|(D\setminus E_l)\cap D_l|\leqslant 1.$$

Indeed, if $\langle m,n\rangle\in D\setminus E_l$ and $\langle q,r\rangle\in D\setminus E_l$ we get

$$A\zeta_l^m+B\zeta_l^n-A\zeta_l^q-B\zeta_l^r=0, \tag{20}$$

hence by Lemma 3 with $\varepsilon=\eta=-1$, $\zeta_l^m-\zeta_l^q=\zeta_l^n-\zeta_l^r=0$; $\langle m,n\rangle\equiv\langle q,r\rangle \bmod l$. Therefore,

$$d^{-2}\Big|\bigcap_{l|d}E_l\Big|\geqslant 1-\sum_{1<l|d}l^{-2}>2-\sum_{l=1}^{\infty}l^{-2}=2-\frac{\pi^2}{6}>0.$$

In case (11) we have

$$|(D\setminus E_l)\cap D_l|\leqslant\begin{cases}1 & \text{if}\quad l\not\equiv 0 \bmod 6,\\ 2 & \text{if}\quad l\equiv 0 \bmod 6.\end{cases}$$

Indeed, if $\langle m, n\rangle \epsilon D\setminus E_l$ and $\langle q, r\rangle \epsilon D\setminus E_l$ we get again (20) and hence it follows by Lemma 3 that

$$\zeta_l^m-\zeta_l^q=\zeta_l^n-\zeta_l^r=0 \quad \text{or} \quad \zeta_l^m=-\zeta_l^q,$$
$$\{-\theta\zeta_l^{n-q},\ \theta\zeta_l^{r-q}\}=\{\zeta_3,\zeta_3^2\};$$
$$\langle m,n\rangle\equiv\langle q,r\rangle \bmod l \quad \text{or} \quad l\equiv 0 \bmod 6,$$
$$\langle m,n\rangle\equiv\langle q+l/2,\ 2q-r+l/2\rangle \bmod l.$$

Therefore,

$$d^{-2}\Big|\bigcap_{l|d}E_l\Big|\geqslant 1-\sum_{1<l|d}l^{-2}-\sum_{\substack{l|d\\ l\equiv 0 \bmod 6}}l^{-2}>2-\frac{37}{36}\sum_{l=1}^{\infty}l^{-2}=2-\frac{37\pi^2}{36}>0.$$

In case (12) let β be the least exponent such that $f(\zeta_{2^\beta})=0$ if such equality is possible, otherwise $\beta=\infty$, $2^{-\beta}=0$. In the former case $2^\beta|d$, since $A(\zeta_{2^\beta}^0-\zeta_{2^\beta}^0)+f(\zeta_{2^\beta})=0$. Set

$$E_l''=\{\langle m,n\rangle \epsilon D\colon\ m\equiv n \bmod l\}$$

and

$$E_l'=\begin{cases}E_l\setminus E_l'' & \text{if} \quad l=2^\beta \text{ or } l \text{ is an odd prime},\\ E_l\cup E_l'' & \text{otherwise}.\end{cases}$$

If l has an odd prime factor p then

$$E_l'\cap E_p'\setminus E_l\subset E_l''\cap E_p'\subset E_l''\setminus E_p''=\emptyset.$$

If $l=2^\alpha$, where $\alpha<\beta$ then by the choice of β

$$E'\setminus E_l\subset E_l''\setminus E_l=\emptyset.$$

If $l=2^\alpha$, where $\alpha\geqslant\beta$ then

$$E_l'\cap E_{2^\beta}'\setminus E_l\subset E_l''\cap E_{2^\beta}'\subset E_l''\setminus E_{2^\beta}''=\emptyset.$$

Hence $\bigcap_{l|d}E_l'\subset\bigcap_{l|d}E_l$ and it remains to estimate $\big|\bigcap_{l|d}E_l'\big|$. With this end we note that

(21) $$|(D\setminus E_l\setminus E_l'')\cap D_l|\leqslant\begin{cases}0 & \text{if} \quad l=2^\beta,\\ 1 & \text{if} \quad l=2,\\ (2,l) & \text{otherwise}.\end{cases}$$

Indeed, if $\langle m,n\rangle \epsilon D\setminus E_l\setminus E_l''$, $\langle q,r\rangle \epsilon D\setminus E_l\setminus E_l''$ we have

(22) $$A(\zeta_l^m-\zeta_l^n)+f(\zeta_l)=A(\zeta_l^q-\zeta_l^r)+f(\zeta_l)=0;\quad m\not\equiv n,\ q\not\equiv r \bmod l,$$

thus (20) holds with $B=-A$, $\zeta_l^m-\zeta_l^n\neq 0$. Hence in virtue of Lemma 3

$$\zeta_l^m=\zeta_l^q,\quad \zeta_l^n=\zeta_l^r \quad \text{or} \quad \zeta_l^m=-\zeta_l^r,\quad \zeta_l^n=-\zeta_l^q$$

and

(23) $$\langle m,n\rangle\equiv\langle q,r\rangle \bmod l \quad \text{or} \quad l\equiv 0 \bmod 2,$$
$$\langle m,n\rangle\equiv\langle r+l/2,\ q+l/2\rangle \bmod l.$$

This gives (21) for $l\neq 2^\beta, 2$. If $l=2^\beta$ then (22) is impossible, thus $D\setminus E_l\setminus E_l''=\emptyset$. Finally, if $l=2$ (22) implies $q\equiv r+1 \bmod 2$, thus (23) is satisfied by only one residue class $\langle m,n\rangle \bmod 2$.

We have further

$$|E_l''\cap D_l|=l.$$

In virtue of Lemma 5 it follows from (21), (24) and the definition of E_l' that

$$d^{-2}|D\setminus E_l'|\leqslant\begin{cases}l^{-1}+l^{-2} & \text{if} \quad l \text{ is an odd prime},\\ l^{-1} & \text{if} \quad l=2^\beta,\\ 4^{-1} & \text{if} \quad l=2\neq 2^\beta,\\ (2,l)\,l^{-2} & \text{otherwise}.\end{cases}$$

Set $\operatorname{ord}_p d=o_p$. We get

$$d^{-2}\sum_{\alpha=1}^{o_2}|D\setminus E_{2^\alpha}'|<\begin{cases}2^{-1}+\sum\limits_{\alpha=2}^{\infty}2^{1-2\alpha}=\frac{2}{3} & \text{if} \quad \beta=1,\\ 4^{-1}+2^\beta+\sum\limits_{\substack{\alpha=2\\ \alpha\neq\beta}}^{\infty}2^{1-2\alpha}=\frac{5}{12}+2^{-\beta}-2^{1-2\beta}<\frac{2}{3} & \text{if} \quad \beta>1;\end{cases}$$

$$e_2=d^{-2}\Big|\bigcap_{\alpha=1}^{o_2}E_{2^\alpha}'\Big|\geqslant 1-d^{-2}\sum_{\alpha=1}^{o_2}|D\setminus E_{2^\alpha}'|>\tfrac{1}{3}=c_2,$$

$$e_p=d^{-2}\Big|\bigcap_{\alpha=1}^{o_p}E_{p^\alpha}'\Big|\geqslant 1-d^{-2}\sum_{\alpha=1}^{o_p}|D\setminus E_{p^\alpha}'|>1-p^{-1}\sum_{\alpha=2}^{o_p}p^{-2\alpha}$$
$$=\frac{p^3-p^2-2p+1}{p(p^2-1)}=c_p \qquad (p>2).$$

On the other hand,

$$\bigcap_{l|d}E_l'=\bigcap_{p^\alpha|d}E_{p^\alpha}'\setminus\bigcup\nolimits_1(D\setminus E_l')\cap\bigcap_{\substack{p^\alpha|d\\ p\nmid l}}E_{p^\alpha}',$$

$$\Big|\bigcap_{l|d}E_l'\Big|\geqslant\Big|\bigcap_{p^\alpha|d}E_{p^\alpha}'\Big|-\sum\nolimits_1\Big|(D\setminus E_l')\cap\bigcap_{\substack{p^\alpha|d\\ p\nmid l}}E_{p^\alpha}'\Big|,$$

where $\bigcup_1$ and $\sum_1$ are taken over all divisors l of d except the prime powers.

The families of sets $\{S(p^{\sigma_p})\}_{p|d} \cup \{S(l)\}$ and $\{S(p^{\sigma_p})\}_{p|d,\, p\nmid l}$, where $S(p^{\sigma_p}) = \bigcap_{a=1}^{\sigma_p} E'_{p^a}$, $S(l) = D\setminus E_l$, satisfy the assumptions of Lemma 5, hence

$$d^{-2}\Big|\bigcap_{l|d} E'_l\Big| \geq \prod_{p|d} e_p - \sum\nolimits_1 d^{-2}|D\setminus E'_l| \prod_{\substack{p|d\\ p\nmid l}} e_p = \prod_{p|d} e_p \Big(1-\sum\nolimits_1 (l,2)\, l^{-2} \prod_{p|l} e_p^{-1}\Big)$$

$$> \prod_{p|d} e_p \Big(1 - \sum_{l=2}^{\infty} (l,2)\, l^{-2}\prod_{p|l} e_p^{-1} + \sum_{p^a>1}(p^a,2)\,p^{-2a}e_p^{-1}\Big).$$

The function $(l,2)\, l^{-2}\prod_{p|l} e_p^{-1}$ is multiplicative. Therefore

$$\sum_{l=2}^{\infty} (l,2)\, l^{-2}\prod_{p|l} e_p^{-1} = \prod_{p=2}^{\infty} \Big(1+\sum_{a=1}^{\infty} (p^a,2)\,p^{-2a}e_p^{-1}\Big) - 1$$

$$= 3\prod_{p=3}^{\infty} \big(1+e_p^{-1}(p^2-1)^{-1}\big) - 1 = 3\prod_{p=3}^{\infty} \Big(1+\frac{p}{p^3-p^2-2p+1}\Big) - 1,$$

$$\sum_{p^a>1}(p^a,2)\,p^{-2a}e_p^{-1} = \sum_{a=1}^{\infty} 2^{1-2a}e_2^{-1} + \sum_{p=3}^{\infty}\sum_{a=1}^{\infty} p^{-2a}e_p^{-1} = 2+\sum_{p=3}^{\infty} \frac{p}{p^3-p^2-2p+1}.$$

In virtue of Lemma 6 we have

$$4-3\prod_{p=3}^{\infty}\Big(1+\frac{p}{p^3-p^2-2p+1}\Big)+\sum_{p=3}^{\infty} \frac{p}{p^3-p^2-2p+1} > 0.2,$$

hence

$$d^{-2}\Big|\bigcap_{l|d}E'_l\Big| > 0.2\, d^2 \prod_{p|d} e_p > 0$$

and the proof in case (12) is complete.

In case (13) let β be the least positive exponent such that $f(\zeta_{2^\beta}) \neq 0$. Since

$$\zeta_{2^{\beta-1}}^{2^{\beta}-2} + \zeta_{2^{\beta-1}}^{0} + f(\zeta_{2^{\beta-1}}) = 0$$

we have $2^{\beta-1}|d_0$, hence by the choice of d, $2^\beta|d$. We set

$$E''_l = \{\langle m,n\rangle \in D:\ m\equiv n \bmod l\},$$

$$E'_l = \begin{cases} E''_l & \text{if } l=2^a,\ a<\beta,\\ \{\langle m,n\rangle\in D:\ m-n\equiv 2^{\beta-1} \bmod 2^\beta\} & \text{if } l=2^\beta,\\ E_l\setminus E''_l & \text{if } l \text{ is an odd prime},\\ E_l\cup E''_l & \text{otherwise}.\end{cases}$$

If l has an odd prime factor p then

$$E'_l\cap E'_p\setminus E_l \subset E''_l\cap E'_p \subset E''_l\setminus E''_p = \emptyset.$$

If $l=2^a$, $0<a\leq\beta$, $\langle m,n\rangle\in E'_l$ then by the choice of β

$$\zeta_l^m+\zeta_l^n+f(\zeta_l) = \begin{cases}2\zeta_l^m\neq 0 & \text{if } a<\beta,\\ f(\zeta_l)\neq 0 & \text{if } a=\beta,\end{cases}$$

thus $E'_l\setminus E_l=\emptyset$.

If $l=2^a$, $a>\beta$ then

$$E'_l\cap E'_{2^\beta}\setminus E_l \subset E''_l\cap E'_{2^\beta}\subset E''_{2^\beta}\cap E'_{2^\beta}=\emptyset.$$

Hence

$$\bigcap_{l|d}E'_l \subset \bigcap_{l|d} E_l$$

and it remains to estimate $\big|\bigcap_{l|d}E'_l\big|$. With this end we note that

$$|(D\setminus E_l\setminus E''_l)\cap D_l| \leq 2. \tag{24}$$

Indeed, if $\langle m,n\rangle\in D\setminus E_l\setminus E''_l$, $\langle q,r\rangle \in D\setminus E_l\setminus E''_l$ we have

$$A(\zeta_l^m+\zeta_l^n)+f(\zeta_l) = A(\zeta_l^q+\zeta_l^r)+f(\zeta_l)=0;\quad m\not\equiv n,\ q\not\equiv r \bmod l,$$

thus (20) holds with $A=B$, $\zeta_l^m+\zeta_l^n\neq 0$. Hence in virtue of Lemma 3

$$\zeta_l^m=\zeta_l^q,\quad \zeta_l^n=\zeta_l^r \quad\text{or}\quad \zeta_l^m=\zeta_l^r,\quad \zeta_l^n=\zeta_l^q$$

and

$$\langle m,n\rangle\equiv\langle q,r\rangle \quad\text{or}\quad \langle r,q\rangle \bmod l. \tag{25}$$

We have further

$$|E''_l\cap D_l| = l,\qquad |E'_{2^\beta}\cap D_{2^\beta}| = 2^\beta. \tag{26}$$

In virtue of Lemma 5 it follows from (24), (26) and the definition of E'_l that

$$d^{-2}|D\setminus E'_l| \leq \begin{cases}2l^{-2} & \text{if } l \text{ composite} \neq 2^a\ (a\leq\beta),\\ l^{-1}+2l^{-2} & \text{if } l \text{ prime}>2.\end{cases} \tag{27}$$

On the other hand, since $E'_{2^\beta}\subset E'_{2^a}$ $(a<\beta)$

$$d^{-2}\Big|\bigcap_{a=1}^{\beta} E'_{2^a}\Big| = d^{-2}|E'_{2^\beta}| = 2^{-\beta}.$$

Set $\operatorname{ord}_p d = o_p$. We get

$$e_2 = d^{-2}\Big|\bigcap_{\alpha=1}^{o_2} E'_{2^\alpha}\Big| \geqslant d^{-2}|E'_{2^\beta}| - d^{-2}\sum_{\alpha=\beta+1}^{o_2} |D\setminus E'_{2^\alpha}|$$

$$> 2^{-\beta} - \sum_{\alpha=\beta+1}^{\infty} 2^{1-2\alpha} = 2^{-\beta} - \tfrac{1}{3}\cdot 2^{1-2\beta} = c_2,$$

$$e_p = d^{-2}\Big|\bigcap_{\alpha=1}^{o_p} E'_{p^\alpha}\Big| \geqslant 1 - d^{-2}\sum_{\alpha=1}^{o_p} |D\setminus E'_{p^\alpha}| > 1 - p^{-1} - 2\sum_{\alpha=2}^{\infty} p^{-2\alpha}$$

$$= \frac{p^3-p^2-3p+1}{p(p^2-1)} = c_p.$$

If $l = 2^\alpha l_1$, $\alpha > 0$, l_1 odd > 1 then

(28) $$d^{-2}|(D\setminus E'_l)\cap E'_{2^\beta}| \leqslant 2^{1-\max(\beta-\alpha,0)} l^{-2}.$$

For $\alpha \geqslant \beta$ the inequality follows at once from (27). In order to show it for $\alpha < \beta$ suppose that $\langle q, r\rangle \in D\setminus E''_l$ and set

$$E'_{l,l_1} = \{\langle m,n\rangle \in D\colon\ \langle m,n\rangle \not\equiv \langle q,r\rangle, \langle r,q\rangle \bmod l_1\},$$

$$E'_{l,2^\alpha} = \{\langle m,n\rangle \in D\colon\ \langle m,n\rangle \not\equiv \langle q,r\rangle, \langle r,q\rangle \bmod 2^\alpha\}.$$

Since $\langle m,n\rangle \in D\setminus E'_l$ implies (25) we have

$$D\setminus E'_l \subset (D\setminus E'_{l,l_1}) \cap (D\setminus E'_{l,2^\alpha}).$$

The sets

$$S(l_1) = D\setminus E'_{l,l_1}, \qquad S(2^\beta) = (D\setminus E'_{l,2^\alpha}) \cap E'_{2^\beta}$$

satisfy the assumptions of Lemma 5, hence

$$d^{-2}|S(l_1)| = l_1^{-2}|S(l_1)\cap D_{l_1}| \leqslant 2l_1^{-2},$$

$$d^{-2}|S(2^\beta)| = 2^{-2\beta}|S(2^\beta)\cap D_{2^\beta}| = \begin{cases} 0 & \text{if } q \not\equiv r \bmod 2^\alpha,\\ 2^{-\alpha-\beta} & \text{if } q \equiv r \bmod 2^\alpha,\end{cases}$$

$$d^{-2}|(D\setminus E'_l)\cap E'_{2^\beta}| \leqslant d^{-2}|S(l_1)\cap S(2^\beta)| = d^{-2}|S(l_1)|\,d^{-2}|S(2^\beta)|,$$

which implies (27).

Now we have

$$\bigcap_{l|d} E'_l = \bigcap_{p^\alpha|d} E'_{p^\alpha} \cap \bigcap_{2p|d} E'_{2p} \setminus {\textstyle\bigcup_1} (D\setminus E'_l) \cap \bigcap_{\substack{p^\alpha|d\\ p\nmid l}} E'_{p^\alpha} \setminus {\textstyle\bigcup_2} (D\setminus E'_l)\cap E'_{2^\beta} \cap \bigcap_{\substack{p^\alpha|d\\ p\nmid 2l}} E'_{p^\alpha},$$

(29) $$d^{-2}\Big|\bigcap_{l|d} E'_l\Big| \geqslant d^{-2}\Big|\bigcap_{p^\alpha|d} E'_{p^\alpha} \cap \bigcap_{2p|d} E'_{2p}\Big| - {\textstyle\sum_1} d^{-2}\Big|(D\setminus E_l) \cap \bigcap_{\substack{p^\alpha|d\\ p\nmid l}} E'_{p^\alpha}\Big| -$$

$$- {\textstyle\sum_2} d^{-2}\Big|(D\setminus E'_l)\cap E'_{2^\beta} \cap \bigcap_{\substack{p^\alpha|d\\ p\nmid 2l}} E'_{p^\alpha}\Big|,$$

where $\bigcup_1$ and $\sum_1$ are taken over all $l|d$ such that $l \equiv 1 \bmod 2$, $l \neq 1, p^\alpha$, $\bigcup_2$ and $\sum_2$ are taken over all $l|d$ such that $l \equiv 0 \bmod 2$, $l \neq 2p$ (p is a prime). $\sum_1$ and $\sum_2$ are estimated easily. Indeed, the family of sets

$$\{S(l)\} \cup \{S(p^{o_p})\}_{p|d,\,p\nmid l}, \quad \text{where} \quad S(l) = D_l\setminus E'_l, \quad S(p^{o_p}) = \bigcap_{\alpha=1}^{o_p} E'_{p^\alpha}$$

satisfies for each l the assumptions of Lemma 5. Hence by (27)

$$\Sigma_1 = {\textstyle\sum_1} d^{-2}|D\setminus E'_l| \prod_{\substack{p|d\\ p\nmid l}} e_p \leqslant \prod_{p|d} e_p {\textstyle\sum_1} 2l^{-2} \prod_{p|l} e_p^{-1} \leqslant \prod_{p|d} e_p {\textstyle\sum_1} 2l^{-2} \prod_{p|l} c_p^{-1}$$

$$< \prod_{p|d} e_p \Big(\sum_{\substack{l=3\\ l\ \mathrm{odd}}}^{\infty} 2l^{-2} \prod_{p|l} c_p^{-1} - \sum_{\substack{p^\alpha \geqslant 3\\ p\ \mathrm{odd}}} 2p^{-2\alpha} c_p^{-1}\Big).$$

The function $l^{-2}\prod_{p|l} c_p^{-1}$ is multiplicative and in the set of odd numbers there is the uniqueness of factorization, thus

(30) $$\sum_{\substack{l=3\\ l\ \mathrm{odd}}}^{\infty} 2l^{-2} \prod_{p|l} c_p^{-1} = 2\prod_{p=3}^{\infty}\Big(1 + \sum_{\alpha=1}^{\infty} p^{-2\alpha} c_p^{-1}\Big) - 2$$

$$= 2\prod_{p=3}^{\infty}\Big(1 + \frac{p}{p^3-p^2-3p+1}\Big) - 2,$$

$$\sum_{\substack{p^\alpha \geqslant 3\\ p\ \mathrm{odd}}} 2p^{-2\alpha} c_p^{-1} = 2\sum_{p=3}^{\infty}\sum_{\alpha=1}^{\infty} p^{-2\alpha} c_p^{-1} = 2\sum_{p=3}^{\infty} \frac{p}{p^3-p^2-3p+1}.$$

We get by Lemma 6

(31) $$\Sigma_1 < \prod_{p|d} e_p (2\cdot 1.46 - 2 - 2\cdot 0.4175) = 0.085 \prod_{p|d} e_p.$$

Similarly, the family of sets

$$\{S(2^{\max(\beta-\alpha,0)} l)\} \cup \{S(p^{o_p})\}_{p|d,\,p\nmid 2l},$$

where $S(2^{\max(\beta-\alpha,0)} l) = (D\setminus E'_l) \cap E'_{2^\beta}$, $S(p^{o_p}) = \bigcap_{\alpha=1}^{o_p} E'_{p^\alpha}$, satisfies for each $l = 2^\alpha l_1$, l_1 odd, the assumptions of Lemma 5. Hence by (28)

$$\Sigma_2 = {\textstyle\sum_2} d^{-2}|(D\setminus E'_l)\cap E'_{2^\beta}| \prod_{\substack{p|d\\ p\nmid 2l}} e_p \leqslant \prod_{\substack{p|d\\ p>2}} e_p {\textstyle\sum_2} 2^{1-\max(\beta-\alpha,0)} l^{-2} \prod_{p|l_1} e_p^{-1}$$

$$< \prod_{\substack{p|d\\ p>2}} e_p \Big(\sum_{\substack{l_1=3\\ l_1\ \mathrm{odd}}}^{\infty} \sum_{\alpha=1}^{\infty} 2^{1-\max(\beta-\alpha,0)-2\alpha} l_1^{-2} \prod_{p|l_1} c_p^{-1} - \sum_{p=3}^{\infty} 2^{-\beta} p^{-2} c_p^{-1}\Big).$$

Now

$$\sum_{a=1}^{\infty} 2^{1-\max(\beta-a,0)-2a} = \sum_{a=1}^{\beta} 2^{1-\beta-a} + \sum_{a=\beta+1}^{\infty} 2^{1-2a} = 2^{1-\beta} - 2^{1-2\beta} + \tfrac{1}{3}\cdot 2^{1-2\beta}$$
$$= 2c_2 \leqslant 2e_2.$$

On the other hand, by (30) and Lemma 6

$$\sum_{\substack{l_1=3\\ l_1 \text{odd}}}^{\infty} 2l_1^{-2} \prod_{p|l_1} c_p^{-1} = 2\prod_{p=3}^{\infty}\left(1+\frac{p}{p^3-p^2-3p+1}\right) - 2 < 2\cdot 1.46 - 2 = 0.92,$$

$$\sum_{p=3}^{\infty} p^{-2}c_p^{-1} = \sum_{p=3}^{\infty} \frac{p^2-1}{p(p^3-p^2-3p+1)} > 0.3804.$$

Hence

$$(32) \qquad \Sigma_2 < \prod_{p|d} e_p\Big(0.92 - 2^{-\beta}e_2^{-1}\sum_{p=3}^{\infty} p^{-2}c_p^{-1}\Big) < \prod_{p|d} e_p\,(0.92 - 2^{-\beta}e_2^{-1}\cdot 0.38).$$

It remains to estimate $|\bigcap_{p^a|d} E'_{p^a} \cap \bigcap_{2p|d} E'_{2p}|$. Here we distinguish two cases $\beta = 1$ and $\beta > 1$. If $\beta = 1$ we put

$$E_2^1 = \{\langle m, n\rangle \in D:\ \langle m, n\rangle \equiv \langle 0, 1\rangle \bmod 2\},$$
$$E_2^2 = \{\langle m, n\rangle \in D:\ \langle m, n\rangle \equiv \langle 1, 0\rangle \bmod 2\},$$

so that

$$(33) \qquad E_2^1 \cup E_2^2 = E_2', \quad E_2^1 \cap E_2^2 = \emptyset.$$

If $E_2'\setminus E'_{2p} = \emptyset$ we put further $E^1_{2p,p} = E^2_{2p,p} = D$ (p prime $\geqslant 3$). If $E_2'\setminus E'_{2p} \neq \emptyset$ let $\langle q, r\rangle \in E_2'\setminus E'_{2p}$. Then also $\langle r, q\rangle \in E_2'\setminus E'_{2p}$ and in view of symmetry we may assume $\langle q, r\rangle \in E_2^1$. We set

$$E^1_{2p,p} = \{\langle m, n\rangle \in D:\ \langle m, n\rangle \not\equiv \langle q, r\rangle \bmod p\},$$
$$E^2_{2p,p} = \{\langle m, n\rangle \in D:\ \langle m, n\rangle \not\equiv \langle r, q\rangle \bmod p\}.$$

Since $\langle m, n\rangle \in D\setminus E'_{2p}$ implies (25) with $l = 2p$, we have

$$E_2' \cap E'_{2p} = E_2^1 \cap E^1_{2p,p} \cup E_2^2 \cap E^2_{2p,p},$$
$$(34) \qquad \bigcap_{p^a|d} E'_{p^a} \cap \bigcap_{2p|d} E'_{2p} = \bigcap_{p|d} S_1(p^{\sigma_p}) \cup \bigcap_{p|d} S_2(p^{\sigma_p}),$$

where

$$S_i(2^{\sigma_2}) = E_2^i \cap \bigcap_{a=1}^{\sigma_2} E'_{2^a}, \quad S_i(p^{\sigma_p}) = \bigcap_{a=1}^{\sigma_p} E'_{p^a} \cap E^i_{2p,p}.$$

The family of sets $\{S_i(p^{\sigma_p})\}_{p|d}$ satisfies for $i = 1, 2$ the assumptions of Lemma 5, and by (33) the two summands in (34) are disjoint, hence

$$d^{-2}|\bigcap_{p^a|d} E'_{p^a} \cap \bigcap_{2p|d} E'_{2p}| = \prod_{p|d} d^{-2}|S_1(p^{\sigma_p})| + \prod_{p|d} d^{-2}|S_2(p^{\sigma_p})|.$$

However, by (33)

$$|S_1(2^{\sigma_2})| + |S_2(2^{\sigma_2})| = |S_1(2^{\sigma_2}) \cup S_2(2^{\sigma_2})| = |E_2' \cap \bigcap_{a=1}^{\sigma_2} E'_{2^a}| = d^2 e_2,$$

$$d^{-2}|S_i(p^{\sigma_p})| \geqslant d^{-2}|\bigcap_{a=1}^{\sigma_p} E'_{p^a}| - d^{-2}|D\setminus E^i_{2p,p}|$$
$$= e_p - p^{-2}|(D\setminus E^i_{2p,p}) \cap D_p| \geqslant e_p - p^{-2}.$$

Hence

$$d^{-2}|\bigcap_{p^a|d} E'_{p^a} \cap \bigcap_{2p|d} E'_{2p}| \geqslant d^{-2}\big(|S_1(2^{\sigma_2})| + |S_2(2^{\sigma_2})|\big)\prod_{\substack{p|d\\ p>2}} (e_p - p^{-2})$$
$$= \prod_{p|d} e_p \cdot \prod_{p|d} (1 - p^{-2}e_p^{-1}) > \prod_{p|d} e_p \cdot \prod_{p=3}^{\infty} (1 - p^{-2}c_p^{-1})$$
$$> \prod_{p|d} e_p\Big(1 - \sum_{p=3}^{\infty} p^{-2}c_p^{-1} + 3^{-2}\cdot 5^{-2}c_3^{-1}c_5^{-1}\Big) > \prod_{p|d} e_p\Big(1.014 - \sum_{p=3}^{\infty} p^{-2}c_p^{-1}\Big).$$

It follows from (29), (31) and (32) that

$$d^{-2}|\bigcap_{l|d} E_l'| \geqslant \prod_{p|d} e_p\Big(0.009 - \sum_{p=3}^{\infty} p^{-2}c_p^{-1} + 2^{-\beta}e_2^{-1}\sum_{p=3}^{\infty} p^{-2}c_p^{-1}\Big) > 0.009\prod_{p|d} e_p > 0.$$

If $\beta > 1$, we put

$$E_2^1 = \{\langle m, n\rangle \in D:\ \langle m, n\rangle \equiv \langle 0, 0\rangle \bmod 2\},$$
$$E_2^2 = \{\langle m, n\rangle \in D:\ \langle m, n\rangle \equiv \langle 1, 1\rangle \bmod 2\}$$

so that again (33) holds.

If $p > 2$ is a prime, $E'_{2p} \neq D$ and $\langle q, r\rangle \in D\setminus E'_{2p}$ we set

$$E'_{2p,p} = \{\langle m, n\rangle \in D:\ \langle m, n\rangle \not\equiv \langle q, r\rangle, \langle r, q\rangle \bmod p\}$$

and we assign p into class P_0, P_1 or P_2 according to whether $\langle q, r\rangle \notin E_2'$, $\langle q, r\rangle \in E_2^1$ or $\langle q, r\rangle \in E_2^2$, respectively.

Since $\langle m, n\rangle \in D\setminus E'_{2p}$ implies (25) with $l = 2p$, the residue classes of $\langle q, r\rangle$, $\langle r, q\rangle$ mod $2p$ are determined uniquely up to a permutation and sets $E'_{2p,p}$, P_1, P_2 are well defined. We have

$$E_2' \cap E'_{2p} = \begin{cases} E_2^2 \cup E_2^1 \cap E'_{2p,p} & \text{if } p \in P_1,\\ E_2^1 \cup E_2^2 \cap E'_{2p,p} & \text{if } p \in P_2,\\ E_2' & \text{otherwise.}\end{cases}$$

Hence

$$E_2' \cap \bigcap_{2p|d} E_{2p}' = E_2^1 \cap \bigcap_{\substack{2p|d\\ p\in P_1}} E_{2p,p}' \cup E_2^2 \cap \bigcap_{\substack{2p|d\\ p\in P_2}} E_{2p,p}'$$

and

$$(35)\qquad \bigcap_{p^\alpha|d} E_{p^\alpha}' \cap \bigcap_{2p|d} E_{2p}' = \bigcap_{p|d} S_1(p^{\sigma_p}) \cup \bigcap_{p|d} S_2(p^{\sigma_p}),$$

where

$$S_i(2^{\sigma_2}) = E_2^i \cap \bigcap_{\alpha=1}^{\sigma_2} E_{2^\alpha}',$$

$$S_i(p^{\sigma_p}) = \begin{cases} E_{2p,p}' \cap \bigcap\limits_{\alpha=1}^{\sigma_p} E_{p^\alpha}' & \text{if} \quad p\in P_i,\\ \bigcap\limits_{\alpha=1}^{\sigma_p} E_{p^\alpha}' & \text{if} \quad p\notin P_i,\ p>2.\end{cases}$$

The family of sets $\{S_i(p^{\sigma_p})\}_{p|d}$ satisfies for $i = 1, 2$ the assumptions of Lemma 5 and by (33) the two summands in (35) are disjoint. Hence

$$d^{-2}\Big|\bigcap_{p^\alpha|d} E_{p^\alpha}' \cap \bigcap_{2p|d} E_{2p}'\Big| = \prod_{p|d} |S_1(p^{\sigma_p})| + \prod_{p|d} |S_2(p^{\sigma_p})|.$$

On the other hand,

$$S_i(2^{\sigma_2}) = \bigcap_{\alpha=1}^{\sigma_2} E_{2^\alpha}' \setminus (D\setminus E_2^i) \cap E_{2^\beta}',$$

$$d^{-2}|S_i(2^{\sigma_2})| \geqslant e_2 - d^{-2}|(D\setminus E_2^i) \cap E_{2^\beta}'|$$
$$= e_2 - 2^{-2\beta}|(D\setminus E_2^i) \cap E_{2^\beta}' \cap D_{2^\beta}| = e_2 - 2^{-\beta-1},$$

$$d^{-2}|S_1(2^{\sigma_2})| + d^{-2}|S_2(2^{\sigma_2})| = d^{-2}|S_1(2^{\sigma_2}) \cup S_2(2^{\sigma_2})| = d^{-2}\Big|\bigcap_{\alpha=1}^{\sigma_2} E_{2^\alpha}'\Big| = e_2,$$

whence

$$d^{-2}|S_i(2^{\sigma_2})| = \frac{e_2}{2}\big(1+(-1)^i\varepsilon\big) \quad \text{where} \quad |\varepsilon| \leqslant 2^{-\beta}e_2^{-1}-1.$$

Further, for $p > 2$

$$d^{-2}|S_i(p^{\sigma_p})| \geqslant d^{-2}\Big|\bigcap_{\alpha=1}^{\sigma_p} E_{p^\alpha}'\Big| - d^{-2}|D\setminus E_{2p,p}'|$$
$$= e_p - p^{-2}|(D\setminus E_{2p,p}') \cap D_p| = e_p - 2p^{-2} \quad \text{if} \quad p\in P_i,$$
$$d^{-2}|S_i(p^{\sigma_p})| = e_p \quad \text{if} \quad p\notin P_i.$$

Hence

$$(36)\qquad d^{-2}\Big|\bigcap_{p^\alpha|d} E_{p^\alpha}' \cap \bigcap_{2p|d} E_{2p}'\Big| \geqslant \prod_{p|d} e_p\big((\tfrac{1}{2}-\tfrac{1}{2}\varepsilon)\,\Pi_1 + (\tfrac{1}{2}+\tfrac{1}{2}\varepsilon)\,\Pi_2\big)$$
$$\geqslant \prod_{p|d} e_p\big(\tfrac{1}{2}\Pi_1 + \tfrac{1}{2}\Pi_2 - \tfrac{1}{2}(2^{-\beta}e_2^{-1}-1)|\Pi_1-\Pi_2|\big),$$

where

$$\Pi_i = \prod_{p\in P_i}(1-2p^{-2}e_p^{-1}) = \prod_{p\in P_i}\Big(1-\frac{2(p^2-1)}{p(p^3-p^2-3p+1)}\Big).$$

It follows from Lemma 6 that

$$\Pi_1\Pi_2 \geqslant \prod_{p=3}^{\infty}\Big(1-\frac{2(p^2-1)}{p(p^3-p^2-3p+1)}\Big) = C > 0.3676$$

and since $1-2\cdot 3^{-2}e_3^{-1} = \frac{7}{15} < \sqrt{C}$

$$\tfrac{1}{2}|\Pi_1 - C\Pi_1^{-1}| \geqslant \tfrac{1}{2}(\tfrac{15}{7}C - \tfrac{7}{15}),$$

$$\tfrac{1}{2}\Pi_1 + \tfrac{1}{2}\Pi_2 \geqslant \tfrac{1}{2}\Pi_1 + \tfrac{1}{2}C\Pi_1^{-1} = \sqrt{C+\tfrac{1}{4}(\Pi_1 - C\Pi_1^{-1})^2} \geqslant \tfrac{1}{2}(\tfrac{15}{7}C + \tfrac{7}{15}) > 0.627,$$

$$|\Pi_1 - \Pi_2| \leqslant 1 - C < 0.632.$$

It follows from (29), (31), (32) and (36) that

$$d^{-2}\Big|\bigcap_{l|d} E_l'\Big| \geqslant \prod_{p|d} e_p\big(0.627 - (2^{-\beta}e_2^{-1}-1)\,0.316 - 1.005 + 2^{-\beta}e_2^{-1}\cdot 0.38\big)$$
$$\geqslant \prod_{p|d} e_p\big(0.002 + (2^{-\beta}e_2^{-1}-1)\,0.064\big) > 0.002\prod_{p|d} e_p > 0$$

and the proof is complete.

Lemma 8. *If $A \neq \pm B$ then each rational factor of $Ax^c + B$ is of degree at least $c|AB|^{-1}$.*

Proof. Each zero of Ax^c+B has absolute value $|BA^{-1}|^{1/c}$. Hence any monic factor of Ax^c+B of degree γ has constant term with absolute value $|BA^{-1}|^{\gamma/c}$. If this term is rational we have in the notation in Lemma 1 of [6]

$$c \leqslant e(B^\gamma A^{-\gamma}, Q) = \gamma e(BA^{-1}, Q).$$

However, since either BA^{-1} or $B^{-1}A$ is not an integer we get by that lemma

$$e(BA^{-1}, Q) = e(B^{-1}A, Q) \leqslant \frac{\log(A^2+B^2)}{2\log 2} \leqslant |AB|,$$

$$\gamma \geqslant c|AB|^{-1}.$$

Proof of Theorem. Let a, b, d be integers from Lemma 7 and set

$$c = a-b+d[d^{-1}(b-d+|f|^*|AB|)], \tag{37}$$

$$e = b+d+d[-bd^{-1}+d^{-1}\log(\|f\|+A^2+B^2)120(4c^2+8)^{\|f\|+A^2+B^2}], \tag{38}$$

where as in [6]

$$|f|^* = \sqrt{\max\{|f|^2, 2\}+2}.$$

It follows

$$c > |f|^*|AB| \geqslant \max(|f|, 2)|AB|. \tag{39}$$

$$e > 120(4c^2+8)^{\|f\|+A^2+B^2}\log(\|f\|+A^2+B^2) > |f|. \tag{40}$$

We note that

$$(Ax^c+B)(A+Bx^c) \neq x^c f(x) f(x^{-1}), \tag{41}$$

$$\big(K(Ax^c+B), Kf(x)\big) = \big(L(Ax^c+B), Lf(x)\big) = 1. \tag{42}$$

(41) follows from (39) by comparison of degrees of both sides, (42) is obvious if $A = \pm B$. If $A \neq \pm B$ any rational factor of Ax^c+B is by Lemma 8 and (39) of degree greater than $|f|$, which implies (42). Assume now

$$n = dt+e \quad (t \geqslant 0) \tag{43}$$

and set in Lemmata 12 and 13 of [6]

$$F(x_1, x_2) = (Ax_2^c+B)x_1+f(x_2), \quad n_1 = n,\ n_2 = 1.$$

The assumption of Lemma 13 is satisfied since by (41), (42)

$$\frac{F(x_1, x_2)}{KF(x_1, x_2)} = \left(\frac{Ax^c+B}{K(Ax^c+B)}, \frac{f(x)}{Kf(x)}\right) = \big(Ax^c+B, f(x)\big)$$

$$= \left(\frac{Ax^c+B}{L(Ax^c+B)}, \frac{f(x)}{Lf(x)}\right) = \frac{F(x_1, x_2)}{LF(x_1, x_2)}.$$

In view of (39)

$$|F| = c > 2; \quad |F|^* = \sqrt{c^2+2}, \quad \|F\| = A^2+B^2.$$

In view of (40) and (43) the numbers n_1, n_2 do not satisfy any relation $\gamma_1 n_1+\gamma_2 n_2 = 0$ with

$$0 < \max\{|\gamma_1|, |\gamma_2|\} \leqslant 120(2|F|^*)^{2\|F\|}\log\|F\|.$$

Therefore, by Lemma 12 of [6] there is an integral matrix $M = [\mu_{ij}]$ of degree 2 such that

$$0 \leqslant \mu_{21} < \mu_{11}, \quad 0 = \mu_{12} < \mu_{22}, \tag{44}$$

$$[n, 1] = [v_1, v_2]M \tag{45}$$

and

$$L\big((Ay_2^{c\mu_{22}}+B)y_1^{\mu_{11}}y_2^{\mu_{21}}+f(y_2^{\mu_{22}})\big) \overset{\text{can}}{=} \text{const}\prod_{\sigma=1}^{s} F_\sigma(y_1, y_2)^{e_\sigma} \tag{46}$$

implies

$$L\big(Ax^{n+c}+Bx^n+f(x)\big) = \text{const}\prod_{\sigma=1}^{s} LF_\sigma(x^{v_1}, x^{v_2})^{e_\sigma},$$

where polynomials $LF_\sigma(x^{v_1}, x^{v_2})$ $(\sigma \leqslant s)$ are either irreducible or constant.

Now by (44) and (46) $\mu_{22} = 1$ and the left hand side of (46) becomes $L\big((Ay_2^c+B)y_1^{\mu_{11}}y_2^{\mu_{21}}+f(y_2)\big)$ which itself is not reducible.

Indeed, since $c > |f|$ and Ay_2^c+B has no multiple factors

$$\pm\frac{f(y_2)}{y_2^{\mu_{21}}(Ay_2^c+B)}$$

is not a power in the field $Q(y_2)$ and by Capelli's theorem

$$y_1^{\mu_{11}}+\frac{f(y_2)}{y_2^{\mu_{21}}(Ay_2^c+B)}$$

is irreducible in this field. It follows that

$$\frac{(Ay_2^c+B)y_1^{\mu_{11}}y_2^{\mu_{21}}+f(y_2)}{\big((Ay_2^c+B)y_2^{\mu_{21}}, f(y_2)\big)}$$

is irreducible. Since by (42) and $f(0) \neq 0$

$$\big(L(Ay_2^c+B)y_2^{\mu_{21}}, Lf(y_2)\big) = 1,$$

we have on the right hand side of (46) $s = 0$ or $s = e_1 = 1$. We infer that $L\big(Ax^{n+c}+Bx^n+f(x)\big)$ is not reducible. By Lemma 13 of [6] we have

$$L\big(Ax^{n+c}+Bx^n+f(x)\big) = K\big(Ax^{n+c}+Bx^n+f(x)\big).$$

Finally by (37), (38) and (43) $n+c \equiv a$, $n \equiv b \bmod d$ and by Lemma 7

$$K\big(Ax^{n+c}+Bx^n+f(x)\big) = Ax^{n+c}+Bx^n+f(x),$$

thus $Ax^m+Bx^n+f(x)$ is irreducible for any $m = n+c$, $n = dt+e$ $(t \geqslant 0)$. By (40) we have $n > |f|$. On the other hand, by (18) and (37)

$$c \leqslant |f|^*|AB|+d \leqslant |f|^*|AB|+3\exp\tfrac{5}{2}|f| \leqslant 5\exp\left(\tfrac{5}{2}|f|+\log|AB|\right)$$

and for $t = 0$ we get by (18) and (38)

$$m = c+e \leqslant c+d+\log(\|f\|+A^2+B^2)\,120(4c^2+8)^{\|f\|+A^2+B^2}$$
$$\leqslant 8\exp\left(\tfrac{5}{2}|f|+\log|AB|\right)+6^{\|f\|+A^2+B^2}\big(108\exp(5|f|+2\log|AB|)^{\|f\|+A^2+B^2}\big)$$
$$< \exp\big((5|f|+2\log|AB|+7)(\|f\|+A^2+B^2)\big).$$

The proof is complete.

Proof of Corollary. If $f(0) \neq 0$ we set $g(x) = Ax^n + Bx^m + f(x)$ and apply Theorem with $A = B = 1$ if $f(1) \neq -2$, with $A = -B = 1$ if $f(1) = -2$.

The inequality for $|g_0|$ follows, even with $\|f\|+3$ replaced by $\|f\|+2$.

If $f(0) = 0$ we set $g(x) = Ax^n + Bx^m + f(x) + 1$ and apply Theorem with $A = B = 1$ if $f(1) \neq -3$, with $A = -B = 1$ if $f(1) = -3$.

If $f(x) \not\equiv 0$ we have $|f(x)+1| = |f|$, $\|f(x)+1\| = f+1$, which implies the inequality for $|g_0|$. If $f(x) \equiv 0$, $|f| = -\infty$ we set $g_0(x) = x$.

References

[1] H. T. Davis, *Tables of higher mathematical functions*, Vol. II, Bloomington, Indiana, 1935.

[2] H. B. Mann, *Linear relations between roots of unity*, Mathematika 12 (1965), pp. 107–117.

[3] J. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. 6 (1962), pp. 64–89.

[4] A. Schinzel, *On the reducibility of polynomials and in particular of trinomials*, Acta Arith. 11 (1965), pp. 1–34.

[5] — *Reducibility of polynomials and covering systems of congruences*, Acta Arith. 13 (1967), pp. 91–101.

[6] — *Reducibility of lacunary polynomials I*, Acta Arith. 16 (1969), pp. 123–159.

Reçu par la Rédaction le 30. 4. 1969

ACTA ARITHMETICA
XVI (1970)

On a generalization of a theorem of Borel

by

SANDRA MONTEFERRANTE (Oakdale, N. Y.)
and P. SZÜSZ (Stony Brook, N. Y.)

1. Let τ be a real number between 0 and 1. A classical theorem of Borel asserts that if we put

$$\tau = \sum_{k=1}^{\infty} \varepsilon_k(\tau) 2^{-k} \quad (\varepsilon_k = 0 \text{ or } 1)$$

then we have for almost all τ

$$\sum_{k=1}^{n} \varepsilon_k(\tau) \sim \frac{n}{2}.$$

An analogous result holds, of course, for expansions with respect to an arbitrary basis, for instance, for decimal expansions.

Now let a be an irrational number with the regular continued fraction expansion

$$a = \{0;\ a_1, a_2, \ldots\} \tag{1.1}$$

and put

$$D_n = \frac{(-1)^n}{\zeta_{n+1} B_n + B_{n-1}} = B_n a - A_n, \tag{1.2}$$

where A_n/B_n are the convergents of a and $\zeta_n = \{a_n; a_{n+1}, \ldots\}$.

It is well known [3] that each τ with $D_1 < \tau < 1 - D_1$ can be represented in the form

$$\tau = \sum_{k=0}^{\infty} C_{k+1}(\tau) D_k \tag{1.3}$$

where $C_1(\tau) < a_1$, $0 \leqslant C_{k+1}(\tau) \leqslant a_{k+1}$ and $C_{k+1}(\tau) = a_{k+1} \Rightarrow C_k(\tau) = 0$. We have uniqueness if in addition we do not allow $C_{k+2i} = a_{k+2i}$ for some k and $i = 1, 2, \ldots$