Number 2

2.718281828459045235360287471 3 …

The Powerful Power Series for e:

Polynomial vanishing and the transcendence of *e*

2.1 Fourier's proof of Euler's slick result

Here we will investigate several features of one of the most famous and important numbers in mathematics, namely, Leonhard Euler's "*e*." Our journey through this chapter sets the stage for much of what follows in our future explorations. To foreshadow the fundamental strategies to come, we open with Joseph Fourier's 1815 clever proof of Euler's result that *e* is irrational.

THEOREM 2.1 *The number e is irrational.*

> *The intuitive idea behind Fourier's approach*
>
> Fourier's strategy was to assume that e is rational, say $e = \frac{r}{s}$, and then use the alleged denominator s to construct another rational number t/u that is amazingly close to r/s. Thus the difference $\left|\frac{r}{s} - \frac{t}{u}\right|$ is a *positive* rational number. Fourier then showed that this positive number is incredibly small; in fact, if d is the least common multiple of s and u, then $\left|\frac{r}{s} - \frac{t}{u}\right| < \frac{1}{d}$. Thus clearing denominators by multiplying through by d, we discover that the awkward-looking *integer* $\left|d\frac{r}{s} - d\frac{t}{u}\right|$ satisfies
>
> $$0 < \left|d\frac{r}{s} - d\frac{t}{u}\right| < 1,$$
>
> which contradicts the Fundamental Principle of Number Theory. Hence e is irrational.

Proof. As we suggested at the end of the previous chapter, the most important property the number e possesses that allows us to classify it as "special" is its representation as an extremely simple infinite series,

$$e = \sum_{n=0}^{\infty} \frac{1}{n!}.$$

Let us now assume that e is rational, say $e = \frac{r}{s}$, where $s \geq 1$. Using s, we construct an excellent rational approximation to r/s. In particular, we consider the rational number formed by truncating the infinite series for e at $n = s$:

$$\sum_{n=0}^{s} \frac{1}{n!}.$$

It immediately follows that $\frac{r}{s} - \sum_{n=0}^{s} \frac{1}{n!}$ is positive. We can clear denominators and thus produce a positive integer by multiplying both sides by $s!$. In doing so, we see that

$$\begin{aligned} s!\left(\frac{r}{s} - \sum_{n=0}^{s} \frac{1}{n!}\right) &= s!\left(e - \sum_{n=0}^{s} \frac{1}{n!}\right) = s!\left(\sum_{n=0}^{\infty} \frac{1}{n!} - \sum_{n=0}^{s} \frac{1}{n!}\right) \\ &= s!\left(\frac{1}{(s+1)!} + \frac{1}{(s+2)!} + \frac{1}{(s+3)!} + \cdots\right) \\ &= \frac{1}{s+1} + \frac{1}{(s+2)(s+1)} + \frac{1}{(s+3)(s+2)(s+1)} + \cdots \end{aligned} \tag{2.1}$$

is a positive integer. However, since $s \geq 1$, we can bound the positive integer in (2.1) from above by a geometric series:

$$\frac{1}{s+1} + \frac{1}{(s+2)(s+1)} + \frac{1}{(s+3)(s+2)(s+1)} + \cdots < \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \cdots = 1.$$

Thus we have constructed an integer between 0 and 1, which is a direct violation of the Fundamental Principle of Number Theory. Thus we conclude that e is irrational. ■

The key step in the previous argument was the construction of the integer in (2.1) by finding a spectacular rational approximation to the assumed-rational number e and then clearing all denominators by multiplying through by $s!$. In fact, this basic theme can be developed into a proof of the transcendence of e. In order to appreciate the subtleties involved in extending Fourier's basic idea, we first consider a proof of the irrationality of $e^{a/b}$ for any nonzero rational number a/b. While the fundamental strategy used in demonstrating that e is irrational will remain intact in the more general argument, producing a spectacular rational approximation will require a considerable amount of ingenuity. Once we have developed the ideas central to the proof of the irrationality of $e^{a/b}$, we will be well prepared to establish the transcendence of e.

Theorem 2.2 *For any nonzero rational number a/b, the number $e^{a/b}$ is irrational.*

2.2 A first attempt at a proof

We begin by observing that establishing Theorem 2.2 is equivalent to proving that e^a is irrational for positive integers a.

Challenge 2.1 *Prove that if e^m is irrational for all integers $m \geq 1$, then for any nonzero rational number a/b, $e^{a/b}$ is irrational.*

Thus by the challenge, we need to prove that e^a is irrational only for positive integers a. The strategy of our argument is straightforward: We adopt the basic plan of attack used in the proof of the irrationality of e. Unfortunately, as we will quickly discover, the most obvious extension of those ideas fails to actually lead to a proof. However, pursuing that obvious, albeit ill-fated, attempt will illustrate the need for a more elaborate adaptation of the argument and also provide some insight into the subtle refinements to come.

We embark on our star-crossed attempt by viewing e^a as a value of the function e^z expressed as the well-known power series

$$e^z = \sum_{n=0}^{\infty} \frac{z^n}{n!}.$$

Let us suppose that e^a equals the rational number r/s. For any index N, we can approximate r/s by $\sum_{n=0}^{N-1} \frac{a^n}{n!}$ and thus see that their difference

$$\frac{r}{s} - \sum_{n=0}^{N-1} \frac{a^n}{n!} = \sum_{n=0}^{\infty} \frac{a^n}{n!} - \sum_{n=0}^{N-1} \frac{a^n}{n!} = \sum_{n=N}^{\infty} \frac{a^n}{n!}$$

is a positive *rational* number. We now wish to estimate this difference.

Challenge 2.2 *Make a change in variables in the indices of the series above to verify the identity*

$$\frac{r}{s} - \sum_{n=0}^{N-1} \frac{a^n}{n!} = \frac{a^N}{N!} \sum_{n=0}^{\infty} \frac{N!a^n}{(N+n)!}. \tag{2.2}$$

The reason for the inclusion of the seemingly superfluous factor $N!$ in both the numerator and denominator of the series in (2.2) is that it allows us to produce a simple and clean upper bound. In particular, since $\frac{(N+n)!}{N!n!}$ is the binomial coefficient $\binom{N+n}{n}$, it is a *positive integer*. Therefore, $1 \leq \frac{(N+n)!}{N!n!}$, and hence we have

$$\frac{N!}{(N+n)!} \leq \frac{1}{n!}. \tag{2.3}$$

In view of this inequality, identity (2.2), and the power series expansion for e^a, we conclude that

$$0 < \frac{r}{s} - \sum_{n=0}^{N-1} \frac{a^n}{n!} \leq \frac{a^N}{N!} e^a.$$

Multiplying the previous inequality by $s(N-1)!$ clears all the denominators of $\frac{r}{s} - \sum_{n=0}^{N-1} \frac{a^n}{n!}$ and yields

$$0 < s(N-1)! \left(\frac{r}{s} - \sum_{n=0}^{N-1} \frac{a^n}{n!} \right) \leq se^a \left(\frac{a^N}{N} \right), \tag{2.4}$$

where the awkward-appearing quantity $s(N-1)! \left(\frac{r}{s} - \sum_{n=0}^{N-1} \frac{a^n}{n!} \right)$ is an *integer*. We recall that the index N is a free parameter. In the special case $a = 1$, we see that for all sufficiently large N, the upper bound in (2.4) is less than 1, and thus we contradict the Fundamental Principle of Number Theory. Hence this argument allows us to conclude—yet again—that e is irrational. In view of Theorem 2.1, however, this conclusion is nothing new.

In the more interesting case $a \neq 1$, if we could select an N such that the upper bound in (2.4) is less than 1, then we would again arrive at a contradiction and would have the irrationality of e^a in the palms of our hands. Unfortunately, by applying inequality (2.4), the irrationality slips through our fingers, since there is no value of N for which the upper bound in (2.4) is less than 1 for $a \neq 1$. Thus, as we cautioned at the opening, this approach fails to yield the desired result.

We now look ahead and foreshadow an improved version of the crucial inequality (2.4). Suppose that we could construct an integer $\mathcal{I}$ satisfying an inequality of the basic shape

$$0 < \mathcal{I} \leq (\text{some constant}) \times \left(\frac{a^N}{(N-1)!} \right) \tag{2.5}$$

(note the appearance of the factorial in the denominator!). Then as N approaches infinity, the upper bound in (2.5) would approach 0, and hence for all sufficiently large choices of N, this new upper bound would indeed be less than 1, and we would have our much sought-after contradiction. This observation is a clue as to how to modify our failed attempt. We desire a rational approximation that is so close to the assumed-rational number e^a that their difference, after clearing denominators, gives rise to a positive integer less than 1. Basically, we require an *improved* rational approximation to e^a.

The intuitive idea for the refinement of the argument

In our first attempt, we obtained a rational approximation to e^a by truncating the power series after N terms to obtain a polynomial, and then evaluating that polynomial at a. That is, we wrote

$$e^z = \sum_{n=0}^{N-1} \frac{z^n}{n!} + \sum_{n=N}^{\infty} \frac{z^n}{n!}$$

and took the first sum to be the approximating polynomial. In particular, if we let $\mathcal{P}(z) = \sum_{n=0}^{N-1} \frac{z^n}{n!}$, then the natural rational approximation we considered was $\mathcal{P}(a)$.

Unfortunately, simply truncating the power series for e^z does not lead to a sufficiently good rational approximation. The fundamental problem with the truncation strategy is that it leads to a polynomial $\mathcal{P}(z)$ that approximates the function e^z reasonably well for *all* z. In fact, we only require an approximation at the particular value $z = a$; but that particular approximation should be an incredibly good one.

Our new point of attack is to find a polynomial that is an amazingly good approximation to e^z at the point $z = a$, but that is not necessarily any better than the previous truncation attempt for other values of z. The basic idea is to split the polynomial $\mathcal{P}(z)$ into two terms and write

$$e^z = \left(\sum_{n=0}^{N-p} \frac{z^n}{n!} + \sum_{n=N-p+1}^{N-1} \frac{z^n}{n!} \right) + \sum_{n=N}^{\infty} \frac{z^n}{n!}. \tag{2.6}$$

If the second polynomial term, $\sum_{n=N-p+1}^{N-1} \frac{z^n}{n!}$, in the previous expression were to vanish at $z = a$, then the first polynomial $\sum_{n=0}^{N-p} \frac{z^n}{n!}$ would give rise to an *amazing* rational approximation to e^z at $z = a$, which, in turn, would allow us to deduce an inequality of the form (2.5). Unfortunately, it is abundantly clear that the middle term $\sum_{n=N-p+1}^{N-1} \frac{z^n}{n!}$ will never vanish at $z = a$.

Since N is a free variable, we can decompose e^z into three terms as in (2.6) for different values of N, say for example, $N_1, N_2, \ldots, N_L$. In this case we would have L different "middle term" polynomials:

$$\sum_{n=N_1-p+1}^{N_1-1} \frac{z^n}{n!}, \sum_{n=N_2-p+1}^{N_2-1} \frac{z^n}{n!}, \ldots, \sum_{n=N_L-p+1}^{N_L-1} \frac{z^n}{n!}.$$

Of course, none of those polynomials vanish at $z = a$. However, perhaps we could string them all together as a linear combination so as to create a *new* polynomial that *would* vanish at our desired point.

Continued

To illustrate this possibility, let us consider the polynomials z^3, z^2, z, together with the constant polynomial 1. Certainly none of these vanish at $z = a$. However, if we consider the linear combination of these polynomials

$$f(z) = z^3 - (1 + a)z^2 + (1 + a)z - (a)1,$$

then we immediately see that

$$f(a) = a^3 - a^3 - a^2 + a^2 + a - a = 0,$$

and hence we have combined our original polynomials to construct a new polynomial that *does* vanish at $z = a$.

Inspired by the previous illustration, we wonder whether it is possible to find indices $N_1, N_2, \ldots, N_L$ and integer coefficients $k_{N_1}, k_{N_2}, \ldots, k_{N_L}$, not all zero, such that if we were to decompose e^z into three terms as in (2.6) for each $N_1, N_2, \ldots, N_L$ and consider the linear combination

$$\sum_{\ell=1}^{L} \left(k_{N_\ell} e^z\right) = \sum_{\ell=1}^{L} \left(k_{N_\ell} \sum_{n=0}^{N_\ell - p} \frac{z^n}{n!}\right) + \sum_{\ell=1}^{L} \left(k_{N_\ell} \sum_{n=N_\ell-p+1}^{N_\ell - 1} \frac{z^n}{n!}\right) + \sum_{\ell=1}^{L} \left(k_{N_\ell} \sum_{n=N_\ell}^{\infty} \frac{z^n}{n!}\right), \tag{2.7}$$

then the combined "middle term" polynomial $\sum_{\ell=1}^{L} \left(k_{N_\ell} \sum_{n=N_\ell-p+1}^{N_\ell-1} \frac{z^n}{n!}\right)$ would vanish at $z = a$. This strategy is precisely the approach that eventually leads to success. Our challenge at hand is now clear: Discover how to construct that linear combination.

2.3 The classic vanishing polynomial trick

We wish to find a polynomial of the form

$$\sum_{\ell=1}^{L} \left(k_{N_\ell} \sum_{n=N_\ell-p+1}^{N_\ell-1} \frac{z^n}{n!}\right) \tag{2.8}$$

that vanishes at $z = a$. Such a polynomial will give rise to an amazing rational approximation to κe^a, for some nonzero integer κ; which, in turn, will allow us to construct an integer less than 1. However, the polynomial in (2.8) must possess some additional structure in order to allow us to conclude that our integer is also positive and therefore contradicts the Fundamental Principle of Number Theory. How do we build a polynomial having the shape of (2.8)? The answer is that we can start with just about any polynomial we wish. To illustrate this vague claim, let us consider the generic polynomial

$$f(z) = c_6 z^6 + c_5 z^5 + c_4 z^4 + c_3 z^3 = \sum_{N=3}^{6} c_N z^N$$

and notice that if we sum its first three derivatives, $f^{(1)}(z) + f^{(2)}(z) + f^{(3)}(z)$, then we have

$$\begin{aligned} f^{(1)}(z) + f^{(2)}(z) + f^{(3)}(z) = \quad & 6c_6 z^5 + \ 5c_5 z^4 + \ 4c_4 z^3 + 3c_3 z^2 \\ + \ & 30c_6 z^4 + 20c_5 z^3 + 12c_4 z^2 + 6c_3 z \\ + \ & 120c_6 z^3 + 60c_5 z^2 + 24c_4 z \ + 6c_3. \end{aligned}$$

If we now factor out the factoral $N!$ from those terms possessing the coefficient c_N, then we are faced with an expression that has an uncanny resemblance to (2.8):

$$\begin{aligned} \sum_{n=1}^{3} f^{(n)}(z) &= \sum_{N=3}^{6} N c_N z^{N-1} + \sum_{N=3}^{6} N(N-1) c_N z^{N-2} \\ &\quad + \sum_{N=3}^{6} N(N-1)(N-2) c_N z^{N-3} \\ &= \sum_{N=3}^{6} N! c_N \left(\frac{z^{N-1}}{(N-1)!} + \frac{z^{N-2}}{(N-2)!} + \frac{z^{N-3}}{(N-3)!} \right) \\ &= \sum_{N=3}^{6} \left(N! c_N \sum_{n=N-3}^{N-1} \frac{z^n}{n!} \right). \end{aligned}$$

Hence we discover that when we sum the appropriate derivatives of the polynomial $f(z)$, we magically arrive at an expression of the form (2.8). This observation can be generalized as follows.

Challenge 2.3 *For integers j and k satisfying $1 \le j \le k$, let $f(z)$ be the polynomial defined by $f(z) = \sum_{n=j}^{k} c_n z^n$. Show that*

$$\sum_{n=1}^{j} f^{(n)}(z) = \sum_{N=j}^{k} \left(N! c_N \sum_{n=N-j}^{N-1} \frac{z^n}{n!} \right).$$

Thus conclude that for any polynomial $f(z)$ having a factor of z^j, for some $j \ge 1$, the sum of its first j derivatives can be expressed in the form (2.8).

The only way a polynomial with integer coefficients can vanish at $z = a$ is for it to have $(z - a)$ as a factor. So one scheme to create a polynomial of the form (2.8) that also vanishes at $z = a$ is to begin with an auxiliary polynomial $f(z)$ that has both a factor of z^j and a factor of $(z-a)^m$. The factor z^j allows us to apply the result from Challenge 2.3, and for a sufficiently large choice of m, the polynomials $f^{(n)}(z)$, for $n = 1, 2, \ldots, j$, will all vanish at $z = a$. Thus we require that the exponent m be greater than the exponent j. These remarks lead us to conclude that a natural choice for $f(z)$ is a polynomial of the form $z^j(z-a)^{j+1}$, for some integer $j \geq 1$.

Challenge 2.4 *Let $f(z) = z^j(z-a)^{j+1}$, for some integer $j \geq 1$, and write it as $f(z) = \sum_{n=j}^{2j+1} c_n z^n$. Show*

$$\sum_{n=1}^{j} f^{(n)}(a) = 0.$$

After studying Challenges 2.3 and 2.4 together with identity (2.6), we find that we should take $j = p-1$ and select our indices appearing in (2.7) to be $N_1 = p-1$, $N_2 = p, N_3 = p+1, \ldots, N_L = 2p-1$. Thus we are led to consider the polynomial

$$f(z) = z^{p-1}(z-a)^p.$$

2.4 The first part of the proof of Theorem 2.2—The elusive estimate

As we remarked earlier, it is enough to prove that e^a is irrational for positive integers a. We now assume that e^a is a rational number, say $e^a = \frac{r}{s}$. Thus we have that

$$\frac{r}{s} = e^a = \sum_{n=0}^{\infty} \frac{a^n}{n!} = \sum_{n=0}^{N-p} \frac{a^n}{n!} + \sum_{n=N-p+1}^{N-1} \frac{a^n}{n!} + \sum_{n=N}^{\infty} \frac{a^n}{n!},$$

for any integers N and p. Next we write the polynomial $f(z) = z^{p-1}(z-a)^p$ as $f(z) = \sum_{n=p-1}^{2p-1} c_n z^n \in \mathbb{Z}[z]$. Thus, given Challenge 2.3, if we consider the linear combination

$$\sum_{N=p-1}^{2p-1} N!c_N \frac{r}{s} = \sum_{N=p-1}^{2p-1} N!c_N e^a = \sum_{N=p-1}^{2p-1} \left(N!c_N \sum_{n=0}^{N-p} \frac{a^n}{n!} \right)$$
$$+ \sum_{N=p-1}^{2p-1} \left(N!c_N \sum_{n=N-p+1}^{N-1} \frac{a^n}{n!} \right) + \sum_{N=p-1}^{2p-1} \left(N!c_N \sum_{n=N}^{\infty} \frac{a^n}{n!} \right),$$

then we conclude that the middle term appearing on the right-hand side is a sum of derivatives of $f(z)$ evaluated at a. Specifically, in view of Challenges 2.3 and 2.4, that middle term $\sum_{N=p-1}^{2p-1} \left(N!c_N \sum_{n=N-p+1}^{N-1} \frac{a^n}{n!} \right)$ equals 0, and hence the previous identity can be expressed simply as

$$\frac{r}{s} \sum_{N=p-1}^{2p-1} N!c_N = \sum_{N=p-1}^{2p-1} \left(N!c_N \sum_{n=0}^{N-p} \frac{a^n}{n!} \right) + \sum_{N=p-1}^{2p-1} \left(N!c_N \sum_{n=N}^{\infty} \frac{a^n}{n!} \right). \tag{2.9}$$

We now define the polynomial approximation $\mathcal{P}_p(z)$ and the tail of the series $\mathcal{T}_p(z)$ by

$$\mathcal{P}_p(z) = \sum_{N=p-1}^{2p-1} \left(N! c_N \sum_{n=0}^{N-p} \frac{z^n}{n!} \right) \quad \text{and} \quad \mathcal{T}_p(z) = \sum_{N=p-1}^{2p-1} \left(N! c_N \sum_{n=N}^{\infty} \frac{z^n}{n!} \right),$$

where we remark that for $N = p - 1$, the inner sum in $\mathcal{P}_p(z)$ is empty and thus equals 0. Hence we observe that each coefficient of $\mathcal{P}_p(z)$ is divisible by p. We can now rewrite (2.9) as

$$\frac{r}{s} \sum_{N=p-1}^{2p-1} N! c_N = \mathcal{P}_p(a) + \mathcal{T}_p(a),$$

which immediately implies

$$\left| \frac{r}{s} \sum_{N=p-1}^{2p-1} N! c_N - \mathcal{P}_p(a) \right| = \left| \mathcal{T}_p(a) \right|.$$

In order to produce an upper bound for the quantity $|\mathcal{T}_p(a)|$, we note that after the change of variables $m = n - N$, we have

$$\mathcal{T}_p(a) = \sum_{N=p-1}^{2p-1} \left(c_N \sum_{m=0}^{\infty} \frac{N!}{(m+N)!} a^{m+N} \right).$$

By inequality (2.3), we recall that $\frac{N!}{(m+N)!} \leq \frac{1}{m!}$, which together with the triangle inequality, the power series expansion for e^a, and the assumption that $a \geq 1$ reveals that

$$\begin{aligned}
\left| \mathcal{T}_p(a) \right| &\leq \sum_{N=p-1}^{2p-1} |c_N| a^N \sum_{m=0}^{\infty} \frac{a^m}{m!} \\
&\leq \sum_{N=p-1}^{2p-1} |c_N| a^{2p-1} \sum_{m=0}^{\infty} \frac{a^m}{m!} \\
&= e^a a^{2p-1} \sum_{N=p-1}^{2p-1} |c_N|. \qquad (2.10)
\end{aligned}$$

Challenge 2.5 *Recall that* $f(z) = z^{p-1}(z-a)^p = \sum_{N=p-1}^{2p-1} c_N z^N$, *where* a *is a positive integer. Apply the Binomial Theorem to show that*

$$f(z) = \sum_{\ell=0}^{p} \binom{p}{\ell} (-a)^{p-\ell} z^{\ell+p-1},$$

and then take $z = -1$ to conclude that

$$\sum_{N=p-1}^{2p-1} |c_N| = (1+a)^p.$$

In view of the bound in (2.10) and Challenge 2.5 we see that

$$\left|\mathcal{T}_p(a)\right| \le e^a a^{2p-1}(1+a)^p.$$

Thus if we define the constants $K_1 = \frac{1}{a}e^a$ and $K_2 = a^2(1+a)$, then we obtain the now-not-so elusive estimate we desire:

$$\left|\frac{r}{s}\sum_{N=p-1}^{2p-1} N!c_N - \mathcal{P}_p(a)\right| = \left|\mathcal{T}_p(a)\right| \le K_1(K_2)^p. \tag{2.11}$$

2.5 The dramatic conclusion of the proof Theorem 2.2—Arithmetic conquers all

We are finally in position to construct the infamous integer that will contradict the Fundamental Principle of Number Theory. That integer is inspired by the quantity bounded by inequality (2.11). If we multiply inequality (2.11) by s, we then see that

$$\left|r\sum_{N=p-1}^{2p-1} N!c_N - s\mathcal{P}_p(a)\right| \le sK_1(K_2)^p. \tag{2.12}$$

Challenge 2.6 *Prove that $r\sum_{N=p-1}^{2p-1} N!c_N - s\mathcal{P}_p(a)$ is an integer.*

In fact, we can actually deduce some divisibility properties for the integer in Challenge 2.6 that will allow us to divide both sides of (2.12) by an appropriate integer in order to obtain an integer whose absolute value is less than 1. We will then show that this integer is nonzero.

Challenge 2.7 *Prove that $(p-1)!$ is a factor of both the integer $r\sum_{N=p-1}^{2p-1} N!c_N$ and the integer $s\mathcal{P}_p(a)$, and therefore is a factor of their difference.*

Thus if we divide inequality (2.12) by $(p-1)!$, then we have

$$\left|\frac{r}{(p-1)!}\sum_{N=p-1}^{2p-1} N!c_N - \frac{s}{(p-1)!}\mathcal{P}_p(a)\right| \le sK_1\frac{K_2^p}{(p-1)!}, \tag{2.13}$$

where the unwieldy quantity

$$\frac{r}{(p-1)!}\sum_{N=p-1}^{2p-1} N!c_N - \frac{s}{(p-1)!}\mathcal{P}_p(a)$$

is an *integer*. It is certainly worth taking a moment to catch our breath and appreciate how far we have journeyed. In particular, notice how closely the previous inequality resembles the upper bound of (2.5), which up until this moment has been only a fantasy.

Our mission now is clear: We need to show that the unwieldy integer in (2.13) is, in fact, *nonzero*. Fortunately, we have a degree of freedom at our disposal that will assist us in our mission—the parameter p. We now will select p to be any *prime* number satisfying $p > \max\{a, r\}$, so we are certain that p will not divide either a or r.

Challenge 2.8 *Prove that for our choice of p given above,*

$$\frac{r}{(p-1)!}\sum_{N=p-1}^{2p-1} N!c_N \not\equiv 0 \bmod p,$$

while

$$\frac{s}{(p-1)!}\mathcal{P}_p(a) \equiv 0 \bmod p.$$

(*Hint: We remark that $c_{p-1} \neq 0$, since in view of the definition of $f(z)$, $|c_{p-1}| = |a^p| \neq 0$.*)

From Challenge 2.8, we conclude that the integer

$$\frac{r}{(p-1)!}\sum_{N=p-1}^{2p-1} N!c_N - \frac{s}{(p-1)!}\mathcal{P}_p(a)$$

is not congruent to 0 modulo p, and thus must be a *nonzero* integer. Putting this observation together with inequality (2.13), we discover that our unwieldy integer satisfies

$$0 < \left|\frac{r}{(p-1)!}\sum_{N=p-1}^{2p-1} N!c_N - \frac{s}{(p-1)!}\mathcal{P}_p(a)\right| \leq sK_1\frac{K_2^p}{(p-1)!}.$$

If we now let the prime number p approach infinity, we see that our upper bound will eventually be less than 1, and thus our unwieldy integer clashes head-on with the Fundamental Principle of Number Theory. This contradiction implies that our assumption that e^a is rational is false. Thus we have established the irrationality of e^a and hence by Challenge 2.1, the irrationality of $e^{a/b}$ for nonzero rational numbers a/b.

2.6 The transcendence of *e*

The previous argument was certainly elaborate and delicate. Some exhausted readers may exclaim, "All that effort just to show the *irrationality* of $e^{a/b}$!" Happily, those readers will now become reinvigorated as we discover that the circle of ideas we have just developed in the previous argument can be quickly adapted and applied to establish the *transcendence* of e.

THEOREM 2.3 *The number e is transcendental.*

Proof. We begin by assuming that e is algebraic. Thus there exist integers $r_0, r_1, \ldots, r_d$, with $r_d \neq 0$, such that

$$r_0 + r_1 e + r_2 e^2 + \cdots + r_d e^d = 0 \tag{2.14}$$

In our demonstration of the irrationality of e^a, we assumed that $r - se^a = 0$ and then found a polynomial $\mathcal{P}_p(z)$ such that $\mathcal{P}_p(a)$ is an amazing approximation to e^a. Thus if we wish to follow the same line of attack in the present context, we must construct a polynomial $\mathcal{P}_p(z)$ such that $\mathcal{P}_p(1), \mathcal{P}_p(2), \ldots, \mathcal{P}_p(d)$ provide amazing rational approximations to $e, e^2, \ldots, e^d$, respectively. Inspired by our previous work, we immediately consider

$$f(z) = z^{p-1}(z-1)^p(z-2)^p \cdots (z-d)^p,$$

which we write as $f(z) = \sum_{n=p-1}^{(d+1)p-1} c_n z^n$. Applying Challenge 2.3, we find that

$$\sum_{n=1}^{p-1} f^{(n)}(z) = \sum_{N=p-1}^{(d+1)p-1} \left(N! c_N \sum_{n=N-p+1}^{N-1} \frac{z^n}{n!} \right).$$

Challenge 2.9 *Given $f(z)$ as defined above, show that*

$$\sum_{n=1}^{p-1} f^{(n)}(t) = 0,$$

for $t = 1, 2, \ldots, d$.

Just as in our earlier argument, here we now use the coefficients of the polynomial $f(z)$ to produce the following particularly advantageous linear combination

$$\begin{aligned}\sum_{N=p-1}^{(d+1)p-1} N! c_N e^z = &\sum_{N=p-1}^{(d+1)p-1} \left(N! c_N \sum_{n=0}^{N-p} \frac{z^n}{n!} \right) \\ &+ \sum_{N=p-1}^{(d+1)p-1} \left(N! c_N \sum_{n=N-p+1}^{N-1} \frac{z^n}{n!} \right) + \sum_{N=p-1}^{(d+1)p-1} \left(N! c_N \sum_{n=N}^{\infty} \frac{z^n}{n!} \right).\end{aligned}$$

By Challenge 2.9, we see that for $t = 1, 2, \ldots, d$, the middle sum vanishes, and so we have

$$e^t \sum_{N=p-1}^{(d+1)p-1} N!c_N = \sum_{N=p-1}^{(d+1)p-1} \left(N!c_N \sum_{n=0}^{N-p} \frac{t^n}{n!} \right) + \sum_{N=p-1}^{(d+1)p-1} \left(N!c_N \sum_{n=N}^{\infty} \frac{t^n}{n!} \right),$$

which, as before, we write as a polynomial term plus a tail term:

$$e^t \sum_{N=p-1}^{(d+1)p-1} N!c_N = \mathcal{P}_p(t) + \mathcal{T}_p(t). \tag{2.15}$$

Arguing as we did in (2.10), we conclude that for $t = 1, 2, \ldots, d$,

$$|\mathcal{T}_p(t)| \leq e^t t^{(d+1)p-1} \sum_{N=p-1}^{(d+1)p-1} |c_N|. \tag{2.16}$$

Our (or, more accurately, your) next challenge is to provide an upper bound for the sum in (2.16).

Challenge 2.10 *Given that* $(z-t)^p = \sum_{n=0}^{p} \binom{p}{n} (-t)^{p-n} z^n$, *show that*

$$\max_{n=0,1,\ldots,p} \left\{ \left| \binom{p}{n} (-t)^{p-n} \right| \right\} \leq t^p \sum_{n=0}^{p} \binom{p}{n} = (2t)^p.$$

Recalling that $z^{p-1}(z-1)^p(z-2)^p \cdots (z-d)^p = \sum_{n=p-1}^{(d+1)p-1} c_n z^n$, *use the previous inequality to conclude that*

$$|c_n| \leq \prod_{t=1}^{d} (2t)^p \leq ((2d)^d)^p. \tag{2.17}$$

Combining inequalities (2.16) and (2.17), together with the observation that the number of coefficients c_n is $dp + 1$, yields

$$|\mathcal{T}_p(t)| \leq e^t t^{(d+1)p-1} (dp+1)((2d)^d)^p \leq e^t t^{(d+1)p-1} d^p ((2d)^d)^p,$$

which, for $1 \leq t \leq d$, implies

$$|\mathcal{T}_p(t)| \leq e^d d^{(d+2)p-1} ((2d)^d)^p = K_1 (K_2)^p, \tag{2.18}$$

where the constants K_1 and K_2 are defined by $K_1 = e^d/d$ and $K_2 = d^2(2d^2)^d$. In view of identities (2.14) and (2.15), together with the observation that $\mathcal{T}_p(0) = 0$, we have that

$$\begin{aligned} r_0\mathcal{P}_p(0) + r_1\mathcal{P}_p(1) + r_2\mathcal{P}_p(2) + \cdots + r_d\mathcal{P}_p(d) \\ &= -r_0\mathcal{T}_p(0) - r_1\mathcal{T}_p(1) - \cdots - r_d\mathcal{T}_p(d) \\ &= -r_1\mathcal{T}_p(1) - r_2\mathcal{T}_p(2) - \cdots - r_d\mathcal{T}_p(d). \end{aligned}$$

Dividing the previous equality by $(p-1)!$ and then applying inequality (2.18) yields

$$\begin{aligned}\left|\frac{r_0}{(p-1)!}\mathcal{P}_p(0)+\sum_{t=1}^{d}\frac{r_t}{(p-1)!}\mathcal{P}_p(t)\right| &= \left|\sum_{t=1}^{d}\frac{r_t}{(p-1)!}\mathcal{T}_p(t)\right| \\ &\le K_1\left(\sum_{t=1}^{d}|r_t|\right)\frac{(K_2)^p}{(p-1)!}. \qquad (2.19)\end{aligned}$$

Challenge 2.11 *Adopting the ideas used in Challenge 2.8, prove that for all sufficiently large prime numbers p,*

$$\frac{r_0}{(p-1)!}\mathcal{P}_p(0)+\sum_{t=1}^{d}\frac{r_t}{(p-1)!}\mathcal{P}_p(t)$$

is a nonzero integer.

So for all sufficiently large prime numbers p, inequality (2.19) violates the Fundamental Principle of Number Theory, and thus we have arrived at a contradiction. Hence e is not algebraic and therefore is, in fact, transcendental. ∎

2.7 Foreshadowing algebraic exponents—The irrationality of $e^{\sqrt{n}}$ and π

In order to inspire the themes we will develop in the next chapter, where we establish the transcendence of e^{α} for nonzero algebraic numbers α, we close our discussion here by considering numbers of the form $e^{\sqrt{a/b}}$, where a/b is a nonzero rational number, and discovering how to modify the arguments of this chapter in order to demonstrate the irrationality of $e^{\sqrt{a/b}}$.

Theorem 2.4 *Let a/b be a nonzero rational number. Then $e^{\sqrt{a/b}}$ is irrational.*

Before considering the proof of this theorem, we pause momentarily to acknowledge and appreciate an immediate, but enormous, consequence.

Corollary 2.5 *The number π is irrational.*

Proof. Suppose that π is a rational number, say $\pi = \frac{c}{d}$. Then by Theorem 2.4 we see that $e^{\sqrt{-c^2/d^2}}$ is irrational. However, in view of one of the most famous identities in mathematics, we have

$$e^{\sqrt{-c^2/d^2}} = e^{(\sqrt{-1}\,)(c/d)} = e^{i\pi} = -1.$$

Thus we are forced to conclude that -1 is an irrational number, which happens to be utterly false. Hence π is indeed irrational. ∎

Proof of Theorem 2.4. Let a/b be a nonzero rational number and let $\alpha = \sqrt{a/b}$. We wish to prove that e^{α} is irrational, so we assume that e^{α} is rational, say $e^{\alpha} = \frac{r}{s}$. Thus we have that

$$r - se^{\alpha} = 0. \tag{2.20}$$

As in our previous arguments, we wish to replace e^{α} by a polynomial approximation $\mathcal{P}(\alpha)$, where $\mathcal{P}(z) \in \mathbb{Z}[z]$, and use it to construct an integer violating the Fundamental Principle of Number Theory. The immediate difficulty with this approach is that if $\mathcal{P}(z)$ is a polynomial with integral coefficients, then $\mathcal{P}(\alpha)$ is an algebraic number, but not necessarily an integer or even a rational number.

To make this crucial point concrete, let us consider the polynomial $\mathcal{P}(z) = z^3 - 4z^2 + 5z + 3$ and notice that $\mathcal{P}(\sqrt{2}\,) = -5 + 7\sqrt{2}$, which is certainly not a rational number and thus would not lead us, in any immediate manner, to an integer that would contradict the Fundamental Principle of Number Theory. However, let us notice that if we evaluate that same polynomial at the conjugate of $\sqrt{2}$, namely $-\sqrt{2}$, then we have $\mathcal{P}(-\sqrt{2}\,) = -5 - 7\sqrt{2}$. While that value is also irrational, we see an interesting phenomenon:

$$\mathcal{P}(\sqrt{2}\,) + \mathcal{P}(-\sqrt{2}\,) = -10,$$

that is, the sum of these values yields an integer. This simple observation inspires us to bring the conjugate of α into the approximation picture in the hope of producing our impossible integer. Indeed, the specific result we require is given by the following challenge.

Challenge 2.12 *Suppose that $\mathcal{P}(z) \in \mathbb{Z}[z]$ has degree d. Then show that $\mathcal{P}(\sqrt{a/b}\,) + \mathcal{P}(-\sqrt{a/b}\,)$ is a rational number and can be written having a denominator equal to b^d.*

The symmetry introduced by considering both α and its conjugate is the critical new step that allows us to move forward. Thus, rather than considering the now unbalanced-looking quantity in (2.20), we consider the more symmetrically appealing identity $(r - se^{\alpha})(r - se^{-\alpha}) = 0$, which gives rise to

$$(s^2 + r^2) - rs(e^{\alpha} + e^{-\alpha}) = 0. \tag{2.21}$$

Next we construct a polynomial, $\mathcal{P}_p(z) \in \mathbb{Z}[z]$, that simultaneously provides a good approximation to *both* e^{α} and $e^{-\alpha}$. Toward this end, we proceed precisely as in our previous arguments by defining $f(z)$ to be

$$f(z) = b^p z^{p-1}(z - \alpha)^p (z + \alpha)^p = z^{p-1}(bz^2 - a)^p \in \mathbb{Z}[z], \tag{2.22}$$

which, as before, we write as $f(z) = \sum_{n=p-1}^{3p-1} c_n z^n$.

We now proceed exactly as we did in the proof of the transcendence of e. Specifically, we apply the polynomial approximation formed by the appropriate linear combinations to the identity in (2.21) to conclude that

$$\left|\frac{s^2+r^2}{(p-1)!}\mathcal{P}_p(0)-\frac{rs}{(p-1)!}(\mathcal{P}_p(\alpha)+\mathcal{P}_p(-\alpha))\right|=\left|\frac{rs}{(p-1)!}(\mathcal{T}_p(\alpha)+\mathcal{T}_p(-\alpha))\right|, \tag{2.23}$$

where the polynomial $\mathcal{P}_p(z)$ and the tail $\mathcal{T}_p(z)$ are as they were defined in the proof of the transcendence of e.

We are now ready to utilize the quantity

$$\frac{s^2+r^2}{(p-1)!}\mathcal{P}_p(0)-\frac{rs}{(p-1)!}(\mathcal{P}_p(\alpha)+\mathcal{P}_p(-\alpha))$$

to construct our nonzero integer. As we have seen in our previous argument, the first term is an integer, but now the second term involves the irrational number α. However, here is where we exploit the symmetry we introduced through the use of the conjugate of α. Specifically, we first notice that by definition of $\mathcal{P}_p(z)$, $\frac{1}{(p-1)!}\mathcal{P}_p(z)$ has integer coefficients. Thus, in view of Challenge 2.12, we could clear denominators and conclude that

$$\frac{b^{3p-1}(s^2+r^2)}{(p-1)!}\mathcal{P}_p(0)-\frac{b^{3p-1}rs}{(p-1)!}(\mathcal{P}_p(\alpha)+\mathcal{P}_p(-\alpha))$$

is an *integer*. The fact that this integer is nonzero follows from the identical argument given in the proof of the transcendence of e. Thus identity (2.23) can be rewritten as

$$\left|\frac{b^{3p-1}(s^2+r^2)}{(p-1)!}\mathcal{P}_p(0)-\frac{b^{3p-1}rs}{(p-1)!}(\mathcal{P}_p(\alpha)+\mathcal{P}_p(-\alpha))\right|$$
$$=\left|\frac{b^{3p-1}rs}{(p-1)!}(\mathcal{T}_p(\alpha)+\mathcal{T}_p(-\alpha))\right|. \tag{2.24}$$

Challenge 2.13 *Using* (2.10) *as a guide, find the analogue to the upper bound of* (2.11) *in this context. Then apply* (2.24) *to produce an inequality similar to* (2.13). *Finally, apply this new inequality to show that the integer in* (2.24) *can be made less than* 1 *for all sufficiently large primes p.*

Thus we have constructed a positive integer less than 1. This contradiction leads us to the conclusion that $e^{\sqrt{a/b}}$ is irrational and brings us to the end of our proof. ∎

The important new idea introduced in the proof of Theorem 2.4 was the balanced application of *both* zeros of the polynomial bz^2-a in the construction of the function $f(z)$ defined in (2.22). The symmetry occurring in $f(z)$ led to the critical fact that $f(z)\in\mathbb{Z}[z]$. The deep idea of considering all the conjugates of an algebraic number α in the construction of the auxiliary polynomial allows us to extend the themes we have developed in this chapter to prove the spectacular result that for any nonzero algebraic number α, the number e^α is transcendental. We carry out this program and explore some of the result's far-reaching and beautiful consequences in the next chapter.

Making Transcendence Transparent
An intuitive approach to classical transcendental number theory
Burger, E.B.; Tubbs, R.
2004, IX, 263 p. 50 illus., Hardcover
ISBN: 978-0-387-21444-3