Irrationality of π and e^k $(k \in \mathbb{Z})$: proof by Hermite interpolation

Hermite: constructed approximations of e^z by rational functions $\frac{A(z)}{B(z)}$, where

$(\forall n_0, n_1 \geq 1)$

(1) $A \in \mathbb{Q}[z]$, $B \in \mathbb{Z}[z]$, B monic

(2) $\deg(A) = n_0$, $\deg(B) = n_1$

(3) $R(z) := B(z)e^z - A(z)$ has zero of order $> n_0 + n_1$ at $z = 0$

(4) $(-1)^{n_1} \frac{n_0!}{n_1!} A \in \mathbb{Z}[z]$ is a monic polynomial

(5) $|R(z)| \leq \frac{|z|^{n_0+n_1+1} e^{|z|}}{n_0!}$ $\quad \forall z \in \mathbb{C}$

Construction: $D = \frac{d}{dz}$, $\delta = z\frac{d}{dz}$ differential operators

$\forall m \geq 0 \quad \delta^m : z^k \longmapsto k^m z^k \Longrightarrow \forall P \in \mathbb{C}[t] \quad P(\delta) : z^k \longmapsto P(k) z^k$

$$f = \sum_{k \geq 0} a_k z^k \longmapsto \sum_{k \geq 0} a_k P(k) z^k$$

Given $n_0, n_1 \geq 1$: the polynomial

$$P = P_{n_0,n_1}(t) = \prod_{j=n_0+1}^{n_0+n_1} (t - j) \quad \text{satisfies} \quad P(\delta)f = \sum_{k=0}^{n_0} P(k) a_k z^k + \sum_{k > n_0+n_1} P(k) a_k z^k$$

$$D(e^z) = e^z \Longrightarrow \underbrace{P(\delta)e^z}_{\underbrace{\sum_{k=0}^{n_0} P(k)\frac{z^k}{k!}}_{A(z) \in \mathbb{Q}[z]} + \underbrace{\sum_{k > n_0+n_1} P(k) \frac{z^k}{k!}}_{R(z)}} = B(z)e^z, \quad B \in \mathbb{Z}[z], \quad B \text{ monic} \quad \Longrightarrow (1), (2), (3)$$

$$\frac{n_0!}{n_1!}(-1)^{n_1} A(z) = \sum_{k=0}^{n_0} \frac{(n_0+n_1-k)!}{n_1!} \binom{n_0}{k} z^k \in \mathbb{Z}[z], \quad \text{monic} \Longrightarrow (4)$$

$$|R(z)| = \left| \sum_{k > n_0+n_1} \frac{(k-n_0-1)!}{(k-n_0-n_1-1)!} \frac{z^k}{k!} = \sum_{\ell \geq 0} \underbrace{\frac{(\ell+n_1)!}{(\ell+n_0+n_1+1)!}}_{\leq \frac{1}{n_0!}} \frac{z^{\ell+n_0+n_1+1}}{\ell!} \right| \leq \frac{|z|^{n_0+n_1+1} e^{|z|}}{n_0!} \Longrightarrow (5)$$

Special case $n_0 = n_1 = n \geq 1$: $\quad B_n(z)e^z - A_n(z) = R_n(z)$, $\quad |R_n(z)| \leq \frac{|z|^{2n+1} e^{|z|}}{n!}$

$A_n, B_n \in \mathbb{Z}[z]$ monic

$R_n(z)$ has zero of order $> 2n$ at $z = 0$

Thm. $\forall a \in \mathbb{Z}_{>0} \quad e^a \notin \mathbb{Q} \quad (\Rightarrow \forall t \in \mathbb{Q}_{>0} \quad e^t \notin \mathbb{Q})$.

Pf: $\underbrace{\underset{\mathbb{Z}}{\underset{\Uparrow}{B_n(a)}} e^a - \underset{\mathbb{Z}}{\underset{\Uparrow}{A_n(a)}}}_{\text{has absolute value} \in \frac{\mathbb{Z}}{q}} = R_n(a) > 0$, $\quad \lim_{n\to\infty} R_n(a) = 0$; if $e^a = \frac{p}{q} \in \mathbb{Q}$

$\Longrightarrow$ has absolute value $\in \frac{\mathbb{Z}}{q} \Longrightarrow\ \geq \frac{1}{q}$ contradiction.

Thm. $\pi \notin \mathbb{Q}$. **Pf**: if $\pi = \frac{a}{b} \in \mathbb{Q}$, take $z = 2ia = 2i\pi b \Longrightarrow e^z = 1$,

$\Rightarrow B_n(2ia) - A_n(2ia) = R_n(2ia)$. If $R_n(2ia) \neq 0 \Longrightarrow |R_n(2ia)| \geq 1$.

$\Delta_n(z) = B_n(z)A_{n+1}(z) - B_{n+1}(z)A_n(z) = B_n R_{n+1} - B_{n+1}R_n \in \mathbb{Z}[z]$ has $\deg(\Delta_n) \leq 2n+1$, leading coefficient $\pm 2z^{2n+1}$, zero of order $> 2n$ at $z = 0 \Longrightarrow \Delta_n(z) = \pm 2z^{2n+1}$.

So if $R_n(2ia) = 0 \Longrightarrow R_{n+1}(2ia) \neq 0 \Longrightarrow |R_{n+1}(2ia)| \geq 1$. But $\lim_{n\to\infty} R_n(2ia) = 0$ — contradiction.

Transcendence of e by Hermite's interpolation

Thm. $e \notin \overline{\mathbb{Q}}$. **Pf:** Fix $m \geq 1$. We are going to show that $1, e, \dots, e^m$ are linearly independent over $\mathbb{Q}$, using the following

Irrationality criterion: let $(\alpha_1, \dots, \alpha_m) \in \mathbb{R}^m$. If $\forall \varepsilon > 0$ $\exists$ matrix

$$A = \begin{pmatrix} \underbrace{\begin{matrix} q_0 \\ \vdots \\ q_m \end{matrix}}_{C_0} & \Bigg| & \underbrace{\begin{matrix} p_{01} \\ \vdots \\ p_{m1} \end{matrix}}_{C_1} & \Bigg| & \cdots & \Bigg| & \underbrace{\begin{matrix} p_{0m} \\ \vdots \\ p_{mm} \end{matrix}}_{C_m} \end{pmatrix} \in M_{m+1}(\mathbb{Z}) \text{ such that } \left\{ \begin{matrix} \det(A) \neq 0 \\ \max\limits_{1 \leq k \leq m} |q_j \alpha_k - p_{jk}| < \varepsilon \\ (\forall j = 0, \dots, m) \end{matrix} \right\}$$

columns C_0, C_1, …, C_m

$$\Downarrow$$

$1, \alpha_1, \dots, \alpha_m$ are linearly independent over $\mathbb{Q}$.

[Note: the converse implication $\Uparrow$ also holds]

Pf: Assume $\exists (\lambda_0, \dots, \lambda_m) \in \mathbb{Z}^{m+1}$ with $L = \max |\lambda_k| \geq 1$, $\lambda_0 + \alpha_1 \lambda_1 + \dots + \alpha_m \lambda_m = 0$. Let A be as above, for $\varepsilon = 1/mL$. The column vector

$$\mathbb{Z}^{m+1} \ni A \begin{pmatrix} \lambda_0 \\ \vdots \\ \lambda_m \end{pmatrix} \text{ is equal to } \lambda_0 \underbrace{\begin{pmatrix} q_0 \\ \vdots \\ q_m \end{pmatrix}}_{\in \mathbb{Z}^{m+1}} + \begin{pmatrix} t_0 \\ \vdots \\ t_m \end{pmatrix}, \quad t_j = \sum_{k=1}^{m} \lambda_k (p_{jk} - \alpha_k q_j) \in \mathbb{Z},$$

$\forall j$ $|t_j| \leq mL \max\limits_{1 \leq k \leq m} |p_{jk} - \alpha_k q_j| < mL\varepsilon = 1 \implies \forall j$ $t_j = 0$. As $\lambda_k \neq 0$ for some $k \neq 0$ $\implies \operatorname{rank}(\underbrace{C_1 - \alpha_1 C_0 | \cdots | C_m - \alpha_m C_0}_{\in M_{(m+1) \times m}(\mathbb{R})}) < m \implies \operatorname{rank}(A) < m+1$ contradiction.

In order to obtain good rational approximations $\frac{p_{jk}}{q_j}$ to e^k $(1 \leq k \leq m)$ (with the same denominator q_j), we construct Hermite's approximations of the functions e^{kx} (—"—) by rational functions (with the same denominator) $\frac{P_{jk}(x)}{Q_j(x)}$

Basic formula: $\forall \lambda, x \in \mathbb{C} \setminus \{0\}$, $\forall f \in \mathbb{C}[t]$, $\deg(f) = N$

$$\int_0^\lambda e^{-xt} f(t)\, dt = \underbrace{\left[-\frac{1}{x} e^{-xt} f(t) \right]_0^\lambda}_{\frac{f(0) - e^{-\lambda x} f(\lambda)}{x}} + \frac{1}{x} \int_0^\lambda e^{-xt} f'(t)\, dt \overset{\text{induction}}{=} \sum_{i=0}^{N} \frac{f^{(i)}(0) - e^{-\lambda x} f^{(i)}(\lambda)}{x^{i+1}}$$

$$\Downarrow$$

$$\boxed{e^{\lambda x} \underbrace{\left(\sum_{i=0}^{N} f^{(i)}(0)\, x^{N-i} \right)}_{Q(x)} - \underbrace{\left(\sum_{i=0}^{N} f^{(i)}(\lambda)\, x^{N-i} \right)}_{P(x)} = \underbrace{x^{N+1} e^{\lambda x} \int_0^\lambda e^{-xt} f(t)\, dt}_{R(x)}}$$

Properties of P, Q, R : (1) $P, Q \in \mathbb{C}[x]$; (2) $\deg(P) = N - \underbrace{\mathrm{ord}_{x=\lambda} f(x)}_{n}$;

(3) $\deg(Q) = N - \underbrace{\mathrm{ord}_{x=0} f(x)}_{n'}$; (4) R is analytic at $x=0$, $\mathrm{ord}_{x=0} R(x) \geq N+1$

(5) If $f \in \mathbb{Z}[t] \Longrightarrow Q(x) \in (n')!\,\mathbb{Z}[x]$; (6) If $f \in \mathbb{Z}[t]$, $\lambda \in \mathbb{Z} \Longrightarrow P(x) \in n!\,\mathbb{Z}[x]$.

(7) If $\lambda, x \in \mathbb{R}_{>0} \Longrightarrow |R(x)| \leq x^{N+1} e^{\lambda x} \sup_{0 \leq t \leq 1} |f(t)|$.

We are going to apply this construction with suitable polynomials $f_0, \dots, f_m \in \mathbb{Z}[t]$, $\deg(f_j) = N_j$, and $\lambda = k \in \{0, 1, \dots, m\}$. We obtain

$$(*) \quad \underbrace{e^{kx} \sum_{i=0}^{N_j} f_j^{(i)}(0) x^{N_j - i}}_{Q_j(x)} - \underbrace{\left(\sum_{i=0}^{N_j} f_j^{(i)}(k) x^{N_j - i} \right)}_{P_{jk}(x)} = \underbrace{x^{N_j+1} e^{kx} \int_0^k e^{-xt} f_j(t)\,dt}_{R_{jk}(x)}$$

$\forall j, k = 0, \dots, m$ $\quad (Q_j(x) = P_{j0}(x))$.

Note: (a) $\deg(P_{jk}) = N_j - \mathrm{ord}_{t=k} f_j(t) = N_j - a_{jk}$, $\quad \deg(Q_j) = N_j - a_{j0}$

(b) If $f_j \in \mathbb{Z}[t] \Longrightarrow P_{jk}(x) \in (a_{jk})!\,\mathbb{Z}[x]$, $\quad Q_j(x) \in (a_{j0})!\,\mathbb{Z}[x]$

We are going to put $x = 1$ in $(*)$. In order to apply the Irrationality criterion, we need to control $\Delta(1)$, where

$$\underset{\mathbb{C}[x]}{\Delta(x)} = \det \left(\underbrace{\begin{matrix} Q_0(x) \\ \vdots \\ Q_m(x) \end{matrix}}_{C_0} \middle| \underbrace{\begin{matrix} P_{01}(x) \\ \vdots \\ P_{m1}(x) \end{matrix}}_{C_1} \middle| \cdots \middle| \underbrace{\begin{matrix} P_{0m}(x) \\ \vdots \\ P_{mm}(x) \end{matrix}}_{C_m} \right) = \det \left(C_0 \middle| \underbrace{C_1 - e^x C_0}_{\mathrm{ord}_{x=0} \geq N_1 + 1} \middle| \cdots \middle| \underbrace{C_m - e^{mx} C_0}_{\mathrm{ord}_{x=0} \geq N_m + 1} \right)$$

$\Longrightarrow \mathrm{ord}_{x=0} \Delta(x) \geq \left(\sum_{k=1}^{m} (N_k + 1) \right)$. On the other hand, $\deg(C_k) \leq \max_{0 \leq j \leq m} (\deg P_{jk}(x))$

$\Longrightarrow \deg \Delta(x) \leq \left(\sum_{k=0}^{m} \max_{0 \leq j \leq m} (N_j - a_{jk}) \right)$ We want the two bounds here coincide $\Longrightarrow$

$\Delta(x) =$ monomial ax^b. Let us try to take $N_0 = \dots = N_m = N$,

$\min_{0 \leq j \leq n} a_{jk} = A$ (independent of k); we want $m(N+1) \overset{?}{=} (m+1)(N-A)$

$\Longleftrightarrow N+1 = (m+1)\underbrace{(A+1)}_{n}$. So we take $f_0, \dots, f_m$ such that $A = n-1$, $N = (m+1)n - 1$, then

$\Delta(x) = a x^{m(m+1)n} = a x^{m(N+1)}$, hence $\Delta(1) = a$.

We need $a \neq 0$, though. Can this be achieved?

If $\underline{a_{jk} > a_{kk} \text{ whenever } j \neq k}$ $(\Longrightarrow n-1 = A = a_{kk})$, then

$\deg(P_{jk}) < \deg(P_{kk})$ if $j \neq k$ $\Longrightarrow$ $\underline{a = \prod_{j=0}^{m} (\text{the leading term of } Q_{jj}(x)) \neq 0}$

So we try to make $\underline{a_{kk} = n-1}$, $\underline{a_{jk} = n}$ for $j \neq k$:

let $n \gg 0$, take $\underline{f_j(t) = (t(t-1)\cdots(t-m))^n)/(t-j) \in \mathbb{Z}[t]}$.
$\underline{(0 \leq j \leq m)}$

The above discussion implies: $\deg(f_j) = N = (m+1)n - 1$

(a) $\deg(P_{jk}) = N - (n - \delta_{jk})$, $\deg(Q_j) = N - (n - \delta_{j0})$

(b) $p_{jk} = P_{jk}(1)/(n-1)! \in \mathbb{Z}$, $q_j = Q_j(1)/(n-1)! \in \mathbb{Z}$

(c) $\det \begin{pmatrix} q_0 & p_{01} & \cdots & p_{0m} \\ \vdots & \vdots & & \vdots \\ q_m & p_{m1} & \cdots & p_{mm} \end{pmatrix} \neq 0$

(d) $\forall\, k = 1, \ldots, m$ $\quad |q_j e^k - p_{jk}| = \frac{e^k}{(n-1)!} \left| \int_0^k e^{-t} f_j(t)\, dt \right| \leq \frac{c_1 \cdot c_2^n}{(n-1)!} \underbrace{< \varepsilon}_{\text{if } n \gg 0}$

$\Downarrow$ Irrationality criterion

$\forall m \geq 1$ $1, e, \ldots, e^m$ are linearly independent over $\mathbb{Q}$

$\Downarrow$

$e \notin \mathbb{Q}$.

Transcendence of e – quantitative version

Thm (Improvement of a result of E. Borel (1899)*, due to Mahler)

$\forall \varepsilon>0\ \forall m\in\mathbb{Z}_{>0}\ \exists\, c=c(m,\varepsilon)>0\ \forall P\in\mathbb{Z}[X]$ such that $\deg(P)=m$

$$|P(e)|>\frac{c}{H(P)^{m+\varepsilon}},\qquad H(P)=\max|\text{coefficients of } P|$$

Note: $\forall t>1\ \exists\, p, q_1,\dots,q_m\in\mathbb{Z},\ |q_j|\le t,\ |q_1e+q_2e^2+\dots+q_me^m-p|<\frac{1}{t^m}$

$\Rightarrow$ the exponent $(m+\varepsilon)$ in Thm cannot be replaced by $m-\varepsilon$.

Pf of Thm. Recall Hermite's identity: $\forall f\in\mathbb{C}[t]$, $\deg(f)=d$

$$\int_0^x f(t)e^{-t}\,dt=[f(t)e^{-t}]_x^0+\int_0^x f'(t)e^{-t}\,dt=\dots=\Big[\underbrace{\big(f(t)+f'(t)+\dots+f^{(d)}(t)\big)}_{F(t)}e^{-t}\Big]_x^0=F(0)-e^{-x}F(x)$$

$\Rightarrow \forall P(t)=a_mt^m+\dots+a_0$, $\boxed{F(0)P(e)-\sum_{k=0}^m a_kF(k)=\sum_{k=0}^m e^k\int_0^k f(t)e^{-t}\,dt}$

Fix $m\ge1$, $\varepsilon>0$.

We can assume: $\forall k\ a_k\in\mathbb{Z}$, $\gcd(a_0,\dots,a_m)=1$; $H(P)=H=\max(|a_0|,\dots,|a_m|)$.

Choice of f (for given P): fix $n\in\mathbb{Z}_{>0}$ such that $\gcd(n,m!)=1$, $n\nmid a_r$ for some r,

take $f(x)=\frac{1}{(n-1)!}\frac{(x(x-1)\cdots(x-m))^n}{x-r}\Rightarrow \forall k=0,\dots,m\quad F(k)\equiv\begin{cases}(-1)^{(m-r)n}(r!\,(m-r)!)^n \pmod n\\ 0\end{cases}$

if $\begin{cases}k=r\\k\ne r\end{cases}\Rightarrow \sum_{k=0}^m a_kF(k)\equiv a_rF(r)\not\equiv0\pmod n\Rightarrow\left|\sum a_kF(k)\right|\ge1.$

On $[0,m]$: $|f(t)|\le m^{(m+1)n-1}/(n-1)!\Rightarrow\left|\sum_{k=0}^m e^k\int_0^k f(t)e^{-t}\,dt\right|\le\frac{m^{(m+1)n-1}He^m}{(n-1)!}\le$

$$F(0)=\int_0^\infty f(t)e^{-t}\,dt\ \Big|\le\underbrace{\int_0^m|f(t)|e^{-t}\,dt}_{<m^{(m+1)n}/(n-1)!}+\underbrace{\int_m^\infty|f(t)|e^{-t}\,dt}_{<\frac{1}{(n-1)!}\underbrace{\int_m^\infty t^{(m+1)n-1}e^{-t}\,dt}_{<\int_0^\infty(\ )=((m+1)n-1)!}}\le n^{mn}e^{c_2n}\quad\boxed{\le He^{c_1n}n^{-n},\ c_1=c_1(m)}$$

$c_2=c_2(m)$

If $Hn^{-n}e^{c_1n}\le\frac12$, then $|F(0)P(e)|\ge\frac12$

$$\Downarrow$$

$$|P(e)|\ge\tfrac12F(0)^{-1}\ge\frac{1}{2n^{mn}e^{c_2n}}.$$

Let $\delta=\frac{\varepsilon}{6m}$. If $H\gg0$, then $\exists\, n\in\left[(1+4\delta)\frac{\log H}{\log\log H},(1+5\delta)\frac{\log H}{\log\log H}\right]$

such that $n\equiv1\pmod{m!}$. Then $Hn^{-(1-\delta)n}<1$ and

$Hn^{-n}e^{c_1n}\le\frac12$ (if $H\gg0$) (exercise!)

$2n^{mn}e^{c_2n}\le H^{m(1+6\delta)}=H^{m+\varepsilon}\qquad\Rightarrow |P(e)|\ge\frac{1}{H^{m+\varepsilon}}$

if $H\gg0$.

Hermite – Lindemann theorem: proof by Gelfond's interpolation

$\overline{\mathbb{Q}} = \{$ algebraic numbers $\alpha \in \mathbb{C} \}$

Thm. $0 \neq \alpha \in \overline{\mathbb{Q}} \Rightarrow e^{\alpha} \notin \overline{\mathbb{Q}}$ (Lindemann, 1882).

We are going to prove the following

Special case (Lambert, 1760's): $0 \neq \alpha \in \mathbb{Q} \Rightarrow e^{\alpha} \notin \mathbb{Q}$

using interpolation techniques invented by Gelfond (1934) to solve Hilbert's 7^{th} problem ($\alpha, \beta \in \overline{\mathbb{Q}}$, $\alpha \neq 0, 1$, $\beta \notin \mathbb{Q} \Rightarrow \alpha^{\beta} \notin \overline{\mathbb{Q}}$); similar method was developed by T. Schneider, also in 1934.

The same argument proves Lindemann's thm, but the notation becomes slightly more involved.

Pf. Assume $0 \neq \alpha \in \mathbb{Q}$, $e^{\alpha} \in \mathbb{Q}$.

Step 1. Construction of a polynomial $0 \neq P \in \mathbb{Z}[X, Y]$ such that the entire function $f(z) = P(z, e^{z})$ has zeros of order $\geq N$ (for fixed large $N \gg 0$) at both $z = 0$ and $z = \alpha$.

Step 2. Maximum principle for $f(z) / z^{N}(z-\alpha)^{N}$ on the disc $\{|z| \leq R\}$ (for certain $R = R_N$ depending on N) $\Rightarrow$ upper bound for the derivatives $f^{(N)}(z)$ at $z = 0, \alpha$.

Step 3. $f^{(N)}(0)$, $f^{(N)}(\alpha)$ are rational numbers with controlled denominators $\Rightarrow$ each of them is either zero, or there is a lower bound for $f^{N}(z)$ $(z = 0, \alpha)$.

Step 4. The upper and lower bounds are contradictory $\Rightarrow f^{(N)}(0) = f^{(N)}(\alpha) = 0 \Rightarrow f(z)$ has zeroes of order $\geq N+1$ at $z = 0$ and $z = \alpha$.

Step 5. Repeat with $N+1$ (and R_{N+1}) etc $\Rightarrow$

$\forall m \geq 0 \quad f^{(m)}(0) = 0 \Rightarrow f \equiv 0 \xRightarrow{\text{exercise}} P = 0$ – contradiction.

In other works, if there are enough zeroes, then there are even more of them!

Step 1. lemma (Thue – Siegel) let $A=(a_{ij})\in M_{m\times n}(\mathbb{Z})$, $m<n$, $\forall i=1,\dots,m$ $\sum_{j=1}^{n}|a_{ij}|\le C_i$. Then $\exists\ x\in\mathbb{Z}^n$ such that

$$Ax=0\in\mathbb{Z}^m \quad\text{and}\quad 0<\max_{1\le j\le n}|x_j|\le (C_1\cdots C_m)^{1/(n-m)}$$

Pf. let $b_i=\sum_{\substack{j=1\\ a_{ij}<0}}^{n}a_{ij}$, $b_i'=\sum_{\substack{j=1\\ a_{ij}>0}}^{n}a_{ij}$ $\Longrightarrow$ $0\le \underbrace{b_i'-b_i}_{\in\mathbb{Z}}\le C_i$

For $B\in\mathbb{N}$ and $x\in\{0,1,\dots,B\}^n$, $Ax=y\in\mathbb{Z}^m$, $Bb_i\le y_i\le Bb_i'$

$\Longrightarrow$ $|A(\{0,1,\dots,B\}^n)|$ (= number of elements of $\{Ax\mid x\in\{0,\dots,B\}^n\}$)

$$\le\prod_{i=1}^{m}(Bb_i'-Bb_i+1)=\prod_{i=1}^{m}(BC_i+1)$$

If $B=[(C_1\cdots C_m)^{1/(n-m)}]$, then $(B+1)^{n-m}=([(C_1\cdots C_m)^{1/(n-m)}]+1)^{n-m}>C_1\cdots C_m$,

$$(B+1)^n>\prod_{i=1}^{m}(B+1)C_i\ge\prod_{i=1}^{m}(BC_i+1)\ \xRightarrow[\text{box principle}]{\text{Dirichlet's}}\ \exists\ x\ne x'\in\{0,\dots,B\}^n,\ Ax=Ax'$$

$$0<\max_{1\le j\le n}|x_j-x_j'|\le[(C_1\cdots C_m)^{1/(n-m)}] \Longleftarrow A(x-x')=0,\ 0\ne x-x'\in\mathbb{Z}^n$$

Construction of $P(X,Y)$: fix $N\in\mathbb{N}$, $N\gg0$; fix $b\in\mathbb{Z}$, $b>0$, $b\alpha,\ be^{\alpha}\in\mathbb{Z}$.

Want $P=\sum_{j=0}^{d_1}\sum_{k=0}^{d_2}p_{jk}X^jY^k$, $f(z)=P(z,e^z)=\sum_{j=0}^{d_1}\sum_{k=0}^{d_2}p_{jk}z^je^{kz}$, $a_{jk}\in\mathbb{Z}$

(d_1,d_2 will depend on N).

$$\forall m\ge0\quad f^{(m)}(z)=\sum_{j=0}^{d_1}\sum_{k=0}^{d_2}p_{jk}\sum_{\ell=0}^{\min(m,j)}\binom{m}{\ell}\frac{j!}{(j-\ell)!}k^{m-\ell}z^{j-\ell}e^{kz}$$

$$\forall\lambda=0,1\quad b^{d_1+d_2}f^{(m)}(\lambda\alpha)=\sum_{j=0}^{d_1}\sum_{k=0}^{d_2}p_{jk}\sum_{\ell=0}^{\min(m,j)}\underbrace{\binom{m}{\ell}\frac{j!}{(j-\ell)!}k^{m-\ell}(b\lambda\alpha)^{j-\ell}(be^{\lambda\alpha})^k\,b^{d_1+d_2-(j-\ell+k)}}_{\in\mathbb{Z}\setminus\{0\}}$$

Condition (Ord_N): $\forall\lambda=0,1$ $\forall m=0,\dots,N-1$ $f^{(m)}(\lambda\alpha)=0$

is a system of $2N$ linear equations for the $(d_1+1)(d_2+1)$ variables $\{p_{jk}\}$. Each equation has coefficients in $\mathbb{Z}$, and the sum of the absolute values of its coefficients is bounded above by

$$C=(d_1+1)(d_2+1)\,2^N d_1!\,d_2^N(1+|\alpha|)^{d_1}(e^{|\alpha|})^{d_2}\,b^{d_1+d_2}\ \xRightarrow[\text{Siegel}]{\text{Thue}}\ \text{if } (d_1+1)(d_2+1)>2N,$$

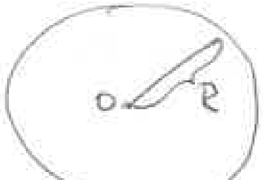
then $\exists\ P\in\mathbb{Z}[X,Y]\setminus\{0\}$ satisfying (Ord_N) with

$$0<\max_{j,k}|p_{jk}|\le C^{2N/((d_1+1)(d_2+1)-2N)}<C^{2N/(d_1d_2-2N)}.$$

Step 2. Assume that $M \geq N$ and that f satisfies (Ord_M)

$\Longrightarrow$ $f(z) = (z(z-\alpha))^M g(z)$, $\quad g(z)$ entire function (= holomorphic in $\mathbb{C}$)

let $R = R_M \gg 0$ (to be chosen later) and apply the maximum principle to g on the disc $D_R = \{ z \in \mathbb{C};\ |z| \leq R \}$:



$$\forall z_0 \in D_R \qquad |g(z_0)| \leq \|g\|_R = \sup \{ |g(z)|;\ |z| = R \}$$

$$\Downarrow$$

$$\forall \lambda = 0,1 \qquad |g(\lambda\alpha)| \leq \|f\|_R \frac{1}{R^M} \underbrace{\sup_{|z|=R} \frac{1}{|z-\alpha|^M}}_{\left(< (2/R)^M \text{ if } |R| > |\alpha| \right)}$$

$$f^{(M)}(\lambda\alpha) = \pm M!\, \alpha^M g(\lambda\alpha)$$

$$\|f\|_R \leq \left(\max_{j,k} |p_{jk}| \right) (d_1+1)(d_2+1)\, R^{d_1} e^{d_2 R}$$

$$\Downarrow$$

$$\forall \lambda = 0,1 \quad \underbrace{b^{d_1+d_2} f^{(M)}(\lambda\alpha)}_{\in \mathbb{Z}} \leq \underbrace{b^{d_1+d_2} M! (1+|\alpha|)^M (d_1+1)(d_2+1) R^{d_1} e^{d_2 R} \left(\frac{2}{R^2} \right)^M C^{2N/(d_1 d_2 - 2N)}}_{e^{u(M)}}$$

Step 3.

Step 4. If we can choose $d_i = d_i(N)$ and $R = R_M$ so that

(*) $\forall M \geq N \gg 0 \quad u(M) < 0$, then Step 2 + Step 3 $\Longrightarrow (\mathrm{Ord}_{M+1})$

Choice of R_M: for $N \gg 0$ fixed and $M \gg N$,

$$u(M) \leq c_1 + c_2 M + \underbrace{\log(M!)}_{\leq M \log(M) + c_3} - 2M(\log R) + c_4 R$$

so we take

$$\boxed{R = M^A, \ A > \frac{1}{2}} \Longrightarrow u(M) \leq 0 \text{ for } M \gg 0.$$

Choice of $d_1(N), d_2(N)$: we need $d_1 d_2$ slightly bigger than $2N$; the terms $d_1!, d_2^N$ in C should be roughly comparable in size.

First try: $\boxed{d_1 = N, \quad d_2 = [\log(N)]}$ $\qquad (N \geq \text{const.})$

this yields $\log(C) \leq 2N \log(N) + \underbrace{c_1(N)}_{\text{something with } |\cdot| \leq c_1 N}$

$$\Longrightarrow u(N) = \underbrace{\log(N!) - 2N \log(N^A) + N\log(N^A)}_{\underbrace{(1-A)}_{>0} N \log N + O(N)} + d_2 N^A + O(N)$$

too big

(we need $\boxed{A < 1}$ to keep $d_2 N^A$ small)

We need to make $\underbrace{\log(d_1!)}_{d_1\log(d_1)+O(d_1)}$ of smaller growth than $N(\log N)$

Second try : $\boxed{d_1 = [N/\log(N)], \quad d_2 = [(\log(N))^2]}$ $\quad \boxed{\begin{array}{c} R = M^A \\ \frac{1}{2} < A < 1 \end{array}}$

For $N \gg 0$ ($N \geq N_0$) $\log(C) \leq d_1(\log d_1) + c_0 N + N\log(d_2) \leq 3N(\log\log N)$.

$\forall M \geq N$,

$$u(M) \leq M\log(M) + c_1 M + d_1\log(M^A) + d_2(M^A) - 2M\log(M^A) + \frac{6N\log\log N}{\log N}$$

$$\leq \underbrace{(1-2A)M\log M + c_1 M + A\frac{N\log M}{\log N} + M^A(\log N)^2}_{v(M,N)}$$

If $N \geq N_1$, then $v(N,N) < 0$. Moreover,

$$\forall x \geq N_1 \quad \frac{\partial v(x,N_1)}{\partial x} = (1-2A)(\log(x)-1) + \underbrace{c_1 + \frac{AN_1}{\log N_1}\cdot\frac{1}{x} + \frac{A(\log N_1)^2}{x^{1-A}}}_{\leq c_1 + \frac{A}{\log N_1} + \frac{A(\log N_1)^2}{N_1^{1-A}} \leq c_2(A)}$$

$\Longrightarrow \exists N_2 \geq N_1 \quad \forall x \geq N_2 \quad \frac{\partial v}{\partial x}(x,N_2) \leq 0 \Longrightarrow \forall x \geq N_2 \quad v(x,N_2) < 0$

$\Longrightarrow \forall M \geq N \geq N_2 \quad u(M) < 0 \Longrightarrow (\mathrm{Ord}_{M+1})$.

Step 5. Induction + Step 4 $\Longrightarrow \forall m \geq 0 \quad f^{(m)}(z) = 0$

$\Longrightarrow \forall z \in \mathbb{C} \quad f(z) = P(z, e^z) = 0 \xRightarrow{\text{lemma}} P = 0$ – contradiction.

Lemma. If $p_0, \dots, p_n \in \mathbb{C}[z]$, if $\forall z \in \mathbb{C}$ $\underbrace{\sum_{k=0}^{n} p_k(z)e^{kz}}_{} = 0 \Rightarrow (\forall k)\ p_k = 0$.

Pf. let $z \in \mathbb{R}$, $z \to -\infty \Rightarrow 0 = \lim_{\mathbb{R} \ni z \to -\infty} = \lim_{\mathbb{R} \ni z \to -\infty} p_0(z)$

$\Rightarrow p_0 = 0$. Divide the relation by e^z and repeat the argument $\Rightarrow p_1 = \dots = p_n = 0$.

This finishes the proof of $(0 \neq \alpha \in \mathbb{Q} \Rightarrow e^\alpha \notin \mathbb{Q})$ by Gelfond's method. In order to prove $(0 \neq \alpha \in \overline{\mathbb{Q}} \Rightarrow e^\alpha \notin \overline{\mathbb{Q}})$, one assumes that $e^\alpha \in \overline{\mathbb{Q}}$ and works in the number field $K = \mathbb{Q}(\alpha, e^\alpha)$. Everything goes through, if one measures the size of $\beta \in K$ by $\max_{\sigma: K \hookrightarrow \mathbb{C}} |\sigma(\beta)|$.