PROOFS OF IRRATIONALITY & TRANSCENDENCE

ASHWIN RAJAN

1. Abstract

In this paper, we will discuss different techniques for showing that numbers are irrational. We will first go over some common and simpler proofs, such as a proof that $\sqrt{2}$ is irrational. Then, we will move on to three main results: proving that e^n, π^n, and $A(n) := \frac{1}{\pi} \arccos\left(\frac{1}{\sqrt{n}}\right)$ are irrational. After we show that these are irrational, we will move on to a few miscellaneous results that use different techniques than the previous ones. We will prove that $\cos 1$ and $\sin 1$ are irrational, and also that $\arccos(\frac{1}{n})$ is irrational for all natural $n \geq 3$.

2. Preliminary Proofs of Irrationality

Let's begin by quickly going over a simple example of proving irrationality.

Lemma 2.1. $\sqrt{2}$ *is irrational.*

This is likely the first proof of irrationality that one will learn, and we will go over the most widely known proof (sometimes attributed to Aristotle, and other times, to Euclid), as it will help us develop some of the tools we need for later.

Aristotle's Proof. Let's assume, for the sake of contradiction, that $\sqrt{2}$ is rational. Thus, it can be represented as an irreducible fraction as $\sqrt{2} = \frac{a_0}{b_0}$. Multiplying by b_0 on both sides, we get $b_0\sqrt{2} = a_0$. Next, we square both sides to get $2b_0^2 = a_0^2$. Because there is a coefficient of 2 on the left hand side, a_0 must be even. Thus, let's substitute $a_0 = 2a_1$ into our equation. Now, we have $b_0^2 = 2a_1^2$. This implies that b_0 is also even. At the beginning we said that $\frac{a_0}{b_0}$ was irreducible, $\gcd a_0, b_0 = 1$. However, we clearly have that a_0 and b_0 are both even, and thus that $\gcd a_0, b_0 \geq 2$. This is a contradiction, and thus, our original assumption that $\sqrt{2}$ is irrational was incorrect. ■

This proof appears rather underwhelming at first; it hinges on the irreducibility of a fraction, which hardly seems to be a proper basis for a proof. One might ask, what if we considered a reducible fraction? Well, let's consider this. Every time we substitute, let's replace (a_i, b_i) with (a_{i+1}, b_{i+1}). Then, we end up with $a_{2i} = 2b_{2i}$ for all nonnegative integers i. So, as i tends to ∞, we find that $\gcd(a_0, b_0)$ also tends to ∞ (at an exponential pace). This also means that a_0 and b_0 tend to ∞, and thus, no finite values of a_0 and b_0 can be chosen to give $\sqrt{2} = \frac{a}{b}$. Thus, $\sqrt{2}$ cannot be expressed as a fraction, and is therefore irrational.

What can we take away from this example to use in other, harder proofs of irrationality? First, we notice that we used a proof by contradiction. It is often more difficult (and requiring of more ingenuity) to come up with a constructive proof. Therefore, we will rely more on proofs that follow this same format: assume that some irrational number r can be expressed as some fraction, then provide some contradiction to show that r actually cannot be expressed as a fraction. Let's put this into action with our next set of proofs.

3. Proof that e^n is irrational

Let's work our way up to showing that e^n is irrational by beginning with some simpler statements regarding e. Before we begin our proofs, let's introduce the Taylor Polynomial for e^x. This will appear in many of our following proofs.

Lemma 3.1. *The Taylor polynomial for* e^x *is* $e^x = 1 + x + \frac{x^2}{2} + \frac{x^3}{6} + \frac{x^4}{24} + \cdots = \sum_{n=0}^{\infty} \frac{x^n}{n!}$.

Date: August 17, 2020.

Proof. Let's define the Taylor polynomial for e^x to be $e^x = \sum_{n=0}^{\infty} a_n x^n$. Differentiating both sides, we get $e^x = \sum_{n=0}^{\infty} n a_n x^{n-1} = \sum_{n=0}^{\infty} a_n x^n$. Equating coefficients, we get $(n+1)a_{n+1} = a_n$. The explicit form for this recursion is clearly $a_n = \frac{a_0}{n!}$. Plugging in $x = 0$ to our Taylor polynomial to solve for x_0, we get $e^0 = 1 = a_0$ because all of the other terms vanish at $x = 0$. Therefore, $a_n = \frac{1}{n!}$, and we have that the Taylor polynomial for e^x is $e^x = \sum_{n=0}^{\infty} \frac{1}{n!}$. ∎

Lemma 3.2. *Euler's number, e, is irrational.*

There are several proofs of this, the first of which was Euler's. He used the fact that e's continued fraction representation was infinite to show that it must be irrational. However, we will go over Fourier's proof, a proof by contradiction that utilizes the Taylor Series for e.

Fourier's proof. Let's suppose, for the sake of contradiction, that $e = \frac{a}{b}$ for integers $a, b > 0$. This is equivalent to $be = a$, and multiplying by $n!$ on both sides, we get $n!\,be = n!\,a$ for all $n \geq 0$. Why did we multiply on both sides by $n!$? Recall that $e^x = \sum_{k=0}^{\infty} \frac{x^k}{k!}$, so $e = \sum_{k=0}^{\infty} \frac{1}{k!}$. We will use this to show that the left hand side of our equation is nonintegral while the right hand side is integral. Looking at the right hand side of our equation, $n!\,a$ is clearly integral for all $n \geq 0$. However, looking at our left hand side, we have

$$n!\,be = bn!\left(1 + \frac{1}{1!} + \frac{1}{2!}\right) + \cdots = bn!\left(1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \cdots + \frac{1}{n!}\right) + bn!\left(\frac{1}{(n+1)!} + \frac{1}{(n+2)!} + \cdots\right).$$

The first term clearly is integral, because when we distribute the $n!$, all the denominators cancel. We suspect, however, that the second term is not integral. It turns out that our second term is approximately $\frac{b}{n}$, and we can see this by a comparison:

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

Therefore, for arbitrarily large n (essentially any $n > b+1$), this second term is definitely not integral. Therefore, for some values of n, the left hand side of the equality is nonintegral and the right hand side of the equality is integral. This is a contradiction! When we multiplied both sides by $n!$, we stated that our new equality must be true for all n; however, we have found some n such that this statement is not true. Therefore, our initial assumption that e is rational was incorrect; e must be irrational. ∎

Once again, we have proven irrationality through contradiction. So, are we done? Does this show that e^n is irrational? Unfortunately, this is not the case, as that is a much stronger statement. For example, $\sqrt[n]{2}$ is irrational for all natural numbers $n \geq 2$, but $(\sqrt[n]{2})^n = 2$ is rational. Thus, let's move on to e^2, and try to follow a similar proof as for e, one that J. Liouville wrote in 1840.

Lemma 3.3. *e^2 is irrational.*

Liouville's Proof. Let's assume, for the sake of contradiction, that $e^2 = \frac{a}{b}$. Unfortunately, trying $e^2 b = a$ doesn't get us anywhere, but, rearranging to get $eb = ae^{-1}$ is much more convenient. This is because of the Taylor Series for e^n, which gives us

$$e = 1 + \frac{1}{1} + \frac{1}{2} + \frac{1}{6} + \frac{1}{24} + \cdots$$

as before, and

$$e^{-1} = 1 - \frac{1}{1} + \frac{1}{2} - \frac{1}{6} + \frac{1}{24} \mp \cdots.$$

Plugging this into our equation, we get

$$b\left(1 + \frac{1}{1} + \frac{1}{2} + \frac{1}{6} + \frac{1}{24} + \cdots\right) = a\left(1 - \frac{1}{1} + \frac{1}{2} - \frac{1}{6} + \frac{1}{24} \mp \cdots\right).$$

Next, we multiply by $n!$. Note that our equation must be true for all n; this will be important as we continue with the proof. This gives us

$$Z_1 + n!\,b\left(\frac{1}{(n+1)!} + \frac{1}{(n+2)!} + \cdots\right) = Z_2 + (-1)^{n+1} n!\,a\left(\frac{1}{(n+1)!} - \frac{1}{(n+2)!} + \frac{1}{(n+3)!} \mp \cdots\right),$$

where $Z_1, Z_2 \in \mathbb{Z}$. As we had shown in the proof of the irrationality of e, the nonintegral part of the left hand side is approximately $\frac{b}{n}$. For large n, the nonintegral part is small, so this means that the left hand side overall will be slightly greater than an integer. Now, let's look at the right hand side of the equation. The nonintegral part: $(-1)^{n+1}n!\,a(\frac{1}{(n+1)!}-\frac{1}{(n+2)!}+\frac{1}{(n+3)!}\mp\cdots)$. We can bound this by

$$\frac{-a}{n}<(-1)^{n+1}n!\,a(\frac{1}{(n+1)!}-\frac{1}{(n+2)!}+\frac{1}{(n+3)!}\mp\cdots)<-a\left(\frac{1}{n+1}-\frac{1}{(n+1)^2}-\frac{1}{(n+1)^3}-\cdots\right)$$
$$=\frac{-a}{n+1}\left(1-\frac{1}{n}\right)<0.$$

But this means that the nonintegral part of the right hand side is just slightly less than an integer for very large n. Thus, we have that $n!\,ae^{-1}$ is slightly smaller than an integer, and from before, we have that $n!\,be$ is slightly larger than an integer for large n, so $n!\,ae^{-1}=n!\,be$ is not true for all n. Because we have reached a contradiction, our original assumption that e^2 is rational is incorrect. ■

The most natural next step is to check if e^3 is irrational, but playing around with the Taylor series for e^x and rearranging $e^3b=a$ gets us nowhere. Possibly looking at e^4 would be nicer?

Lemma 3.4. *e^4 is irrational.*

It is indeed easier to deduce that e^4 is irrational. However, we cannot immediately jump into the proof using the same technique as we did in showing that e and e^2 were irrational is not going to work. Taking $be^2=ae^{-2}$ and multiplying by $n!$, then taking the nonintegral parts isn't enough to prove that this equality is false. In our previous proofs, we picked an arbitrary large n for $n!$, but in this case, it will be more convenient to take a large $n=2^m$ and multiply by $\frac{2n!}{2^n}$. Why 2^n? To see why, let's introduce Legendre's theorem.

Lemma 3.5 (Legendre's Theorem)**.** *The number of factors of p in $n!$ is*

$$v_p(n!\,)=\lfloor\frac{n}{p}\rfloor+\lfloor\frac{n}{p^2}\rfloor+\lfloor\frac{n}{p^3}\rfloor+\cdots$$

.

Note that although this looks like an infinite series, it's actually not. Because of the floors, as soon as $p^x>n$, the rest of the terms become 0.

Proof. For every multiple of p less than or equal to n, we add 1 to $v_p(n!\,)$ because each of those contributes one factor of p. The number of multiples of p less than or equal to n is $\lfloor\frac{n}{p}\rfloor$. We also have to account for higher powers of p. So, each multiple of p^2 less than or equal to n will contribute two factors of p, one of which was already accounted for. The number of multiples of p less than or equal to n is $\lfloor\frac{n}{p^2}\rfloor$. We follow the same pattern, adding one for each multiple of a power of p less than or equal to n. This gives us the series $\lfloor\frac{n}{p}\rfloor+\lfloor\frac{n}{p^2}\rfloor+\lfloor\frac{n}{p^3}\rfloor+\cdots$. ■

Notice that this theorem only deals with prime numbers. If we have $v_x(n)$, with $x=p_1^{e_1}p_2^{e_2}p_3^{e_3}\cdots p_i^{e_i}$, then $v_x(n)=\min(\frac{v_{p_1}(n)}{e_1},\frac{v_{p_2}(n)}{e_2},\frac{v_{p_3}(n)}{e_3},\ldots,\frac{v_{p_i}(n)}{e_i})$. Now that we have this in mind, what's so special about $n=2^m$? It's natural to try to find the number of factors of 2 in $n!$.

Lemma 3.6. *The number of factors of 2 in $n!$ if $n=2^m$ is exactly $n-1$. The number of factors of 2 in $x!$ if $x\neq 2^m$ is less than $x-1$.*

Proof. We calculate $v_2n!=\lfloor\frac{n}{2}\rfloor+\lfloor\frac{n}{4}\rfloor+\lfloor\frac{n}{8}\rfloor+\cdots$. Substituting $n=2^m$, we can remove all the floors up until $\lfloor\frac{2^m}{2^{m+1}}\rfloor$ because all previous values will be integral. Therefore, we have $2^{m-1}+2^{m-2}+2^{m-3}+\cdots+4+2+1+0+\cdots=2^m-1=n-1$ factors of 2 in $n!$.

Let's consider the second part. We have $v_2x!=\lfloor\frac{x}{2}\rfloor+\lfloor\frac{x}{4}\rfloor+\lfloor\frac{x}{8}\rfloor+\cdots$. If $x=2^a\cdot n$, then $\lfloor\frac{x}{2^{a+1}}\rfloor<\frac{x}{2^{a+1}}$. Therefore, $\lfloor\frac{x}{2}\rfloor+\lfloor\frac{x}{4}\rfloor+\lfloor\frac{x}{8}\rfloor+\cdots<\frac{x}{2}+\frac{x}{4}+\frac{x}{8}+\cdots 1=x-1$. ■

This means that multiplying by $\frac{n!}{2^{n-1}}$ does not have any effect on the parity of either side of the equation. Now that we are equipped with this information, let's begin our proof of Lemma 3.3.

Proof of Lemma 3.3. Let's begin in the same fashion as we did for proving that e^2 is irrational. Assume, for the sake of contradiction, that e^4 is rational, and can be expressed as $\frac{a}{b}$. Then, we have $be^2=ae^{-2}$. As we said previously, it is more convenient to multiply by $\frac{n!}{2^{n-1}}$ (compared to $n!$ as in previous proofs), with $n = 2^m$. This gives us

$$b\frac{n!}{2^{n-1}}e^2 = a\frac{n!}{2^{n-1}}e^{-2}.$$

As in previous proofs, we substitute using the Taylor Series for e:

$$e^2 = 1 + \frac{2}{1} + \frac{4}{2} + \frac{8}{6} + \frac{16}{24} + \cdots + \frac{2^4}{r!} + \cdots$$

and

$$e^{-2} = 1 - \frac{2}{1} + \frac{4}{2} - \frac{8}{6} \pm \cdots + \frac{(-2)^r}{r!} + \cdots.$$

For $r \leq n$, we have the following summands

$$b\frac{n!}{2^{n-1}}\frac{2^r}{r!} \quad \text{and} \quad a\frac{n!}{2^{n-1}}\frac{(-2)^r}{r!}.$$

It is not too difficulty to show that these are integral under our condition that $r \leq n$. For the first case, we have our first expression $E_1 = b\frac{n!}{2^{n-1}}\frac{2^r}{r!}$, and counting factors of 2, we have that $v_p(E_1) \geq (n-1) - (n-1) + r - (r-1) = 1$. The same thing is true for $E_2 = a\frac{n!}{2^{n-1}}\frac{(-2)^r}{r!}$ (because the only thing that's changed is a factor of $(-1)^n$, and the arbitrary coefficient was changed from b to a). Now, let's consider the nonintegral parts of both sides of our equation. The left hand side of our equation has nonintegral part for $r \geq n+1$, which is

$$2b\left(\frac{2}{n+1} + \frac{4}{(n+1)(n+2)} + \frac{8}{(n+1)(n+2)(n+3)} + \cdots\right).$$

Using our same bounding from before, we get that for large n, this is very close to $\frac{4b}{n}$. For large n, this is a very small positive number. Next, we consider the right hand side of our equation for $r \geq n+1$, which is

$$2a\left(-\frac{2}{n+1} + \frac{4}{(n+1)(n+2)} - \frac{8}{(n+1)(n+2)(n+3)} \pm \cdots\right).$$

Using our same bounding from before, this is very close to $-\frac{4a}{n}$. For large n, this is a very small negative number. Therefore, our left hand side is slightly larger than an integer for large n, and our right hand side is slightly smaller than an integer for large n. Therefore, both sides can't be equal and we have a contradiction. Thus, our original assumption that e^4 is rational was incorrect, so e^4 must be irrational. ■

Unfortunately, as we found before, manipulations aren't enough to show that e^3 is irrational. The same is true for odd powers of e. After all, doing $e^{2x+1} = \frac{a}{b}$ and manipulating it to $be^{x+1} = ae^{-x}$ isn't really helpful, because the powers on each side are uneven. However, Charles Hermite discovered an idea to prove that these odd powers of e are irrational, which in fact is able to generalize to all rational powers of e.

Theorem 3.7. *e^r is irrational for all rational r.*

We can't directly prove this; we must first introduce the following function, which as a few useful properties.

Lemma 3.8. *For some fixed $n \geq 1$, define*

$$f(x) = \frac{x^n(1-x)^n}{n!}.$$

1. *The function $f(x)$ is a polynomial of the form $f(x) = \frac{1}{n!}\sum_{i=n}^{2n} c_i x^i$, where the coefficients c_i are integers.*
2. *For $0 < x < 1$ we have $0 < f(x) < \frac{1}{n!}$.*
3. *The derivatives $f^{(k)}(0)$ and $f^{(k)}(1)$ are integers for all $k \geq 0$.*

Proof. It is evident that the numerator of our function will have integer coefficients on all the terms when expanded, because the coefficients in each multiplicand is integral. The only thing that our first statement says other than that is that, when expanded, our expression contains terms of degree n to $2n$. When $(1-x)^n$ is expanded, the terms have degree $0, 1, 2, \ldots, n-2, n-1, n$. Thus, when each of these terms are multiplied by x^n, the degrees become $n, n+1, n+2, \ldots 2n-2, 2n-1, 2n$.

The numerator is $(x - x^2)^n$. This is maximized when $x - x^2$ is maximized. We have $x - x^2 = -(x - 0.5)^2 + 0.25$, which means that there is a maximum at 0.5. Therefore, we have that the maximum is $\frac{1}{4^n n!}$.

The minima are at $x = 0$ and $x = 1$, as $f(x) = 0$ there, and all values of $f(x)$ for $0 \leq x \leq 1$ are nonnegative. Therefore, for $0 < x < 1$ we have $0 < f(x) < \frac{1}{4^n n!} < \frac{1}{n!}$.

Because all the terms in our function have degree $d : n \leq d \leq 2n$ as shown in in part 1, if $0 \leq k \leq n-1$, each term will have a factor of x in it, meaning that the kth derivative will vanish at 0. The same is true for $2n+1 \leq k$, as the kth derivative will then universally be 0. Then, in the range $n \leq k \leq 2n$, the kth derivative at 0 will be $f(k)(0) = \frac{k!}{n!}c_k$. Since c_k is an integer, and $k \geq n$, this is integral for all k.Next, let's examine $f^{(k)}(1)$. Using the handy fact that $f(x) = f(1-x)$, we get $f^{(k)}(x) = (-1)^k f^{(k)}(1-x)$. This means that $f^{(k)}(1) = (-1)^k f^{(0)}$, and since we have shown that $f(k)(0)$ is integral for all k, $f(k)(1)$ is also integral for all k.

■

With this lemma, we are now ready for our culminating proof of irrationality of powers of e.

Proof of Theorem 3.7. Let's assume, for the sake of contradiction, that $e^{\frac{s}{t}} = \frac{p}{q}$ for integral s and t. If $e^{\frac{s}{t}}$ is rational, then so is $(e^{\frac{s}{t}})^t = e^s$. Therefore, it is enough to show that e^s cannot be rational for any integer s. Now, assume for the sake of contradiction that $e^s = \frac{a}{b}$ for integers $a, b \geq 0$, and (this will become important later) n that is large enough such that $n! > as^{2n+1}$. Now, define

$$F(x) := s^{2n}f(x) - s^{2n-1}f'(x) + s^{2n-2}f''(x) \mp \cdots + f^{(2n)}(x),$$

where $f(x)$ is the function defined in Lemma 3.7. Since $f^{(k)}(x) = 0$ for $k > 2n$, we can rewrite $F(x)$ as an infinite sum:

$$F(x) = s^{2n}f(x) - s^{2n-1}f'(x) + s^{2n-2}f''(x) \mp \cdots.$$

This infinite series gives us that

$$F'(x) = -sF(x) + s^{2n+1}f(x).$$

We introduce a factor of e^{sx} to get $e^{sx}F(x)$. Differentiating using the product rule and our equation above gives us

$$\frac{d}{dx}[e^{sx}F(x)] = se^{sx}F(x) + e^{sx}F'(x) = s^{2n+1}e^{sx}f(x).$$

Let's define

$$N := b\int_0^1 s^{2n+1}e^{sx}f(x)dx = b[e^{sx}F(x)]_0^1 = be^sF(1) - bF(0) = aF(1) - bF(0).$$

We know that this is an integer, because $f^{(k)}(1)$ and $f^{(k)}(0)$ are integers for all integral $k \geq 0$, from part 3 of Lemma 3.7 (and since $F(x)$ is the sum of several of these multiplied by integers). Using part 2 of Lemma 3.7, we have that

$$0 < N = b\int_0^1 s^{2n+1}e^{sx}f(x)dx < bs^{2n+1}e^s\frac{1}{n!} = \frac{as^{2n+1}}{n!} < 1,$$

because of our condition on n when we introduced it. This shows that N cannot be an integer, a contradiction, meaning that our original assumption, that e^s for $s \in \mathbb{Z}$ can be rational, is incorrect. Because e^s for integral s cannot be rational, neither can e^r for rational r. ■

Before we continue, let's introduce a few key terms:

Definition 3.9 (Algebraic Number)**.** An Algebraic Number is a complex number which is a solution of some nonzero, single-variable polynomial.

(1) $\sqrt{2}$ is an Algebraic Number, because it is a solution of $x^2 - 2 = 0$.
(2) $i = \sqrt{-1}$ is an Algebraic Number, because it is a solution of $x^2 + 1 = 0$.
(3) $a + bi$ is Algebraic Number, because it is a solution of $x^2 - a^2 - b^2 = 0$.

Definition 3.10 (Transcendental Number)**.** A Transcendental Number is a number that is not Algebraic over .

(1) e is a Transcendental Number because it is not a solution to any nonzero, single-variable polynomial.
(2) Similarly, $\log 2$[1] is a Transcendental Number.

[1]Although this statement is also true in base-10, note that all civilized mathematicians use log as the natural logarithm.

However, claiming that e^r is irrational for all rational r is not the strongest claim we can make; e is in fact transcendental (if you don't see why this is stronger, consider $2+\sqrt{3}$). Proofs that numbers are transcendental are in general very difficult; the first proof that a number is transcendental was of e, in 1873 by Hermite.

Theorem 3.11. *e is a Transcendental Number over $\mathbb{Q}$.*

Let's go over Hermite's proof, but before, let's go over a quick lemma.

Lemma 3.12. *The nth derivative of $h(x)=f(x)g(x)$ is $h^{(n)}(x)=\sum_{i=0}^{n}\binom{n}{i}f^{(i)}(x)g^{(n-i)}(x)$.*

Proof. Let's do a proof by induction. Beginning with our base case, which we'll consider to be $n=1$, we get that $h'(x)=f'(x)g(x)+f(x)g'(x)$ by the product rule. This works out with our formula. Next, assuming that $h^{(n)}(x)=\sum_{i=0}^{n}\binom{n}{i}f^{(i)}(x)g^{(n-i)}(x)$ is true, let's differentiate again with respect to x. We get

$$h^{(n+1)}(x)=\sum_{i=0}^{n}[\binom{n}{i}f^{(i+1)}(x)g^{(n-i)}(x)+\binom{n}{i}f^{(i)}(x)g^{(n-i+1)}(x)].$$

Rearranging terms gives us the equivalent sum:

$$\sum_{i=0}^{n+1}(f^{(i)}(x)g^{(n+1-i)}(x))(\binom{n}{i}+\binom{n}{i-1})=\sum_{i=0}^{n+1}\binom{n+1}{i}f^{(i)}(x)g^{(n+1-i)}(x),$$

which completes the inductive step. ■

Hermite's Proof of Theorem 3.10. Suppose, for the sake of contradiction, that e is algebraic. Then, we have $a_me^m+\cdots+a_1e+a_0=0$, with $a_i\in\mathbb{Z}$, and $a_0,a_m\neq 0$. Define

$$j(x)=\frac{x^{p-1}(x-1)^p(x-2)^p\cdots(x-m)^p}{(p-1)!},$$

where p is some unspecified prime. Furthermore, define

$$J(x):=j(x)+j'(x)+\cdots+j^{(mp+p-1)}(x).$$

Because $j(x)$ has degree $mp+p-1$, the dth derivative wtih $d>mp+p-1$ vanishes. We can thus write $J(x)$ as an infinite series $J(x)=j(x)+j'(x)+j''(x)+\cdots$. For $0<x<m$, $|j(x)|\leq\frac{m^{p-1}m^pm^p\cdots m^p}{(p-1)!}=\frac{m^{mp+p-1}}{(p-1)!}$. We also note that for $-m<x\leq 0$, $|j(x)\leq\frac{(2m)^{p-1}(2m)^p\cdots(2m)^p}{(p-1)!}=\frac{(2m)^{mp+p-1}}{(p-1)!}$ $J(x)$ also has the convenient property that

$$\frac{d}{dx}[e^{-x}J(x)]=e^{-x}[J'(x)-J(x)]=-e^{-x}j(x)$$

because $e^{-x}[J'(x)-J(x)]$ telescopes. Using this fact, we have

$$a_s\int_0^s e^{-x}j(x)dx=a_s[-e^{-x}J(x)]_0^s=a_sJ(0)-a_se^{-s}J(s).$$

We want to cancel out the e^{-s}, so we multiply by e^s to get $e^sa_sJ(0)-a_sJ(s)$. Now, we sum over $s=0,1,2\ldots,m$ to get

$$\sum_{s=0}^{m}a_se^s\int_0^s e^{-x}j(x)dx=\sum_{s=0}^{m}a_se^sJ(0)-a_sJ(s)=\sum_{s=0}^{m}a_se^sJ(0)-\sum_{s=0}^{m}a_sJ(s).$$

The first sum is simply 0, because at the beginning of this proof, we had $a_me^m+\cdots+a_1e+a_0=0$. This leaves us with $-\sum_{s=0}^{m}a_sJ(s)$. Substituting $J(x)=j(x)+j'(x)+\cdots+j^{(mp+p-1)}(x)$, we get $-\sum_{s=0}^{m}\sum_{i=0}^{mp+p-1}a_sj^{(i)}(s)$. We claim that $j^{(i)}(s)$ is an integer, and is divisible by p when $s=0$ and $i=p-1$. Let's handle the easy cases first, then move on to the harder one; we know that the degree of the terms of $j(x)$ range from $p-1$ to $mp+p-1$. So, for $j^{(i)}(s)$ where $0<i<p-1$, there is always at least one factor of $x(x-1)(x-2)\cdots(x-m)$ and since s is an integer $0\leq s\leq m$, that means that the ith derivative in this case is 0. Next, because the degree of $j(x)$ is $mp+p-1$, $j^{(i)}(x)$, where $i\geq mp+p$, must be 0 for all x. So far, all of our expressions have evaluated to 0, which is a multiple of p. Lastly, we must deal with the case of $j^{(i)}(s)$, where $p-1\leq i\leq mp+p-1$. Notice that we have a special case when $i=p-1$ and $s=0$,

because there are only $p-1$ copies of x in $j(x)$. We will consider this case after the others. Let's consider each s separately. We, by Lemma 3.11, have that

$$j^{(i)}(s) = \sum_{y=0}^{i} \binom{i}{y} \frac{q^{(y)}(s)}{(p-1)!} g^{(i-y)}(s),$$

where $q(x) = ((x-s)^p)$ and

$$g(x) := x^{p-1}(x-1)^p \cdots (x-s-1)^p (x-s+1)^p \cdots (x-m)^p.$$

Because the rth derivative of $(x-s)^p$ at $x = s$ is 0 when $0 \leq r < p$, every term of our summation except the last cancels out, and we are left with $\binom{n}{n}\frac{q^{(p)}(s)}{(p-1)!}g(s) = pg(s)$. Since $g(s)$ is the product of the pth power of several integers, $g(s)$ is definitely an integer, and our result is a multiple of p when $i \neq p-1$ or $s \neq 0$.

Now, let's look at our special case of $i = p-1$ and $s = 0$. By Lemma 3.11, we have that $j^{(p-1)}(0) = \sum_{y=0}^{p-1} \binom{p-1}{y} \frac{q^{(y)}(0)}{(p-1)!} g^{(i-y)}(0)$. Similarly to our previous cases, we have that the only term that is nonzero is the last term, because $q^{(r)}(0) = 0$ for $0 \leq r < p-1$. Then, we are left with the equivalent expression $\binom{p-1}{p-1}\frac{q^{(p-1)}(0)}{(p-1)!}g(0)$, which simplifies nicely to $g(0)$. This gives us $j^{(p-1)}(0) = (-1)^p(-2)^p(-3)^p \cdots (-m)^p$. We now choose p to be larger than m, so that this product cannot have a factor of p in it. Now, as p tends to ∞, the magnitude of the right-hand side grows arbitrarily large, but more importantly, is nonzero. Meanwhile, the for $-m < x < m$, $|j(x)| \leq \frac{(2m)^{mp+p-1}}{(p-1)!}$, so as p tends to ∞, $|j(x)|$ tends to 0 from $-m < x < m$, so $j(x)$ becomes, essentially, a straight line around $x = 0$, meaning that $j^{(p-1)}(0)$ tends to 0. This is a contradiction, as for arbitrarily large p, the left-hand side approaches 0, and the right-hand side approaches ∞. Because we have reached a contradiction, our original assumption, that e is an algebraic number, must have been incorrect, and thus, e must be a transcendental number. ■

This was a pretty involved proof, but why did we do it? The proof of e being transcendental actually has some applications, one of which we will discuss later, being the irrationality of $\log 2$.

4. Irrationality of π[2]

Although the equation $C = \pi d^2$ is extremely well known, the proof that C and d are incommensurable is actually nontrivial, and not very well-known. Let's go through Ivan Niven's proof of π's irrationality, which is interestingly very similar in structure to the proof that e^r is irrational for all rational r.

Lemma 4.1. *π is irrational.*

Before we begin with this proof, we need to introduce a function with some specific properties.

Lemma 4.2. *Define $g(x) := \frac{x^n(a-bx)^n}{n!}$, where a and b are integers greater than 0. Then,*

(1) *$n!\,g(x)$ has integral coefficients, and has terms of degree greater than or equal to n.*
(2) *$g(x)$ and $g^{(i)}(x)$ have integral values for $x = 0$ and $x = \frac{a}{b}$.*

Proof. The first part of the lemma is simple: the degrees of the terms are $d : n \leq d \leq 2n$, and the coefficients are of the form $(-1)^{n-m}\binom{n}{m}a^m b^{n-m}$, which must be integral.

The second part of the lemma is nontrivial. We know that $g(0) = 0$, and $g(\frac{a}{b}) = 0$. We also know that for all $0 < i < n$, $g^{(i)}(x)$ has a factor of $x(a-bx)$, so $g^{(i)}(0) = 0$ and $g^{(i)}(\frac{a}{b}) - 0$ for $0 < i < n$. Because, as we stated in the first part of the lemma, the degree of $g(x)$ is $2n$, $g^{(i)}(x) = 0$ for $i > 2n$ for any x. We are left with the case of $g^{(n+i)}(x)$ where $0 \leq i \leq n$. To show that this is integral, let's find an explicit form for $g^{(i+n)}(0)$. This requires finding the term with degree $i+n$ (as all other terms will vanish at the $i+n$th derivative and when $x = 0$). This term will be

$$\frac{\binom{n}{i}(a^{2n-i})(-b)^i x^i}{n!},$$

[2]The correct equation is $C = r\tau$, but unfortunately, mathematicians have not fully embraced the superior circle constant yet. Please do your part to give τ the recognition it deserves.

and the *ith* derivative of this with respect to x is

$$\frac{\binom{n}{i}(a^{n-i})(-b)^i x^{i+n}}{n!}.$$

The $i+n$th derivative of this (with respect to x) is

$$\binom{n}{i}(a^{n-i})(-b)^i \frac{(i+n)!}{n!},$$

which is clearly an integer. Since $g(x) = g(\frac{a}{b} - x)$, both $g^{(k)}(0)$ (what we just showed), and $g^{(k)}(\frac{a}{b})$ are integers for all nonnegative integers k. ■

Now that we have our function, we are ready to move on to the proof of π's irrationality.

Niven's proof. Let's assume, for the sake of contradiction, that $\pi = \frac{a}{b}$, where $0 < a, b \in \mathbb{Z}$. We define the following polynomial:

$$G(x) := g(x) - g^{(2)}(x) + g^{(4)}(x) - \cdots + (-1)^n g^{(2n)}(x)$$

for some constant n. We know that $n!\,g(x) = x^n(a - bx)^n$ (note that these are the same a, b from the numerator and denominator of π) has integral coefficients, and all of its terms have degree $d : d \geq n$ from Lemma 4.2. We also have that the derivatives $g^{(i)}(x)$ have integral values for $x = 0$ and $x = \frac{a}{b} = \pi$. Taking the derivative of $G'(x)\sin x - G(x)\cos x$, we get

$$\frac{d}{dx}[G'(x)\sin x - G(x)\cos x] = G''(x)\sin x + G(x)\sin x = g(x)\sin x.$$

Because of this nice cancellation, we have

$$A = \int_0^\pi g(x)\sin x dx = [G'(x)\sin x - G(x)\cos x]_0^\pi = G(\pi) + G(0).$$

Since $g^{(i)}(0)$ and $f^{(i)}(\pi)$ are integers, so is $G(\pi)$ and $G(0)$, and thus, their sum. We have $(G(\pi) + F(0)) \in \mathbb{Z}$. We also have that for $0 < x < \pi$, and for some n large enough that $\frac{\pi^n a^n}{n!} < 1$, $0 < g(x)\sin x < \frac{\max(x^n) \cdot \max((a-bx)^n) \cdot \max(sinx)}{n!} <$ [3] $\frac{\pi^n a^n}{n!} < 1$. Therefore, A is both integral and between 0 and 1 exclusive, a clear contradiction. Because we have reached a contradiction, our initial assumption, that π is rational, must be incorrect. ■

We've shown that π is irrational. However, as we've stated before, it is stronger to say that x^2 is irrational than to say that x is irrational. In fact, the proof that π^2 is irrational shockingly similar to the proof that e^r is irrational because it utilizes the same equation

$$f(x) = \frac{x^n(a - bx)^n}{n!}$$

from before.

Theorem 4.3. *π^2 is irrational.*

Proof. Assume, for the sake of contradiction, that π^2 is irrational and can be expressed as $\frac{a}{b}$ for integers $a, b > 0$. We will now define the polynomial

$$H(x) := b^n\left(\pi^{2n} f(x) - \pi^{2n-2} f^{(2)}(x) + \pi^{2n-4} f^{(4)}(x) \mp \cdots\right),$$

[4] which satisfies $H''(x) = -\pi^2 H(x) + b^n \pi^{2n+2} f(x)$. From part 3 of Lemma 3.7, we have that $H(0)$ and $H(1)$ are integers (if this is not immediately obvious, try plugging in $\pi^2 = \frac{a}{b}$). Differentiating by using the product rule gives us

$$\frac{d}{dx}[H'(x)\sin\pi x - \pi H(x)\cos\pi x] = (H''(x)\sin\pi x + \pi H'(x)\cos\pi x - \pi H'(x)\cos\pi x + \pi^2 H(x)\sin\pi x$$
$$= \sin\pi x(H''(x) + \pi^2 H(x)) = b^n \pi^{2n+2} f(x)\sin\pi x$$

[3] Note that this is not less than or equal to because our range is from 0 to π, exclusive

[4] This is the same function $f(x)$ that was defined in Lemma 3.7.

per our differential equation above. Plugging in $a = b\pi^2$, we get that this simplifies to $\pi^2 a^n f(x)\sin\pi x$. Using this, we get

$$M := \pi \int_0^1 a^n f(x)\sin\pi x dx = [\frac{1}{\pi}H'(x)sin\pi x - F(x)\cos\pi x]_0^1,$$

which simplifies to $F(0) + F(1)$ because $\sin 0 = 0, \sin\pi = 0, \cos 0 = 1$, and $\cos\pi = -1$. We know that M is a positive integer, because $F(0)$ and $F(1)$ are integers (a result that follows from Lemma 3.7), and because M is the integral of a function that is positive, except on the boundary. From part 2 of Lemma 3.7, we have that and since we can always choose n to be large enough such that $\frac{\pi a^n}{n!} < 1$, we have $0 < M = \pi\int_0^1 a^n f(x)\sin\pi x dx < \frac{\pi a^n}{n!} < 1$. This is a contradiction, because we have that M is integral, but also that it is between 0 and 1 exclusive. Because we have reached a contradiction, our initial assumption, that π^2 is rational, must have been incorrect. ∎

Interestingly, π^2's irrationality has some important applications. Let's consider the following:

Corollary 4.4. *There are infinitely many prime numbers.*

There is a quick proof of this using π^2's irrationality.

Proof. When we see π^2, the first thing that should pop into our mind is $\sum_{n=1}^{\infty}\frac{1}{n^2} = \frac{\pi^2}{6}$. Because of the fundamental theorem of arithmetic, all positive integral n can be expressed as the product of primes (including 1, which is the product of 0 primes). This gives us

$$\sum_{n=1}^{\infty}\frac{1}{n^2} = \prod_{\text{p prime}}(1 + \frac{1}{p^2} + \frac{1}{p^4} + \cdots) = \prod_{\text{p prime}}\frac{p^2}{p^2-1}$$

. Assume, for the sake of contradiction, that there are finitely many primes. The product of finitely many rational numbers is necessarily a rational number, so $\prod_{\text{p prime}}\frac{p^2}{p^2-1}$ must be rational. However, we know that it is equal to $\frac{\pi^2}{6}$, which is irrational. This is a contradiction, and thus, our original assumption that there are only finitely many primes was incorrect. ∎

Now, we have shown that π^2 is irrational. However, how do we know it's not the cube root, or even the nth root of some rational number r. We can show this is true by proving that π is transcendental, or not algebraic. However, this proof requires the use of the Lindemann-Weierstrass Theorem, which is far beyond the scope of this paper. We will go over a proof of π being transcendental by assuming the Lindemann-Weierstrass Theorem to be true. Before we introduce the Lindemann-Weierstrass Theorem, we need to define a few terms.

Definition 4.5 (Linearly Independent)**.** Several vectors $v_1, v_2, \ldots, v_n$ are said to be Linearly Independent if $C_1v_1 + C_2v_2 + \cdots C_nv_n = 0$ if and only if $C_i = 0$ for all $1 \le i \le n$.

Definition 4.6 (Algebraically Independent)**.** Given a field K, and A, a K-algebra, elements $y_1, y_2, y_3, \ldots, y_n$ are algebraically independent over K if there are no polynomial relations $F(y_1, y_2, y_3, \ldots, y_n) = 0$ with coefficients in K.

Lemma 4.7 (Lindemann-Weierstrass Theorem)**.** *If $\alpha_1, \ldots, \alpha_n$ are algebraic numbers that are linearly independent over the rational numbers $\mathbb{Q}$, then $e^{\alpha_1}, \ldots, e^{\alpha_n}$ are algebraically independent over $\mathbb{Q}$.*

We will also need to introduce a few more terms before we begin our proof of π being transcendental.

Definition 4.8 (Symmetric Polynomial)**.** A symmetric polynomial is a function that remains unchanged no matter the permutation of the inputs. Equivalently, f is a symmetric polynomial if $f(x_1, x_2, \ldots, x_n) = f(y_1, y_2, \ldots, y_n)$ where $y_1 = x_{\Pi i}$, where Pi is an arbitrary permutation on $1, 2, \ldots, n$.

Example. One example of a symmetric polynomial is $xy + x + y$, as if y is assigned to x and x is assigned to y, the expression remains the same.

Now that we've introduced what a symmetric polynomial is, we are ready to define the more pertinent Elementary Symmetric Polynomials.

Definition 4.9 (Elementary Symmetric Polynomial)**.** An elementary symmetric polynomial on n variables is $e_k(X_1, X_2, \ldots, X_n) = \sum_{1\le j_1<j_2<\cdots<j_k\le n} X_{j_1}X_{j_2}\cdots X_{j_k}$.

This may look familiar to you; these are essentially the expressions you get in Vieta's formulas if the leading coefficient is 1.

Lemma 4.10 (Fundamental theorem on symmetric functions)**.** *Any symmetric polynomial can be expressed in terms of the elementary symmetric polynomials.*

Proving this lemma is beyond the scope of this paper, so we will take this theorem to be true.[5]

Theorem 4.11. *π is a transcendental over $\mathbb{Q}$.*

Proof. Suppose, for the sake of contradiction, that π is algebraic, and thus satisfies an algebraic equation with coefficients in $\mathbb{Q}$. Because the set of algebraic numbers is closed over multiplication, πi is also algebraic, and thus is the root of an algebraic equation with integral coefficients $\theta_1(x) = 0$, which has solutions $\alpha_1 = i\pi, \alpha_2, \alpha_3, \ldots$. Using Euler's identity $e^{i\pi} + 1 = 0$, we have that

$$(e^{\alpha_1} + 1)(e^{\alpha_2} + 1) \cdots (e^{\alpha_n} + 1) = 0.$$

Now, we construct an algebraic equation with integral coefficients whose roots are the exponents in the expansion of our previous equation. First, let's consider the exponents $a_i + a_j$, with $i \neq j$. By Vieta's formulas in combination with the fact that $\theta_1(x)$ must have integral coefficients, we know that the elementary symmetric functions of $\alpha_1, \alpha_2, \ldots, \alpha_n$ are rational numbers (not necessarily integral, because the leading coefficient might be greater than 1). Therefore, the quantities of the form $a_i + a_j$ are the roots of $\theta_2(x) = 0$, an algebraic equation with integral coefficients. Similarly, we sum the αs taken three at a time, providing the $\binom{n}{3}$ roots of $\theta_3(x) = 0$. We continue along the same pattern to get $\theta_4(x) = 0, \theta_5(x) = 0, \ldots, \theta_n(x) = 0$, all algebraic equations with integral coefficients, whose roots are the sums of the αs taken $4, 5, \ldots, n$ at a time respectively. The product of all of these equations is $\theta_1(x)\theta_2(x) \cdots \theta_n(x) = 0$, which has roots that are the exponents in the expansion of $(e^{\alpha_1} + 1)(e^{\alpha_2} + 1) \cdots (e^{\alpha_n} + 1)$. Deleting any roots at $x = 0$ gives us

$$\theta(x) = cx^r + c_1 x^{r-1} + \cdots + c_r,$$

whose roots are β_1, β_2, β_3,..., β_r, the nonvanishing exponents in the expansion of $(e^{\alpha_1}+1)(e^{\alpha_2}+1)\cdots(e^{\alpha_n}+1)$. Therefore, we can expand this expression to get $e^{\beta_1} + e^{\beta_2} + \cdots + e^{\beta_r} + k = 0$, where k is some positive integer. Let's define

$$f(x) := \frac{c^s x^{p-1}(\theta(x))^p}{(p-1)!},$$

where $s = rp - 1$, and p is a prime that is to be specified. We also define

$$F(x) := f(x) + f^{(1)}(x) + f^{(2)}(x) + \cdots + f^{(s+p+1)}(x),$$

noting that the derivative of $e^{-x}F(x)$ is $-e^{-x}f(x)$. Thus, we have

$$e^{-x}F(x) - e^0 F(0) = \int_0^\pi -e^{-\xi} f(\xi) d\xi.$$

Now, we substitute $\xi = \tau x$, to get

$$F(x) - e^x F(0) = -x \int_0^1 e^{(1-r)x} f(\tau x) d\tau.$$

Summing x over our roots $\beta_1, \beta_2, \ldots, \beta_r$, we get

$$\sum_{j=1}^{r} F(\beta_j) + kF(0) = \sum_{j=1}^{r} \beta_j \int_0^1 e^{(1-r)\beta_j} f(\tau\beta_j) d\tau.$$

From our definition of $f(x)$, we can see that

$$\sum_{j=1}^{r} f^{(t)}(\beta_j) = 0$$

for $0 \leq t < p$ because there will always be a copy of $\theta(x)$ in the numerator of $f^{(t)}$ for t in the stated range. We also know that $(p-1)!\,f(x)$ has integral coefficients. Because the product of p consecutive integers is divisible by all of $1, 2, 3, \ldots p$ and thus $p!$, pth and higher derivatives of $(p-1)!\,f(x)$ are polynomials in x

[5]Domenico Senato's "A Bijective Proof of the Fundamental Theorem on Symmetric Functions" article provides an alternative proof that does not require Abstract Algebra.

that have integral coefficients divisible by $p!$. This means that the pth and higher derivatives of $f(x)$ have integral coefficients which are all divisible by p. We also know, from the definition of $f(x)$ that all of the coefficients are also divisible by c^s. Thus, for $t \geq p$, the quantity $f^{(t)}(\beta_j)$ is a polynomial in β_j of degree at most $p-1+pr = s$, each of whose coefficients is divisible by pc^s. A symmetric function of $\beta_1, \beta_2, \ldots, \beta_r$ with integral coefficients and of degree at most s is an integer (because these are the roots of a polynomial with integral coefficients) provided each coefficient is divisible by c^s, by the fundamental theorem on symmetric functions. Therefore, the symmetric function $\sum_{j=1}^{r} f^{(t)}(\beta_j) = pk_t$, for $t = p, p+1, p+2, \ldots, p+s$, where the k_t are integers. It follows that $\sum_{j=1}^{r} F(\beta_j) = p\sum_{t=p}^{p+s} k_t$. Now, to finish proving that $\sum_{j=1}^{r} F(\beta_j) + kF(0)$ is a nonzero integer, we must show that $kF(0)$ is an integer that is not a multiple of p. We know from the definition of $f(x)$ that

$$f^{(t_1)}(0) = 0, f^{(p-1)}(0) = c^s c_r^p, f^{(t_2)}(0) = pK_{t_2},$$

where $t_1 = 0, 1, 2 \ldots, p-2$, $t_2 = p, p+1, \ldots, p+s$, and K_{t_2} are integers. If p is chosen to be greater than any of c, c_r, k, then $c^s c_r^p \not\equiv 0 \pmod p$. Therefore, $\sum_{j=1}^{r} F(\beta_j) + kF(0)$ is a nonzero integer. Now, the right hand side of the same equation is

$$\sum_{j=1}^{r} \beta_j \int_0^1 e^{(1-r)\beta_j} f(\tau\beta_j) d\tau$$

, which is a finite sum whose terms can each be made arbitrarily small by making p arbitrarily large. Therefore, we have that the left hand side is a nonzero integer, but the right hand side is very close to 0 for large p, a contradiction. Because we have reached a contradiction, our original assumption, that π is algebraic, must have been incorrect. ■

We have shown that π is transcendental, but why do we care? Algebraic numbers have clear applications with functions, but transcendental numbers are *negatively* defined, as in they are defined to strictly not have some property. Therefore, their applications are less obvious, but π being transcendental does have some important applications. For example:

Corollary 4.12. *Given a straightedge and a compass, we cannot construct a circle and a square with the same area.*

This problem is colloquially known as "Squaring the Circle," and is suprisingly nontrivial, requiring a few important steps. We will not go over the full proof, but we will go over a sketch of some important Lemmas and the overall structure of the proof. First, we need to figure out which numbers are constructible, and define exactly what those are!

Definition 4.13 (Constructible number)**.** A number n is said to be constructible if, given a straightedge and a compass, and knowing the length of 1 unit, we can construct a straight line that is n units long.

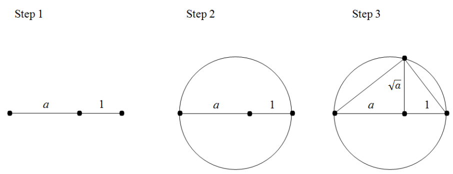
The idea of a constructible number is very simple, but finding all the operations the set of constructible numbers is closed on is tricky, and proving that those are the only operations is extremely difficult.

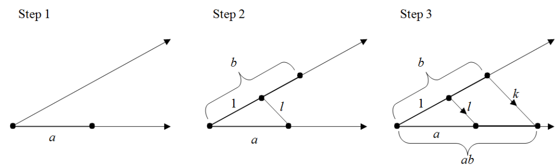
Lemma 4.14. *The constructible numbers are only closed over addition, subtraction, multiplication, division, and square roots.*

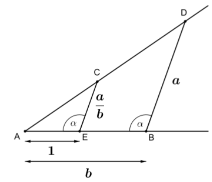
We will not go through a rigorous proof, but we will give an explanation of how to achieve each of these operations.

Proof. Addition and subtraction are clear; we simply use our straightedge to add/remove values to/from each other. Multiplication and division are a little trickier, but still quick to find—we take similar triangles to create ratios. The square root is where the compass comes in. We draw a circle with radius $a+1$, then draw a chord perpendicular to the diameter to divide the diameter into lengths of a and 1. The chord's length is n By power of a point, we have that $\frac{n^2}{4} = a$, and thus that $\frac{n}{2} = \sqrt{a}$. The chord is split in two evenly, so each of the halves has length $\sqrt{a}$. ■

Below are diagrams of how to find show that the constructible numbers are closed over square roots, multiplication, and division (as addition and subtraction are trivial).







The following lemma requires abstract algebra to prove, so we will take it to be true, and continue with the sketch of the proof.

Lemma 4.15. *All constructible numbers are algebraic over* $\mathbb{Q}$*,*

Taking this to be true, we have a circle with area πr^2, and without loss of generality, let $r = 1$. Therefore, we need to construct a square with area π, and thus side length $\sqrt{\pi}$. Because π is transcendental, $\sqrt{\pi}$ must be too (if $\sqrt{\pi}$ were a root of some polynomial $P(x)$, then π would be a root of $P(\sqrt{x})$, which can be manipulated to have terms of integral degree). Since $\sqrt{\pi}$ is transcendental, it is not constructible, a according to our lemma above. Therefore, we cannot "Square the Circle." Interestingly, it took nearly 2000 years since the problems introduction (in approximately 200 BC, by the Greeks) to prove that that squaring the circle is impossible. Despite the fact that many had conjectured that it was impossible over the previous years, the proof hinged on the fact that π is transcendental, which was only proven in 1882 by Lindemann.

The following final theorem about π is trivial with the information we have now.

Theorem 4.16. π^r *is irrational for all rational* r*.*

Unlike e^r, there are not many proofs that π^r is irrational for rational r that do not rely on π being transcendental. However, with this fact, our proof is very simple.

Proof. For the same reason as in our proof of e^r, proving that π^r is irrational is equivalent to proving that π^z is irrational for integers z, which is equivalent top roving that $\pi^|z|$, as if π^z is irrational, then so is π^{-z}. Because π is transcendental, there is no $q(\pi)^z = p$, with integers q, p, and z. Therefore, there is no $\pi^z = \frac{p}{q}$, and thus, π^z is irrational, and so is π^r. ■

In general, this type of proof is not optimal; taking a stronger claim and apply it to show that our statement is true is a very backward train of thought. When avoidable, we do not use this type of proof.

5. Miscellaneous Proofs of Irrationality

The first proof we will discuss is regarding inverse cosine, which is relatively simple.

Theorem 5.1. *For every odd integer* $n \geq 3$*, the number*

$$A(n) := \frac{1}{\pi} \arccos\left(\frac{1}{n}\right)$$

is irrational.

We know that $A(2) = \frac{1}{4}$ and $A(4) = \frac{1}{3}$, so we have to restrict our result to odd numbers.

Proof. We will use the sum-to-product formula for cosine:

$$\cos\alpha + \cos\beta = 2\cos\frac{\alpha+\beta}{2}\cos\frac{\alpha-\beta}{2}.$$

Using $\alpha = (k+1)\phi$ and $\beta = (k-1)\phi$ yields

$$cos(k+1)\alpha = 2cos\phi\cos k\phi - \cos(k-1)\phi.$$

Taking $\phi_n = \arccos(\frac{1}{\sqrt{n}})$, which clearly has $\cos\phi_n = \frac{1}{\sqrt{n}}$, under the domain $0 \le \phi_n \le \pi$. We have that

$$\cos k\phi_n = \frac{A_n}{\sqrt{n}^k}$$

defines a sequence A_k. We claim that A_k is a sequence of integral values, where no A_i is divisible by n. Let's look at the first few terms of our sequence. For $k = 0$, we have $\cos 0 = \frac{A_0}{=}1$, and for $k = 1$, we have $\cos\phi_n = \frac{A_1}{\sqrt{n}}$, which yields $A_1 = 1$ because $\cos\phi_n = \frac{1}{\sqrt{n}}$. Using our recurrence from before,

$$cos(k+1)\alpha = 2cos\phi\cos k\phi - \cos(k-1)\phi,$$

we get

$$cos(k+1)\alpha_n = \frac{2}{\sqrt{n}}\frac{A_k}{\sqrt{n}^k} - \frac{A_{k-1}}{\sqrt{n}^{k-1}} = \frac{2A_k - nA_{k-2}}{\sqrt{n}^{k+1}}.$$

Because the left hand side $\cos(k+1)\phi_n = \frac{A_{k+1}}{\sqrt{n}^{k+1}}$, we get $A_{k+1} = 2A_k - nA_{k-1}$. For odd n (so the coefficient of 2 does not complicate things), A_k must be a multiple of n for A_{k+1} to be a multiple of n. Since $A(1) = 1$ is not a multiply of any odd $n \ge 3$, A_i is not a multiple of n and must be integral for all i because our recurrence has integral coefficients. Now, let's assume, for the sake of contradiction, that

$$A(n) = \frac{1}{\pi}\phi_n = \frac{k}{\ell}$$

for integers $k, \ell > 0$. Then, clearing denominators gives us $\ell\phi_n = k\pi$. Taking the cosine of both sides, we get

$$\cos k\pi = \frac{A_\ell}{\sqrt{n}^\ell}.$$

The left hand side is ± 1, so $\sqrt{n}^\ell = \pm A_\ell$ is an integer, with $\ell \ge 2$, which rearranges to get $\frac{\pm A_\ell}{n} = \sqrt{n}^{\ell-2}$, which is an integer. This means that A_ℓ has at least on factor of n, a contradiction (as we deduced that A_i is not a multiple of n for any i because of the recurrence relation). Because we reached a contradiction, our assumption that $A(n)$ is rational is incorrect; $A(n)$ is irrational. ■

Whenever we prove something, especially something solitarily, it's important to ask "Why?" Why do we care about this result? Indeed, $A(n)$'s irrationality does have some important applications, particularly to Hilbert's third problem. In particular, this lemma is one of the key steps to showing that a regular tetrahedron cannot be equidecomposible with a cube.

Lemma 5.2. *For positive integers m_1, n_1 and integer k, $m_1 \arccos\frac{1}{3} = n_1\frac{\pi}{2} + k\pi$ has no solutions.*

Proof. We know that $\arccos\frac{1}{3} \ne \frac{p\pi}{q}$ by our proof of $A(n)$'s irrationality. Isolating $\arccos\frac{1}{3}$, we get

$$\arccos\frac{1}{3} = \frac{\pi}{m_1}(0.5n_1 + k)).$$

This is a contradiction, because since $m_1, n_1 \in \mathbb{Z}$, we have a representation of $\arccos\frac{1}{3}$ in terms of $\frac{p\pi}{q}$, which is impossible. Therefore, there must be no solutions (m_1, n_1, k). ■

Although $A(n)$ seemed like a rather specific function, its irrationality is actually applicable to other problems! Let's continue with some proofs regarding when sin and cos are irrational.

Let's first consider a few basic cases, then work our way up. Before we begin, however, we need to find the Taylor polynomial for $\sin x$ (and we can simply differentiate it to get the Taylor polynomial for $\cos x$.

Lemma 5.3. *The Taylor polynomial for $\sin x$ is $\sum_{n=0}^{\infty}\frac{(-1)^n x^{2n+1}}{(2n+1)!}$*

Proof. Define the Taylor polynomial to be $\sin x = \sum_{n=0}^{\infty} a_n x^n$. We know that

$$\sin^{(1)}(x) = \cos x, \sin^{(2)}(x) = -\sin x, \sin^{(3)}(x) = -\cos x, \sin^{(4)}(x) = \sin x,$$

so differentiating our Taylor polynomial four times, we get $\sin x = \sum_{n=0}^{\infty} a_n x^n = \sin^{(4)}(x) = \sum_{n=0}^{\infty} a_n n(n-1)(n-2)(n-3)x^{n-4}$. Equating coefficients gives us $a_n = a_{n+4}(n+4)(n+3)(n+2)(n+1)$. So, we have $a_{4x+k} = \frac{k! a_k}{(4x)!}$ for $0 \le k \le 3$. Now, let's consider our base cases $\sin x, \sin^{(1)}(x) = \cos x, \sin^{(2)}(x) = -\sin x, \sin^{(3)}(x) = -\cos x$ at $x = 0$. All the terms except the constant a_0 vanish in our first case, so we get $\sin 0 = 0 = a_0$. Next, we get $\sin'(x)_{x=0} = \cos 0 = 1 = a_1$. Continuing, we get $\sin^{(2)}(x)_{x=0} = -\sin 0 = 0 = 2a_2$, and thus

$a_2 = 0$. Finally, we have $\sin^{(3)}(x)_{x=0} = -\cos 0 = -1 = 6a_3$, so $a_3 = \frac{-1}{6}$. Our initial conditions give us that the Taylor polynomial for $\sin x$ is $\sum_{n=0}^{\infty} \frac{(-1)^n x^{2n+1}}{(2n+1)!}$. ■

Corollary 5.4. *The Taylor polynomial for* $\cos x$ *is* $\sum_{n=0}^{\infty} \frac{(-1)^n x^{2n}}{(2n)!}$

Proof. This is trivial given the Taylor polynomial for $\sin x$. Simply differentiate both sides of sine's Taylor polynomial and we get $\sum_{n=0}^{\infty} \frac{(-1)^n x^{2n}}{(2n)!}$. ■

Now that we have introduced the Taylor polynomials for $\sin x$ and $\cos x$, we are ready to move onto our first proof.

Lemma 5.5. *The value* $\sin 1$ *is irrational*[6].

The way we will go about proving this is by using the Taylor Series for $\sin x$ at $x = 1$, and showing that multiplying by $(2n+1)!$ for any n cannot yield an integral result.

Proof. Assume for the sake of contradiction, that $\sin 1 = \frac{p}{q}$. Let's plug in $x = 1$ to our Taylor Polynomial to get $\sum_{n=0}^{\infty} \frac{(-1)^n}{(2n+1)!}$. This gives us $\frac{1}{1!} - \frac{1}{3!} + \frac{1}{5!} \mp \cdots$. Let's multiply this by $(2n+1)!$, where n is large enough that $\frac{(2n+1)!}{q} \in \mathbb{Z}$. Multiplying, we get

$$Z_1 + \sum_{i=0}^{\infty} (-1)^{n+i+1} \frac{(2n+1)!}{(2n+3+2i)!},$$

where $Z_1 \in \mathbb{Z}$. Let's examine

$$0 < |A| = |\sum_{i=0}^{\infty} (-1)^{n+i+1} \frac{(2n+1)!}{(2n+3+2i)!}| < \frac{2n+1}{2n+3} < \frac{1}{(2n+3)(2n+2)} < 1.$$

Since we have that the absolute value of the fractional part of our sum is bounded by $0 < |A| < 1$, we have that $(2n+1)! \sin 1 = (2n+1)! \frac{p}{q} = Z_2 p = Z_1 \pm |A|$ for $Z_2 \in \mathbb{Z}$. Therefore, we have an integer, $Z_2 p$, is equal to $Z_1 \pm |A|$, which is not an integer. Because we have reached a contradiction, our assumption, that $\sin 1$ is rational, was incorrect. ■

We will not go over the proof for $\cos 1$, because slightly editing the proof for the Taylor polynomial for $\cos x$ is enough to prove that $\cos 1$ is irrational.

Intuitively, it makes sense that $\sin 1$ is irrational; after all, it doesn't have any factor of π in it.

Shifting away from trigonometric functions, we have $\log 2$. Once again, we can see that this is likely irrational, but let's definitively prove it.

Lemma 5.6. $\log 2$ *is irrational.*

Since this is the natural log, we sense that this question is somewhat related to whether e^x is rational. And in fact, that would be correct; we can use the fact that e, and thus, e^x is transcendental in our proof.

Proof. Let's assume, for the sake of contradiction, that $\log 2 = \frac{p}{q}$ (where p and q are integers), which gives us that $q \log 2 = p$, and thus, that $2^q = e^p$ for positive integers p and q. However, we know that e is transcendental, and thus, it cannot be the solution to polynomial $x^p = 2^q$. Therefore, there are no positive integers p and q such that $2^q = e^p$, meaning that we have a contradiction. Because we have reached a contradiction, our assumption that $\log 2$ is rational must have been incorrect. ■

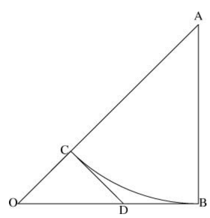
6. Techniques for Proving Irrationality

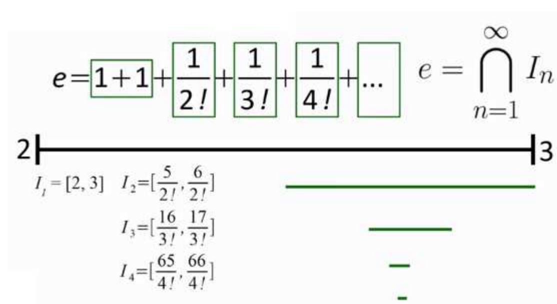
Although ideally we could have gone through several different techniques for proving irrationality through the different proofs, the most common ones are exactly of the previous ones. For simpler ones, we simply use a proof by contradiction, setting some irrational number $I = \frac{p}{q}$ and then doing a few manipulations to reach a contradiction. For more complicated ones, many proofs simply use a well thought-out function that has a few specific properties, then use that to show a contradiction. However, are there other types of proofs? Although many well-known proofs conform to the above types, there are many other types of proofs that can prove irrationality.

[6]Note that, like civilized mathematicians, we use radians by default.

6.1. **Geometric Proofs.** When we think of irrational numbers related to geometry, one of the first ones that comes to mind is π. Of course, the ratio between the diameter and the circumference is π, but how would be prove that their ratio is irrational? Currently, there is no geometric proof of π's irrationality, which is surprising because of π's definition being based on geometry. Luckily, another number is intimately related to geometry is $\sqrt{2}$. The most common proof that is taught was discussed at the beginning of this paper, but there are other proofs. Interestingly, the two most well-known geometric proofs of $\sqrt{2}$'s irrationality rely on Infinite Descent, just as the first proof we covered did. We will go over only one of the proofs, which is based on similar triangles.

Geometric Proof of Lemma 2.1. Before we begin, note that the (left) diagram below this proof depicts our construction. We assume, for the sake of contradiction, that $\sqrt{2}$ is a rational number. Therefore, we have $\sqrt{2} = \frac{p}{q}$ for $p, q \in \mathbb{Z}$, and $\gcd(p, q) = 1$. We can create a right triangle $\triangle ABO$ with the right angle at B with side lengths q, q, p, because $2q^2 = p^2$. This is the smallest such right triangle with integral side lengths because p and q share no factors. Now, draw in the $\frac{\pi}{4}$ sector of a Circle A with radius AB, and define the intersection point of Circle A and line segment AO to be point C. Now, draw the line tangent to the circle at point C, which is perpendicular to AO. Then, this line intersects OB at D, creating line CD, and triangle $\triangle OCD$. We know that $\triangle OCD \sim \triangle ABO$ by AAA similarity. We claim that $\triangle OCD$ also has integral sides. Because AB and AC are both radii of the same circle, $AB = AC = q$. Then, $OA - AC = OC$, so $OC = p - q$, and because $\triangle OCD$ is isosceles, $OC = CD = p - q$. We know by equal tangents that $CD = DB = p - q$, which means that $Od = 2q - p$. $2q - p$ and $p - q$ are both integral, because p, q are integral. Therefore, we have found a smaller similar triangle with integral side lengths, and we have a contradiction. Therefore, our assumption that $\sqrt{2}$ is rational must have been incorrect. ■





There are also geometric proofs that $\sqrt{m}$ is irrational for numbers that aren't perfect squares, but perhaps more interesting (and different) is a geometric proof that e is irrational. Instead of relying on a direct geometric construction, we will simulate the Taylor Series on a number line, as depicted above, on the right.

Geometric Proof of Lemma 3.2. Before we begin, note that the number line above (on the right) includes the diagram for our geometric proof. Consider the portion of the number line I_1 from 2 to 3. Take the second half of that portion of the number line, I_2, which gives us the section from 2.5 to 3. Next, take the the second third of I_2, which gives us I_3. Given some I_n, we find I_{n+1} by taking the second of $n+1$ equally spaced portions of I_n. this effectively adds $\frac{1}{(n+1)!}$ after every portion, simulating the Taylor Series for e. The intersection of I_n for all positive integral n is the sole point e on the number line.

We know that the for $n > 1$, I_{n+1} lies entirely within I_n, and the bounds for In are $\frac{a_1}{n!}$ and $\frac{a_2}{n!}$ (where a_1 and a_2 yield fractions as close as possible to e), which together imply that e does not lie on a point with denominator $n!$ for any positive n. However, this is a contradiction, because $e = \frac{p}{q} = \frac{p(q-1)!}{q!}$. Because we have reached a contradiction, our original assumption that e is rational must have been incorrect. ■

Geometric proofs, however, are at their core the same as the other types; they follow a proof by contradiction, and then use techniques in geometric form that are analagous to the algebraic form we have seen before, or at least use similar techniques. In fact, any proof by contradiction will fall prey to this, so the only other proof that is structurally different is a proof that is *not* by contradiction. However, is this even possible? After all, irrationality is negatively defined, so can we directly prove that a number is irrational, rather than proving that it is not rational. In fact, we can prove irrationality without a proof by contradiction.

6.2. **Direct Proofs.** Technically, it is not possible to provide a completely constructive proof; somewhere down the line, we are using a proof by contradiction, but there are several proofs that are structurally different and distinctly more direct than our other proofs. For example, proofs using continued fractions show that there is a nonrepeating infinite continue fraction representation of some number, which must be irrational. We will not discuss a specific proof of irrationality with continued fractions, because a major part of the proof is deriving the continued fraction, which is difficult.

Furthermore, another common type of proof is a bounding proof, which shows that there is a minimum difference between some rational number and any rational number, with the bound often in terms of the denominator of the rational approximation. Let's go over one example, with $\sqrt{2}$.

Bounding Proof of Lemma 2.1. Given two numbers p and q, the highest power of 2 dividing $2q^2$ is odd, and the highest power of 2 dividing p^2 is even. Therefore, p^2 and $2q^2$ must be distinct integers, and thus $|2q^2 - p^2| \geq 1$, Now, our approximation

$$|\sqrt{2} - \frac{p}{q}| = |\frac{q\sqrt{2} - p}{q}| = |\frac{2q^2 - p^2}{q(q\sqrt{2} + p)}| = |\frac{2q^2 - p^2}{q^2(\sqrt{2} + \frac{p}{q})}| \geq |\frac{1}{q^2(\sqrt{2} + \frac{p}{q})}| \geq \frac{1}{3q^2}.$$

The last inequality is true because because we assume that $\sqrt{2} + \frac{p}{q} \leq 3$, or that $\frac{p}{q} \leq 3 - \sqrt{2}$. If this weren't true, then we would already have a bound on the difference between $\frac{p}{q}$ and $\sqrt{2}$, so we assume it to be true to take the other case. We have a lower bound on the difference between $\sqrt{2}$ and $\frac{p}{q}$ for any integral, positive p, q. Therefore, $\sqrt{2}$ is distinctly apart from any rational. ■

Unlike our previous proofs, this is proving not that $\sqrt{2}$ is not rational, but instead proving that there is a distinction between $\sqrt{2}$ and any rational number.

7. Conclusion

Overall, proof by contradiction is one of the most prevalent methods of proving irrationality, but there are a few subdivisions within proof by contradiction that dictate how we go about the proof. More powerful, however, than irrationality is transcendence. Transcendence is extremely difficult to prove (note that we didn't even go over the full proof of π and e's transcendence because we did not prove the Lindemann-Weierstrass theorem), and consequently, very few numbers are proven to be transcendental. In fact, it is still unknown if πe, $\pi + e$, π^e, π^π, and e^e are transcendental. Even the proofs of irrationality were somewhat difficult, because although we were able to go over the proofs quickly, coming up with the functions with those specific properties is difficulty, especially during the first such proofs, such as in proving that e^4 is irrational. Many of the functions went unmotivated in this paper because it is simply very difficult to find those functions; other than searching for certain properties, we have no way of knowing why some certain function was chosen.

The deceivingly simple ideas of irrationality and transcendence hide their true nature: extremely difficult to prove. However, irrationality and transcendence continue to be very important properties, so we will continue searching for more proofs.

References

[1] Tom M. Apostol. Irrationality of the square root of two - a geometric proof. 2000.
[2] Arthur Jones. Abstract algebra and famous impossibilities. 1991.
[3] Steve Mayer. The transcendence of π. 2006.
[4] Ivan Niven. A simple proof that π is irrational. 1947.
[5] Ivan Niven. Irrational numbers. 1956.
[6] Miles Reid. Undergraduate commutative algebra. 1995.
[7] Jonathan Sondow. A geometric proof that e is irrational and a new measure of its irrationality. 2006.
[8] Karin Usadi Katz and Mikhail G. Katz. Meaning in Classical Mathematics: Is it at Odds with Intuitionism? *arXiv e-prints*, page arXiv:1110.5456, October 2011.
[9] Eric W. Weisstein. e continued fraction. 2020.
[10] Eric W. Weisstein. Pi approximations. 2020.