Pi is Transcendental:
Von Lindemann's Proof Made Accessible to Today's Undergraduates

Randy K. Schwartz
2 February 2006

Introduction

The proof that pi is a transcendental number, first provided by Carl Louis Ferdinand von Lindemann in 1882, was and remains one of the most celebrated results of modern mathematics. It was of interest in its own right, and it also resolved a host of questions that had focused the attention of mathematicians since ancient times.

The problem of "squaring the circle"— that is, constructing with straightedge and compass alone a square whose area equals that of a given circle— was one of the great problems of classical geometry. Ancient Greek geometers studying the circle had proven that the circumference, or "periphery", is proportional to the diameter, and that the area is proportional to the square of the radius. The proportionality constant in each case was eventually denoted by "pi", the first letter of the word "periphery" in Greek. The problem of squaring the circle, as well as several related problems, thus amounted to constructing the number pi by geometric means.

Successively more accurate approximations of pi by rational (and, thus, constructible) numbers, were achieved during ancient, medieval, and modern times, first by the use of purely geometric methods such as the construction of regular polygons inscribed or circumscribed about the circle, and later by the use of analytic methods such as Machin's formula. Eventually, in 1761, pi was proven to be irrational by Johann Heinrich Lambert, who employed a complicated approach based on continued fractions.[1] However, the irrationality of pi does not resolve the matter of squaring the circle, since many irrational numbers (most obviously, $\sqrt{2}$) are constructible.

Several of the classical construction problems, such as the trisection of an arbitrary angle, were proven impossible by showing that their solution would amount to constructing the roots of an irreducible polynomial of high degree.[2] Von Lindemann's work on pi showed that the squaring of the circle is an impossible problem in an even more profound sense, because he showed that no polynomial of *any* degree and with rational (or equivalently, integral) coefficients can include pi among its roots. Such numbers are said to be *transcendental* or *nonalgebraic*.

Von Lindemann, a professor of mathematics at the University of Freiburg, was a specialist in geometry and analysis, and had completed his doctoral thesis on a topic in non-Euclidean geometry under the direction of the renowned Felix Klein at Erlangen.[3] The French mathematician Charles Hermite had already established the transcendence of *e* in an 1873 paper [4] based largely on methods of number theory. While von Lindemann's proof [5] of the transcendence of pi does not actually rely on the transcendence of *e*, it uses substantially the same methods as those that had been employed by Hermite, together with the fact that $1 + e^{\pi i} = 0$, a consequence of Euler's formula. Interestingly, the latter equation is the only property of pi that comes into play in the proof, and it is used near the very beginning.

Successively modified and simplified versions of von Lindemann's proof were published (still in German) by Karl Weierstrass (1885), Paul Gordan (1893), and H. Weber (1902) [6]. All of these were still based largely on number theory. For example, Weber's proof [7] explicitly invokes Fermat's "little theorem" that if *p* is a prime that does not divide the integer *a*, then a^{p-1} is congruent to 1 (mod *p*). A proof based more on analytic methods, together with a few key number-theoretic facts, was published in 1952 by R. Steinberg and R. M. Redheffer at UCLA.[8]

My goal in this paper is to convey von Lindemann's result in a form that will be accessible to the average undergraduate mathematics major. I have mainly followed the presentation given by Hardy and Wright [9], which in turn is based on modifications and simplifications of von Lindemann's approach provided by Edmund Georg Hermann Landau and Oskar Perron. I have provided clarifying details where necessary, have simplified some of the notation, and have rearranged some of the order of presentation. I have also provided an introductory discussion, "Polynomial Preliminaries", to explain some key points of polynomial theory that are needed in the proof, including results from the "theory of equations" that are no longer normally taught to undergraduates, even back in my own day. Much of that introductory discussion, including my Lemmata 1 and 2 (which correspond to Theorems 203 and 202, respectively, in Hardy and Wright), is set forth without formal proof. Instead, I devised a series of convincing polynomial examples whose concreteness will provide the undergraduate reader greater insight than would be provided by a more abstract treatment like that given in the sources I have used.

Polynomial Preliminaries

As a necessary prelude to our presentation of von Lindemann's proof, we must recall some familiar properties of polynomial equations, and establish some less familiar ones.

The Fundamental Theorem of Algebra tells us that any polynomial of degree *n*, with complex coefficients, has exactly *n* complex roots if repeats are counted. Of course, what is true of the field of complex numbers is not true of other sets. For instance, if the coefficients are real, we are not guaranteed *n* real roots. Likewise with rational or integral coefficients.

On the other hand, the set of roots of a polynomial is such that certain *functions* of the roots are predictably well-behaved. For instance, if a polynomial with rational coefficients has complex roots, these occur in conjugate pairs, and the sum or product of any pair of conjugate roots will be real (in fact, rational). More generally, any *symmetric polynomial* of the roots will be rational. Although we will not give a proof, we provide an example below that suggests why this fact is true. This fact is a manifestation of the yet more general Fundamental Theorem of Symmetric Polynomials, part of the "theory of equations" developed by Viète, Girard, Descartes, Fermat, and others.

We call a polynomial *symmetric* if its value is unchanged by all permutations of its variables.

Ex 1. $f(x,y)=3x^2+4xy+3y^2$

$f(y,x)=3y^2+4yx+3x^2 = f(x,y)$, so *f* is symmetric.

Ex 2. $g(x,y)=3x^2+4xy+4y^2$

$g(y,x)=3y^2+4yx+4x^2 \neq g(x,y)$, so g is not symmetric.

Ex 3. Consider $f(x)=3x^3-x^2-x-4$

$=(3x-4)(x^2+x+1)$, with roots $x_1=\frac{4}{3}, x_2=-\frac{1}{2}+\frac{\sqrt{3}}{2}i, x_3=-\frac{1}{2}-\frac{\sqrt{3}}{2}i$.

Some symmetric polynomials of these roots include:

$$x_1 + x_2 + x_3 = \tfrac{4}{3} + (-\tfrac{1}{2} + \tfrac{\sqrt{3}}{2} i) + (-\tfrac{1}{2} - \tfrac{\sqrt{3}}{2} i) = \tfrac{1}{3}$$
$$x_1^2 + x_2^2 + x_3^2 = \tfrac{16}{9} + (-\tfrac{1}{2} - \tfrac{\sqrt{3}}{2} i) + (-\tfrac{1}{2} + \tfrac{\sqrt{3}}{2} i) = \tfrac{7}{9}$$
$$x_1 x_2 + x_1 x_3 + x_2 x_3 = (-\tfrac{2}{3} + \tfrac{2}{3}\sqrt{3}i) + (-\tfrac{2}{3} - \tfrac{2}{3}\sqrt{3}i) + 1 = -\tfrac{1}{3}$$
$$x_1 x_2 x_3 = \tfrac{4}{3}$$

Notice that, in each case, the irrational or imaginary parts "cancel each other out", and the result is rational. Notice, too, that since the highest-degree coefficient of *f* is 3, any symmetric polynomial of the *tripled* roots $3x_1, 3x_2, 3x_3$ will be an integer.

Next, consider an integral polynomial *f* of degree *m*, i.e.,

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_m x^m = \sum_{n=0}^{m} a_n x^n \text{ for integers } a_0, a_1, \ldots$$

As a notational convenience, Landau and others adopted an unusual symbolism that allows conciseness in writing certain often-recurring expressions involving the coefficients a_n and factorials of the exponents *n*. Specifically, they defined an associated polynomial of the same degree,

$$f(x+h) = f(x) + f'(x) + f''(x) + \cdots + f^{(m)}(x) \qquad \text{Eqn (1)}$$

It is very important to keep in mind that in this notation, *h* does not signify an actual quantity, nor does the plus sign in *x* + *h* signify an actual addition.[10] To avoid confusion, in this paper only the symbol *h* will be used in this special role, and *h* will not be used in any other role.

Some examples of this notation:

Ex 4. If $f(x) = x^3$, then $f(x+h) = x^3 + 3x^2 + 6x + 6$.

Ex 5. If $f(x) = 2 + 3x + 5x^2$, then $f(x+h) = (2 + 3x + 5x^2) + (3 + 10x) + 10$
$= 15 + 13x + 5x^2$.

As a special case of Eqn (1), note that substituting *x* = 0 leads to

$$f(h) = f(0) + f'(0) + f''(0) + \cdots + f^{(m)}(0)$$
$$f(h) = a_0 + a_1 + 2a_2 + 6a_3 + \cdots + m!a_m \qquad \text{Eqn (2)}$$

and as a further special case, note that substituting $f(x) = x^m$ in Eqn (2) leads to

$$h^m = 0 + 0 + 0 + \cdots + 0 + m! = m! \quad . \qquad \text{Eqn (3)}$$

We now make some observations that can be summarized concisely in this new notation.

Ex 6. Consider $f(x) = 2 + 3x + 5x^2$. Now pick an arbitrary integer, say 10.

Let $F(x) = \frac{x^{10}}{9!} f(x) = \frac{1}{9!}(2x^{10} + 3x^{11} + 5x^{12})$.

Then $F(h) = \frac{1}{9!}[2(10!) + 3(11!) + 5(12!)]$ using Eqn (3)

$$F(h) = 2(10) + 3(11 \cdot 10) + 5(12 \cdot 11 \cdot 10),$$

the result being a multiple of 10 due to the divisibility of each factorial by 9!.

This suggests, more generally, that for any integral polynomial and any integer $n > 1$, if $F(x) = \frac{x^n}{(n-1)!} f(x)$, then $F(h)$ is a multiple of n, or in other words $F(h) \equiv 0 \pmod{n}$.

In addition, if we let $G(x) = \frac{x^9}{9!} f(x) = \frac{1}{9!}(2x^9 + 3x^{10} + 5x^{11})$,

$$\text{then } G(h) = \frac{1}{9!}[2(9!) + 3(10!) + 5(11!)]$$

$$G(h) = 2 + 3(10) + 5(11 \cdot 10),$$

the result once again being an integer (due to the divisibility of each factorial by 9!), but this time congruent to 2, the 0th-degree term of f.

This suggests, more generally, that for any integral polynomial and any integer $n > 1$, if $G(x) = \frac{x^{n-1}}{(n-1)!} f(x)$, then $G(h) \equiv f(0) \pmod{n}$. Thus:

Lemma 1. Let f be an integral polynomial, and n a positive integer.

(a) If $F(x) = \frac{x^n}{(n-1)!} f(x)$, then $F(h) \equiv 0 \pmod{n}$.

(b) If $G(x) = \frac{x^{n-1}}{(n-1)!} f(x)$, then $G(h) \equiv f(0) \pmod{n}$.

The h notation also helps us relate polynomials to the Taylor series expansion for e^x. Returning to the polynomial used in Example 4,

Ex 7.
$$\begin{aligned}(x+h)^3 &= x^3 + 3x^2 + 6x + 6 \\ &= 6(\tfrac{x^3}{6} + \tfrac{x^2}{2} + \tfrac{x}{1} + 1) \\ &= 6[e^x - (\tfrac{x^4}{24} + \tfrac{x^5}{120} + \cdots)] \quad \text{using the Taylor series expansion for } e^x \\ &= 6e^x - x^3(\tfrac{x}{4} + \tfrac{x^2}{20} + \cdots).\end{aligned}$$

More generally,

$$(x+h)^n = n!e^x - x^n[\tfrac{x}{n+1} + \tfrac{x^2}{(n+1)(n+2)} + \cdots].$$

Now define

$$u_n(x) = \tfrac{x}{n+1} + \tfrac{x^2}{(n+1)(n+2)} + \cdots$$

so that

$$\begin{aligned}(x+h)^n &= n!e^x - x^n u_n(x) \\ &= h^n e^x - x^n u_n(x).\end{aligned}$$

Thus,

$$h^n e^x = (x+h)^n + x^n u_n(x) \quad \cdot$$

Now define

$$\varepsilon_n(x) = \frac{u_n(x)}{e^{|x|}}$$, where |x| denotes the magnitude of the complex number x,

so that

$$h^n e^x = (x+h)^n + x^n \varepsilon_n(x) e^{|x|}$$

$$\sum_{n=0}^{m} a_n h^n e^x = \sum_{n=0}^{m} a_n (x+h)^n + \sum_{n=0}^{m} a_n x^n \varepsilon_n(x) e^{|x|}$$

$$e^x \sum_{n=0}^{m} a_n h^n = \sum_{n=0}^{m} a_n (x+h)^n + e^{|x|} \sum_{n=0}^{m} a_n x^n \varepsilon_n(x) .$$

Thus, we have shown the following principle, which crystallizes a relation between polynomial and exponential functions:

Lemma 2. For any polynomial $f(x) = \sum_{n=0}^{m} a_n x^n$, if we let $f^*(x) = \sum_{n=0}^{m} a_n x^n \varepsilon_n(x)$,

then $e^x f(h) = f(x+h) + e^{|x|} f^*(x)$.

Proof of the Transcendance of Pi

Suppose, by way of proof by contradiction, that π were algebraic, i.e., a root of an integral polynomial:

$$b_0 + b_1\pi + b_2\pi^2 + b_3\pi^3 + \cdots + b_k\pi^k = 0 \quad \text{for integers } b_0, b_1, \ldots$$

This would imply that πi is a root of an integral polynomial of no more than twice that degree, since we would have:

$$b_0 - ib_1(\pi i) - b_2(\pi i)^2 + ib_3(\pi i)^3 + b_4(\pi i)^4 + \cdots + b_k\pi^k = 0$$

$$[b_0 - b_2(\pi i)^2 + b_4(\pi i)^4 - + \cdots] = i[b_1(\pi i) - b_3(\pi i)^3 + - \cdots]$$

$$[b_0 - b_2(\pi i)^2 + b_4(\pi i)^4 - + \cdots]^2 = -[b_1(\pi i) - b_3(\pi i)^3 + - \cdots]^2$$

$$[b_0 - b_2(\pi i)^2 + b_4(\pi i)^4 - + \cdots]^2 + [b_1(\pi i) - b_3(\pi i)^3 + - \cdots]^2 = 0 .$$

Renaming the variables, we can therefore deduce an integral polynomial equation satisfied by πi:

$$c_0 + c_1 x + c_2 x^2 + \cdots + c_m x^m = 0 \quad \text{for integers } c_0, c_1, \ldots \qquad \text{Eqn (4)}$$

By the Fundamental Theorem of Algebra this equation has m roots, call them ω_1, ω_2, …, ω_m, including πi. Focusing on the latter one first, by Euler's formula we have

$$e^{\pi i} = \cos\pi + i\sin\pi = -1 + 0i$$

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

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

The mere fact $1 + e^{\pi i} = 0$ does not imply that π is transcendental, even if we couple with this the fact that *e* itself is transcendental. Rather— and this is the key idea of the proof, and the main reason for its complexity— this fact must be combined with similar information about all of the other roots (besides *πi*) of the assumed polynomial in Eqn (4). These roots would have to be related to one another in ways that were explored above in Polynomial Preliminaries and that we will now exploit.

We now form similar terms for the other roots and multiply the results, knowing that the product is zero since at least one factor (the one with *πi*) is zero:

$$(e^0 + e^{\omega_1})(e^0 + e^{\omega_2})\cdots(e^0 + e^{\omega_m}) = 0\,.$$

Multiplying out,

$$e^0 + (e^{\omega_1} + e^{\omega_2} + \cdots + e^{\omega_m}) + (e^{\omega_1+\omega_2} + e^{\omega_1+\omega_3} + \cdots) + (e^{\omega_1+\omega_2+\cdots+\omega_m}) = 0\ .$$

Note that each term in the above expression corresponds to one of the 2^m subsets of the set of roots ω_1, ω_2, …, ω_m. We also record, for later reference, that each exponent is a symmetric integral polynomial of those roots. Renaming the exponents α_1, α_2, …, we get

$$\sum_{i=1}^{2^m} e^{\alpha_i} = 0\,.$$

The proof will amount to showing that the left side of this equation equals a nonzero integer plus a proper fraction, and so cannot equal zero, giving us the contradiction that we sought.

Recall that $\alpha_1 = 0$, and note that some of the other α_i could conceivably vanish as well (although of course, not all of them). We now re-index the α_i so that the first *n* of them are the nonvanishing ones:

$$\sum_{i=1}^{n} e^{\alpha_i} + \sum_{i=n+1}^{2^m} e^0 = 0$$

$$\sum_{i=1}^{n} e^{\alpha_i} + q = 0\text{, setting the integer } q = 2^m - n. \qquad \text{Eqn (5)}$$

With special reference to the highest-degree coefficient c_m of the polynomial in Eqn (4), we now choose any large prime number *p* satisfying

$$p > q,\quad p > c_m,\quad p > |\,(c_m\alpha_1)(c_m\alpha_2)\cdots(c_m\alpha_n)\,|$$

and consider the polynomial

$$\phi(x) = \frac{c_m^{p-1}}{(p-1)!} x^{p-1} [c_m^n (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)]^p \qquad \text{Eqn (6)}$$

whose degree is $np + p - 1$. Multiplying Eqn (5) by $\phi(h)$ gives

$$\phi(h)\sum_{i=1}^{n} e^{\alpha_i} + q\phi(h) = 0$$

$$\sum_{i=1}^{n} e^{\alpha_i}\phi(h) + q\phi(h) = 0 \quad \text{since } \phi(h) \text{ is independent of } i$$

$$\sum_{i=1}^{n} [\phi(\alpha_i + h) + e^{|\alpha_i|}\phi^*(\alpha_i)] + q\phi(h) = 0 \quad \text{by Lemma 2}$$

$$\sum_{i=1}^{n} \phi(\alpha_i + h) + \sum_{i=1}^{n} \phi^*(\alpha_i) e^{|\alpha_i|} + q\phi(h) = 0$$

$$s_1 \; + \; s_2 \; + \; s_3 \; = 0 \text{, by way of abbreviation.} \qquad \text{Eqn (7)}$$

We now systematically evaluate s_1, s_2, and s_3.

First, we will show that s_1 is an integral multiple of the chosen prime p. To evaluate s_1, we start with Eqn (6) and note that shifting the polynomial $\phi(x)$ by any of the displacements α_i creates a net additional factor x, i.e., p of them versus $p - 1$:

$$\phi(x+\alpha_i) = \frac{c_m^{p-1}}{(p-1)!} (x+\alpha_i)^{p-1} [c_m^n (x+\alpha_i-\alpha_1)(x+\alpha_i-\alpha_2)\cdots(x+\alpha_i-\alpha_{i-1})(x)(x+\alpha_i-\alpha_{i+1})\cdots(x+\alpha_i-\alpha_n)]^p$$

$$= \frac{x^p}{(p-1)!} c_m^{p-1} (x+\alpha_i)^{p-1} [c_m^n (x+\alpha_i-\alpha_1)(x+\alpha_i-\alpha_2)\cdots(x+\alpha_i-\alpha_{i-1})(x+\alpha_i-\alpha_{i+1})\cdots(x+\alpha_i-\alpha_n)]^p .$$

Summing the results gives

$$\sum_{i=1}^{n} \phi(x+\alpha_i) = \frac{x^p}{(p-1)!} \sum_{i=1}^{n} c_m^{p-1} (x+\alpha_i)^{p-1} [c_m^n (x+\alpha_i-\alpha_1)(x+\alpha_i-\alpha_2)\cdots(x+\alpha_i-\alpha_{i-1})(x+\alpha_i-\alpha_{i+1})\cdots(x+\alpha_i-\alpha_n)]^p .$$

The summation portion of the right side is a polynomial in x of degree $(p - 1) + (n - 1)\, p = np - 1$. Multiplying out, and combining like terms, we get

$$\sum_{i=1}^{n} \phi(x+\alpha_i) = \frac{x^p}{(p-1)!} \sum_{j=1}^{np-1} \beta_j x^j \qquad \text{Eqn (8)}$$

where each coefficient β_j is a symmetric integral polynomial of the constants $c_m\alpha_1$, $c_m\alpha_2$, …, $c_m\alpha_n$. Recall that each α_i is itself a symmetric integral polynomial of ω_1, ω_2, …, ω_m, which are the roots of a polynomial having integer coefficients, with c_m being the highest-degree coefficient. Recalling Example 3 above, by the

Fundamental Theorem of Symmetric Polynomials we can conclude that β_j is an integer for $j = 0, 1, \ldots, np - 1$. This allows us to apply Lemma 1(a) to Eqn (8), yielding

$$\sum_{i=1}^{n} \phi(h + \alpha_i) \equiv 0 \pmod{p}$$

$$s_1 \equiv 0 \pmod{p} \ . \qquad \text{Eqn (9)}$$

Next, we will show that s_2 can be made vanishingly small by choosing the prime p to be sufficiently large. To evaluate s_2 we first note, from DeMoivre's formula and the Triangle Inequality for complex numbers, that

$$|z_1 z_2| = |z_1||z_2| \quad \text{and} \quad |x - \alpha_i| \le |x| + |\alpha_i| \quad \text{for } i = 1, 2, \ldots$$

Thus,

$$|(x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n)| \le (|x| + |\alpha_1|)(|x| + |\alpha_2|)\cdots(|x| + |\alpha_n|)$$

But by Eqn (6),

$$|\phi(x)| \le \left| \frac{c_m^{p-1}}{(p-1)!} x^{p-1} [c_m^n (x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n)]^p \right| ,$$

so

$$|\phi(x)| \le \frac{|c_m|^{np+p-1} |x|^{p-1} [(|x| + |\alpha_1|)(|x| + |\alpha_2|)\cdots(|x| + |\alpha_n|)]^p}{(p-1)!} .$$

As we let p increase without bound, $(p - 1)!$ eventually overtakes the pth power of any constant, so the right-hand fraction can be made arbitrarily small. Thus, $|\phi(x)|$ can be made arbitrarily small by sufficiently large choice of p. The same can be said of $|\phi^*(x)|$, since by definition each term of ϕ^* is identical to the corresponding term of ϕ except for the additional factor $\varepsilon_n(x)$, which is independent of p. Thus, $|\phi^*(x)|$ can be made arbitrarily small, and we chose p in such a way that

$$|s_2| = \left| \sum_{i=1}^{n} \phi^*(\alpha_i) e^{|\alpha_i|} \right| < 1 \ . \qquad \text{Eqn (10)}$$

Finally, we will show that s_3 is an integer not divisible by p. To evaluate s_3, recall the definition of ϕ from Eqn (6),

$$\phi(x) = \frac{c_m^{p-1}}{(p-1)!} x^{p-1} [c_m^n (x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n)]^p$$

$$\phi(x) = \frac{x^{p-1}}{(p-1)!} c_m^{p-1} [c_m^n (x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n)]^p .$$

Multiplying out, and combining like terms, we get

$$\phi(x) = \frac{x^{p-1}}{(p-1)!}\sum_{j=1}^{np}\gamma_j x^j \qquad \text{Eqn (11)}$$

where each coefficient γ_j is a symmetric integral polynomial of the constants $c_m\alpha_1$, $c_m\alpha_2$, …, $c_m\alpha_n$. For example, the lowest-degree coefficient is

$$\gamma_0 = c_m^{p-1}[c_m^n(0-\alpha_1)(0-\alpha_2)\cdots(0-\alpha_n)]^p$$

$$= (-1)^{np}c_m^{p-1}[(c_m\alpha_1)^p(c_m\alpha_2)^p\cdots(c_m\alpha_n)^p].$$

Again by the Fundamental Theorem of Symmetric Polynomials, γ_j must be an integer for $j = 0, 1, \ldots, np$. We can thus apply Lemma 1(b) to Eqn (11), so that $\phi(h)$ is an integer satisfying

$$\phi(h) \equiv \gamma_0 \pmod{p},$$

that is,

$$\phi(h) \equiv (-1)^{np}c_m^{p-1}[(c_m\alpha_1)^p(c_m\alpha_2)^p\cdots(c_m\alpha_n)^p] \pmod{p}.$$

Thus,

$$s_3 = q\phi(h) \equiv (-1)^{np}qc_m^{p-1}[(c_m\alpha_1)^p(c_m\alpha_2)^p\cdots(c_m\alpha_n)^p] \pmod{p}.$$

Note, then, that p does not divide s_3, since we defined the prime in such a way that

$$p > q, \quad p > c_m, \quad p > |(c_m\alpha_1)(c_m\alpha_2)\cdots(c_m\alpha_n)|.$$

Thus, s_3 is not congruent to 0 (mod p). Combining this with Eqn (9) implies that neither is $s_1 + s_3$ congruent to 0 (mod p). In particular, it cannot be *equal* to zero:

$$s_1 + s_3 \neq 0,$$

and so in absolute value,

$$|s_1 + s_3| \geq 1.$$

Combining this with Eqn (7), we get

$$|-s_2| \geq 1$$

$$|s_2| \geq 1,$$

which contradicts Eqn (10).

Thus, our original supposition that π is algebraic was false, QED.

Endnotes

1. Accessible proofs of the irrationality of *e* and pi, utilizing the Taylor series expansion of e^x and other analytic properties of the exponential and sinusoidal functions, are provided by G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Fifth edition (Oxford: Clarendon Press, 1993), pp. 46-47.

2. See Felix Klein, *Famous Problems of Elementary Geometry*, trans. Wooster Woodruff Beman and David Eugene Smith (Mineola, NY: Dover, 1956, 2003), esp. pp. 13-15.

3. John J. O'Connor and Edmund F. Robertson, "Carl Louis Ferdinand von Lindemann", available on the MacTutor History of Mathematics archive at the School of Mathematics and Statistics, University of St. Andrews, Scotland, http://www-groups.dcs.st-and.ac.uk/~history/Mathematicians/Lindemann.html.

4. Charles Hermite, "Sur la function exponentielle", *Comptes Rendus de l'Académie des Sciences* 77 (1873), pp. 18-24, 74-79, 226-233, and 285-293; also available in Charles Hermite, *Œuvres*, vol. 3 (Paris: Gauthier-Villars, 1912), pp. 150-181.

5. Ferdinand von Lindemann, "Ueber die Zahl π", *Mathematische Annalen* 20 (1882), pp. 213-225.

6. Karl Weierstrass, "Zu Hrn. Lindemann's Abhandlung: 'Über die Ludolph'sche Zahl'", *Sitzungsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin* 2 (1885), pp. 1067-1086; Paul Gordan, "Transcendenz von *e* und π", *Mathematische Annalen* 43 (1893), pp. 222-224; H. Weber, *Lehrbuch der Algebra, Vols. I-II* (New York: Chelsea, 1902).

7. I am basing this on my reading of a redaction of Weber's proof, in English, given in Heinrich Dörrie, *100 Great Problems of Elementary Mathematics: Their History and Solution* (New York: Dover, 1965), pp. 128-137 (Number 26, "The Hermite-Lindemann Transcendence Theorem").

8. R. Steinberg and R. M. Redheffer, "Analytic proof of the Lindemann theorem", *Pacific Journal of Mathematics* 2 (1952), pp. 231–242. Also available online at http://projecteuclid.org/Dienst/UI/1.0/Summarize/euclid.pjm/1103051870.

9. Hardy and Wright, op. cit., pp. 170-177.

10. On the other hand, the use of $x + h$ helped motivate the definition in Eqn (1) as a formal Taylor expansion.