e is a transcendental number

Basic definitions

- For any polynomial $f \in \mathbb{Z}[X] = a_0 + a_1 X + \cdots + a_n X^n$, $\bar{f} := |a_0| + |a_1|X + \cdots + |a_n|X^n$. This is `f_bar` in `e_trans_helpers2.lean`
- For any prime number p and natural number n we can define a polynomial $f_{p,n} \in \mathbb{Z}[X]$ as $X^{p-1}(X-1)^p \cdots (X-n)^p$. This is `f_p` in `e_transcendental.lean`.
- $f_{p,n}$ has degree $(n+1)p-1$. This is `deg_f_p` in `e_transcendental.lean`.
- With f an integer polynomial and any nonnegative real number t, we associate f with an integral $I(f,t)$ to be

  $$\int_0^t e^{t-x} f(x) \mathrm{d}x$$

  This is `II` in `e_trans_helpers2.lean`
- If f has degree n, then using integrating by part n times we have

  $$I(f,t) = e^t \sum_{i=0}^{n} f^{(i)}(0) - \sum_{i=0}^{n} f^{(i)}(t)$$

  This is `II_eq_I` in `e_trans_helpers2.lean`.
- For any polynomial $g \in \mathbb{Z}$ with degree n and coefficient g_i, $J_p(g)$ is defined to be

  $$J_p(g) = \sum_{i=0}^{n} g_i I(f_{p,n}, i)$$

  This is `J` in `e_transcendental.lean`.

So if $g(e) = 0$, we will have

$$\begin{aligned}
J_p(g) &= \sum_{i=0}^{n} g_i I(f_{p,d}, i) && [\texttt{J_eq1 in e_transcendental.lean}] \\
&= \sum_{i=0}^{n} g_i e^i \sum_{j=0}^{(n+1)p-1} f_{p,n}^{(j)}(0) - \sum_{i=0}^{n} g_i \sum_{j=0}^{(n+1)p-1} f_{p,n}^{(j)}(i) && [\texttt{J_eq2 in e_transcendental.lean}] \\
&= 0 - \sum_{i=0}^{n} \sum_{j=0}^{(n+1)p-1} g_i f_{p,n}^{(j)}(i) && [\texttt{J_eq3 in e_transcendental.lean}] \\
&= -\sum_{i=0}^{n} \sum_{j=0}^{(n+1)p-1} g_i f_{p,n}^{(j)}(i) && [\texttt{J_eq in e_transcendental.lean}] \\
&= -\sum_{j=0}^{(n+1)p-1} \sum_{i=0}^{n} g_i f_{p,n}^{(j)}(i) && [\texttt{J_eq'' in e_transcendental.lean}]
\end{aligned}$$

We are going to deduce two contradictory bounds for $J_p(g)$ with a large prime p.

Lower bound

We want to prove that for some $M \in \mathbb{R}$, $J_p(g) = -g_0(p-1)!(-1)^{np}n^p + p!M$ where n is the degree of g. This is `J_eq_final` in `e_transcendental.lean`.

To evaluate the $J_p g$, we will split the big sum $\sum_{j=0}^{(n+1)p-1}$ to three sums: $j < p-1$, $j = p-1$ and $j > p-1$.

Using the notation as above, for any prime p and natural number n, we have the followings :

- If $j < p-1$ then in this case, in fact all the summand is zero. This is because
  - $f_{p,n}^{(j)}(0) = 0$. This is `deriv_f_p_k_eq_zero_k_eq_0_when_j_lt_p_sub_one` in `e_transcendental.lean`
  - $f_{p,n}^{(j)}(i) = 0$ for all $0 < i \leq d$. This is `deriv_f_p_k_eq_zero_k_ge_1_when_j_lt_p_sub_one` in `e_transcendental.lean`

  Thus
  $$\sum_{j=0}^{p-2} \sum_{i=0}^{n} g_i f_{p,n}^{(j)}(i) = 0$$
  This is `J_partial_sum_from_one_to_p_sub_one` in `e_transcendental.lean`.
- If $j = p-1$ then
  - $f_{p,n}^{(j)}(0) = (p-1)!(-1)^{np}n!^p$. This is `deriv_f_p_zero_when_j_eq_p_sub_one` in `e_transcendental.lean`
  - $f_{p,n}^{(j)}(i) = 0$ for all $i > 0$. This is `deriv_f_p_when_j_eq_p_sub_one` in `e_transcendental.lean`

  Thus
  $$\sum_{i=0}^{n} g_i f_{p,n}^{(p-1)}(i) = (p-1)!g_0(-1)^{np}n!^p$$
  This is `J_partial_sum_from_p_sub_one_to_p` in `e_transcendental.lean`.
- If $j > p-1$ then $p!|f_{p,n}^{(j)}(k)$ for all $k = 0, \cdots, n$. This is `when_j_ge_p_k` in `e_transcendental.lean`.

  Then
  $$p!| \sum_{j=p}^{(n+1)p-1} \sum_{i=0}^{n} g_i f_{p,n}^{(j)}(i)$$
  This is `J_partial_sum_rest` in `e_transcendental.lean`

Then if $g \in \mathbb{Z}$ is any polynomial with degree n and coefficient g_i with $g_0 \neq 0$ and e as a root then, from above we can show that there is some $M \in \mathbb{Z}$ such that

$$J_p(g) = -g_0(p-1)!(-1)^{np}n!^p + M \times p!$$

This is `J_eq_final` in `e_transcendental.lean`

So if we choose p to be a prime number such that $p > n$ and $p > |g_0|$, then $|J_p(g)| = (p-1)!\,|-g_0(-1)^{np}n!^p + Mp|$. So $(p-1)! \leq J_p(g)$. Because otherwise $|-g_0(-1)^{np}n!^p + Mp| = 0$. So $p|g_0 n!^p$, then either $p|g_0$ or $p|n!^p$. The first case cannot happen as we chose $p > |g_0|$. The second happens if and only if $p|n!$ but we chose $p > n$. This is basically what happened in `abs_J_lower_bound` in `e_transcendental.lean`

Upper bound

This time we utilize the integral definition of I. For a prime p and $g \in \mathbb{Z}$ is any polynomial with degree n and coefficient g_i and e as a root then. Let us define $M \in \mathbb{R}$ to be

$$(n+1)\left(\max_{0\leq i\leq n}\{|g_i|\}(n+1)e^{n+1}\right)(2(n+1))^{n+1}$$

Then

$$\begin{aligned}
|J_p(g)| &\leq \sum_{i=0}^{n}\left|g_i i e^i \overline{f_{p,n}}(i)\right| && [\texttt{abs_J_ineq1}'' \text{ in } \texttt{e_transcendenta} \\
&\leq (n+1)\max_{0\leq i\leq n}\{|g_i|\}(n+1)e^{n+1}(2(n+1))^{p+pn} && [\texttt{sum_ineq_1} \text{ in } \texttt{e_transcendenta} \\
&\leq (n+1)^p\left(\max_{0\leq i\leq n}\{|g_i|\}\right)^p(n+1)^p\left(e^{n+1}\right)^p(2(n+1))^{p+pn} && [\texttt{sum_ineq_2} \text{ in } \texttt{e_transcendenta} \\
&= M^p && [\texttt{abs_J_upper_bound} \text{ in } \texttt{e_transcendenta}
\end{aligned}$$

The point is for some real number c (independent of p, depending on g), $|J_p(g)| \leq c^p$.

The desired contradiction

We use that for any real number $M \geq 0$ and an integer z then there is a prime number $p > z$ such that $(p-1)! > M^p$ to get a contradiction. This fact is `contradiction` in `e_transcendental.lean`.

Assume e is algebraic and $g \in \mathbb{Z}[X]$ admits e as a root with degree n and coefficient g_i. We can assume $g_0 \neq 0$ by dividing a suitable power of X if necessary. This process is `make_const_term_nonzero` in `e_transcendental.lean`. The fact that after this possible change e is still a root of g is `non_zero_root_same` in `e_transcendental.lean`. Then we know that for some real number c independent of g, we have $(p-1)! \leq J_p(g) \leq c^p$ for all $p > |g_0|$ and $p > d$. But this is not possible by the previous paragraph.