P−9

Hermite の恒等式と π の超越性

Hermite's identity and the transcendence of π

岡田 裕紀[1]
Okada Hironori

Abstract

In 1873, Ch.Hermite proved that the number e is transcendental. Herimite's proof is based on Hermite's identity. In this report, we give a sketch of a proof to show the transcendence of π using Hermite's identity.

1 Hermite's identity

Hermite's method gives the following statement, which is equivalent to the transcendence of e : for any $m \geqslant 1$ the numbers $1, e, e^2, \dots, e^m$ are linearly independent over $\mathbb{Q}$. One uses the technique described in which the construction of the simultaneos rational approximations to powers of e is based on the so-called *Hermite's identity*.

LEMMA 1 (Hermite's identity). Let $f(x)$ be a polynomial of degree ν with real coefficients. Set

$$F(x) = f(x) + f'(x) + \cdots + f^{(\nu)}(x). \tag{1}$$

Then we have

$$e^x \int_0^x f(t)e^{-t}dt = F(0)e^x - F(x). \tag{2}$$

PROOF Integrating by parts, we obtain the relation

$$\int_0^x f(t)e^{-t}dt = f(0) - f(x)e^{-x} + \int_0^x f'(t)e^{-t}dt. \tag{3}$$

If we repeat this process $\nu + 1$ times, we arrive at the equality

$$\int_0^x f(t)e^{-t}dt = F(0) - F(x)e^{-x},$$

from which (2) follows.

The equality (2) is called "Hermite's identity".

2 Transcendental of π

The mathematicians of antiquity were in search of way of computing the area of a circle. It was this that led to the famous problem of squaring the circle and to various rational approximations to π. The irrationality of π was proven by J.H.Lambert in 1766.

The problem of squaring the circle is the following question : Starting with the radius of a circle and using only ruler and compass, is it possible to construct the side of a square that has the same area as the circle? It was not until two thousand years later that this question was answered in the negative when F.Lindemann in 1882 proved that π is transcendental.

THEOREM 1 (F.Lindemann). The number π is transcendental.

PROOF The proof that follows is relied on the equation $e^{\pi i} + 1 = 0$ and Lemmma 1. We suppose that the theorem is false, i.e., that π is an algebraic number. Then $\gamma = \pi i$ is also algebraic. Let $\nu = \deg \gamma$, and let $\gamma = \gamma_1, \dots, \gamma_\nu$ be the conjugates of γ over $\mathbb{Q}$. Since $e^\gamma + 1 = 0$, we have

$$\prod_{i=1}^{\nu}(1 + e^{\gamma_i}) = 0.$$

Expanding this product, we obtain

$$\prod_{i=1}^{\nu}(1 + e^{\gamma_i}) = \sum_{\varepsilon_1=0}^{1} \cdots \sum_{\varepsilon_\nu=0}^{1} \exp(\varepsilon_1\gamma_1 + \cdots + \varepsilon_\nu\gamma_\nu) = 0. \tag{4}$$

The exponents inside the multiple sum in (4) include some which are nonzero, e.g., when $\varepsilon_1 = 1$ and $\varepsilon_2 = \cdots = \varepsilon_\nu = 0$, and also some which are zero, e.g., when $\varepsilon_1 = \cdots = \varepsilon_\nu = 0$. Suppose that there are precisely m nonzero exponents and $a = 2^\nu - m$ which are zero, $a \geqslant 1$. Then, if we let $\alpha_1, \dots, \alpha_m$ denote the nonzero exponents, we can rewrite (4) as follows :

$$a + e^{\alpha_1} + \cdots + e^{\alpha_m} = 0, \quad a \geqslant 1. \tag{5}$$

We now show that the numbers $\alpha_1, \dots, \alpha_m$ are the set of roots of a polynomial $\psi(x) \in \mathbb{Z}[x]$ of degree m. To see this, we observe that the polynomial

$$\varphi(x) = \prod_{\varepsilon_1=0}^{1} \cdots \prod_{\varepsilon_\nu=0}^{1} (x - (\varepsilon_1\gamma_1 + \cdots + \varepsilon_\nu\gamma_\nu)),$$

[1] 日大理工・院 (前)・数学

considered as a polynomial in $\gamma_1,\dots,\gamma_\nu$ with coefficients in $\mathbb{Z}[x]$, is symmetric in $\gamma_1,\dots,\gamma_\nu$. Hence, $\varphi(x)$ is in $\mathbb{Q}[x]$. The roots of the degree 2^ν polynomial $\varphi(x)$ are $\alpha_1,\dots,\alpha_m$ and 0 with multiplicity a. Then, the degree m polynomial $x^{-a}\varphi(x)\in\mathbb{Q}[x]$ has precisely the number $\alpha_1,\dots,\alpha_m$ as its roots. If we let $r\in\mathbb{N}$ be the least common denominator of the coefficients of this polynomial, then the polynomial

$$\psi(x)=\frac{r}{x^a}\varphi(x)=b_mx^m+\cdots+b_1x+b_0\in\mathbb{Z}[x],\qquad b_m>0,\ b_0\neq 0,$$

also has precisely $\alpha_1,\dots,\alpha_m$ as its roots.

In Hermite's identity (2) we successively set $x=\alpha_1,\dots,\alpha_m$. By (5), we obtain :

$$-aF(0)-\sum_{k=1}^{m}F(\alpha_k)=\sum_{k=1}^{m}e^{\alpha_k}\int_0^{\alpha_k}f(t)e^{-t}dt. \tag{6}$$

In (6) we set

$$\begin{aligned}f(x)&=\frac{1}{(n-1)!}b_m^{mn-1}x^{n-1}\psi^n(x)\\&=\frac{1}{(n-1)!}b_m^{(m+1)n-1}x^{n-1}(x-\alpha_1)^n\cdots(x-\alpha_m)^n,\end{aligned}\tag{7}$$

where n is a sufficiently large natural number. We shall show that with this choice of $f(x)$ the equality (6) leads to a contradiction.

We obtain :

$$f^{(l)}(0)=0,\quad l=0,1,\dots,n-2,\quad f^{(n-1)}(0)=b_m^{mn-1}b_0^n.$$

Put A such that

$$F(0)=\sum_{l=n-1}^{(m+1)n-1}f^{(l)}(0)=b_m^{mn-1}b_0^n+nA, \tag{8}$$

then we have $A\in\mathbb{Z}$.

Since α_k is a root of $f(x)$ of multiplicity of n, we get also :

$$f^{(l)}(\alpha_k)=0,\quad l=0,1,\dots,n-1;\ k=1,\dots,m. \tag{9}$$

The l-th derivative of $x^{n-1}\psi^n(x)$ has integer coefficients which are all divisible by $n!$. Hence, for $l>n$ the coefficients of $f^{(l)}(x)$ are integers divisible by $b_m^{mn-1}n$. Then, from (9), we have

$$F(\alpha_k)=\sum_{l=n}^{(m+1)n-1}f^{(l)}(\alpha_k)=nb_m^{mn-1}\Phi(\alpha_k),\qquad k=1,\dots,m,\quad \Phi(z)\in\mathbb{Z}[z]. \tag{10}$$

The numbers $\beta_k=b_m\alpha_k,\ k=1,\dots,m$, are algebraic integers which make up the complete set of roots of a polynomial of degree m in $\mathbb{Z}[x]$ with leading coefficient 1. Furthermore, there exists a polynomial $H(x)\in\mathbb{Z}[x]$, such that

$$b_m^{mn-1}\Phi(\alpha_k)=H(\beta_k).$$

Hence,

$$\sum_{k=1}^{m}b_m^{mn-1}\Phi(\alpha_k)=\sum_{k=1}^{m}H(\beta_k). \tag{11}$$

Put $B=\sum_{k=1}^{m}H(\beta_k)$, therefore we have $B\in\mathbb{Z}$. From (8), (10) and (11) we find that

$$aF(0)+\sum_{k=1}^{m}F(\alpha_k)=a\,b_0^n\,b_m^{mn-1}+n(aA+B). \tag{12}$$

Now let n be any natural number satisfying the conditions

$$(n,b_0b_m)=1,\quad n>a. \tag{13}$$

Then the right side of (12) is an integer which is not divisible by n, and so is nonzero. Hence,

$$\left|aF(0)+\sum_{k=1}^{m}F(\alpha_k)\right|\geqslant 1. \tag{14}$$

We now find an upper bound for the right side of (6). Suppose that all of the points $\alpha_1,\dots,\alpha_m$ are contained in the circle $|x|\leqslant R$. We denote

$$\max_{|x|\leqslant R}|b_m^m\psi(x)|=C,$$

where C does not depend on n. Then

$$\max_{|x|\leqslant R}|f(x)|\leqslant\frac{R^{n-1}C^n}{(n-1)!}.$$

Hence, there exists an $n_0\in\mathbb{N}$ such that for any $n\geqslant n_0$ which satisfies (13) we have the inequalities

$$\begin{aligned}\left|\sum_{k=1}^{m}e^{\alpha_k}\int_0^{\alpha_k}f(x)e^{-x}dx\right|&\leqslant\sum_{k=1}^{m}\left|\int_0^{\alpha_k}|f(x)|\left|e^{(\alpha_k-x)}\right|dx\right|\\&\leqslant\frac{R^{n-1}e^R}{(n-1)!}C^n\sum_{k=1}^{m}\left|\int_0^{\alpha_k}dx\right|\\&\leqslant me^R\frac{(RC)^n}{(n-1)!}<1.\end{aligned}\tag{15}$$

The inequalities (14) and (15), along with (6), lead to the contradiction $1<1$. The theorem is proved.

References

[1] D.W.Masser, Yu.V.Nesterenko, H.P.Schlickewei, & M.Waldschmidt, Diophantine Approximation : Lectures from the C.I.M.E.Summer School held in Cetraro 2000, F.Amoroso & U.Zannier (eds.), Lecture Notes in Math., 1819, Springer, 2003.

[2] A.N.Parshin & I.R.Schfarevich (eds.), N.I.Fel'dman & Yu.V.Nesterenko (authors), *Number Theory IV*, Encyclopaedia of Math., vol.44, 1998.

[3] A. B. Shidlovskii, *Transcendental Numbers*, Studies in Math., vol.12, *Walter de Gruyter,* 1989.