21. Transcendence of e

Theorem 21.1. *e is transcendental.*

Lemma 21.2. *If $p(x) \in \mathbb{Z}[x]$ is a polynomial with integer coefficients then*

$$\int_0^\infty x^m p(x) e^{-x} \, \mathrm{d}x \equiv p(0) m! \mod (m+1)!.$$

In particular, if $(m+1)$ does not divide the constant term $p(0)$ then

$$\int_0^\infty x^m p(x) e^{-x} \, \mathrm{d}x \neq 0.$$

Proof. If $k \in \mathbb{N}$ then

$$\begin{aligned} I_k &= \int_0^\infty x^k e^{-x} \, \mathrm{d}x \\ &= \left[-x^k e^{-x} \right]_0^\infty + k \int_0^\infty x^{k-1} e^{-x} \, \mathrm{d}x \\ &= k \int_0^\infty x^{k-1} e^{-x} \, \mathrm{d}x \\ &= k I_{k-1} \\ &= k! I_0 \\ &= k!. \end{aligned}$$

As $k!$ divides $(k+1)!$ it follows that

$$\int_0^\infty x^m p(x) e^{-x} \, \mathrm{d}x \equiv p(0) m! \mod (m+1)!.$$ □

Proof of (21.1). Suppose not, suppose that e is algebraic. Then we can find integers $a_0, a_1, a_2, \dots, a_n$, $a_0 \neq 0$ such that

$$a_n e^n + a_{n-1} e^{n-1} + \dots + a_1 e + a_0 = 0.$$

Let r be a natural number, which we will fix later, and let

$$I_b^c = \int_b^c x^r [(x-1)(x-2)\dots(x-n)]^{r+1} e^{-x} \, \mathrm{d}x,$$

where $0 \leq b < c \leq \infty$. Suppose we multiply the relation above by I_0^∞ and split the result into two parts

$$P_1 + P_2 = 0,$$

where

$$\begin{aligned} P_1 &= a_0 I_0^\infty + a_1 e I_1^\infty + \dots + a_n e^n I_n^\infty \\ P_2 &= \qquad\quad a_1 e I_0^1 \; + \dots + a_n e^n I_0^n. \end{aligned}$$

We will show that $P_1/r!$ is a nonzero integer while

$$\left|\frac{P_2}{r!}\right| < 1,$$

for an appropriate choice of r.

Making the change of variable $y = x - k$, we obtain

$$\begin{aligned}
a_k e^k I_k^\infty &= a_k \int_k^\infty x^r [(x-1)(x-2)\dots(x-n)]^{r+1} e^{-(x-k)}\,\mathrm{d}x \\
&= a_k \int_0^\infty (y+k)^r [(y+k-1)(y+k-2)\dots(y+k-n)]^{r+1} e^{-y}\,\mathrm{d}y \\
&= \begin{cases} a_0 \int_0^\infty y^r p_0(y) e^{-y}\,\mathrm{d}y & \text{for } k = 0 \\ a_k \int_0^\infty y^{r+1} p_k(y) e^{-y}\,\mathrm{d}y & \text{for } 0 < k \le n, \end{cases}
\end{aligned}$$

for certain polynomials $p_i(y) \in \mathbb{Z}[y]$.

(21.2) implies that every term in P_1 is an integer and all but the first is divisible by $(r+1)!$. It follows that

$$\begin{aligned}
P_1 &\equiv a_0 p_0(0) r! \\
&\equiv a_0 (-1)^{n(r+1)} (n!)^{r+1} r! \mod (r+1)!.
\end{aligned}$$

Therefore, if

$$(r+1, a_0 n!) = 1,$$

then P_1 is a nonzero multiple of $r!$.

Now we turn to the problem of bounding $|P_2|$. Let

$$\begin{aligned}
M &= \max_{0 \le x \le n} |x(x-1)\dots(x-n)| \\
N &= \max_{0 \le x \le n} |(x-1)\dots(x-n)e^{-x}|.
\end{aligned}$$

Then for $1 \le k \le n$

$$\begin{aligned}
|a_k k I_k^\infty| &\le |a_k| \int_0^k M^r N\,\mathrm{d}x \\
&= k|a_k| M^r N
\end{aligned}$$

so that

$$|P_2| \le (|a_1|e + 2|a_2|e^2 + \dots + n|a_n|e^n) M^r N.$$

If we fix M then $M^r = o(r!)$ and so $|P_2| < r!$ for all sufficiently large r. Pick one such r such that

$$(r+1, a_0 n!) = 1. \qquad \square$$