Pade Approximations and the Transcendence of π

Ernie Croot

March 9, 2007

1 Introduction

Lindemann proved the following theorem, which implies that π is transcendental:

Theorem 1 *Suppose that $\alpha_1, ..., \alpha_k$ are non-zero algebraic numbers, and that $\beta_1, ..., \beta_k$ are distinct algebraic numbers. Then,*

$$\alpha_1 e^{\beta_1} + \cdots + \alpha_k e^{\beta_k} \ \neq \ 0.$$

The reason that this implies that π is transcendental is that if π were algebraic, then so is $i\pi$, which would mean

$$0 \ = \ e^{i\pi} + 1 \ \neq \ 0.$$

We will not prove this general result (of Lindemann), but will instead show only that e^α can never equal -1 for any algebraic number α, which proves π is transcendental because $e^{\pi i} = -1$. The proof for the general case uses similar ideas to this special case.

2 The Proof

2.1 The Idea: Pade Approximations

We begin by recalling the standard proof that e is irrational: Suppose e is rational. Then, $n!e$ must be an integer for all n sufficiently large; however,

$$n!e \ = \ I_n + \frac{1}{n+1} + \frac{1}{(n+1)(n+2)} + \frac{1}{(n+1)(n+2)(n+3)} + \cdots,$$

where I_n is the integer

$$2n! + \frac{n!}{2!} + \frac{n!}{3!} + \cdots + 1.$$

It is easy to see that for n sufficiently large, $n!e = I + \delta$, where $\delta \in (0, 1)$, which contradicts the fact that $n!e$ is an integer; so, e must have been irrational.

Actually, what this proof gives us is the even stronger fact that there exists an infinite sequences of integers f_n and g_n tending to infinity, such that

$$f_n e - g_n \ \to \ 0.$$

Indeed, just take $f_n = n!$ and $g_n = I_n$. This brings us to the following basic fact:

Fact. If α is some (possibly complex) number for which there exist sequences of integers $f_n, g_n \to \infty$ such that

$$f_n\alpha - g_n \ \to \ 0, \text{ and } f_n\alpha - g_n \ \neq \ 0,$$

then α is irrational.[1]

To show that e^α, α is a non-zero rational, is irrational we will find such f_n and g_n. First, we begin with the case where α is an integer. If we can show this, then it follows that for any rational a/b we have $e^{a/b}$ is irrational (on taking bth powers).

Our sequence of f_n's and g_n's comes from what are called *Pade approximations* to e^x. Basically, a Pade approximation is a pair of polynomials $f(x)$ and $g(x)$ such that

$$e^x \ \sim \ \frac{f(x)}{g(x)}$$

for x near 0.

There are methods for finding such good pairs f and g, and the simplest is to just use linear algebra. Basically, we try to find $f(x)$ and $g(x)$ of degree n so that the Taylor expansion of

$$g(x)e^x - f(x)$$

[1]The proof is obvious, since if $\alpha = a/b$ were rational, then $|a/b - g_n/f_n| = 0$ or is at least $1/bf_n$. Multiplying through by f_n gives the result.

about $x = 0$ begins

$$c_{2n+1}x^{2n+1} + c_{2n+2}x^{2n+2} + \cdots$$

This uniquely determines f and g up to scalar multiples.

Such g and f can be found using the "pade" command in Maple; for example, Maple gives that in the case where g and f have degree 4,

$$e^x \ \sim \ \frac{1 + \frac{x}{2} + \frac{3x^2}{28} + \frac{x^3}{84} + \frac{x^4}{1680}}{1 - \frac{x}{2} + \frac{3x^2}{28} - \frac{x^3}{84} + \frac{x^4}{1680}}.$$

Notice here that $g(x) = f(-x)$. This follows since if

$$g(x)e^x - f(x)$$

has order of vanishing $2n + 1$ at $x = 0$, then so does

$$e^{-x}(g(x)e^x - f(x)) \ = \ g(x) - e^{-x}f(x).$$

We want to find a nice form for these approximations, and we begin as follows: If $A(x)$ is any polynomial of degree m, then

$$\int_0^x e^{-t}A(t)dt \ = \ \sum_{j=0}^{m} A^{(j)}(0) \ - \ e^{-x}\sum_{j=0}^{m} A^{(j)}(x).$$

An obvious question is whether there are polynomials $A(t) = A(t, x)$ for which these approximations to e^{-x} coincide with the Pade polynomials $f(x)$ and $g(x)$ mentioned above. By trying this for a few small cases (small values of n), one quickly discovers that, yes, in fact letting

$$A(t, x) \ = \ \frac{t^n(t - x)^n}{n!}$$

and letting

$$f(x) \ = \ \sum_{j=0}^{2n} A^{(j)}(x, x), \text{ and } g(x) \ = \ f(-x) \ = \ \sum_{j=0}^{2n} A^{(j)}(0, x), \qquad (1)$$

(the derivatives here are with respect to t), both of which turn out to have degree n, we find that $g(x)/f(x)$ is the Pade approximation to e^{-x} of degree n; and so, $f(x)/g(x)$ is the Pade approximation to e^x of degree n.

We can prove that this choice of $A(t,x)$ indeed gives Pade approximations rather easily: We have that

$$\left| \int_0^x \frac{e^{-x} t^n (t-x)^n}{n!} dx \right| \ < \ \frac{x \cdot x^n \cdot x^n}{n!} \ = \ \frac{x^{2n+1}}{n!}. \tag{2}$$

This upper bound guarantees that the integral has order of vanishing at least $2n+1$ about $x=0$, and thus proves that the integral generates Pade approximations.

Just to check, here is what Maple gives for Pade polynomial approximations of degree 8 for e^{-x}:

$$e^{-x} \ \approx \ \frac{1 - \frac{x}{2} + \frac{7x^2}{60} - \frac{x^3}{60} + \frac{x^4}{624} - \frac{x^5}{9360} + \frac{x^6}{205920} - \frac{x^7}{7207200} + \frac{x^8}{518918400}}{1 + \frac{x}{2} + \frac{7x^2}{60} + \frac{x^3}{60} + \frac{x^4}{624} + \frac{x^5}{9360} + \frac{x^6}{205920} + \frac{x^7}{7207200} + \frac{x^8}{518918400}}. \tag{3}$$

Maple also gives

$$\int_0^x \frac{e^{-t} t^8 (t-x)^8}{8!} dt \ = \ g(x) - e^{-x} f(x),$$

where $f(x) = g(-x)$ and

$$\begin{aligned} f(x) \ = \ & x^8 + 72x^7 + 2520x^6 + 55440x^5 + 831600x^4 + 8648640x^3 \\ & + 60540480x^2 + 259459200x + 518918400. \end{aligned}$$

This polynomial $f(x)$ is the same as the polynomial in the denominator in (3) up to a factor of $518918400 = 16!/8!$.

The advantage to working with this integral formula for the Pade approximations is that it allows us to give easy bounds for how well $g(x)/f(x)$ approximates e^{-x}, as we will see. Before we do this, however, let us first verify that the $f(x)$ and $g(x)$ described in (1) are both in $\mathbb{Z}[x]$: When we sum up $A^{(j)}(t,x)$ over all $j = 0, ..., n$, we get a bunch of terms of the form $cx^i(t-x)^j/n!$. If we set $t = x$, then this term is 0 unless $j = 0$; but, if $j = 0$, then we must have taken n or more derivatives to get that term from

$A(t,x)$, meaning that $n!$ divides c. Similarly, if we set $t=0$, then the term $cx^i(t-x)^j/n!$ is 0 unless $i=0$, which also would mean that $n!$ divides c. So, all the (non-zero) terms of $A(x,x)$ and $A(0,x)$ have integer coefficients, which implies that these polynomials belong to $\mathbb{Z}[x]$.

Now, from the upper bound (2) we find that letting x be a positive integer a, we get non-zero integers f_n and g_n satisfying

$$|f_n e^{-a} - g_n| \ \leq \ \frac{a^{2n+1}}{n!},$$

which can be made arbitrarily small by taking n sufficiently large. The fact that this difference is non-zero also follows from the integral formula:[2] If n even, it is clear that

$$\int_0^x \frac{e^{-t}t^n(t-x)^n}{n!}dt \ > \ 0,$$

and when n is odd this integral is less than 0.

2.2 The Irrationality of π

The Pade estimates in the previous section for e^x hold equally well for purely imaginary numbers $x=i\theta$, where θ is an integer. In this case, we find that

$$|e^{-i\theta}f(i\theta) - g(i\theta)| \ \leq \ \frac{|\theta|^{2n+1}}{n!},$$

where f and g are the degree n Pade approximation polynomials for e^{-x}. Let us see that $g(i\theta)$ is non-zero for all sufficiently large n: We have that $g(x)$ is a sum of successive derivatives (with respect to t) of $A(t,x)=t^n(t-x)^n/n!$ evaluated at 0. Among the terms in this sum there will be only one term which is not divisible by n, and that term is $(-x)^n$. So,

$$g(x) \ \equiv \ (-x)^n \pmod{n}.$$

Therefore, if n is a large number coprime to an integer θ, we will have that

$$g(i\theta) \ \equiv \ (-i\theta)^n \ \not\equiv \ 0 \pmod{n},$$

[2]In the next subsection we will give a different argument for why this difference is nonzero.

which implies $g(i\theta) \neq 0$. Thus, for infinitely many n, $g(i\theta)$ is non-zero. A similar argument shows that

$$f(x) \equiv x^n \pmod{n}.$$

So, if $e^{i\theta} = 1$, then for odd n, we find that

$$e^{i\theta} f(i\theta) - g(i\theta) \equiv 2(i\theta)^n \pmod{n}$$

Thus, if n is a large odd number coprime to θ, this will be non-zero, and it follows that for such n,

$$e^{i\theta} f(i\theta) - g(i\theta) \neq 0.$$

Notice here that this modulo n argument did not help up out at all as far as finding good rational approximations to e^{-x}. It was only needed to show that a certain linear form did not vanish. In the full Lindemann proof something similar is true: One must show that a certain linear form does not vanish, and one uses arithmetic properties of (generalized) Pade polynomials to do this.

Suppose now that $\theta = \pi$ is a rational number. Then, let d be an even number such that $d\pi$ is an integer. Then, the above argument shows that

$$|f(id\pi) - g(id\pi)| < \frac{(d\pi)^{2n+1}}{n!},$$

which means that the left-hand-side must be 0 for n sufficiently large, since it lies in $\mathbb{Z}[i]$. We have reached a a contradiction, and it follows that π is irrational.

2.3 Taking Stock of What We Have

Comment 1. What made our Pade integral proofs work was the that

$$f_n e^{-a} - g_n$$

was small but non-zero. What made this difference small was the fact that we could divide by $n!$ in our definition of $A(t, x)$. What allowed us to divide by $n!$ was that $A(t, x)$ had order of vanishing n at $t = 0$ and $t = x$.

Comment 2. In our proofs we really didn't need an inequality as strong as

$$|f_n e^{-a} - g_n| \ < \ \frac{a^{2n+1}}{n!}.$$

We could prove our irrationality results even where the right-hand-side is as large as $a^{2n+1}/(n!)^{1/k}$, for any fixed positive integer k. So, we have room to breathe as far as generalizing our result.

Comment 3. By modding out $f(x)$ and $g(x)$ by n for certain n, we were able to tell that $f_n e^{-i\theta} - g_n$ was non-zero. Note that this did not help up to find these good approximations f_n and g_n – it was only necessary for showing that the linear form didn't vanish.

2.4 Generalized Pade Approximations

We can generalize the integral representation for Pade approximations, to find approximations at several points $x_1, ..., x_k$ at once. It turns out that if $m > n \geq 1$ are integers, then we have that for $i = 1, ..., k$,

$$e^{x_i} \int_0^{x_i} \frac{e^{-t} t^m (t-x_1)^n (t-x_2)^n \cdots (t-x_k)^n}{n!} dx \ = \ f_i(x_1, ..., x_k) - e^{x_i} g(x_1, ..., x_k),$$

where

$$f_i(x_1, ..., x_k), g(x_1, ..., x_k) \in \mathbb{Z}[x_1, ..., x_k],$$

where g is a symmetric polynomial in $x_1, ..., x_k$. The integral here is taken along any path in the complex plane connecting 0 and x_i.

Notice here that the polynomial g does not depend on the choice of i. This is an incredibly useful fact, because it means that we get a simultaneous approximation

$$e^{x_1} \ \approx \ \frac{f_1(x_1, ..., x_k)}{g(x_1, ..., x_k)}, ... \ , \ e^{x_k} \ \approx \ \frac{f_k(x_1, ..., x_k)}{g(x_1, ..., x_k)},$$

where all the denominators are the same. Moreover, the fact that g is symmetric in $x_1, ..., x_k$ means that if $\alpha_1, ..., \alpha_k$ are all the conjugates of some algebraic number α, then $g(\alpha_1, ..., \alpha_k)$ is a rational.

Let us see that, indeed, g is symmetric in $x_1, ..., x_k$: If we let

$$A(t, x_1, ..., x_k) \ = \ \frac{t^m (t-x_1)^n \cdots (t-x_k)^n}{n!},$$

then we note that

$$g(x_1, ..., x_k) \;=\; \sum_{j=0}^{m+kn} A^{(j)}(0, x_1, ..., x_k), \tag{4}$$

where the derivatives here are with respect to t. Since $A(t, x_1, ..., x_k)$ is symmetric in $x_1, ..., x_k$, it is clear that every term in this sum is too, and it follows that g is symmetric in $x_1, ..., x_k$.

Before closing this subsection, let us see that these polynomials f and g can be made to satisfy certain congruence restrictions that will later enable us to show that certain linear forms don't vanish (as was needed in the proof that π is irrational). If we expand out the right-hand-side of (4) in powers of t, we will get something like this:

$$g(x_1, ..., x_k) \;=\; \cdots \;+\; \left.\frac{ct^{r_0}(t-x_1)^{r_1}\cdots(t-x_k)^{r_k}}{n!}\right|_{t=0} + \cdots, \tag{5}$$

where the constant c is divisible by

$$\frac{m!}{r_0!}\frac{n!}{r_1!}\cdots\frac{n!}{r_k!}.$$

This term will evaluate to 0 unless $r_0 = 0$. So,

$$\frac{m!}{n!} \text{ divides } g(x_1, ..., x_k).$$

We also have that for certain values of n, $g(\alpha_1, ..., \alpha_k) \neq 0$ if $\alpha_1, ..., \alpha_k$ are conjugates of some algebraic number: Even though $m!/n!$ divides $g(x_1, ..., x_k)$, there is exactly one term which is not divisible by $n \cdot m!/n!$, namely the term where $r_1 = \cdots = r_k = n$. This term is

$$\frac{m!(-1)^k(x_1 \cdots x_k)^n}{n!}. \tag{6}$$

For roots $\alpha_1, ..., \alpha_k$ of $u_k x^k + u_{k-1}x^{k-1} + \cdots + u_0 \in \mathbb{Z}[x]$, and n is coprime to u_k, let g be the power of n dividing $m!/n!$. Then, g is the exact power of n dividing the term (6), and n^{g+1} divides all other terms of $g(\alpha_1, ..., \alpha_k)$. Thus,

n^{g+1} does not divide $g(\alpha_1, ..., \alpha_k)$, and it follows that g does not vanish for such n.

Next, we consider

$$f_i(x_1, ..., x_k) \;=\; \cdots \;+\; \left.\frac{ct^{r_0}(t-x_1)^{r_1}\cdots(t-x_k)^{r_k}}{n!}\right|_{t=x_i} \;+\; \cdots$$

The only way that this typical term can be non-zero is if $r_i = 0$, which will mean that c is divisible by $n!$. Such non-zero terms will have

$$\frac{c}{n!} \;=\; \frac{m!}{r_0!}\frac{n!}{r_1!}\cdots\frac{n!}{r_{i-1}!}\frac{n!}{r_{i+1}!}\cdots\frac{n!}{r_k!}.$$

So, all but one of these non-zero terms will have coefficient divisible by m or n; that term is

$$x_i^m(x_i-x_1)^n\cdots(x_i-x_{i-1})^n(x_i-x_{i+1})^n\cdots(x_i-x_k)^n.$$

So, if we were to choose m and n to both be divisible by a large prime p, then

$$f_i(x_1, ..., x_k) \;\equiv\; x_i^m(x_i-x_1)^n\cdots(x_i-x_k)^n \pmod{p}.$$

If we further had $x_1, ..., x_k$ are conjugates of some algebraic number α, and if m and n are divisible by the order of the unit group in $\mathbb{Z}(x_1, ..., x_k)/p$, then, in fact,

$$f_i(x_1, ..., x_k) \;\equiv\; 1 \pmod{p}. \tag{7}$$

2.5 The Transcendence of π

As mentioned earilier, it suffices to show that if α is algebraic, then e^α is not -1.

The obvious first thing to try is to directly apply the idea used to show that $e^{i\theta} \neq 1$: We would get that for certain $f_n(x), g_n(x) \in \mathbb{Z}[x]$,

$$f_n(\alpha)e^{-\alpha} - g_n(\alpha) \;\approx\; 0,\; f_n(\alpha) - g_n(\alpha) \neq 0.$$

The difficulty now is that $f_n(\alpha)$ and $g_n(\alpha)$ are not integers (in general), but are only algebraic numbers.

An natural approach for how to fix this problem (of having algebraic numbers, instead of integers) is to somehow add or multiply through by conjugates of α to produce rationals. But how? Well, it turns out that the following idea works: To show that $e^\alpha \neq -1$, it suffices to show that

$$\prod_{i=1}^{k}(e^{\alpha_i}+1) \;\neq\; 0,$$

where $\alpha_1, ..., \alpha_k$ are the conjugates of α.

If we expand this product out we get

$$1 + (e^{\alpha_1} + \cdots + e^{\alpha_k}) + \cdots + e^{\alpha_1+\cdots+\alpha_k}.$$

We can write this as

$$\beta_0 + \beta_1 e^{\delta_1} + \cdots + \beta_h e^{\delta_h}, \tag{8}$$

where the β_i's are positive integers, and where the δ_i's are distinct non-zero sums of the α_i's; moreover, this sum is symmmetric in the α's when we write the δ_j's in terms of α_i's.

Now we use a simultaneous Pade approximation to these e^{δ_i}'s described in the previous subsection; so, here our Pade approximations take the form

$$e^{\delta_i}\int_0^{\delta_i}\frac{e^{-t}t^m(t-\delta_1)^n\cdots(t-\delta_h)^n}{n!}dt \;=\; f_i(\delta_1,...,\delta_h) - e^{\delta_i}g(\delta_1,...,\delta_h).$$

So, (8) is approximately

$$\beta_0 + \sum_{i=1}^{h}\beta_i\frac{f_i(\delta_1,...,\delta_h)}{g(\delta_1,...,\delta_h)}. \tag{9}$$

The quality of this approximation can be determined by bounding the above integral. It turns out that, applying basic inequalities, we get that (9) differs from (8) by at most

$$\frac{hB(2D)^{m+hn+1}e^{2|D|}}{n!|g(\delta_1,...,\delta_h)|}$$

where

$$D \;=\; \max_{i=1,...,h}|\delta_i|, \text{ and } B \;=\; \max_{i=1,...,h}|\beta_i|.$$

Now suppose that (8) is 0. We know that there is some integer $d \geq 1$ such that $d^n g(\beta_1, ..., \beta_h) \in \mathbb{Z}$ and $d^n f_i(\delta_1, .., \delta_h)$ is an algebraic integer for all i; moreover, we can arrange that $m!/n! | d^n g(\delta_1, ..., \delta_h)$ (recall that $m!/n!$ divides the polynomial $g(x_1, ..., x_h)$). Then, we get that

$$\left| \beta_0 d^n g(\delta_1, ..., \delta_h) + d^n \sum_{i=1}^{h} \beta_i f_i(\delta_1, ..., \delta_h) \right| \ < \ \frac{hB(2dD)^{m+hn+1} e^{2D}}{n!}. \qquad (10)$$

If we have that $m \approx \kappa n$, for some constant κ, then as $n \to \infty$, the right-hand-side of (10) goes to 0, because $n!$ dominates the numerator (it has growth $n^{n(1-o(1))}$, whereas the numerator is only exponential in n).

The left-hand-side of (10) turns out to be an integer, because $d^n g(\delta_1, ..., \delta_h)$ is an integer, and because the remaining sum is symmetric in $\delta_1, ..., \delta_h$ (it takes a little work to see that). If we further had that the left-hand-side of (10) is non-zero, then we would have a contradiction, meaning that $e^\alpha \neq -1$. This is where those congruence conditions we developed in the previous subsection come in: We suppose that m and n are divisible by some large prime number p (determined below), that $m!/n!$ is also divisible by p, and that, further, m and n are divisible by the order of the unit group of $\mathbb{Z}(\delta_1, ..., \delta_h)/p$ so that, as in (7),

$$d^n f_i(\delta_1, ..., \delta_h) \ \equiv \ d^n \ \equiv \ 1 \pmod{p}.$$

In order for this to be possible we need that p does not divide the discriminant of $(x - \delta_1) \cdots (x - \delta_h)$ (recall that $f_i(\delta_1, ..., \delta_h) = (\delta_i - \delta_1) \cdots$). Now, as $p | m!/n! | d^n g(\delta_1, ..., \delta_h)$, we conclude that (after removing the absolute value symbols) the left-hand-side of (10) is congruent modulo p to

$$\beta_1 + \cdots + \beta_h \pmod{p},$$

which is clearly non-zero for p large enough.