Squaring the Circle:
Ancient Problems and Modern Solutions

Contents

> Meton: Ah! These are my special rods for measuring the air ... so all I have to do is to attach this flexible rod at the upper extremity, take the compasses, insert the point here, and - you see what I mean?
> Peisthetaerus: No.
> Meton: Well I now apply the straight rod - so - thus squaring the circle: and there you are.
>
> *Aristophanes, 'Birds'*

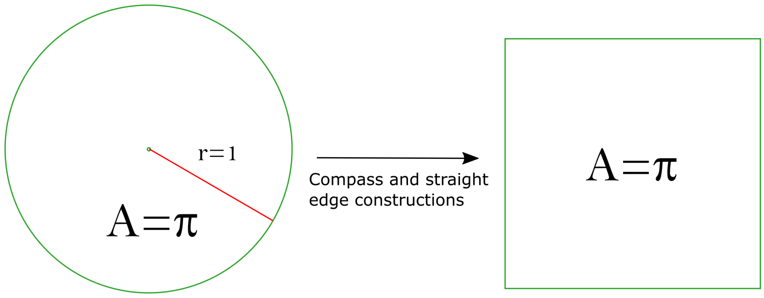
1 Introduction

In 1882, in Freiburg in Germany, Ferdinand von Lindemann disproved a conjecture which had stood unproven for the previous two millennia. This problem, one of the most obstinate in academic history, finally fell to the relentless tide of mathematical endeavour and discovery; Lindemann had disproved the possibility of squaring the circle.

1.1 Squaring the Circle

Squaring the Circle is one of the oldest questions in mathematics. Although the earliest dat of its study is not known, it is thought to date to before 428BC and was well known even at that time[4, 8]. Its statement is simple:

Conjecture. Squaring the Circle, Version 1:
Given a circle of unit radius, it is possible to construct a square of the same area in finitely many steps using only an idealised straight edge and compass.



Despite its apparent triviality, its proof (or disproof) has been pondered by some of the greatest minds in mathematics. Given its antiquity, it should not be surprising that is also one of the most famous problems in mathematics. Indeed, the phrase "like squaring the circle" has entered the English language in its own right, to describe an impossible task.[1]

1.2 Notoriety

To modern readers, given the synonymy of "squaring the circle" with the word "impossible", it may be surprising that it was thought by many to be possible until the mid 19^{th} century[5]. In fact even after it was disproved amateur mathematicians continued to publish false 'proofs', to mixed responses of acclaim and ridicule.[2] This was at least in part due to a misunderstanding of what the question was actually asking, and how it was disproved. In light of this, let us begin to consider the solution.

[1]This makes researching it very difficult. The phrase is used in the titles of articles in fields from economics to psychology to nuclear physics.

[2]Most famously, in 1897 Edward J. Goodwin attempted to have the Indiana General Assembly pass a bill declaring his method of squaring the circle as fact. It implicitly redefined π as 3.2, and was eventually rejected. [6]

2 Compasses and Straight Edges

Before we can understand Lindemann's approach to the question, we need to understand more about compass and straight edge constructions, and what it means for a number to be *constructible*.

2.1 Elementary Constructions

Most people come into contact with compass and straight edge constructions in high school. The idea is to construct shapes, angles, and lengths using an 'idealised compass and straight edge'; a pair of compasses which can stretch infinitely far and an infinitely long ruler with no distances marked on.
Using these tools, we can:

- draw a line passing through two points
- extend an existing line indefinitely
- draw a circle about a point which passes through another point
- define points at the intersections of lines (and/or circles)

and nothing else. This limited set of operations allows us construct a lot of things: squares, equilateral triangles, perpendicular bisectors through points, bisectors of angles, and many more.[3] As well as this, there is some notion of arithmetic which we can perform with these tools. It is this that shall be explored in this chapter.

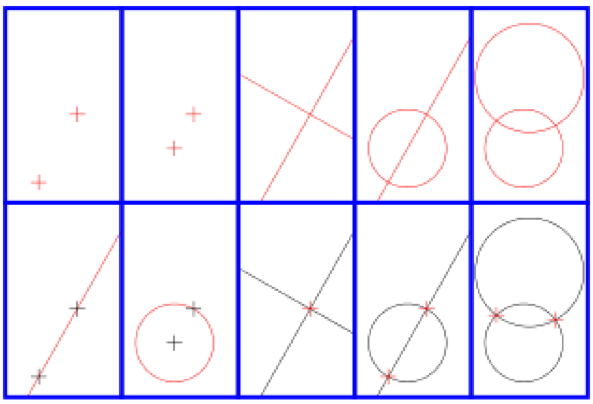


Figure 1: The basic operations which can be done within compass and straight edge constructions. [1]

[3]The proofs and constructions of these objects are not given in this essay, but can be found for example in Book 1 of Euclid's Elements [3]

2.2 Constructible Numbers

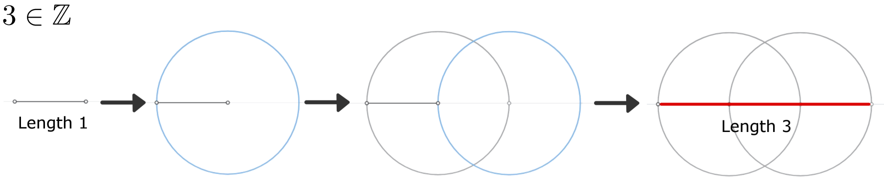
The constructible numbers are the numbers we can 'make' using a pair of compasses and a straight edge. There are two slightly different ways of defining them:

2.2.1 Ancient Greek definition

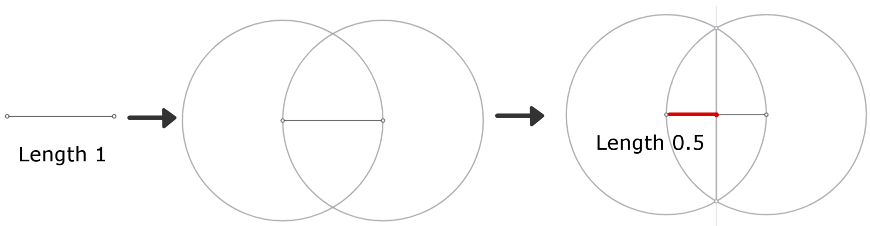
Definition. *(Ancient Greek definition) Take some line segment in the plane and call it length 1. Then we say a number* $n \in \mathbb{R}_{>0}$ *is* constructible *if, using a compass and straight edge, we can create a line segment of length* n *in finitely many steps.*

For example, these are all constructible numbers according to the Greek definition:

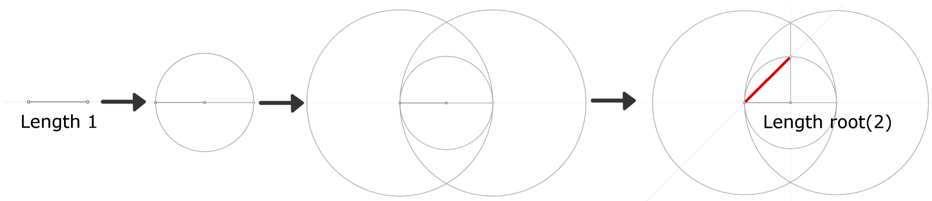
- $3 \in \mathbb{Z}$



- $\frac{1}{2} \in \mathbb{Q}$



- $\sqrt{2} \in \mathbb{R} \backslash \mathbb{Q}$



2.2.2 Modern definition

The definition above was the one used by the Ancient Greeks, but we can expand it to the more modern idea of the complex plane in an intuitive way. We begin by considering the given initial unit line to be the line between $(0, 0)$ and $(1, 0)$ in the complex plane. We then define some concepts:

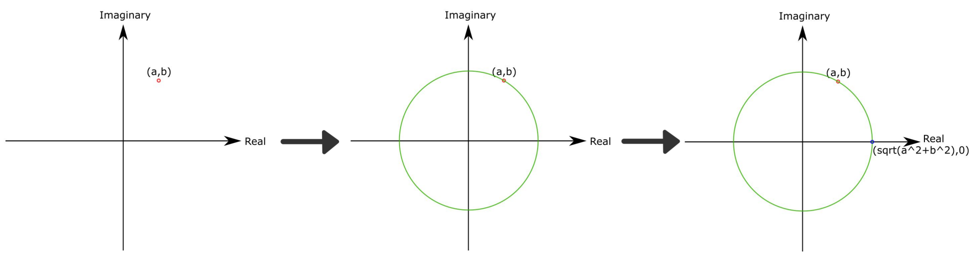
Definition. *A point (x, y) in the plane is called a* constructible point *if a series of straight lines and circles may be drawn starting from the unit line such that (x, y) is the intersection point of*

- *Two lines,*
- *Two circles, or*
- *A line and a circle*

Definition. *A number $\alpha = a + bi \in \mathbb{C}$ is a* constructible number *if the point (a, b) in the plane is a* constructible point*.*

This definition allows us to precisely define the numbers we can draw with these tools: the compasses and straight edge only let us draw circles and straight lines, so any point we can define is the intersection of some combination of these. Further, any line segment can only be defined by the points which mark its endpoints[4]. Hence the numbers we can reach are controlled precisely by the points we can create as intersections of these elements.

Note in particular that this new definition works with our other definition for positive real numbers: if a line of some length $\beta \in \mathbb{R}_{>0}$ can be drawn in the plane, we can imagine setting our compasses to the length of this line and drawing a circle of radius β about the origin. This circle will intersect the line $y = 0$ at $(\beta, 0)$, and so β is constructible by our new definition (the same clearly works in the other direction for $\mathbb{R}_{>0}$).



[4]This the third definition of Book 1 of Euclid's Elements [3]

2.3 Closure of the Constructible Numbers

Now that we have defined what the constructible numbers are, we consider what we can do with them.

Claim. *The only five operations which can be done using a pair of compasses and a straight edge are* $+, -, \times, \div,$ *and* $\sqrt{\ }$.

This is a long proof, which works based on considering the possible intersection points of a general circle and straight line in Cartesian coordinates. The proof is omitted here but can be found in [2]. For a flavour, we shall see how to take square roots:

Proof. (*Square roots can be taken using a compass and straight edge*)
Let $\alpha := a + bi$ be constructible. Construct line of length $|\alpha| + 1$ and draw a circle with this line as its diameter. Construct a perpendicular to the diameter 1 unit from its intersection with the circle. The length of this perpendicular between the diameter and the circle is $\sqrt{|\alpha|} = |\sqrt{\alpha}|$.

Then draw the line connecting α and the origin. Using results from [3] we can bisect the angle between this line and the positive x-axis. The intersection of this bisecting line and a circle about the origin of radius $|\sqrt{\alpha}|$ is the point $\sqrt{\alpha}$, which can be easily shown by considering that

$$\alpha = re^{i\theta}, r \in \mathbb{R}_{>0}, \theta \in [0, 2\pi]$$

and so

$$\sqrt{\alpha} = \sqrt{r}e^{i\frac{\theta}{2}}$$

□

2.3.1 Classification by Towers of Sets

Since we already know that we can easily construct any rational, we can now completely classify the constructible numbers as the quadratic closure of the rational numbers[5]. To consider this a little more rigorously:

Definition. *We may define a set K of sequences of sets (K_n) as follows:*

$$K_0 := \mathbb{Q}$$
$$K_{i+1} := \{a + b\sqrt{c_i} : a, b \in K_i\} \text{ for some fixed } c_i \in K_i.$$

Note that the sequence $(K_n) \in K$ then depends on the choices of c_i. Then we can say that the set of constructible numbers is

$$\{x \in \mathbb{C} : x \in K_i \text{ for some } i < \infty, \text{ where } K_i \in (K_n) \text{ for some } (K_n) \in K\}$$

Which is precisely the set of all numbers which can be reached using finitely many applications of the operations $+, -, \times, \div,$ *and* $\sqrt{\ }$.

With this behind us, we can see where π stands with the constructible numbers.

[5] the smallest field containing the rationals which is closed under square roots

2.4 Lindemann's Approach to Squaring the Circle

Lindemann's solution to the problem of Squaring the Circle uses an alternative phrasing of the conjecture:

Conjecture. Squaring the Circle, Version 2
The number π is constructible.

Proof. (Equivalence of conjectures)
Version 1 $\Rightarrow$ Version 2:
Take a unit circle in the plane. The area of this circle is

$$\pi r^2 = \pi \times 1^2 = \pi$$

Hence any square with the same area as this circle has area π, and so side length $\sqrt{\pi}$. Then π is constructible by squaring this side length.

Version 1 $\Leftarrow$ Version 2:
π is constructible $\Rightarrow$ $\sqrt{\pi}$ is constructible, since the constructible numbers are closed under square roots. Then constructing a square with a given side length is trivial using the elementary constructions above (a full construction is given in [3]). This square will have area

$$\sqrt{\pi}^2 = \pi = \text{Area of unit circle}$$

$\square$

Using this reduction of the question, Lindemann was able to see this not as a question of geometry but of algebra. If the problem of squaring the circle were impossible, all that would be required to prove it would be to show that π is not constructible.

3 Algebraic Numbers

We now examine a set of numbers which may seem tangential to our question, but is in fact very useful: the *algebraic numbers.*

3.1 The algebraic numbers

Definition. *(From [10]) A number $\alpha \in \mathbb{R}$ is called* algebraic over $\mathbb{Q}$ *(or just* algebraic*) if there exists a nonzero polynomial f with coefficients in $\mathbb{Q}$ such that $f(\alpha) = 0$. A number $x \in \mathbb{R}$ which is not algebraic is called transcendental. We define the set of algebraic numbers as $\bar{\mathbb{Q}}$.*

Some common examples of algebraic numbers are:

- $\frac{a}{b} \in \mathbb{Q}$, the root of $bx - a = 0$
- $\sqrt[n]{a}, a \in \mathbb{Z}$, a root of $x^n - a = 0$
- $i \in \mathbb{C}$, a root of $x^2 + 1 = 0$

3.2 Classification of the algebraic numbers

The algebraic numbers are actually a field, but before we can show this we must first understand the following theorem.

3.2.1 Fundamental Theorem of Symmetric Functions

Definition. *A symmetric function in n variables is a function f such that for any permutation $\sigma \in S_n$,*

$$f(x_1, x_2, \dots, x_n) = f(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)})$$

i.e. changing the order of the variables does not change the value of the function. For example,

$$f(x, y) := x^2y^3 + x^3y^2 \tag{1}$$

is a symmetric function in two variables.

Definition. *The elementary symmetric functions in n variables*

$$\{e_i : i \in \{1, \dots, n\}\}$$

are the symmetric functions formed by taking sums of groups of variables i at a time. For example,

$$\begin{aligned} e_1 &:= x_1 + \cdots + x_n \\ e_2 &:= x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n \\ e_3 &:= x_1x_2 \dots x_n \end{aligned}$$

.

Theorem. *(Fundamental Theorem of Symmetric Functions)*
For any symmetric function $f \in \mathbb{K}[x_1, \ldots, x_n]$, there is some function $g \in \mathbb{K}[e_1, \ldots, e_n]$ such that

$$f(x_1, \ldots, x_n) = g(e_1, \ldots, e_n)$$

For example using (1),

$$\begin{aligned} f(x, y) &= x^2y^3 + x^3y^2 \\ &= (x + y)(x^2y^2) \\ &= (x + y)(xy)^2 \\ &= e_1(e_2)^2 \end{aligned}$$

Proof. The proof is omitted for the sake of brevity here, but may be found in [9]. □

3.2.2 Closure of the algebraic numbers

We can now use the previous theorem to prove our claim.

Claim. *The algebraic numbers are a field.*

Proof. (Adapted from [9]) Note firstly that $\bar{\mathbb{Q}} \subset \mathbb{C}$ which is a field, so we need only show closure of $\bar{\mathbb{Q}}$ under addition and multiplication, and the existence of inverses within the set.

Let $\alpha, \beta \in \bar{\mathbb{Q}}$ Then there exist polynomials with integer coefficients

$$\begin{aligned} f(x) &:= f_nx^n + \ldots f_1x + f_0, \text{ and} \\ g(x) &:= g_mx^m + \ldots g_1x + g_0 \end{aligned}$$

such that $f(\alpha) = 0$ and $g(\beta) = 0$.

1. α is a root of $f(x)$, so $-\alpha$ is a root of $f(-x)$ which clearly has integer coefficients. Hence $-\alpha \in \bar{\mathbb{Q}}$.

2. Since α is a root of f,

   $$f(\alpha) = f_n\alpha^n + \ldots f_1\alpha + f_0 = 0$$

   Multiplying both sides by α^{-n}, we get

   $$f_n + \ldots f_1\alpha^{n-1} + f_0\alpha^{-n} = 0$$

   Hence α^{-1} is a root of $\bar{f}(x) := f_0x^n \ldots f_{n-1}x + f_n$, and $\alpha^{-1} \in \bar{\mathbb{Q}}$

3. Let $\{\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n\}$ be the roots of f, and $\{\beta = \beta_1, \beta_2, \ldots, \beta_m\}$ be the roots of g, so

$$f(x) = \prod_{i=1}^{n}(x - \alpha_i) \text{ and}$$
$$g(x) = \prod_{j=1}^{m}(x - \beta_j)$$

   We then define a function F as

$$F(x) := \prod_{i=1}^{n}\prod_{j=1}^{m}(x - (\alpha_i + \beta_j))$$

   Clearly $(\alpha + \beta) = (\alpha_1 + \beta_1)$ is a root of F, so we need only show that F has rational coefficients.

   If we consider the expansion of F, it's clear that the coefficients of x are symmetric polynomials in $\alpha_1, \alpha_2, \ldots, \alpha_n$ and $\beta_1, \beta_2, \ldots, \beta_m$. If we fix one of these coefficients, we can consider it as a polynomial in $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ with coefficients in $\mathbb{Q}[\beta_1, \beta_2, \ldots, \beta_m]$. Since it is symmetric, we know by the Fundamental Theorem of Symmetric Polynomials (3.2.1) that it is also a polynomial in the symmetric sums $e_1, \ldots, e_n$ of the α_is with coefficients in $\mathbb{Q}[\beta_1, \beta_2, \ldots, \beta_m]$. Since we also know that all of the symmetric sums $e_1, \ldots, e_n$ are coefficients in f, we know that they are all rational. Hence each coefficient of F is a symmetric polynomial in $\beta_1, \beta_2, \ldots, \beta_m$ with rational coefficients. Using the Fundamental Theorem of Symmetric Functions again in the same way, we can see that the symmetric sums $e'_1, \ldots, e'_n$ of the β_is are also rational numbers, since they are the coefficients of g. Therefore all of the coefficients of F are rational, and so $(\alpha + \beta) \in \bar{\mathbb{Q}}$.

4. Use the exact same argument as in 3, but letting

$$F(x) := \prod_{i=1}^{n}\prod_{j=1}^{m}(x - \alpha_i\beta_j)$$

$\square$

3.3 Relation to the constructible numbers

Claim. *Let α be a constructible number, so $\alpha \in K_r$ for some $r \in \mathbb{N}$ and $(K_n) \in K$. Then for every $l \leq r$, α is a root of some polynomial of order 2^l with coefficients in K_{r-l}.*

Proof. We will proceed by induction on l.

Clearly α satisfies the polynomial $(x - \alpha) = 0$, which has order $2^0 = 1$ and coefficients in K_r.
Assume then that α is the root of some polynomial of order 2^{n-1} and coefficients in $K_{r-(n-1)}$. Then we may write this polynomial (after dividing by the leading coefficient if necessary) as

$$x^{2^{n-1}} + a_{(2^{n-1}-1)}x^{(2^{n-1}-1)} + \cdots + a_1 x + a_0 = 0$$

where each $a_i \in K_{r-(n-1)}$. Then we know that if $n \leq r$ each a_i may be written as $a_i = \beta_i - \gamma_i\sqrt{C}$, for some β_i, γ_i and fixed $C \in K_{r-n}$.
Then we can rewrite the above equation as

$$x^{2^{n-1}} + \cdots + (\beta_n - \gamma_n\sqrt{C})x^n + \cdots + (\beta_1 - \gamma_1\sqrt{C})x + (\beta_0 - \gamma_0\sqrt{C}) = 0$$

and so

$$x^{2^{n-1}} + \cdots + \beta_n x^n + \cdots + \beta_1 x + \beta_0 = \sqrt{C}(\cdots + \gamma_n x^n + \cdots - \gamma_1 x + \gamma_0)$$

Then we can square both sides and see that

$$(x^{2^{n-1}} + \cdots + \beta_n x^n + \cdots + \beta_1 x + \beta_0)^2 - C(\cdots + \gamma_n x^n + \cdots + \gamma_1 x + \gamma_0)^2 = 0$$

Which is a polynomial with coefficients in K_{r-n} and order $2(2^{n-1}) = 2^n$. Since all we have done is rearrange, α is still a root. Hence by induction the proposition holds for all $l \leq r$. □

Theorem. *If $\alpha \in \mathbb{C}$ is constructible, then α is algebraic.*

Proof. By setting $l = r$ in the previous result, we can see that if α is a constructible number, then it is the root of a polynomial with coefficients in $K_0 = \mathbb{Q}$ and so is algebraic. □

This is an important result for our problem. We showed in 2.4 that it is possible to square the circle only if π is constructible. We now know that

$$\pi \text{ is constructible} \Rightarrow \pi \text{ is algebraic.}$$

Hence if we can show that π is transcendental, then it cannot be constructible, and so *it is impossible to square the circle.*

4 The Transcendental Nature of π

In order to prove that π is transcendental, Lindemann proved a very elegant theorem, which now bears his name along with that of his contemporary Karl Weierstrass, who generalised it to the version below.

4.1 Lindemann-Weierstrass Theorem

Before we state the theorem, first let us define algebraic independence.

Definition. *A set of numbers* $\{\alpha_1, \ldots, \alpha_k\}$ *is* algebraically independent *over a field* $\mathbb{K}$ *if every polynomial* $f : \mathbb{C}^k \to \mathbb{C}$ *with coefficients in* $\mathbb{K}$ *has* $f(\alpha_1, \ldots, \alpha_k) \neq 0$

For example, the set $\{2\pi^2 + e, \pi, e\}$ is not algebraically independent over $\mathbb{Q}$ since if $f(x, y, z) := x - 2y^2 - z$ then

$$f(2\pi + e, \pi, e) = (2\pi^2 + e) - 2(\pi)^2 - (e) = 0$$

Theorem. (Lindemann-Weierstrass) *Let* $a_1, a_2, \ldots, a_n$ *be algebraic numbers which are linearly independent over* $\mathbb{Q}$*, i.e.:*

$$b_1, b_2, \ldots, b_n \in \mathbb{Q} \text{ and } b_1a_1 + b_2a_2 + \ldots + b_na_n = 0 \Rightarrow b_i = 0 \ \forall i$$

Then $e^{a_1}, e^{a_2}, \ldots e^{a_n}$ *are algebraically independent over* $\mathbb{Q}$*.*

This theorem has an extremely long and complicated proof, which may be found in its entirety in [7] but is omitted in this essay.

Corollary. *In particular in the case where* $n = 1$ *above, if* α *is an algebraic number,* e^α *is transcendental, since it is not the root of a polynomial in one variable with rational coefficients.*

Using this, we can prove that π is transcendental easily.

Proof. Assume for the sake of contradiction that π is algebraic. We already know that i is an algebraic number and that the algebraic numbers form a field, so clearly $i\pi$ is an algebraic number. But then by the corollary above, we would have that $e^{i\pi}$ is transcendental.

Clearly this is not the case, since by Euler's Identity

$$e^{i\pi} = -1$$

So then we have a contradiction and our assumption was wrong - and so π is transcendental. □

Hence, by proving this theorem, Lindemann had solved the ancient problem of Squaring the Circle, and proved that it is, indeed, impossible.

5 Conclusion

Lindemann's exposition of this elusive truth is noteworthy not just for the result itself but also for the paradigm shift it represents. For thousands of years, mathematics was dominated by geometry, and geometric approaches to long standing problems. In the 19$^{\text{th}}$ century, great minds used the new tools of rigorous algebra and analysis to shine light over the hidden connections between distinct areas of mathematics. New approaches simultaneously broadened mathematics and brought it closer together, allowing previously intractable problems to reveal themselves. In this way, Squaring the Circle is exemplary of how mathematics must expand in order to advance, and how the ripples of new ideas can be felt even in seemingly unconnected areas.

References

[1] Wikimedia Commons. *Basic ruler-compass construction demonstration.* 2015. URL: `https://commons.wikimedia.org/wiki/File:Basic-construction-demo_vector.svg`.

[2] Richard Courant and Herbert Robbins. *What Is Mathematics? An Elementary Approach to Ideas and Methods.* Oxford University Press, 1996. ISBN: 0195105192.

[3] Euclid. *The Thirteen Books of the Elements Translated By Sir Thomas Heath 3 Vols.* Dove Publishing, 2000. ISBN: 0486600882.

[4] Sir Thomas Heath. *A History of Greek Mathematics, Vol. 1: From Thales to Euclid.* Dover Publications, 1981. ISBN: 0486240738.

[5] Augustus de Morgan. *A Budget of Paradoxes.* Cosimo Classics, 2007. ISBN: 1602063206.

[6] Indianapolis News. *"The Mathematical Bill. Fun-Making In the Senate Yester-day Afternoon–Other Action".* Feb. 13, 1897. URL: `https://newspapers.library.in.gov/cgi-bin/indiana?a=d&d=INN18970213-01.1.11`.

[7] Ivan Niven. "The Generalized Lindemann Theorem". In: *Irrational Numbers.* Mathematical Association of America, 1956, p. 117.

[8] Plutarch. *Moralia. On Exile.* URL: `https://doi.org/10.4159/dlcl.plutarch-exile.1959`.

[9] Bruce Reznick. *Algebraic Numbers.* URL: `https://www.math.uiuc.edu/~reznick/algebraicnumber.pdf`.

[10] Paulo Ribenboim. *Classical Theory of Algebraic Numbers (Universitext).* Springer, 2001. ISBN: 0387950702.