A MATHEMATICAL APPROACH TO MATHEMATICS APPRECIATION

by
John J. Benedetto

July, 1977 LECTURE NOTE 17

to my glb

PREFACE

This book represents the consolidation of two projects: first, it contains the substance of a history of mathematics course for mathematics majors that I've developed and taught during the past eight years; and, second, it presents the theme of studying historically the emergence of algebra and analysis and their interplay in the development of mathematics. The mode of presentation is mathematical with more a respect for the historical process than any historical expertise. The theme certainly warrents a more thorough, advanced, and scholarly presentation; whereas the level of this book reflects my own limitations, the background of my audience, and the self-imposed constraint of introducing such a theme to this audience.

The reader will notice more algebra than analysis in the text. In fact, it is frequently more convenient to trace the growth of an algebraic topic than to do the same for an analytic topic, since the latter generally involves extensive technical machinery for anything beyond a superficial study. As noted in the previous paragraph, I attempt to indicate analytic (resp., algebraic) input to such algebraic (resp., analytic) topics. Also, the fundamental theorems of arithmetic, algebra, and calculus truly influence the essence of mathematics and I emphasize them in the text, fully developing the first two.

Chapter 1 considers the importance of formulas in mathematics and examines the logic and language of mathematics. I use the Pythagorean theorem as the essential topic both as a

"creative formula" and as a means of introducing the reader to the mathematical contributions of the Babylonians and Greeks. The Pythagorean theorem led to the problem of incommensurability; and this, in turn, led to the analytic problem of constructing the real numbers and the algebraic problem of determining which numbers are irrational. In the context of the Pythagorean theorem I also characterize the Pythagorean triples, an algebraic result in Diophantine equations, as well as showing how the Pythagorean theorem is used to deal with the analytic result of defining arc length. The mathematical treatment runs from the fundamental theorem of arithmetic to Hilbert space.

In Chapter 2 I concentrate on the mathematics of Archimedes and Diophantus; and, although Archimedes in particular had broad mathematical range, I consider their roles in the development of analysis and algebra, respectively. The treatment is in part quite technical, but I hope that a reasonable historical perspective of mathematics through the time of Diophantus has been presented by the end of Chapter 2.

Chapter 3 begins with the theory of algebraic equations and its history. Then I give a complete treatment of the fundamental theorem of algebra stressing its essential analytic ingredients. Finally, I give the solutions to the classical construction problems and show their relation to modern algebra. In each topic I distinguish, at least by example, between algebraic and analytic concepts and techniques.

Various sections of the text are labelled "Biographical sketches" of specific mathematicians whom I discuss at those points in my course. I omit such biographical material in the book since it provides a source of non-technical reading assignments and since I would only be repeating well-known biographies that I have read. Section 1.2.6 is the first section of "Biographical sketches," and I give some general references there; special books for specific mathematicians are inserted appropriately. These "Biographical sketches" are also a convenient place to mention mathematical topics, appropriate to the individuals being sketched, which are exposited in other books in an excellent way and which I develop at this point, e.g., section 1.4.3.

NOTATION

$\mathbb{N}$ is the set $\{1,2,\cdots\}$ of positive integers; $\mathbb{Z}$ is the set $\{0,\pm1,\pm2,\cdots\}$ of integers; and $P = \{2,3,5,\cdots\} \subseteq \mathbb{N}$ is the set of prime numbers. $\mathbb{Q}$ and $\mathbb{R}$ are the fields of rational and real numbers, respectively; and $\mathbb{Z}^n$ and $\mathbb{R}^n$ are the sets of all n-tuples of integers and real numbers, respectively. $[a]$ denotes the greatest integer less than or equal to $a \in \mathbb{R}$; and $\underline{\text{card } X}$ denotes the cardinality of the set X.

TABLE OF CONTENTS

1. The Pythagorean theorem

In this chapter we shall indicate the importance of formulas in mathematics. In particular, we will discuss the Pythagorean formula and some of its developments concerning both language and proof as related to the growth and content of mathematics itself.

1.1 The irrational introduction to mathematics

1.1.1 The Pythagorean theorem

Pythagoras of Samos lived during the 6^{th} century B.C. and died or was murdered about 500 B.C.; he was a contemporary of Buddha and Confucius. The Pythagorean theorem was known to the Babylonians during Hammurabi's reign (c. 1750 B.C.) [Neugebauer, p. 36]. The Pythagorean theorem is

$$a^2 + b^2 = c^2, \tag{1.1}$$

where a and b are the lengths of the sides and c is the length of the hypotenuse of a given right triangle.

We'll give two proofs of (1.1). The key fact that we use is that the sum of the angles of a triangle is equal to the sum of two right angles; we refer to [Hilbert] for precise definitions of angle, equal angles, and the sum of angles.

Our first proof is due to the Hindu, Bhaskara (12^{th} century A.D.); a relatively thorough popular treatment of his work is given in [Scott, pp. 71-78].

Proof of (1.1). Take a square with side of length c, and assume $a \geq b$.

Because of the above result on the sum of the angles of a triangle we can partition the square as in Figure 1, where S is a square each of whose sides has length a - b.

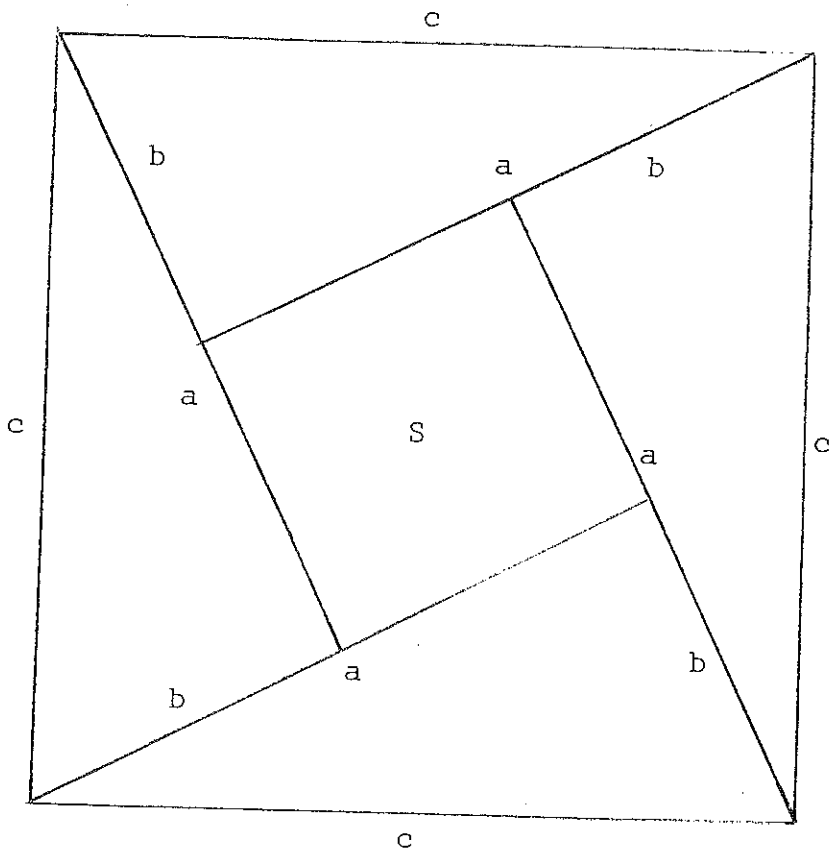


Figure 1

Thus, $c^2 = 4\left(\frac{1}{2}ab\right) + (a-b)^2$; and this yields (1.1).

q.e.d.

Proof of (1.1). Partition a square with side of length a+b as in Figure 2 and Figure 2'.

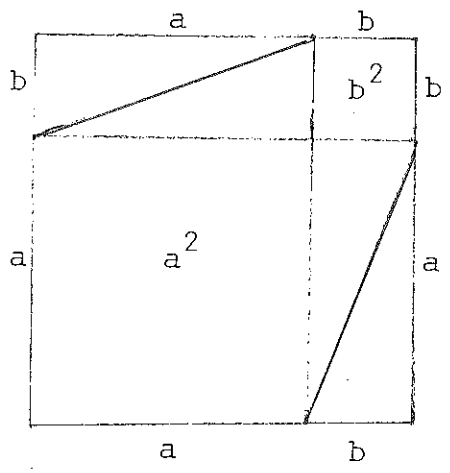


Figure 2

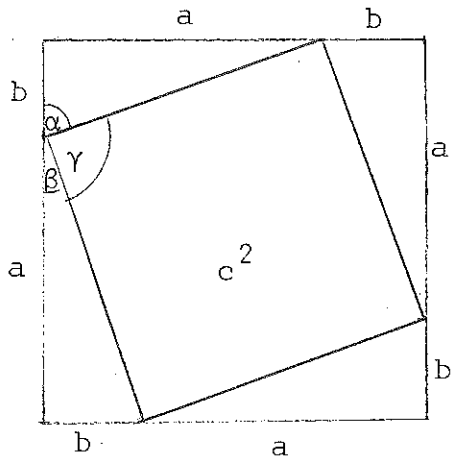


Figure 2'

Angle γ is a right angle since angles α and β add up to a right angle.

We obtain (1.1) by discarding the four equivalent right triangles in each square.

q.e.d.

In his Elements, Euclid (365-275) followed the Pythagorean theorem by its converse: if a triangle with sides having lengths a,b, and c satisfies (1.1) then it is a right triangle.

Later in this chapter we shall discuss irrational numbers and the problem of incommensurability, as well as rendering a criticism of the Greek geometric method. Thus it is worthwhile to point out that the Pythagorean theorem is a geometric statement about the equality of areas. Whatever its ultimate faults, there is a reason for the geometric approach of the Greeks. In fact, if we were able to proceed algebraically, and not

geometrically, in the Pythagorean theorem, then we would need a means to express areas in terms of numbers. To compare areas in the context of numbers leads to the problem of incommensurability, e.g., the irrationality of $\sqrt{2}$, which was an explicit stumbling block to the Greeks and which is the subject of a good deal of the material in this chapter.

1.1.2 The Babylonians and the Pythagoreans

The Babylonian mathematical contribution is significant for its algebraic approach to problems. The need for rigorous proof became central for the Greek mathematical school, but the Babylonian numerical and algebraic techniques diminished in importance at the hands of the geometrical Greeks, e.g., [van der Waerden, p. 125]. Geometric proof and the axiomatic method became the means of securing and defining truth for Greek mathematicians; in fact, as Zeuthen has pointed out, geometric construction was regarded as proof of existence for the Greeks. Unfortunately, the singlemindedness with which the Greek school sought geometric demonstrations ultimately served to inhibit development of new mathematical concepts as well as to block the Babylonian algebraic advances for 3,000 years. We shall see that there were some algebraic and analytic developments in Greek mathematics, but these tended to suffer in the long range because of the geometric influence. Concerning such developments, there was a continuity of sorts with the Babylonian heritage, and the most spectacular figure in this transition was Pythagoras.

Pythagoras is a mystery. Herodotus (480-425) writes respectfully and Heraclitus (537-475) speaks disparagingly of him, e.g., [Bochner, 1966, p. 359; van der Waerden, p. 93]; Plato (428-348) says nothing at all about him whereas Aristotle (384-322) wrote his biography which is lost. It is conjectured that Pythagoras travelled to Egypt and was taken as a prisoner to Babylon where he learned the material that later bacame the basis for the Pythagorean school's philosophy, theology, sociology, and (even) mathematics of number. The Babylonians had a less catholic role in mind for their mathematical results.

The Pythagorean school was in southeastern Italy, mainly in the ancient city of Croton. Supposedly, its motto was "All is number"; and they assigned integers to concepts such as justice and opportunity. Analogously, but on an entirely different level and context, Gödel (1906-), the eminent logician, assigns integers to formulas in formal systems, e.g., [Nagel and Newman, Chapter 7]. The Pythagoreans did not consider rational numbers as such, but were very much interested in analyzing pairs of integers. Their doctrine proclaimed that God had ordered the universe by means of integers, that God is unity and the world is plurality, and that harmony, consisting of ratios of integers, is divine and restores unity to the contrasting elements of the world [van der Waerden, p. 93]. In this setting they discovered the role of rational numbers in music noting, for example, that when a string is shortened by half, the tone produced by plucking it is an octave higher.

The step from rational numbers to irrational numbers or, equivalently, the problem of incommensurability is a generally Greek proposition which we'll discuss in the remainder of section 1.1 and in section 1.2. By taking $a = b = 1$, we see the relation of this issue with (1.1). On the other hand, the Babylonians did give approximate rational values of $\sqrt{2}$ with an error of less than $22/(60)^4$ [Neugebauer, p. 35]; naturally, (1.1) must have been involved in such calculations, although the precise method is not known and there is no evidence that they had any awareness at all, contrary to the Greeks, of the significance of incommensurability.

There is a natural problem related to the above remarks. In the spirit of the Pythagorean enthusiasm for number, Archytas (430- B.C.) of Tarentum (present day Taranto, Italy) stated about 375 B.C. that not geometry but arithmetic alone could provide satisfactory proofs; and yet, a generation later, the geometric axiomatic method was born. Besides Croton and Tarentum the other major ancient Greek city in southern Italy was Elea, and the axiomatic posture attained by Greek mathematics has its source in the Eleatic dialectic. In any case, the reason for this apparent change in emphasis concerns the irrationality of $\sqrt{2}$ which we now discuss.

1.1.3 The origin of irrational numbers

When and how were irrational numbers discovered? The two questions are closely related since certain proofs would not be

considered possible if they were supposed to have occurred too early; and there are at least two different modern opinions on the matter. One group, including O. Becker, E. Frank, O. Neugebauer, H. Vogt, and H.G. Zeuthen, claim the discovery came about 410 B.C., with some of these contending that the discovery could not have come before the time of Archytas, say, 375 B.C. The other view, developed by [von Fritz], puts the discovery that $\sqrt{2}$ is irrational much earlier. Both views produce the same list of protagonists in later developments.

By way of definition, we say that two segments are commensurable if the ratio of their lengths is a rational number, and such segments are incommensurable if the ratio of their lengths is not rational. Originally, the Greeks discovered incommensurable segments when comparing the sides having length $a = b = 1$ of an isosceles right triangle whose hypotenuse has length c. The modern statement that "$\sqrt{2}$ is irrational" is equivalent to the statement that c and a are incommensurable lengths. This realization of incommensurability was the first instance of a mathematical situation dealing with the impossibility of a certain phenomenon, viz., the impossibility of the comfortable notion of commensurability; and the conceptual subtlety required to pose and solve the related problem of incommensurability which we'll state in section 1.2.1 indicates a great intellectual advance over previous mathematical results.

One of the problems in pinning down the period of discovery of incommensurability is the terminology "so-called Pythagoreans" used by Aristotle. Frank makes a sharp distinction between the Pythagorean school (of Pythagoras) and these "so-called Pythagoreans" whom he claims were contemporaries of Plato and deeply influenced by his philosophy, e.g., [von Fritz, p. 249]. This distinction ultimately forms part of the basis for his guess.

Plato's dialogue Theaetetus was written in 368 B.C. after Theaetetus' death in battle. Theaetetus (414-369) was a friend of Plato and is the foremost algebraic force in Greek mathematics [van der Waerden, pp. 168 ff.]. The date of the dialogue is 399 B.C. which was the year of Socrates' death; and in the dialogue the old mathematician Theodorus of Cyrene (in North Africa) (470- B.C.) is cast in the role of proving the irrationality of $\sqrt{3},\sqrt{5},\sqrt{6},\cdots,\sqrt{17}$, cf., Proposition 1.1 b, to the 17 year old Theaetetus, working out each case separately. One interpretation of this data is that Theodorus was establishing his own contribution to the theory by beginning with $\sqrt{3}$ instead of $\sqrt{2}$ and that the proof for $\sqrt{2}$ was well known at the time. Since he was an old man then, Theodorus' discoveries were probably made much earlier than 399 B.C.; but even if this were not the situation, the omission of the $\sqrt{2}$ case indicates that this result was indeed established significantly earlier, especially in light of the fact that mathematical knowledge traveled so slowly then. [von Fritz] argues that Hippasus of Metapontum discovered the

irrationality of $\sqrt{2}$. Hippasus was of a generation before Theodorus and was a Pythagorean philosopher with an extensive list of scientific accomplishments. [Szabó] takes von Fritz's position as far as the time of initial discovery, but argues against any contributions by Theodorus. Heath notes that Democritus (460-350) wrote about irrational lines and solids, and as such it is difficult to resist the conclusion that the irrationality of $\sqrt{2}$ was discovered before Democritus' time.

There is strong evidence developed by Hasse and Scholz in 1928 and van der Waerden in 1940 that the paradoxes of Zeno of Elea (500- B.C.) and the discovery of incommensurability are closely related conceptually and chronologically, cf. section 1.1.5. Their thesis has three aspects: first, the paradoxes are not directed against the problem of infinite divisibility of geometric magnitudes, but their aim is to support the theory of the Eleatic metaphysicist Parmenides (540- B.C.) who posits a single immutable "whole"; second, "infinitesimal" methods were not part of the existing mathematics at Zeno's time; and third, it was the problem of incommensurability and not infinite divisibility that was responsible for the initiation of the axiomatic method.

A major problem in pinpointing the "when" of our initial question in this section is to determine the "how". Aristotle affirms that the proof we give in Proposition 1.1a, and that is in an appendix of Book 10 of Euclid's Elements, is the

original; this would seem to endorse the position of Becker, Frank, et alii since an initial effort requiring such logical procedures and abstract thinking would be unlikely too early in Greek mathmatical development. [von Fritz, pp. 255 ff.] gives an interesting argument indicating that perhaps the proof below was not the initial one, and suggests an alternate geometrical procedure which would have been at the disposal of Hippasus. Zeuthen has suggested possible geometric proofs that Theodorus could have used for the different integers he considered [Hardy and Wright, Sections 4.5 and 4.6]; and Zeuthen's choice of proof for $\sqrt{2}$ (settled before Theodorus) is consistent with von Fritz's theory, although Zeuthen generally sides with the other camp.

1.1.4 Theaetetus and specific irrational numbers

The theory of irrationals began in the Pythagorean school, and the really sophisticated treatment of irrationals in Book 10 of Euclid's Elements is due to Theaetetus; it seems safe to say that twentieth century man does not completely understand Book 10. Theaetetus was an algebraist, just as Eudoxus of Cnidus (408-355), who also studied irrational numbers, was an analyst [van der Waerden, pp. 189-190], cf. section 1.2.1. The distinction is important and exists equally well among modern mathematicians. The algbraic flavor of Theaetetus' results is reflected in Proposition 1.1 b,c; Eudoxus, on the other hand, developed the irrational numbers as the completion of the rationals. Chronologically, the problems discussed in Book 10 led to Eudoxus'

work which appears in Book 5.

We now provide some of the mathematics whose proofs and origins we have been discussing.

The proof of Proposition 1.1 is an example of a reductio ad absurdum argument. This means that we assume the contrary of what we intend to prove, and obtain a contradiction to a known specified fact by means of a logical argument and this assumption; we then conclude that the assumption is false and therefore what we wanted to prove in the first place is true. This type of argument derives from the ideas of Parmenides and Zeno, and as such is another Eleatic influence on the structure of systematic and deductive mathematics. The proof of Proposition 1.1 b,c also uses the unique factorization theorem or Fundamental Theorem of Arithmetic: each integer $n \in \mathbb{N}$ can be written in a unique way as a product

$$n = \prod_{p \in F \subseteq P} p^{n_p},$$

where $n_p \in \mathbb{N}$ and card $F < \infty$, i.e., Theorem 1.1. As we shall see in section 1.3.1, the Fundamental Theorem of Arithmetic follows from the Euclidean algorithm; and the Euclidean algorithm probably had its source in the Pythagorean theory of music [Szabó] and in any event evolved from attempts to estimate $\sqrt{2}$. We'll discuss the Euclidean algorithm in section 1.2.3.

Proposition 1.1. a. $\sqrt{2}$ is an irrational number.

b. If $n \geq 1$ and $m \geq 2$ are integers and $n \neq k^m$ for some $k \in \mathbb{N}$, then $n^{1/m}$ is irrational.

c. If $z \in \mathbb{R}$ is a root (i.e., a zero) of the equation

$$x^m + c_{m-1} x^{m-1} + \cdots + c_0 = 0,$$

where each $c_j \in \mathbb{Z}$, then either $z \in \mathbb{Z}$ or z is irrational.

Proof a. Assume $\sqrt{2} = a/b$ where $(a,b) = 1$, i.e., a and b are relatively prime integers.

We have $2b^2 = a^2$ and so a^2 is even which, in turn, implies that $a = 2n$, an even integer.

Thus $2b^2 = 4n^2$ and so b^2 and, hence, b are even.

Since a and b are even we obtain a contradiction to the hypothesis that $(a,b) = 1$.

b. Assume $n^{1/m} = a/b$ where $(a,b) = 1$ and $b > 1$; we have $b^m n = a^m$.

Since $b > 1$ it has a prime factor p; and since $b^m n$ and a^m have the same unique factorization into primes, we have $p \mid a^m$.

Thus, $p \mid a$.

This contradicts the hypothesis that $(a,b) = 1$.

c. The proof follows that of part b and we omit the details.

q.e.d.

It is possible to prove Proposition 1.1 b using the technique of part a and not using the Fundamental Theorem of Arithmetic; in this case the proof of part b becomes more difficult.

Proposition 1.2 e is an irrational number.

Proof. We'll prove that $e^{-1} = \sum_{n=0}^{\infty} (-1)^n/n! \notin \mathbb{Q}$. We set $s_k = \sum_{n=0}^{k} (-1)^n/n!$ and so

$$(1.2) \quad 0 < e^{-1} - s_{2k-1} = \sum_{n=2k}^{\infty} (-1)^n/n! < 1/(2k)! .$$

Multiplying both sides of (1.2) by $(2k-1)!$ we have

$$(1.3) \quad \forall\, k \geq 1,\ 0 < (2k-1)!(e^{-1} - s_{2k-1}) < 1/(2k) \leq 1/2 .$$

By definition of s_{2k-1}, $(2k-1)!s_{2k-1} = n_k \in \mathbb{Z}$.
Assume $e^{-1} = a/b$ where $(a,b) = 1$. In this case we can choose
k large enough so that $(2k-1)!e^{-1} = m_k \in \mathbb{Z}$.
By (1.3), $m_k - n_k \in (0,1/2)$ for such k; and this is the
desired contradiction.

q.e.d.

1.1.5 Achilles and the tortoise.

Zeno's paradox concerning Achilles and the tortoise is: Achilles is faster than the tortoise and there is to be a race in which the tortoise starts ahead of Achilles; Achilles can never pass the tortoise because when he reaches the place where the tortoise began, the tortoise will have moved ahead, etc. We'll now show that this argument is faulty and that the problem can be resolved in terms of the theory of infinite series.

Suppose that Achilles (A) runs at 10 kilometers per hour and that the tortoise (T) manages to average 1 kilometer per hour. Assume that T starts 1 kilometer ahead of A. A scorecard is given in Figure 3.

t Time elapsed (in hours)	0	$\frac{1}{10}$	$\frac{1}{10} + \frac{1}{100}$	...
Position of A	0	1	$1 + \frac{1}{10}$	...
Position of T	1	$1 + \frac{1}{10}$	$1 + \frac{1}{10} + \frac{1}{100}$	...

Figure 3

At a given moment t we measure the time for Achilles to go from his position to the tortoise's position at t. Thus, at $t = 1/10$ hours, we measure how long it takes A to reach the position $1 + \frac{1}{10}$, given that A is then at the position 1; the time elapsed is 1/100 hours, and in 1/100 of an hour T goes 1/100 kilometers. In this way we see that in $\sum_{1}^{\infty} 1/10^n$ hours T and A are both at the position $\sum_{0}^{\infty} 1/10^n$. Since $\sum_{1}^{\infty} 1/10^n = (1/10)/(1 - \frac{1}{10}) = 1/9$ and $\sum_{0}^{\infty} 1/10^n = 1/(1 - \frac{1}{10}) = 10/9$, we see that after 1/9 hours both T and A are at the position 10/9 (even though T started at position 1); and after this, A goes ahead.

1.2 The real number system

1.2.1 The problem of incommensurability

Archimedes (287-212) considered Eudoxus of Cnidus to be the finest mathematician before him. Cnidus was southeast of both Athens and Samos and north across the Mediterranean from Alexandria.

Eudoxus was a student of Archytas before studying with Plato. Unfortunately, none of Eudoxus' original work is extant.

The problem of incommensurability which Eudoxus solved, and which appears in Book 5 of Euclid's Elements, was to reconcile the fact of incommensurable segments with the existing Pythagorean theory of commensurable ones. The Pythagoreans could determine when two rational numbers were equal, e.g., section 1.2.3; the problem which Eudoxus solved was to give criteria, compatible with the rational case, determining what it should mean for two ratios of lengths of incommensurable segments to be equal.

Besides any intellectual motivation, the problem of incommensurability was kept in the eye of the erudite by the prestigious Plato, whose devious rhetoric assured his listener that not to know about incommensurability was unworthy of a civilized person and Greek.

1.2.2 Eudoxus and the Axiom of Archimedes

Definition 4 of Book 5 of Euclid's Elements is: magnitudes are said to have a ratio to one another which are capable, when multiplied, of exceeding one another, cf., the clearer statement in Proposition 1.3. Later Archimedes noted that this statement is really an axiom; and, although he gave credit to Eudoxus for originally formulating it, it is customarily referred to as the Axiom of Archimedes. The Axiom of Archimedes is an essential property of $\mathbb{R}$; and Eudoxus and Archimedes realized its essential nature for coping with the problem of incommensurability. To illustrate the fundamental nature of the Axiom of Archimedes it is convenient for the moment to use a twentieth century definition

of $\mathbb{R}$ and then to derive the Axiom of Archimedes: $\mathbb{R}$ is the ordered field for which the least upper bound axiom holds, e.g., [Birkhoff and MacLane, Chapter 4]. Beginning with this definition we easily prove

Proposition 1.3 (The Axiom of Archimedes). For any $x \in \mathbb{R}$ there is $n \in \mathbb{Z}$ such that $n > x$.

Proof Let $X = \{k \in \mathbb{Z} : k \leq x\}$. x is an upper bound for X and so X has a least upper bound $y \in \mathbb{R}$ by the least upper bound axiom. Thus $y - \frac{1}{2}$ is not an upper bound for X, and so there is an integer $k \in X$ for which $k > y - \frac{1}{2}$.
Hence $k + 1 > y + \frac{1}{2} > y$ so that $k + 1 \notin X$. Consequently,

$k + 1 = n > x$ by the definition of X.

q.e.d.

Using Proposition 1.3 it is easy to prove that *if $x,y \in \mathbb{R}$ and $x < y$ then there is $r \in \mathbb{Q}$ for which $x < r < y$*.

It turns out that Euclid's axioms for geometry are really not sufficient to avoid some embarrassing questions. For example, in Euclid's very first result he constructs an equilateral triangle ΔABC, given two points A and B, by drawing circles about A, resp., B, through B, resp., A. As Leibnitz (1646-1716) pointed out, Euclid failed to prove that the circles intersect! In fact, the Axiom of Archimedes does not close this gap (sic); but it did lead the way to the formulation of an axiom such as the least upper bound axiom. [Hilbert] is basic sequel to Euclid's Elements as far as analyzing the proper axiomatization to obtain Euclidean geometry, cf., [Poincaré].

There is a relation between Euclid's parallel axiom, the Axiom of Archimedes, and the statement that the sum of the angles of a triangle is equal to two right angles. This last statement is essential in the proofs of the Pythagorean theorem and it can be proved from the parallel axiom. Conversely, when combined with the Axiom of Archimedes, it implies the parallel axiom.

1.2.3 The Euclidean algorithm

Given two segments a and b where a is longer than b. Then a is an integral number n of b's plus c, where $0 \leq c < b$. Suppose we can find one half of any segment b, as we can with a piece of string by folding it in half. Then $c \leq \frac{1}{2}b$ or $\frac{1}{2}b < c < b$. In the former case, $a = nb + c$ where c can be estimated by a halving of b; in the latter case, we have $a = (n + \frac{1}{2})b + d$, where $0 < d < \frac{1}{2}b$. Continuing in this way we have a practical process for measuring a in terms of b since, practically speaking, small enough errors are irrelevant.

At the level of abstraction that geometry had reached before Eudoxus, the intellectual requirement for such a measurement was much more rigorous.

If a and b are in $\mathbb{N}$ and $a \geq b$, then the Euclidean algorithm, which was known to the Pythagoreans, provides a systematic means of measuring a relative to b, cf., the remark before Proposition 1.1 in section 1.1.4.

We compute

$$a = q_1 b + r_1, \quad 0 \leq r_1 < b,$$

where q_1 and r_1 are non-negative integers. If $r_1 = 0$ we stop. If $r_1 > 0$, we compute

$$b = q_2 r_1 + r_2, \quad 0 \leq r_2 < r_1,$$

where q_2 and r_2 are non-negative integers. Again, if $r_2 = 0$ we stop; otherwise we compute

$$r_1 = q_3 r_2 + r_3, \quad 0 \leq r_3 < r_2.$$

We continue in this fashion and eventually reach a stop situation, i.e.,

$$r_{n-2} = q_n r_{n-1} + r_n, \quad 0 < r_n < r_{n-1}, \tag{1.4}$$

and

$$r_{n-1} = q_{n+1} r_n. \tag{1.5}$$

The procedure stops since there are only finitely many positive integers r less than b.

This computation is the Euclidean algorithm to find the greatest common (integer) divisor, denoted by (a,b), of a and b. We have

Proposition 1.4 Given $a,b \in \mathbb{N}$ where $a \geq b$. With the above notation, we have $r_n = (a,b)$.

Proof a. Note that $r_n | r_{n-1}$ by (1.5) and so $r_n | r_{n-2}$ by (1.4). We proceed in this way from the last step to the first of the above computation, and obtain that $r_n | a$ and $r_n | b$.

b. Assume $c | a$ and $c | b$. We must show $c \leq r_n$ and we'll do this by showing that $c | r_n$.

From the first step of the computation, we have $c | r_1$, and so,

by the second step, $c|r_2$.

Proceeding "down the algorithm" we see that $c|r_n$.

q.e.d.

Setting $a_1 = a/r_n$ and $b_1 = b/r_n$, and taking r_n as a common unit, we measure a as a_1 r_n's and b as b_1 r_n's, where $a_1, b_1 \in \mathbb{N}$; r_n serves as a unit. a_1/b_1 provides the simplest expression for measuring a in terms of b since $(a_1, b_1) = 1$ by the definition of r_n.

If a and b are not both integers and we compute as above, requiring that each $q_j, r_j \in \mathbb{Q}$, then the procedure needn't be finite. For example, if $a = \sqrt{2}$ and $b = 1$ then the procedure never ends.

1.2.4 The Eudoxus - Dedekind theory of real numbers

Techniques such as the Euclidean algorithm allowed a satisfactory means of determining when two pairs of commensurable segments should be equal. We introduce Eudoxus' solution to the problem of incommensurabulity by the following two observations:

a. Given $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$ where $a,b,c,d \in \mathbb{Z}$; then $\frac{a}{b} = \frac{c}{d}$ if and only if for each pair of integers $m,n \in \mathbb{Z}$,

$$ma = nb \implies mc = nd.$$

b. Suppose a and b, respectively, c and d, are the lengths of incommensurable segments. Then by the definition of incommensurability, there are no integers $m,n \in \mathbb{Z} \setminus \{0\}$ for which $ma = nb$, respectively, $mc = nd$. On the other hand, if $\frac{a}{b} = \frac{c}{d}$ and $ma > nb$ then $mc > nb$.

The following is Eudoxus' definition which encompasses both the commensurable and incommensurable cases. $\frac{a}{b} = \frac{c}{d}$ if one and only one of the following conditions holds for each pair of integers m and n: $ma > nb$ implies $mc > nd$; $ma = nb$ implies $mc = nd$; $ma < nb$ implies $mc < nd$. It is of course logically unsatisfactory to define what is meant by "equal incommensurable ratios" without defining an "incommensurable ratio". Euclid made a less than eloquent statement of Eudoxus' definition [Euclid, Book 5, Definition 5]: magnitudes are said to be in the same ratio, the first to the second and the third to the fourth, when, if any equimultiples whatever be taken of the first and third, and any equimultiples whatever of the second and fourth, the former equimultiples alike exceed, are alike equal to, or alike fall short of, the latter equimultiples respectively taken in corresponding order.

The "real numbers" r defined by Eudoxus in the above definition have the characteristic feature of partitioning the rational numbers into three disjoint sets:

$$S(<,r) = \{q \in \mathbb{Q}: \ q \text{ is less than } r\},$$

$$S(=,r) = \{q \in \mathbb{Q}: \ q \text{ is equal to } r\},$$

$$S(>,r) = \{q \in \mathbb{Q}: \ q \text{ is greater than } r\}.$$

One problem with Eudoxus' definition of a "real number" r is that r is considered as a ratio of two segments and so, ultimately, we depend on the axioms of geometry to determine for us which ratios exist. We shall see in Chapter 3 that the constructions in Euclidean geometry with straightedge and compass do not yield

all of the real numbers. Nevertheless, this idea of partitioning $\mathbb{Q}$ into three disjoint classes in order to solve the problem of incommensurability provided a fundamental aspect of formulating the "proper" definition of $\mathbb{R}$.

In work beginning in the late 1850's and developed systematically in the 1870's, Dedekind (1831-1916) "cut" the geometrical umbilical cord and defined a "real number" corresponding to <u>each</u> partition $S(<)$, $S(=)$, $S(>)$ of $\mathbb{Q}$ with the properties that $S(<) \neq \emptyset$, $S(>) \neq \emptyset$, $S(=)$ contains at most one element, $S(<)$, resp., $S(>)$, contains no smallest, resp., largest, element, and

$$\forall\, q \in S(<) \quad \text{and} \quad \forall\, p \in S(=) \cup S(>), \quad q < p$$

$$\forall\, q \in S(>) \quad \text{and} \quad \forall\, p \in S(=) \cup S(<), \quad q > p.$$

Beginning in this way, Dedekind defined finally and properly the set of real numbers. Thorough technical accounts of Dedekind's approach are found in [Landau; Rudin]. The foundational problem of defining properly the set $\mathbb{R}$ and the continuous real number line $\mathbb{R}$ was also taken up by Hamilton (1805-1865), Weierstrass (1815-1897), Méray (1835-1911), Cantor (1845-1918), and Heine (1821-1881).

1.2.5 <u>The Weierstrass - Cantor theory of real numbers</u>

It was natural by the mid-19th century to define irrational numbers as limits of rationals; but, as Cantor explicitly observed in 1883 and as Weierstrass probably stated in his lectures on irrational numbers in the late 1850's, such a limit doesn't logically exist until irrationals are defined, cf., the similar remark prior to Euclid's statement of Eudoxus' defintion.

In his paper on Fourier series, where in fact he formulated the Riemann integral, Riemann (1826-1866) posed the uniqueness problem for trigonometric series: given a series $\sum_{n\in\mathbb{Z}} c_n e^{inx}$; for what sets $F \subseteq [0,2\pi)$ does the condition

$$\forall\, x \in [0,2\pi) \setminus F, \quad \lim_{N\to\infty} \sum_{|n|\le N} c_n e^{inx} = 0$$

imply that

$$\forall\, n \in \mathbb{Z}, \quad c_n = 0?$$

In 1870, Cantor proved the result first for $F = \emptyset$ and then for F a finite set. By late 1871 he had proved the result for certain infinite sets and his exposition became closely tied in with the following definition of $\mathbb{R}$ which he developed more thoroughly in 1883.

A fundamental sequence $\{x_n : n = 1,\cdots\} \subseteq \mathbb{Q}$ is defined by the property that

(1.6) $\forall\, \varepsilon > 0 \quad \exists\, N$ such that $\forall\, n,m > N$,

$$|x_n - x_m| < \varepsilon.$$

By definition a real number r is a fundamental sequence $\{x_n\}$, and so $\mathbb{R}$ is the set of all fundamental sequences. It is possible for two different fundamental sequences $\{x_n : n=1,\cdots\}$ and $\{y_n : n=1,\cdots\}$ to define the same real number r if

(1.7) $\forall\, \varepsilon > 0 \quad \exists\, N$ such that $\forall\, n > N$, $|x_n - y_n| < \varepsilon$.

Algebraic operations and a linear ordering can be well-defined on $\mathbb{R}$ in terms of the corresponding notions on the rational

terms of fundamental sequences. Cantor then proved that $\mathbb{R}$ is complete in the sense that if (1.6) is true for $\{x_n: n=1,\cdots\} \subseteq \mathbb{R}$ then there is $\{y_n: n=1,\cdots\} \subseteq \mathbb{Q}$ for which (1.7) is satisfied.

1.2.6 Biographical sketches - Cantor (1845-1918), Dedekind (1831-1916), and Weierstrass (1815-1897)

The Dictionary of scientific biography, edited by C. Gillispie, as well as the biographical references in [May] are the major sources of material for the sections of "Biographical sketches". These sections are meant to include human interest data, mathematical contributions, and mathematical perspective. In this particular section the mathematical perspective included a discussion of the introduction of rigor into analysis at the hands of Gauss (1777-1855), Abel (1802-1829), Bolzano (1781-1848), and Cauchy (1789-1857) and treated the close mathematical relation between Cantor and Dedekind, e.g., [Grattan-Guiness]. We also discussed Cantor's continuum hypothesis and the influence of trigonometric series on his theory of sets, e.g., [Gödel] and [Benedetto; Dauben], respectively.

1.3 Some algebraic developments

1.3.1 The fundamental theorem of arithmetic

The Euclidean algorithm leads directly to the Fundamental Theorem of Arithmetic which we used in Proposition 1.1. The Fundamental Theorem of Arithmetic was first explicitly recorded in 1801 in [Gauss, Art. 16]. It is an easy consequence of [Euclid, Book 7, Prop. 30] once the mathematical-notational development of the late 16^{th} century had been achieved; but with the state of

mathematics at Euclid's time, the "Fundamental Theorem of Arithmetic" given in [Euclid, Book 9, Prop. 14] is only valid for integers $n = \prod_{p \in F \subseteq P} p$, where card $F < \infty$ and $p,q \in F$ implies $p \neq q$, e.g., [Bochner, 1974, pp. 827-828; Hendy].

Proposition 1.5 (Division lemma) Given $a,b \in \mathbb{N}$. If $c \in \mathbb{N}$, $c|ab$, and $(a,c) = 1$, then $c|b$.

Proof By hypothesis, $r_n = (a,c) = 1$ so that multiplying each step of the Euclidean algorithm by b yields

$$\begin{aligned} ba &= bq_1c + br_1 \\ bc &= bq_2r_1 + br_2 \\ &\vdots \\ br_{n-2} &= bq_nr_{n-1} + b \\ br_{n-1} &= bq_{n+1} \cdot \end{aligned}$$

Starting from the first step of this calculation and using the hypothesis $c|ab$ we compute that $c|br_1$, then $c|br_2$, etc., down to $c|br_{n-2}$ and $c|br_{n-1}$.
Thus, from the penultimate step, we obtain $c|b$.

q.e.d.

If $p \in P$, $a \in \mathbb{N}$, and $p \nmid a$, then $(p,a) = 1$. Consequently, as a corollary of Proposition 1.5 we have Euclid's first theorem

Proposition 1.6 Given $a,b \in \mathbb{N}$ and $p \in P$. If $p|ab$ then $p|a$ or $p|b$.

It is now easy to prove

Theorem 1.1 (Fundamental Theorem of Arithmetic) Each integer $n \in \mathbb{N}$ can be written in a unique way as a product

$$n = \prod_{p \in F \subseteq P} p^{n_p},$$

where $n_p \in \mathbb{N}$ and card $F < \infty$.

Proof i. We shall first prove that n is a product of primes. This will not require Proposition 1.6.

If $n \in P$ we are done.

If $n \notin P$ then there is $1 < m < n$ for which $m|n$. Let d be the least such m.

Note that if $d \notin P$ then there is $1 < c < d$ for which $c|d$. Since $c|d$ and $d|n$ we have $c|n$, and this contradicts the definition of d. Consequently, $d = p_1 \in P$.

Hence, $n = p_1 n_1$ where $1 < n_1 < n$. We now proceed with n_1 as we did with n.

Thus to prove that n is a product of primes, it is sufficient to show that some $n_j \in P$; but this follows since $1 < n_j < n_{j-1} < n$.

ii. To prove the uniqueness of representation we shall use Proposition 1.6

Suppose n has the representations

$$\prod_{1}^{k} p_j^{k_j} = \prod_{1}^{m} q_i^{m_i}, \tag{1.8}$$

where $p_j, q_i \in P$, $p_1 < p_2 < \cdots$, $q_1 < q_2 < \cdots$, and $k_j, m_i \in \mathbb{N}$.

Take some p_j, $1 \le j \le k$. Since p_j divides the left hand side of (1.8) it also divides the right hand side. The fact that the q_i's are prime tells us that p_j is some q_i.

Thus each p_j is a q_i and vice-versa. In particular, $k = m$.

We now observe that $p_j = q_j$ for each $j = 1,\cdots,k$. In fact, if $p_1 = q_i > q_1$ and $q_1 = p_j \ge p_1$ we have $p_1 > p_1$, a contradiction.

Finally we must show that $k_j = m_j$ for each $j = 1,\cdots,k$.

If $k_j > m_j$ then, dividing each side of (1.8) by $p_j^{m_j}$ and using the information we've just deduced, we have

$$(1.9)\quad p_1^{k_1} \cdots p_{j-1}^{k_{j-1}} p_j^{k_j - m_j} p_{j+1}^{k_{j+1}} \cdots p_k^{k_k} = p_1^{m_1} \cdots p_{j-1}^{m_{j-1}} p_{j+1}^{m_{j+1}} \cdots p_k^{k_k}.$$

We obtain a contradiction since p_j divides the left hand side of (1.9) but not the right hand side. Therefore $k_j \le m_j$.

We obtain an analogous contradiction by assuming $k_j < m_j$. Therefore $k_j = m_j$.

q.e.d.

1.3.2 The Pythagorean theorem and Fermat's last theorem

Another algebraic outgrowth of the Pythagorean formula concerns so-called Pythagorean triples. Not only did the Babylonians discover the Pythagorean formula, but they solved the harder problem of finding all triples $(a,b,c) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$, $abc \neq 0$, for which $a^2 + b^2 = c^2$; such a triple of integers is a Pythagorean triple. Of course, since the Babylonians dealt more or less exclusively with integers it is not surprising that they should want to find the integer solutions of (1.1). The fact that they solved the problem

around the time of Hammurabi is verified by tablet 322 of Columbia University's Plimpton collection, e.g., [Boyer, Chapter 3.8; Neugebauer; van der Waerden, pp. 78-80]. Obviously $(a,b,c) = (3,4,5)$ is a Pythagorean triple, and we shall see in Theorem 1.2 that there are infinitely many Pythagorean triples.

Fermat's last theorem asserts that the equation

$$a^n + b^n = c^n, \tag{1.10}$$

where $n > 2$ is a given integer, has no solutions $(a,b,c) \in \mathbb{N} \times \mathbb{N} \times \mathbb{N}$ for which $abc \neq 0$. Although this statement has been proved for many integers $n > 2$, it has not been proven for every integer $n > 2$. Fermat (1601-1665) claimed to have proven the assertion but did not write down the proof. It is reasonable to expect that he did not have a proof. Attempts to prove Fermat's last theorem have led to the development of large portions of modern algebra. Perhaps the most striking instance of such development concerns Kummer's (1810-1893) theory of ideal numbers. During the mid-1840's Kummer thought that he had proved Fermat's last theorem. His manuscript was submitted to Dirichlet (1805-1859) who noted that Kummer's proof would be correct if certain complex numbers (e.g., Chapter 3) could be decomposed in a unique way into "complex primes"; Dirichlet expressed his belief that unfortunately such numbers do not generally satisfy this unique factorization property, a fact asserted by Jacobi (1804-1851) not later than the beginning of 1839 [Birkhoff, 1974, p. 335]. Kummer's error was based on his feeling and/or oversight that the uniqueness part of the Fundamental Theorem of Arithmetic for the set $\mathbb{N}$ has an analogue for certain sets of "complex integers". This setback led Kummer to his

theory of ideal numbers whose sole purpose from Kummer's point of view was to give proofs of Fermat's last theorem and the general reciprocity law; from this, Dedekind introduced the important notion of an ideal and the general algebraic theory associated with it. An interesting discussion of this and other historical facets of Fermat's last theorem is found in [Dickson], cf., [Vandiver]. It is Littlewood's (1885-) feeling [Littlewood, pp. 58 ff] that Dedekind's general concept of ideal should have come before and, in fact, have suggested Dedekind's construction of $\mathbb{R}$.

Fermat's last theorem is true for each $n = 4m$, $m \geq 1$ (Exercise 1.1). It has also been verified for each prime $n = p \leq 4001$ as well as many other special cases. It is easy to see that if Fermat's last theorem is true for each odd prime then it is true for every $n > 2$. Even if (1.10) is satisfied for some fixed n, the solutions must be few and far between. In fact, Mumford (1937-) has shown that if $\{(a_m,b_m,c_m): m = 1,\cdots\}$ is any such sequence of solutions arranged so that $c_m \leq c_{m+1}$ for each m, then there are constants $r > 0$ and s such that

$$\forall\, m, \quad c_m > 10^{(10^{rm+s})}.$$

1.3.3 The characterization of Pythagorean triples

In order to determine the set of Pythagorean triples, note that we can assume without loss of generality that any solution $(a,b,c) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$, $abc \neq 0$, of (1.1) satisfies

$$a,b,c > 0. \tag{1.11}$$

Also, if $d|a$ and $d|b$ then $d|c$. Hence, if $(a,b) = d$ and $a = da'$, $b = db'$, $c = dc'$ then $(a',b',c') \in \mathbb{N} \times \mathbb{N} \times \mathbb{N}$ is a solution of (1.1) with the property that $(a',b') = 1$. Consequently, we shall assume that the solutions $(a,b,c) \in \mathbb{N} \times \mathbb{N} \times \mathbb{N}$, $abc \neq 0$, satisfy

(1.12) $$(a,b) = 1,$$

and, in particular, a and b are not both even. Even more, we shall now verify that for such solutions of (1.1) we have

(1.13) a (resp., b) is even and b (resp., a) is odd.

To do this, assume the contrary, and suppose $2|(a-1)$ and $2|(b-1)$. Then since

$$c^2 - 2 = a^2 + b^2 - 2 = (a-1)(a+1) + (b-1)(b+1),$$

we observe that $4|(c^2-2)$ (for if $2|(a-1)$ then $2|(a+1)$). Consequently, there is $k \in \mathbb{N}$ for which $c^2 = 2 + 4k$, an even number. Thus, $c = 2j$ for some $j \in \mathbb{N}$; and when we substitute this into $c^2 = 2 + 4k$ we find that $4(j^2-k) = 2$, a contradiction.

Theorem 1.2 a. Let (a,b,c) be a Pythagorean triple satisfying (1.11), (1.12), and (1.13). Then there are integers $n > m > 0$, one even and one odd, for which $(m,n) = 1$ and such that

(1.14) $$a = 2mn, \quad b = n^2 - m^2, \quad c = m^2 + n^2.$$

b. If $n > m > 0$ are integers, one even and one odd, for which $(m,n) = 1$, and if a,b, and c are defined by (1.14),

then (a,b,c) is a Pythagorean triple satisfying (1.11), (1.12), and (1.13).

Proof b is immediate. In particular, from (1.14)

$$a^2 + b^2 = 4m^2n^2 + (n^2-m^2) = n^4 + 2(mn)^2 + m^4 = c^2.$$

a.i. Let a be even so that b and c are odd.

Note that $(b,c) = 1$; for if $d|b$ and $d|c$ then $d|a$, and so $d = 1$ by (1.12).

Since b and c are odd, $\frac{1}{2}(c-b)$ and $\frac{1}{2}(c+b)$ are positive integers; the positivity follows from (1.1) and (1.11).

Also, $(\frac{c-b}{2}, \frac{c+b}{2}) = 1$ for otherwise we'd contradict the fact that $(b,c) = 1$; in fact, if $d|((c-b)/2)$ and $d|((c+b)/2)$ then $d|((c-b)/2 \pm (c+b)/2)$.

$a/2 \in \mathbb{N}$ since a is even.

From (1.1) we have $a^2 = (c+b)(c-b)$ and so

$$(\frac{a}{2})^2 = (\frac{c+b}{2})(\frac{c-b}{2}). \tag{1.15}$$

a. ii. Using the fact that the two factors on the right hand side of (1.15) are relatively prime we shall prove that $(c+b)/2 = n^2$ and $(c-b)/2 = m^2$, where $m,n \in \mathbb{N}$, $n > m > 0$, and $(m,n) = 1$.

Let $p \in P$ divide $a/2$. From Proposition 1.6, p divides $(c+b)/2$ or $(c-b)/2$, but not both because $(\frac{c-b}{2}, \frac{c+b}{2}) = 1$.

Thus, if $p \nmid (\frac{c-b}{2})$ then $p^2 | (\frac{c+b}{2})$ since $p^2 | (\frac{a}{2})^2$.

In this way we compute that $(c+b)/2$ is a perfect square n^2.

A similar calculation works to obtain $m^2 = (c-b)/2$.

Obviously, $n > m > 0$ and $(m^2,n^2) = 1$ by the properties of $(c+b)/2$ and $(c-b)/2$. Clearly, $(m,n) = 1$, for otherwise we'd have $(m^2,n^2) \neq 1$.

(1.14) follows from (1.15) and the way we've defined m and n.

It remains to show that n odd (resp., even) implies m even (resp., odd); this follows if we prove that $m+n$ is odd. We have $b = n^2 - m^2 = (n+m)(n-m)$ so that since b is odd it is necessary that both $n+m$ and $n-m$ be odd.

q.e.d.

The following result yields Fermat's last theorem for the cases $n = 4m$, $m \in \mathbb{N}$, e.g., Exercise 1.1.

Theorem 1.3 (Fermat) Let (a,b,c) be a Pythagorean triple satisfying (1.11), (1.12), and (1.13), and let A be the area of the right triangle whose sides have length a and b and whose hypotenuse has length c. Then $A \neq h^2$ for $h \in \mathbb{N}$.

Proof i. Using Theorem 1.2 we have

$$A = \frac{1}{2}ab = mn(n^2-m^2) \in \mathbb{N}. \tag{1.16}$$

We shall assume that $A = h^2$ for some $h \in \mathbb{N}$ and obtain a contradiction.

ii. Since $(m,n) = 1$, we see that m, n, $m+n$, and $m-n$ are pairwise relatively prime.

For example, if $d|(m+n)$ and $d|(m-n)$ then $d|2m$ and $d|2n$. Consequently, $(m,n) = 1$ implies $d = 2$ or $d = 1$; but $d \neq 2$ since $m+n$ and $m-n$ are odd (recalling that if n

is odd (resp., even) then m is even (resp., odd)).

Because m, n, $m+n$, and $m-n$ are pairwise relatively prime we use (1.16), Theorem 1.1, and our assumption to observe that each of the four integers m, n, $m\pm n$ is a square of an integer.

iii. Let $m = u^2$, $n = v^2$, $n - m = s^2 = u^2 - v^2$, and $n + m = t^2 = u^2 + v^2$, where $s,t,u,v \in \mathbb{N}$.

Using the fact that m, n, $m\pm n$ are pairwise relatively prime we check that s,t,u,v are pairwise relatively prime.

We have

$$(1.17) \quad 2u^2 = s^2 + t^2 \quad \text{and} \quad 2v^2 = t^2 - s^2 = (t+s)(t-s).$$

Since m and n are odd and even (i.e., one is odd and one is even), we see that s^2 and t^2 are odd; thus s and t are odd, and hence $t+s$ and $t-s$ are even.

Consequently, from (1.17), v is even. Setting $v = 2v_1$ for some $v_1 \in \mathbb{N}$, we obtain

$$(1.18) \qquad 2v_1^2 = \left(\frac{t+s}{2}\right)\left(\frac{t-s}{2}\right)$$

from (1.17).

iv. Since $(s,t) = 1$, we note that $\left(\frac{t-s}{2}, \frac{t+s}{2}\right) = 1$; and we then use (1.18) to observe that either $(t-s)/2$ or $(t+s)/2$ is even.

Suppose that $(t-s)/2$ is even.

Using (1.18), the fact that $\left(\frac{t-s}{2}, \frac{t+s}{2}\right) = 1$, and Theorem 1.1, we can write

(1.19) $\frac{t+s}{2} = j^2$ and $\frac{t-s}{2} = 2k^2$ where $v_1^2 = j^2k^2$.

Adding and subtracting in (1.19) we obtain $s = 2k^2 - j^2$ and $t = 2k^2 + j^2$; and substituting this into the first equation of (1.17) yields

(1.20) $$u^2 = (j^2)^2 + (2k^2)^2.$$

We would have also come to (1.20) if we took $(t+s)/2$ to be even.

v. With the assumption in part i we have derived by (1.20) a new right triangle with sides having lengths j^2, $2k^2$, and u. Its area is

$$A_1 = j^2k^2 = v_1^2 = (\frac{v}{2})^2,$$

the square of an integer.
Noting that $v^2 = n$ we have $A_1 = \frac{n}{4}$ and so $A_1 < A$ from (1.16). In this way we obtain a contradiction to the assumption in part i; for generally we can derive $A_{i+1} < A_i$ where each A_i is the square of an integer.

q.e.d.

The process of "descending" from A_i to A_{i+1} in the above proof is called Fermat's method of infinite descent.

1.3.4 Factorization and sums of perfect squares

We shall investigate the possibility of writing a given odd integer $N \in \mathbb{N}$ in the form

(1.21) $$N = a^2 + b^2, \text{ for some } a,b \in \mathbb{N}.$$

If N has the form (1.21) then, without loss of generality, a is odd and b is even. Thus, $a = 2j+1$ and $b = 2k$ so that $N = 4j^2 + 4j + 1 + 4k^2 = 4m + 1$; that is, <u>if an odd integer $N \in \mathbb{N}$ can be written in the form (1.21) then $N = 4m + 1$ for some $m \in \mathbb{N}$</u>. Fermat asserted the following "converse": <u>if $N = p \in P$ can be written as $p = 4m + 1$ for some $m \in \mathbb{N}$ then p has a unique representation in the form (1.21)</u>; this result was proved by Euler (1707-1783) in a letter to Goldbach (1690-1764) in 1749. The set of primes less than 100 which can be written as $4m + 1$ is $\{5,13,17,29,37,41,53,61,73,89,97\}$ and it is interesting to check the Fermat-Euler result for these numbers. It is not difficult to prove that if $N = 4m - 1$ then N does not have a representation of the form (1.21); and that each positive odd integer has the form $4m + 1$ or $4m - 1$ for some $m \in \mathbb{N} \cup \{0\}$.

<u>Theorem 1.2</u> characterizes a subset of those integers which can be written as the sum of two perfect squares. Generally, <u>$n \in \mathbb{N}$ is a sum of two squares if and only if each prime factor of n of the form $4m + 3$ has even exponents</u> (in the standard unique factorization of n).

We have just observed that no odd prime has more than one representation of the form (1.21). It has been known since the time of Euler - or before - that if an odd integer $N \in \mathbb{N}$ can be written in (at least) two different ways as a sum of squares, then N can be factored in terms of these two partitions. In fact, we have

<u>Proposition 1.7</u> Given $N = a^2 + b^2 = c^2 + d^2 \in \mathbb{N}$ where a and

c are odd and b and d are even. Set $k = (a-c, d-b)$ and define h, j, and m by the formulas

$$h = \frac{a-c}{k}, \quad j = \frac{d-b}{k}, \quad \text{and} \quad m = \frac{d+b}{h}.$$

Then

$$N = \left(\left(\frac{k}{2}\right)^2 + \left(\frac{m}{2}\right)^2\right)(j^2 + h^2). \tag{1.22}$$

For example, write $221 = 10^2 + 11^2 = 5^2 + 14^2$ so that (1.22) yields $221 = (17)(13)$.

It turns out that the problem of representing an integer as a sum of at least two perfect squares has an extensive history and deals ultimately in some difficult aspects of analysis, e.g., [Hardy, Chapter 9].

1.3.5 Biographical sketch - Fermat (1601-1665)

Besides [Bell, 1937; Gillispie] and some of the other references on Fermat in [May], we used [Mahoney; Weil, 1973] as far as general biography was concerned and [Bell, 1961; Mordell] in our discussion of Fermat's last theorem. The analysis in [Weil, 1974] notes an important relation between certain cases of Fermat's last theorem and elliptic curves, cf., section 3.2.2. We also discussed Descartes (1596-1650), Mersenne (1588-1648), and Pascal (1623-1662) at this point for the sake of perspective; and presented Fermat's contributions to the differential calculus [Coolidge; May; Struik].

1.4 Some analytic developments

1.4.1 Arc length

Because of the Pythagorean theorem the distance s between

two points (x_1,y_1) and (x_2,y_2) in the plane is $s = ((x_1-x_2)^2 + (y_1-y_2)^2)^{\frac{1}{2}}$. This notion generalizes perfectly so that we can define the distance s between two points $(x_1,\cdots,x_n),(y_1,\cdots,y_n) \in \mathbb{R}^n$ to be $s = ((x_1-y_1)^2 + \cdots + (x_n-y_n)^2)^{\frac{1}{2}}$.

Let $f: [a,b] \to \mathbb{R}$ be a function with the property that both f and f' are differentiable on an open interval containing $[a,b]$. For a given $x \in [a,b)$ choose $\Delta x > 0$ for which $x + \Delta x \leq b$. By the Pythagorean theorem the distance in the plane between the points $(x,f(x))$ and $(x+\Delta x,f(x+\Delta x))$ is

$$\Delta x \left(1 + \left(\frac{f(x+\Delta x) - f(x)}{\Delta x} \right)^2 \right)^{\frac{1}{2}} .$$

Next, for any partition, $a = x_0 < x_1 < x_2 < \cdots < x_n = b$, of $[a,b]$, we form the Riemann sum

$$\sum_{j=0}^{n-1} (x_{j+1} - x_j) \left(1 + \left(\frac{f(x_{j+1}) - f(x_j)}{x_{j+1} - x_j} \right)^2 \right)^{\frac{1}{2}} .$$

Because of our hypotheses on f and f', it is possible to show that such sums, which are the lengths of rectilinear segments "close" to the graph of f, tend to a number

$$L = \int_a^b (1 + (f'(x))^2)^{\frac{1}{2}} dx .$$

As such we <u>define</u> the <u>arc length</u> of the graph $\{(x,f(x)): x \in [a,b]\}$ of f to be L. This formula involves an algebraic argument (the Pythagorean theorem), an analytic argument (the taking of limits to form the Riemann integral), and a reasonable definition to introduce the notion of length for curved lines.

1.4.2 Hilbert space

An important ramification of the Pythagorean theorem concerns the notion of Hilbert space. This structure evolved at the hands of Volterra (1860-1940), Fredholm (1866-1927), Hilbert (1862-1943), E. Schmidt (1876-1959), Fréchet (1878-), F. Riesz (1880-1956), Weyl (1885-1955), and von Neumann (1903-1957) shortly after the turn of this century (von Neumann's work was done during the period 1927-1929).

Mathematical physicists studied the motion of a vibrating string and saw that under special physical constraints the behavior of the string is given by Fourier series. This development occurred in the 18^{th} and early 19^{th} centuries, and was responsible for the crystallization of some of the basic notions of analysis. The study of vibrating strings or membranes with fewer or different constraints led to more complicated equations, and as such some intermediate problems arose which seemed tractable for initial study. For example, the motion of certain vibrating strings or membranes whose mass is not equidistributed can first be analyzed in the following time independent way. It is conceivable that after a period of time the membrane is in a state of non-trivial equilibrium in the sense that the membrane is in motion, and the motion is determined by the inner forces of the body acting upon itself; in particular, the motion is no longer considered to be time dependent. The problem in this case is to determine the motion of the equilibrium state, and the differential equation characterizing this motion is time independent. Volterra and Fredholm noticed that certain of these differential systems could be formulated in terms

of integral equations. For example, some equilibria problems associated with the behavior of the vibrating string led to integral equations of the form

$$(1.23) \quad \forall\, x \in [0,1],\ f(x) - \int_0^1 K(x,y)f(y)dy = g(x),$$

where K and g are given and f is to be found, e.g., [Petrovskiĭ; Riesz and Nagy, sections 99 and 100].

Using a method due to Liouville (1809-1882) and C. Neumann (1832-1925), Volterra solved (1.23) for special kernels K; his major work appeared in 1897 and is now a standard example in functional analysis texts. Volterra also explicitly noticed that integral equations like (1.23) are really limiting cases of n linear equations in n unknowns where K corresponds to the matrix of coefficients. In 1900, the Swedish mathematician Fredholm constructed a determinant $D(\lambda)$ corresponding to the kernel λK and constructed solutions f to the equation

$$(1.24) \qquad f(x) - \int_0^1 \lambda K(x,y)f(y)dy = g(x)$$

in terms of $D(\lambda)$ so long as $D(\lambda) \neq 0$. The device of introducing λ into the discussion dates from related work by Poincaré (1854-1912) in 1894 and actually Fredholm does not explicitly introduce any such parameters [Bellman, 114-141; Kline, 1052-1070; Reid, 274-279] give expositions of Fredholm's results and Hilbert's subsequent research which led to Hilbert space theory.

One facet of Hilbert's work was to notice that if $g = 0$ in (1.24), then the problem of finding the "eigenvalues" λ and the "eigenfunctions" f is the analogue for integrals of the transforma-

tion of a quadratic form onto the principal axes. The main result for this latter topic is the principal axes theorem: a symmetric quadratic form

$$\sum a_{ij} x_i x_j = 0, \quad a_{ij} = a_{ji},$$

in $\mathbb{R}^n$ can be rewritten by means of an "orthogonal" transformation as $\sum_{i=1}^{n} \lambda_i x_i^2$ [Courant and Hilbert, volume 1]. The physicist, Lord Rayleigh (1842-1919), needed and made use of the analogue of this result for an infinite number of variables.

Hilbert and some of the others mentioned with him at the beginning of this section verified Lord Rayleigh's act of faith by introducing the Hilbert space H of sequences $x = \{x_n \in \mathbb{R}: n=1,\cdots\}$ for which $\sum x_n^2 < \infty$ in line with their own work on (1.24). They set $\|x\| = \left(\sum x_n^2\right)^{1/2}$ and $(x,y) = \sum x_n y_n$ for $x = \{x_n \in \mathbb{R}: n=1,\cdots\}$, $y = \{y_n \in \mathbb{R}: n=1,\cdots\} \in H$; and then, because of the finite dimensional situation, they defined x and y to be orthogonal if $(x,y) = 0$. The Pythagorean theorem for H followed from these definitions: if $x,y \in H$ are orthogonal then

$$\|x + y\|^2 = \|x\|^2 + \|y\|^2. \tag{1.25}$$

Take $H = \mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$, $x = (1,0) \in \mathbb{R}^2$, and $y = (0,1) \in \mathbb{R}^2$. Then $(x,y) = 0$, $\|x\| = \|y\| = 1$, $x + y = (1,1) \in \mathbb{R}^2$, and $\|x + y\| = \sqrt{2}$. Consequently, we have (1.25) for this special case.

The development of Hilbert space theory and its structural power in organizing and analyzing large classes of integral equations received an added boost - H. Weyl refers to it as a "sort of miracle" - when it was found that Hilbert space theory provided a good mathe-

matical model for the quantum theory introduced by Heisenberg (1901-) and Schrödinger (1887-1961) in 1925, e.g., [von Neumann].

1.4.3 Biographical sketches - Fourier (1768-1830) and Newton (1642 -1727)

Besides [Gillispie; May] we used [Baron; Boyer, 1949; Struik, pp. 253 ff. and pp. 282 ff.] for our discussion of Newton and the calculus and [Benedetto; Grattan-Guiness, 1972; Riemann; Zygmund] for our discussion of Fourier and Fourier series.

Our treatment of the calculus emphasized the Fundamental Theorem of Calculus, cf., section 2.3.3, including its role as a creative formula in real variable, by means of absolute continuity [Benedetto], and in Schwartz's theory of distributions, by means of integration by parts; we refer to section 1.5.1 for some remarks about "creative formulas." We note that Theorem 2.3, in which we prove that $\pi \notin \mathbb{Q}$, uses the Fundamental Theorem of Calculus.

We mentioned Fourier series in section 1.4.2 with respect to the vibrating string problem. D'Alembert (1717-1783), Euler (1707-1783), and Lagrange (1736-1813) each made profound studies of this problem; but it was Daniel Bernoulli (1700-1782) who first saw that a relatively arbitrary graph f (of the string) might be represented as a sum of trigonometric functions. Fourier later grasped this idea in a fundamental way and noted

that the coefficients in this sum are given in terms of integrals each of whose integrands contains f and a trigonometric function. These integrals are the Fourier coefficients and had actually been used much earlier by Euler.

We observed that the study of Fourier series led finally to the proper notion of function by Dirichlet (1805-1859). Dirichlet made major contributions to Fourier analysis and number theory, and, in the former topic, he used Cauchy's theory of integral for defining Fourier coefficients. Dirichlet realized that more complicated graphs of the type mentioned above, could be represented by Fourier series if more refined theories of the integral were available. It was in this context that Riemann (1826-1866) introduced the Riemann integral [Riemann] and its corresponding Fundamental Theorem of Calculus. Riemann's work on trigonometric series led to Cantor's basic research on set theory, e.g., section 1.2.5.

Finally, we discussed the essential relation between Hilbert space theory and Fourier series.

1.5 Mathematical language and logic

1.5.1 Formulas and mathematical language

We have used the Pythagorean theorem as a "creative" formula. Such a formula is an expression whose fundamental clarity and conciseness is an efficacious sign leading inextricably to the development of new mathematical ideas. In this chapter we have followed the Pythagorean formula along some algebraic and analytic paths.

The logic and precision in mathematical language is a fundamental aspect of mathematical life, as opposed to its context, cf. section 1.5.3. With due respect to the effective attack by the oddest couple, Rome and Christianity, on Greek intellectual traditions, a good argument for the Greek demise centers about its basic mathematical masochism, viz., inadequate algebraic notation and mathematical language, cf., section 2.3.1.

1.5.2 Jeremy Bentham

Besides being the "language of the sciences" (Galileo (1564-1643)), mathematics is to some extent the language of other seemingly totally unrelated pursuits.

An interesting example of this situation is embodied in the work of Jeremy Bentham (1748-1832), especially in his important criticism of the law and the notion of natural rights. His "sacred truth" is "that the greatest happiness of the greatest number is the foundation of morals and legislation"; [Bentham] is his major work on this issue. From our point of view we are interested in Bentham's insistance on mathematical language in the discussion of law and morals; Bentham coined the terms "maximize" and "minimize" to discuss the "optimal control problem" of maximizing pleasure while minimizing pain.

He considered the inalienable rights constitutionalized by various democracies to be "fictitious entitities" (Bentham's term). For Bentham, rights are not created by asserting their existence; in reality they are created by a legislature prohibiting

certain acts. Bentham writes: "To know then how to expound a right carry your eye to the act which, in the circumstances in question, would be a violation of that right; the law creates the right by prohibiting that act." A corollary is that "for every right which the law confers on one party,••• it thereby imposes on some other party a duty or obligation."

His approach was to try to find the reality of a given word and "to measure the worth of that reality by the standard of utility" [Bronovski and Mazlish, p. 444]. His radicalism was to construct a philosophy of law and morals logically with a great emphasis on the study of language and codification (one of his words) of material. Bentham as well as Comte (1798-1857) generally share the honor of influencing Mill's (1806-1873) positivism, and as such an argument can be developed that Bentham was a precursor of twentieth century logical positivism, e.g., [Ayer; Pap]; and that perhaps the study of the logical foundations of mathematics and the philosophical problems of physics could not have taken place if the philosophical milieu (along with economic factors) of logical positivism did not exist.

Bentham's predilection with mathematical form is illustrated by his comment on mischievous acts: "There may be other points of view, according to which mischief might be divided ••• ; but this does not prevent the division here given from being an exhaustive one. A line may be divided in any one of an infinity of ways, and yet without leaving in any one of those cases any remainder."

1.5.3 Logic in mathematics

Logical positivism as a philosophical position on language and truth leads to out final comment in this section, cf., [Ayer; Benacerraf and Putnam; Weyl, Chapter 1]. The importance of symbolic and/or precise language and the necessity of that intellectual pacifier, a logical foundation, seem distinct from the content of mathematics itself.

The Intuitionist logical position developed by L.E.J. Brouwer (1882-1966) requires that mathematical proofs be constructive; for example, reductio ad absurdum arguments are not allowed in Brouwer's program, e.g., [Brouwer]. In reaction to this stance, Hilbert commented that "most of the results of modern mathematics would have to be abandoned (under Brouwer's approach), and to me the most important thing is not to get fewer results but to get more results." With regard to Hilbert's remark, Hans Lewy (1904-) (who was a Privatdozent at Göttingen at the time of Hilbert before becoming professor at University of California at Berkeley) added: "If we have to go through so much trouble as Brouwer says, then nobody will want to be a mathematician any more. After all it is a human activity. Until Brouwer can produce a contradiction in classical mathematics, nobody is going to listen to him. That is the way, in my opinion, that logic has developed. One has accepted principles until such time as one notices that they may lead to contradiction and then he has modified them. I think this is the way it will always be. There may be lots of contradictions hidden somewhere; and as soon as they appear, all mathematicians will wish to have them

eliminated. But until then we will continue to accept those principles that advance us most speedily." A similar sentiment is given in [Gleason, Preface]: "there are mathematicians who claim that there is no difference between mathematics and set theory, but I believe this claim can be dismissed. No mathematician of my acquaintance would abandon his field if an apparently insurmountable contradiction were discovered in the general concept of a subset."

The axiom of choice is: let S be any non-empty collection of non-empty sets; there is a function f defined on S such that

$$\forall S \in S, \quad f(S) \in S.$$

It turns out that the rather ethereal statement of the axiom yields a good deal of down to earth mathematics. A discussion of the axiom of choice is found in [Benedetto]. The Intuitionists do not allow themselves the sinful pleasure of the axiom, and are forced into some rather awkward situations. For example, in defining the real number system $\mathbb{R}$ by means of (1.6), the Intuitionists can't obtain the usual "intuitive" property that $\mathbb{R}$ is linearly ordered. On the other hand, Brouwer's program has recently achieved some significant mathematical success in [Bishop], cf., [Birkhoff, 1975; Stolzenberg].

1.5.4 Biographical sketches - Hilbert (1862-1943) and Poincaré (1854-1912)

Besides [Bell, 1937; Gillispie] and the reference in [May] we also used [Reid] in this discussion.

Exercises for Chapter 1

1.1 a. Use Theorems 1.2 and 1.3 to prove that $a^4 - b^4 = c^2$ has no solution $(a,b,c) \in \mathbb{N} \times \mathbb{N} \times \mathbb{N}$.

b. Use part a to prove Fermat's last theorem for the case $n = 4m$, $m \in \mathbb{N}$.

1.2 Write $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ where $k = 0,\cdots,n, k! = k(k-1)\cdots 2\cdot 1$, and $0! = 1$. If $n \in \mathbb{N}$ and we expand the expression $(a+b)^n$, its coefficients are $\binom{n}{k}$, $k = 0,\cdots,n$; these are the binomial coefficients of $(a+b)^n$. We now form the following matrix. The n^{th} row consists of the $n+1$ numbers $\binom{n}{k}$, $k = 0,\cdots,n$, between the columns $2n$ and $3n$, and zeros elswhere. Prove that $n \in \mathbb{N}$ is a prime if and only if each number in the n^{th} column is divisible by its corresponding row number. For example, the non-zero elements of the 13^{th} column are 10 at row 5 and 6 at row 6; and the non-zero elements of the 14^{th} column are 5 at row 5, 15 at row 6, and 1 at row 7. This observation is due to H. Mann and D. Shanks.

1.3 Find the errors in the following false proof of the following (false) improvement of the Pythagorean theorem: given a triangle whose sides have lengths a,b, and c; then $a + b = c$. "Proof." $P = a + b + c$ is the perimeter. As in Figure 4, we let $a_{1,1} = a_{1,2} = \frac{1}{2}a$; and draw the line of length $b_{1,1}$ parallel to the line of length b, and set $b_{1,2} = b - b_{1,1}$.

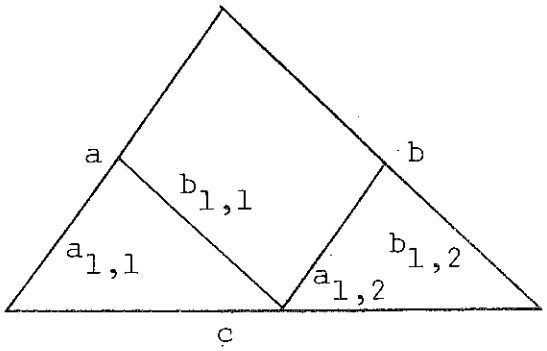


Figure 4

Then $P = c + (a_{1,1}+a_{1,2}) + (b_{1,1}+b_{1,2})$. We then perform the same construction on each of the two small triangles in Figure 4; thus, to start we set $a_{2,1} = a_{2,2} = \frac{1}{2} a_{1,1}$ and $a_{2,3} = a_{2,4} = \frac{1}{2} a_{1,2}$. Once again we obtain $P = c + \sum_{1}^{4} a_{2,j} + \sum_{1}^{4} b_{2,j}$. At the n^{th} step we have 2^n little triangles within the original and the sum of the perimeters of these triangles is P, e.g., Figure 5.

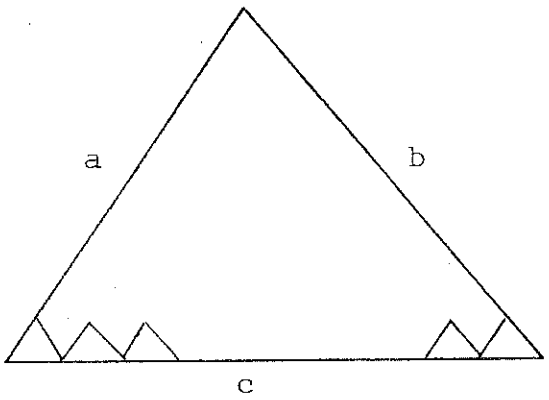


Figure 5

Obviously, the heights of these little triangles tend to zero since the $a_{n,j}$ and $b_{n,j}$ tend to zero for large n, and so the saw-tooth form "$\wedge\wedge\cdots\wedge\wedge$" in Figure 5 approaches the base line of length c as n tends to infinity. On the other hand,

$$\forall\, n, \quad a + b = \sum_{j=1}^{2^n} a_{n,j} + \sum_{j=1}^{2^n} b_{n,j};$$

and so $a + b + c = P = c + c$. This yields our (false) result.

Eudoxus and Archimedes were able to compute the area of certain closed curves by means of tiny triangles. As we'll see in Chapter 2, they proceeded much more cleverly than we did in this exercise.

1.4 Let (a,b,c) and (a',b',c') be Pythagorean triples satisfying (1.11), (1.12), and (1.13). Prove that $cc' - (ab'-a'b)$ is a perfect square. In fact, this expression is equal to $(n(n'-m') + m(n'+m'))^2$ where, for example, $a = 2mn$, $b = n^2 - m^2$, and $c = n^2 + m^2$.

1.5 Consider the formulas $q_n = p_1 p_2 \cdots p_n + 1$, where $p_1 = 2$, $p_2 = 3, \cdots$ and p_j is the j-th prime, and $F_n = 2^{2^n} + 1$. F_n is a Fermat number.

a. Use q_n to prove that there are infinitely many primes.

b. What is the first value of n for which $q_n \notin P$?

c. Use F_n to prove that there are infinitely many primes.

d. Fermat conjectured that $F_n \in P$ for all n. In 1732

Euler showed that $641 | F_5$. Verify this fact without a mind-boggling long division.

e. Prove Bertrand's postulate: $p_{n+1} - p_n < p_n$.

f. Define $2^{(1)} = 2$, $2^{(2)} = 2^2 = 4$, $2^{(3)} = 2^{2^{(2)}} = 16, \cdots$, $2^{(n)} = 2^{2^{(n-1)}}, \cdots$. Prove that there is $r \in \mathbb{R}$ such that for each n, $[(2^{(n)})^r] \in P$, where $[\alpha]$ is the integer part of α. (Hint. From part e we can construct a sequence $\{q_n : n \in \mathbb{N}\} \subseteq P$ such that for each n

$$2^{q_n} < q_{n+1} < 2^{q_n+1}.$$

Set $r_n = \log_2 (\log_2(\cdots \log_2 q_n)) \cdots)$, the n-times iterated logarithm to the base 2, and define $r = \lim r_n$.)

g. $M_n = 2^n - 1$, $n \in \mathbb{N}$, is a Mersenne number. These numbers are named after the French priest Father Marin Mersenne, cf., section 1.3.5. In the preface of his book Cogitata Physica - Mathematica (1644) he asserted that $M_p \in P$ for certain primes. Verify that $M_{13} \in P$ but $M_{15} \notin P$. In 1903, F.N. Cole (1861-1926) observed that $M_{67} = (193,707,721)(761,838,257,287)$; in 1876 E. Lucas (1842-1891) was first able to show that $M_{67} \notin P$. The largest known prime is the Mersenne number M_{19937}.

Remark It is not known if $Q = \{p \in P : p + 2 \in P\}$ is an infinite set. Related to this problem is the Goldbach conjecture: if $n > 4$ is even then $n = p + q$ for some $p,q \in P$. Goldbach stated this

in a letter to Euler in 1742. In 1937, the Russian Vinogradov (1891-) proved that all odd numbers from some (yet to be determined) point on are sums of three odd primes. More recently, Bombieri (1940-) has constructed "asymptotic sieves" to close in on the Goldbach conjecture.

1.6 Johann Bolyai (1802-1860), Gauss, and Lobachevsky (1792-1856) formulated a non-Euclidean geometry in which Euclid's parallel axiom was not valid. Lobachevsky published his work first in 1826 and this geometry is "hyperbolic" in a certain well-defined way [Hilbert and Cohn-Vossen]. Riemann's geometry was the next and even more profound step in geometrical research; in terms of Riemann's theory, hyperbolic geometry is a two-dimensional Riemannian manifold with constant negative curvature where the Riemannian metric is hyperbolic distance. Hyperbolic geometry achieved some intuitive appeal with the so-called Cayley-Klein and Poincaré models. Poincaré used his model to study certain differential equations and analytic functions.

We shall describe the Poincaré model of hyperbolic geometry. The hyperbolic plane H is the set $\{(x,y): y > 0\} \subseteq \mathbb{R} \times \mathbb{R}$, and a point of H is defined to be an element of H. A straight line in H is a circular arc in $\{(x,y): y > 0\}$ which meets the x-axis at right angle(s), e.g., Figure 6.

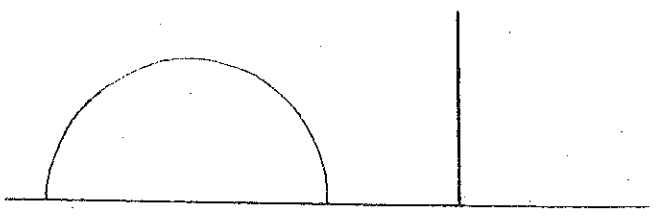


Figure 6

The angle at the point of intersection of two rays R_1 and R_2 in H is the ordinary Euclidean angle determined by the tangents, e.g., Figure 7.

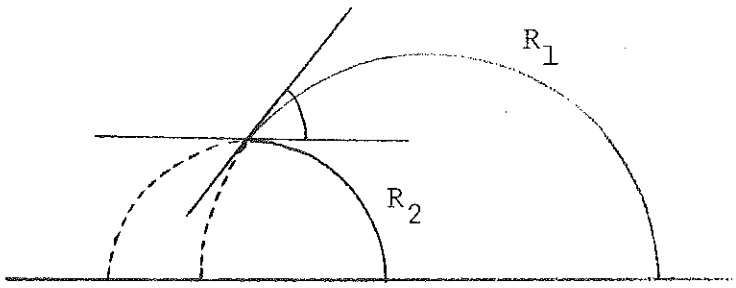


Figure 7

If $p,q \in H$ then the hyperbolic length $d(p,q)$ of the segment pq is defined in the following way. Let L be the unique line in H for which $p,q \in L$, let $a \leq b$ be the limit points of L on the x-axis, and let $p' \leq q'$ be the projections of p and q onto the x-axis. Set

$$d(p,q) = \frac{1}{2} \log \frac{(a-p')(b-q')}{(a-q')(b-p')} .$$

With these definitions we can prove that, except for Euclid's parallel axiom, the axioms of Euclidean geometry as found in [Euclid; Hilbert] are satisfied. Also, hyperbolic length can be defined in terms of the "Euclidean" arc length integrals introduced in section 1.4.1.

a. Prove that Euclid's parallel axiom is not satisfied in hyperbolic geometry.

b. Prove that the sum of the angles of a triangle in hyperbolic geometry is less that 2π radians, cf., with the discussion at the end of section 1.2.2.

Bibliography for the Introduction and Chapter 1

A.J. Ayer, Language, truth, and logic (1936), Dover, N.Y.

M. Baron, The origins of the infinitesimal calculus, Pergamon Press, N.Y., 1969.

E.T. Bell, Men of mathematics, Simon and Schuster, N.Y., 1937.

E.T. Bell, The last problem, Simon and Schuster, N.Y., 1961.

R. Bellman, editor, Modern mathematical classics, Dover, N.Y., 1961.

P. Benacerraf and H. Putnam, editors, Philosophy of mathematics, Prentice-Hall, Englewood Cliffs, N.J., 1964.

J. Benedetto, Lectures on real variable and integration, Math. Leitfäden, B.G. Teubner, Stuttgart, 1976.

J. Bentham, Introduction to the principles of morals and legislation (1789).

G. Birkhoff, Review of Novy's "Origins of modern algebra" Hist. Math. 1 (1974) 333-337.

G. Birkhoff, editor, "Foundations of mathematics" Hist. Math. 2 (1975) 503-533.

G. Birkhoff and S. MacLane, A survey of modern algebra, second edition, The Macmillan Company, N.Y., 1953.

E. Bishop, Foundations of constructive analysis, McGraw-Hill, N.Y., 1967.

S. Bochner, The role of mathematics in the rise of science, Princeton University Press, 1966.

S. Bochner, "Mathematical reflections" Amer. Math. Monthly 81 (1974) 827-852.

C. Boyer, A history of mathematics, J. Wiley and Sons, N.Y., 1968.

C. Boyer, The history of the calculus and its conceptual development (1949), Dover, N.Y., 1959.

J. Bronowski and B. Mazlish, The western intellectual tradition, (1960), Harper Torchbook, N.Y., 1962.

L.E.J. Brouwer, "Intuitionism and Formalism" BAMS 20 (1913) 81-96.

J.L. Coolidge, "The story of tangents" Amer. Math. Monthly 54 (1947) 515-525.

R. Courant and D. Hilbert, Methods of mathematical physics volume 1, Wiley (Interscience), N.Y., 1953.

J. Dauben, "The trigonometric background to G. Cantor's theory of sets" Arch. Hist. Exact Sci. 7 (1971) 181-216.

L.E. Dickson, "Fermat's last theorem and the origin and nature of the theory of algebraic numbers" Annals of Math. 18 18 (1916-1917) 161-187.

Euclid, Elements, translation and commentary by T.L. Heath, second edition unabridged, Dover, N.Y., 1956.

C.F. Gauss, Disquisitiones Arithmeticae (1810), translated by A. Clarke, S.J., Yale University Press, 1966.

C. Gillispie, (editor), Dictionary of scientific biography, C. Scribner's Sons, N.Y.

A. Gleason, Fundamentals of abstract analysis, Addison-Wesley, Reading, Ma., 1966.

K. Gödel, "Cantor's continuum hypothesis" Amer. Math. Monthly 54(1947) 515-525.

I. Grattan-Guiness, "The rediscovery of the Cantor-Dedekind correspondence", Jber Deutsch Math.-Verein 76 (1974) 104-139.

I. Grattan-Guiness (with J.R. Ravetz) Joseph Fourier, 1768-1830 MIT Press, Cambridge, Mass., 1972.

G.H. Hardy, Ramanujan, Chelsea, N.Y.

G.H. Hardy and E. Wright, An introduction to the theory of numbers, 4th edition, Oxford University Press, 1960.

M. Hendy, "Euclid and the fundamental theorem of arithmetic", Hist. Math. 2 (1975) 189-191.

D. Hilbert, Foundation of geometry, 1902 translation, The Open Court Publishing Company, LaSalle, Illinois, 1950.

D. Hilbert and S. Cohn-Vossen, Geometry and the imagination (1932), Chelsea Publishing Company, N.Y., 1956.

M. Kline, Mathematical thought from ancient to modern times, Oxford University Press, 1972.

E. Landau, Grundlagen der Analysis (1930), Chelsea Publishing Company, N.Y., 1960.

J.E. Littlewood, A mathematician's miscellany, Methuen and Co. Ltd., London, 1953.

M. Mahoney, The mathematical career of Pierre de Fermat, Princeton University Press, 1973.

K. May, Bibliography and research manual of the history of mathematics, University of Toronto Press, 1973.

L. Mordell, Three lectures on Fermat's last theorem, Cambridge University Press, 1921.

E. Nagel and J.R. Newman, Gödel's proof, New York University Press, 1960.

O. Neugebauer, The exact sciences in antiquity, second edition, Dover, N.Y., 1969.

A. Pap, An introduction to the philosophy of science, Free Press of Glencoe, N.Y., 1962.

I. Petrovskiĭ, Integral equations, Graylock Press, Rochester, N.Y., 1957.

H. Poincaré, Review of Hilbert's "Foundations of geometry" BAMS 10 (1903) 1-23.

C. Reid, Hilbert, Springer-Verlag, Heidelberg, 1970.

B. Riemann, "Sur la possibilité de répresenter une fonction par une série trigonométrique" Oeuvres mathématiques, Gauthier-Villars, Paris, 1898.

F. Riesz and B. Sz.-Nagy, Functional analysis, F. Ungar Publishing Co., N.Y., 1955.

W. Rudin, Principles of mathematical analysis, second edition, McGraw-Hill, N.Y., 1964.

G. Sarton, Introduction to the history of science, Williams and Wilkins Co., Baltimore, 1927.

J.F. Scott, A history of mathematics, Taylor and Francis Ltd., London, 1969.

L. Steen, "Highlights in the history of spectral theory" Amer. Math. Monthly 8 (1973) 359-381.

G. Stolzenberg, Review of Bishop's "Foundations of constructive analysis" BAMS 76 (1970) 301-323.

D. Struik, A source book in mathematics 1200-1800, Harvard University Press, 1969.

Á. Szabó, Anfänge der griechischen Mathematik, R. Oldenbourg, Munich-Vienna, 1969.

B. van der Waerden, Science awakening, Noordhoff Ltd., Groningen, Holland, 1954.

H.S. Vandiver, "Fermat's last theorem", Amer. Math. Monthly 53 (1946) 555-578.

K. von Fritz, "The discovery of incommensurability by Hippasus of Metapontum", Annals of Math. 45 (1945) 242-264.

J. von Neumann, Mathematical foundations of quantum mechanics, Princeton University Press, 1955.

A. Weil, "The future of mathematics" Great currents of mathematical thought (1948) ed. F.LeLionnais, Volume 1, Dover (1971) 321-336, (also published in Amer. Math. Monthly 57(1950) 295-306).

A. Weil, Review of Mahoney's "Fermat" BAMS 79 (1973) 1138-1149.

A. Weil, "Two lectures on number theory, past and present" L'Enseignement Math. 20 (1974) 87-110.

H. Weyl, Philosophy of mathematics and natural science, Princeton University Press, 1949.

H. Weyl, "A half-century of mathematics", Amer. Math. Monthly 58 (1951) 523-553.

A. Zygmund, "Fourier series", Encyclopedia Britannica 9 (1954) 564A-565.

List of characters in alphabetical order (Introduction and Chapter 1)

N. Abel (1802-1829)

Archimedes (287-212)

Archytas (430- B.C.)

Aristotle (384-322)

J. Bentham (1748-1832)

D. Bernoulli (1700-1782)

Bhaskara (1114-1185)

J. Bolyai (1802-1860)

B. Bolzano (1781-1848)

E. Bombieri (1940-)

L.E.J. Brouwer (1882-1966)

Buddha (560-480)

G. Cantor (1845-1918)

A. Cauchy (1789-1857)

F.N. Cole (1861-1926)

A. Comte (1798-1857)

Confucius (-478 B.C.)

J. D'Alembert (1717-1783)

R. Dedekind (1831-1916)

Democritus (460-350)

R. Descartes (1596-1650)

P. Dirichlet (1805-1859)

Euclid (365-275)

Eudoxus of Cnidus (408-355)

L. Euler (1707-1783)

P. Fermat (1601-1665)

J. Fourier (1768-1830)

M. Fréchet (1878-)

I. Fredholm (1866-1927)

C. Galileo (1564-1643)

C. Gauss (1777-1855)

K. Gödel (1906-)

C. Goldbach (1690-1764)

W. Hamilton (1805-1865)

Hammurabi (c. 1750 B.C.)

H. Heine (1821-1881)

W. Heisenberg (1901-)

Heraclitus (537-475)

Herodotus (480-425)

D. Hilbert (1862-1943)

Hippasus of Metapontum (500- B.C.)

C.G.J. Jacobi (1804-1851)

E. Kummer (1810-1893)

J.L. Lagrange (1736-1813)

G. Leibnitz (1646-1716)

H. Lewy (1904-)

J. Liouville (1809-1882)

J.E. Littlewood (1885-)

N. Lobachevsky (1792-1856)

E. Lucas (1842-1891)

C. Méray (1835-1911)

M. Mersenne (1588-1648)

J.S. Mill (1806-1873)

D Mumford (1937-)

C. Neumann (1832-1925)

I. Newton (1642-1727)

Parmenides of Elea (540- B.C.)

B. Pascal (1623-1662)

Plato (428-348)

H. Poincaré (1854-1912)

Pythagoras (570-500)

Lord Rayleigh (1842-1919)

B. Riemann (1826-1866)

F. Riesz (1880-1956)

E. Schmidt (1876-1959)

E. Schrödinger (1887-1961)

Socrates (470-399)

Theaetetus (414-369)

Theodorus of Cyrene (470- B.C.)

I. Vinogradov (1891-)

J. von Neumann (1903-1957)

K. Weierstrass (1815-1897)

A. Weil (1906-)

H. Weyl (1885-1955)

Zeno of Elea (500- B.C.)

2. An Alexandrian duet - Archimedes and Diophantus

2.1 Archimedes

2.1.1 Biographical sketch - Archimedes (287-212)

2.1.2 The method of exhaustion

We know how to define the area of a rectangle or triangle but it is a more subtle problem to define properly the "area" of a subset S of a plane enclosed by curves which are not straight lines. The Eudoxus-Archimedes method of exhaustion attacks this problem by "exhausting" S of as many triangles and squares as we can and keeping track of the area of these rectilinear objects. This method demands ad hoc ingenuity depending on the subset considered as well as a technique to deal with the obvious limiting process involved; the limiting process involves the Axiom of Archimedes.

We shall illustrate the method of exhaustion in Theorem 2.1; this result is found in [Euclid, Book 12, Proposition 2]. Note that we are being illogical but reasonable by assuming (to begin with) that there is a well-defined number A which is the area within the circle C.

Theorem 2.1 Let A_i be the area within the circle C_i whose radius is r_i, $i = 1,2$. Then

$$\frac{A_1}{A_2} = \left(\frac{r_1}{r_2}\right)^2 . \tag{2.1}$$

Proof We shall prove that the inequality $A_1/A_2 > (r_1/r_2)^2$ leads to a contradiction. A similar argument works for

$$A_1/A_2 < (r_1/r_2)^2.$$

Suppose $A_1/A_2 > (r_1/r_2)^2$. Then there is $A < A_1$ such that

$$\frac{A}{A_2} = \left(\frac{r_1}{r_2}\right)^2 ; \tag{2.2}$$

here we have used the fact that $\mathbb{R}$ has no "gaps", cf., the Axiom of Archimedes.

We now inscribe each C_i with a sequence of regular polygons $P_{i,n}$, $n = 1,\cdots,$ where, for each n, $P_{i,n}$ has 2^{n+1} sides.

Let $A_{i,n} = A_i - A(P_{i,n})$, where $A(P_{i,n})$ is the area of $P_{i,n}$; then $\frac{1}{2} A_{i,n} > A_{i,n+1}$, a fact which is most easily seen by a drawing before checking it analytically.

From the Axiom of Archimedes there is n for which

$A_1 - A > \frac{1}{2^n} A_{1,1}$, and so

$$A_1 - A > \frac{1}{2^n} A_{1,1} > \frac{1}{2^{n-1}} A_{1,2} > \frac{1}{2^{n-2}} A_{1,3} > \cdots > A_{1,n+1}.$$

Therefore $A_1 - A > A_{1,n+1} = A_1 - A(P_{1,n+1})$ and we have

$$A(P_{1,n+1}) > A. \tag{2.3}$$

It is routine to verify that

$$\frac{A(P_{1,n+1})}{A(P_{2,n+1})} = \left(\frac{r_1}{r_2}\right)^2 , \tag{2.4}$$

so that by combining (2.2) and (2.4) we obtain

$$\frac{A}{A_2} = \frac{A(P_{1,n+1})}{A(P_{2,n+1})} .$$

Consequently, because of (2.3) we must have $A(P_{2,n+1}) > A_2$,

and this is the desired contradiction since $P_{2,n+1}$ is inscribed within C_2.

q.e.d.

A detailed analysis of this argument is made by Heath in [Euclid].

Remark 1 We have talked about the area within a circle in Theorem 2.1 In fact, we must define the notion of such an area, and the argument in Theorem 2.1 can be properly spruced-up to yield a well-defined and intuitively reasonable number A_i corresponding to C_i.

2. The formula (2.1) asserts the existence of the number π. In fact, if $r_2 = 1$ then for any circle C, we have the formula, $A = \pi r^2$, where π is the area A_2 (and r and A are the radius and area corresponding to C). Naturally, it is interesting to evaluate π. The famous classical problem of squaring the circle is to find out if a line segment of length π can be determined by a ruler and compass construction. We shall discuss the evaluation of π in section 2.1.4 and the squaring of the circle problem in section 3.3.

2.1.3 Archimedes' 1 : 2 : 3 theorem

2.1.3.1 Archimedes' mechanical proofs

Before determining the area within parabolic segments, etc., geometrically by the method of exhaustion, Archimedes frequently first solved the problems by means of mechanics [Archimedes, Chapter 7 section 8 and pp. 241-243; Heath, pp. 288-290].

Archimedes' Method (ie., On mechanical theorems, method (addressed) to Eratosthenes), discovered in Constantinople by J.L. Heiberg in 1906, contains these mechanical methods. These mechanical proofs are actually the basis of present-day solutions in terms of integration theory; although from Archimedes' point of view they provided the heuristic basis that led to his "rigorous" geometric proofs. Also, some aspects of Archimedes' geometric solutions of area problems can be dealt with quite easily in terms of differentiation techniques. An argument has been made in [Bachmakova] that Archimedes did use a form of the differential calculus in his heuristic proofs.

2.1.3.2 Background for the 1 : 2 : 3 theorem

Let T be an isosceles triangle whose base is twice its height. We inscribe T in a semi-circle C which, in turn, we inscribe in a rectangle R, e.g., Figure 8.

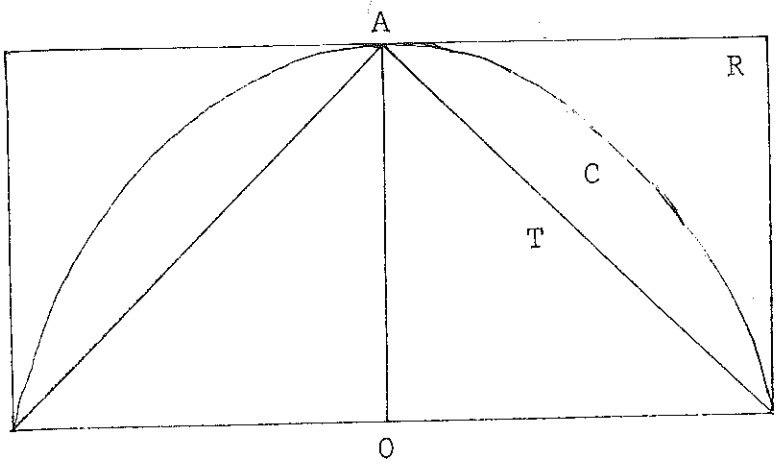


Figure 8

We generate the corresponding cone, hemisphere, and cylinder by

rotating T, C, and R about the segment AO. The respective volumes of these three solids are denoted by V_1, V_2, and V_3. Archimedes' 1 : 2 : 3 theorem is

Theorem 2.2 $V_1/V_2 = 1/2$ and $V_2/V_3 = 2/3$.

Archimedes proves this result geometrically in [Archimedes, On the sphere and cylinder]. He claims that Democritus discovered the fact that $V_1/V_3 = 1/3$ but that the part of the proof depending on the method of exhaustion was due to Eudoxus. This proof is found in [Euclid, Book 12, Proposition 10]. Archimedes completed the proof of Theorem 2.2 by proving that $V_1/V_2 = 1/2$. Archimedes obviously considered this to be a remarkable result since he asked that his tombstone have the carving of a spere inscribed in a cylinder. This request was followed and Cicero (106- 43), the Roman orator, found the tombstone when he was quaestor of Sicily. At that time the tombstone had been neglected, and Cicero was responsible for its restoration (the tombstone was again forgotten and recently rediscovered in 1965). Unfortunately, Cicero more than balanced this action with the remark: "Among the Greeks nothing was more glorious than mathematics. But we (the Romans) have limited the usefulness of this art to measuring and calculating."

2.1.3.3 Mechanical proof that $V_1/V_2 = 1/2$

Using the notation of section 2.1.3.2, we shall verify that $V_1/V_2 = 1/2$. We shall give the mechanical proof that is in Archimedes' Method; this proof uses the Democritus-Eudoxus result that $V_3 = 3V_1$.

We begin by describing the law of the lever, viz., (2.5): the lever in Figure 9 is in equilibrium if

$$aA = bB, \tag{2.5}$$

where A and B are weights having distance a and b, respectively, from the fulcrum Δ.

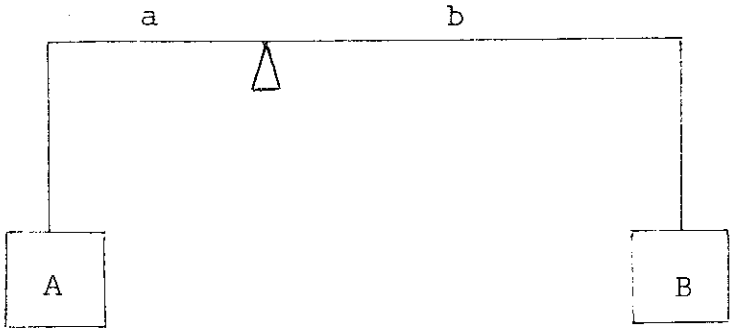


Figure 9

Figure 10 is the drawing we shall use to prove $V_1/V_2 = 1/2$. Let S be a sphere of radius r and center O; we'll work on a plane P through O. Take perpendicular diameters AB and CD of S (in P).

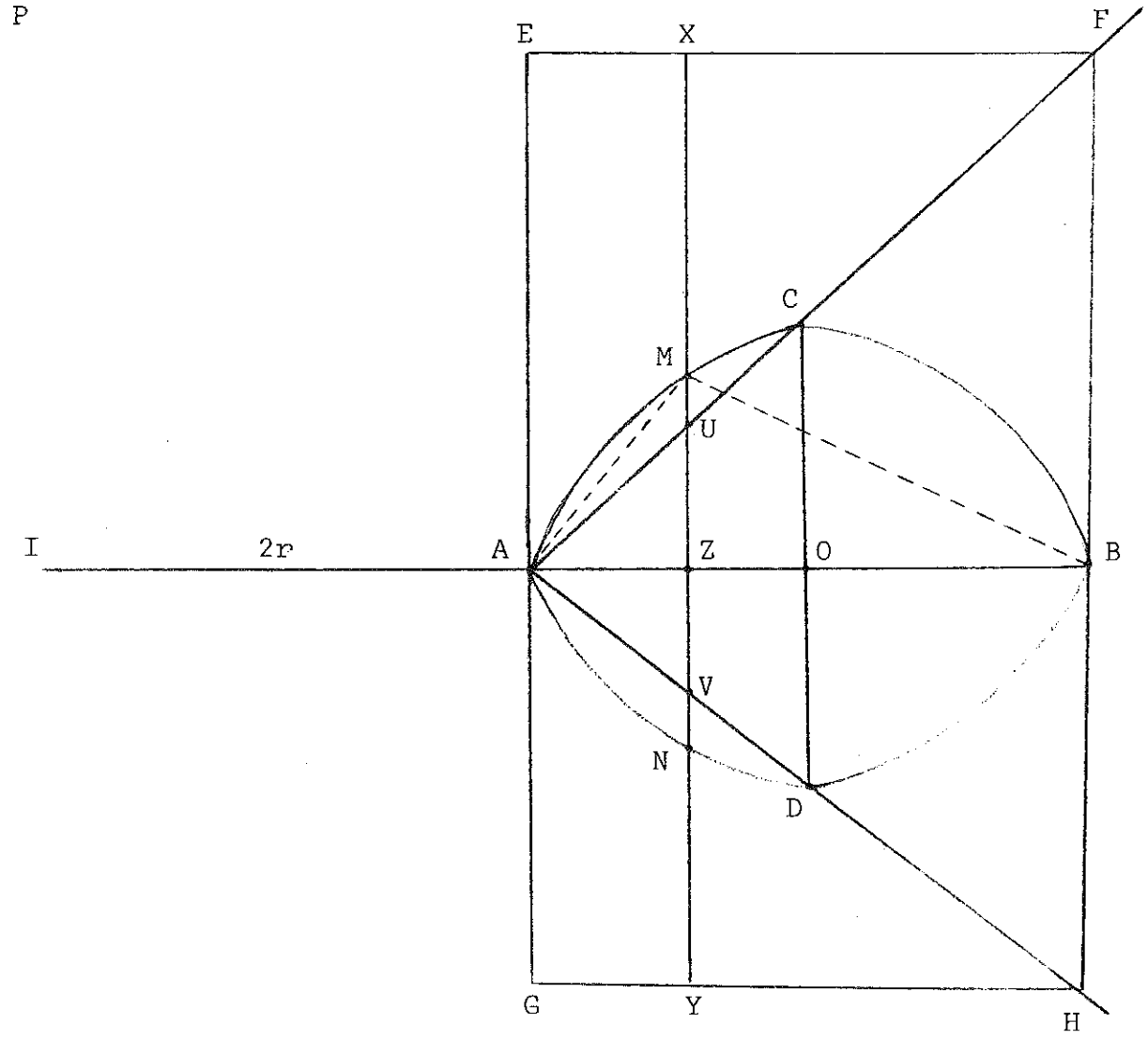


Figure 10

When we rotate the triangle ΔACD about the segment AO we obtain a cone inscribed in the hemisphere obtained by rotating the arc CAD about AO. We also form the rectangle $EFGH$ determined by the lines parallel to the circle at A and B, and by the points F and H which are on the lines AC and

AD. Let XY be a line intersecting AO at Z and parallel to CD. Also, XY intersects the circle at M and N and the triangle ΔACD at U and V. Finally, we extend AB to the point I so that the lengths $|IA|$ and $|IB|$ satisfy $|IA| = 2r$ and $|IB| = 4r$, respectively.

Note that

$$|FB| = |BH| = 2r. \tag{2.6}$$

In fact, ΔAOC and ΔABF are similar triangles, and so (2.6) follows since $|AB| = 2r$, $|AO| = r$, and $|OC| = r$. Next set $|UZ| = a$ and $|MZ| = b$, and note that $|AZ| = a$ since ΔAUZ is a right triangle and the angle $\sphericalangle ZAU$ is $\pi/4$ radians. Consequently, the right triangle ΔAMZ has the property that

$$|AM|^2 = a^2 + b^2. \tag{2.7}$$

Observe that ΔAMB is a right triangle with right angle at M since AB is a diameter. Thus,

$$|AM|^2 = (2r)^2 - |MB|^2. \tag{2.8}$$

From the right triangle ΔZMB we obtain

$$b^2 = |MB|^2 - (2r-a)^2. \tag{2.9}$$

(2.7) and (2.9) yield

$$|AM|^2 = a^2 + |MB|^2 - (2r)^2 + 4ra - a^2; \tag{2.10}$$

so that by adding (2.8) and (2.10) we obtain

$$|AM|^2 = 2ra. \tag{2.11}$$

Also we combine (2.7) and (2.11), and have

$$2ra = a^2 + b^2; \tag{2.12}$$

we write this as

$$2r(\pi(a^2+b^2)) = a\pi(2r)^2. \tag{2.13}$$

We now rotate our figure about IB so that the circle generates S, the triangle ΔAFH generates a cone whose base is a circle of radius $|BF| = 2r$ and whose height is $|AB| = 2r$, and the rectangle EFGH generates a cylinder whose base has radius $|BF| = 2r$ and whose height is $|AB| = 2r$. In this rotation, XY determines a plane which intersects the cone in a circle C_c of radius a, the sphere in a circle C_S of radius b, and the cylinder in a circle C_C of radius 2r. With this notation and the fact that $|AI| = 2r$, (2.13) becomes

$$|AI|(A(C_c) + A(C_S)) = |AZ|A(C_C), \tag{2.14}$$

where A( ) represents area.

(2.14) should be compared with (2.5); in fact, we suppose IZ is a lever with fulcrum at A. Heuristically, then, we consider circular discs with weights proportional to their areas so that (2.14) expresses the law of the lever. Consequently, if we consider n such cuts XY equidistributed by the points $A = Z_0, Z_1, \cdots, Z_n = 0$ along AO, then we can think of the sum of n areas A( ) as approximating the volume V of the corresponding solid. Thus, since $|AI| = 2r$, the left-hand side of (2.14) becomes

(2.14 left) $$2r(V_1 + V_2).$$

For the right-hand side we see from the equidistribution that

$$\sum_{j=1}^{n} |AZ_j| A(C_C) = \frac{1}{n} \tilde{V}_3 \sum_{1}^{n} |AZ_j|$$

(2.14 right) $$= \frac{1}{n} \tilde{V}_3 \, r\left(\frac{1}{n}+\frac{2}{n}+\frac{3}{n}+\cdots+\frac{n}{n}\right)$$

$$= \frac{r}{n^2} \tilde{V}_3 \, \frac{n(n+1)}{2},$$

where $\tilde{V}_3 = \pi(2r)^2 r$ is the volume of the cylinder whose base has radius $|AE| = 2r$ and whose height is $|AO| = r$. Since $V_3 = \pi r^3$, we have $\tilde{V}_3 = 4V_3$. Therefore, equating (2.14 left) and (2.14 right), we compute

(2.14) $$V_1 + V_2 = V_3$$

since $\lim_{n\to\infty} (n+1)/n = 1$. We now use the Democritus-Eudoxus result, $V_3 = 3V_1$, to obtain Archimedes' theorem, $V_2 = 2V_1$.

2.1.3.4 Surface area of spheres

Once Archimedes had proved the 1 : 2 : 3 theorem, he made the statement [Archimedes]: "From this theorem,•••, I conceived the notion that the surface (area) of any sphere is four times as great as (the area of) a great circle in it; for, judging from the fact that (the area of) any circle is equal to (the area of) a triangle with base equal to the circumference and height equal to the radius of the circle, I apprehended that, in like manner, (the volume of) any sphere is equal to (the volume of) a cone with base equal to the surface (area) of the sphere and height equal

to the radius." In fact, this result on the surface area of spheres is true, and is proved rigorously (geometrically) in [Archimedes, On the sphere and cylinder], cf., [Meschkowski] for a relatively easy reading of this proof.

2.1.4 π

2.1.4.1 Archimedes' computation

In light of his interest in figures with circular parts it is not surprising that Archimedes sought to evaluate the constant determined by Theorem 2.1 and which Euler baptized "π" (from the Greek "perimetros"). In fact, he proved that

$$3\frac{10}{71} < \pi < 3\frac{10}{70}$$

in his work [Archimedes, Measurement of a circle], cf., Exercise 2.7.

Considerable effort had been made in estimating the value of π before Archimedes' attempt; an interesting discussion is found in [Beckmann].

By means of Archimedes' method, Ludolph van Ceulen (1540-1610) of Leyden computed π to 35 decimal places using inscribed and circumscribed polygons having 2^{62} sides. A good deal of his life was spent on this project.

2.1.4.2 π in the sky

The following data concerning the decimal expansion of π are amusing [Tietze, p. 100].

Four decimal places are sufficient to determine the circumference of a circle to within 1 mm. if the radius is less than

30 meters. If the radius is as large as the distance from the earth to the sun then 15 places are sufficient to determine the circumference to within a meter.

Suppose we have π to 100 places, and consider the following situation. Take a spere S with center the earth and radius the distance d to Sirius; it would take 8 3/4 light years to reach the surface of our sphere S from here. Suppose we fill S with microbes so that each cubic millimeter contains 10^{12} (a trillion) microbes. Next, put all of these microbes in S on a straight line such that the distance between any two of them is d; and form a circle whose radius r is the distance from the first to the last (of the microbes). If the decimal expansion of π to 100 places is denoted by π_0 then

$$|2\pi r - 2\pi_0 r| < 10^{-7} \text{ mm.}$$

This observation was made in 1889 by Hermann Schubert (1848-1911).

These examples perhaps undermine the clever mnemonics that have been devised for π, e.g., [Eves, pp. 61-62; Tietze, p. 104].

2.1.4.3 π is irrational

The following result was first proved using continued fractions by the Swiss J.H. Lambert (1728-1777) in 1761.

Theorem 2.3 π^2 is irrational and therefore π is irrational.

Proof a. Define

$$\forall\, n \geq 1 \text{ and } \forall\, x \in [0,1],\quad f_n(x) = \frac{x^n(1-x)^n}{n!},$$

and observe that for each $n \geq 1$ we have

(2.15) $\forall\, x \in (0,1),\quad 0 < f_n(x) < 1/n!$

b. We note that

$$\forall\, j \geq 0,\quad f_n^{(j)}(0) \in \mathbb{Z};$$

and so by the symmetric definition of f_n we also have

$$\forall\, j \geq 0,\quad f_n^{(j)}(1) \in \mathbb{Z}.$$

Further, f_n is a polynomial of degree $2n$, and therefore $f_n^{(2n+2)}$ is identically 0.

c. Assume $\pi^2 = a/b$ where $a,b \in \mathbb{N}$. Define

$$F_n(x) = b^n\{\pi^{2n} f_n(x) - \pi^{2n-2} f_n^{(2)}(x) + \pi^{2n-4} f_n^{(4)}(x) - \cdots + (-1)^j \pi^{2n-2j} f_n^{(2j)}(x) \cdots (-1)^n f_n^{(2n)}(x)\}.$$

From part b and our hypothesis about π^2 we see that $F_n(0), F_n(1) \in \mathbb{Z}$.

d. We now compute

$$\begin{aligned}
&\frac{d}{dx}\left(F_n'(x)\sin \pi x - \pi F_n(x)\cos \pi x\right) \\
&\quad = \sin \pi x \left(F_n^{(2)}(x) + \pi^2 F_n(x)\right) \\
&\quad = b^n \sin \pi x \Big(\pi^{2n} f_n^{(2)}(x) - \pi^{2n-2} f_n^{(4)}(x) + \cdots + (-1)^n f_n^{(2n+2)}(x) \\
&\qquad + \pi^{2n+2} f_n(x) - \pi^{2n} f_n^{(2)}(x) + \pi^{2n-2} f_n^{(4)}(x) - \cdots + (-1)^n \pi^2 f_n^{(2n)}(x)\Big) \\
&\quad = b^n \pi^{2n+2} f_n(x) \sin \pi x,
\end{aligned}$$

where the last equality follows since $f_n^{(2n+2)}(x) = 0$.

Thus,

$$\frac{d}{dx}\left(F_n'(x)\sin \pi x - \pi F_n(x)\cos \pi x\right) = \pi^2 a^n f_n(x)\sin \pi x.$$

Integrating, we obtain

$$\pi^2 a^n \int_0^1 f_n(x)\sin \pi x dx = \pi(F_n(1) + F_n(0)),$$

and so

$$\pi a^n \int_0^1 f_n(x)\sin \pi x dx \in \mathbb{Z}. \tag{2.16}$$

On the other hand we have

$$\forall\, n \geq 1, \quad 0 < \pi a^n \int_0^1 f_n(x)\sin \pi x dx < \pi a^n/n!;$$

the first inequality follows from the positivity of $f_n(x)$ and $\sin \pi x$ on $(0,1)$, and the second follows from (2.15). For large n, $\pi a^n/n! < 1$; and so for such n,

$\pi a^n \int_0^1 f_n(x)\sin \pi x dx \in (0,1)$; this contradicts (2.16). Thus π^2 can't be rational, and hence π itself is irrational.

q.e.d.

Note the similarity in idea of proof between Theorem 2.3 and Proposition 1.2, where we showed that $e \notin \mathbb{Q}$. In 1882, C.L.F. Lindemann (1852-1939) proved that not only is π irrational, but it is also a transcendental number. As we shall see, this latter fact provides a negative solution to the squaring of the circle problem.

2.2 Diophantus

2.2.1 Biographical information

It is not certain exactly when Diophantus of Alexandria lived, although most historians of mathematics have sufficent evidence to place his writings in the interval 150-350 A.D. A guess is made by Tannery on the following evidence [Diophantus, p.2], cf., [Neugebauer, pp. 178-179] for a refutation of sorts. There is an admittedly corrupt 11^{th} century letter by the Byzantine Michael Psellus (1018-1080) dealing with Egyptian computational techniques in which he says: "Diophantus dealt with it more accurately, but the very learned Anatolius (-283 A.D.) collected the most essential parts of the doctrine as stated by Diophantus in a different way and in the most succinct form, dedicating his work to Diophantus." Now, Anatolius wrote this about 278-279 A.D. and was the (Catholic) Bishop of Laodicea shortly thereafter. If one could assume that there was a teacher-student relationship between Diophantus and Anatolius, given the dedication, then we might guess that Diophantus' research period was about 250 A.D.

Tannery has also suggested that Diophantus was a Christian although there seem to be good arguments against this [Diophantus, p. 2].

We have precise information about Diophantus' age. There is a collection of 46 arithmetical epigram-problems assembled mostly by the grammarian Metrodorus (c. 500 A.D.) and found in the Anthologia Palatina; generally, the solution to each such problem is equivalent to solving a simple system of simultaneous linear equations. One of these is the following epigram-problem

concerning Diophantus' age x: his boyhood lasted $1/6$ of his life; his beard grew after $1/12$ more; after $1/7$ more he married, and his son was born 5 years later; the son lived to $1/2$ his father's age, and the father died four years after his son. Thus,

$$x = \frac{1}{6}x + \frac{1}{12}x + \frac{1}{7}x + 5 + \frac{1}{2}x + 4,$$

which leads to $9 = x(1 - \frac{1}{2} - \frac{1}{6} - \frac{1}{7} - \frac{1}{12})$, and so

$$9 = x\frac{84-42-14-19}{84};$$

consequently, $x = 84$. The 19^{th} century mathematician Augustus De Morgan (1806-1871) played the same game: "I was x years old in the year x^2" $(x = 43)$.

The Anthologia Palatina contains problems similar to those in the Rhind papyrus. The Rhind papyrus was written about 1650 B.C. by the scribe Ahmes and was taken from even earlier work. It is named after the Scottish Egyptologist A. Henry Rhind (1833-1863) who bought the text in Luxor in 1858 and then willed it to the British museum; it was published in 1927.

2.2.2 Arithmetica

Diophantus' major work is the Arithmetica [Diophantus, 129-246], cf., [van der Waerden, pp. 282-286], of which six of the original books are extant. This treatise introduces a certain amount of symbolism in the discussion of algebraic problems; the use of symbolism is, of course, important, and extensive discussions of Diophantus' syncopated algebra are found in the literature, e.g., [Diophantus; Heath].

The Arithmetica contains 189 problems dealing with polynomial equations $P(x_1,\cdots,x_n) = 0$, where P has integer coefficients and where $x_1,\cdots,x_n$ are the variables; it is desired to find solutions $(x_1,\cdots,x_n) \in \mathbb{Z}^n$. Such equations with these constraints on the polynomial and the solution space are Diophantine equations; an interesting modern survey of results in this field is found in [LeVeque, pp. 4-24]. Diophantus actually considered positive rational solutions and his equations did not go beyond the fourth degree.

Among the particular results given by Diophantus we mention the following. There is the characterization of Pythagorean triples that we gave in Chapter 1 and which was known to the Babylonians. He was able to solve $ax_1^2 + bx_1 + c = x_2^2$ for the cases a or c equal to 0, a or c a square, and

$$b = 0 \quad \text{and} \quad a + c = n^2, \quad n \in \mathbb{Z},$$

cf., Pell's equation in Theorem 2.6. Finally, we note that he could solve the simultaneous equations

$$a_1x_1^2 + b_1x_1 + c_1 = x_2^2$$

$$a_2x_1^2 + b_2x_1 + c_2 = x_3^2$$

(e.g., [Diophantus, Chapter 4; Swift, pp. 166 ff.]).

The German mathematician Hermann Hankel (1839-1873) gave the following comment on Diophantus in his book on the history of mathematics. "The reader will now be desirous to become acquainted with the classes of indeterminate problems which Diophantus treats

of, and with his methods of solution. As regards the first point, we must observe that included in the 130 (or so) indeterminate problems, of which Diophantus treats in his great work, there are over 50 different classes of problems, strung together on no recognisable principle of grouping, except that the solution of the earlier problems facilitates that of the later. The first Book is confined to determinate algebraic equations; Books II to V contain for the most part indeterminate problems, in which expressions involving in the first or second degree two or more variables are to be made squares or cubes. Lastly, Book VI is concerned with right-angled triangles regarded purely arithmetically, in which some linear or quadratic function of the sides is to be made a square or a cube. That is all that we can pronounce about this varied series of problems without exhibiting singly each of the fifty classes. Almost more different in kind than the problems are their solutions, and we are completely unable to give an even tolerably exhaustive review of the different turns which his procedure takes. Of more general comprehensive methods there is in our author no trace discoverable: every question requires a quite special method, which often will not serve even for the most closely allied problems. It is on that account difficult for a modern mathematician even after studying 100 Diophantine solutions to solve the 101st problem; and if we have made the attempt, and after some vain endeavours read Diophantus' own solution, we shall be astonished to see how suddenly he leaves the broad high-road, dashes into a side-path and with a quick turn reaches the goal, often enough a goal with

reaching which we should not be content; we expected to have to climb a toilsome path, but to be rewarded at the end by an extensive view; instead of which our guide leads by narrow, strange, but smooth ways to a small eminence; he has finished! He lacks the calm and concentrated energy for a deep plunge into a single important problem; and in this way the reader also hurries with inward unrest from problem to problem, as in a game of riddles, without being able to enjoy the individual one. Diophantus dazzles more than he delights. He is in a wonderful measure shrewd, clever, quick-sighted, indefatigable, but does not penetrate thoroughly or deeply into the root of the matter. As his problems seem framed in obedience to no obvious scientific necessity, but often only for the sake of the solution, the solution itself also lacks completeness and deeper signification. He is a brilliant performer in the art of indeterminate analysis invented by him, but the science has nevertheless been indebted, at least directly, to this brilliant genius for few methods, because he was deficient in the speculative thought which sees in the True more than the Correct. That is the general impression which I have derived from a thorough and repeated study of Diophantus' arithmetic."

For perspective it is well to juxtapose Euler's remark: "Diophantus himself, it is true, gives only the most special solutions of all the questions which he treats, and he is generally content with indicating numbers which furnish one single solution. But it must not be supposed that his method was restricted to these very special solutions. In his time the use of letters to

denote undetermined numbers was not yet established, and consequently the more general solutions which we are now enabled to give by means of such notation could not be expected from him. Nevertheless, the actual methods which he uses for solving any of his problems are as general as those which are in use today; nay, we are obliged to admit that there is hardly any method yet invented in this kind of analysis of which there are not sufficiently distinct traces to be discovered in Diophantus."

2.2.3 Hilbert's tenth problem

In 1900, David Hilbert gave his famous list of 23 problems [Hilbert]. The tenth problem on this list is: given the polynomial equation

$$\bar{P}(x_1,\cdots,x_n) = 0 \tag{2.17}$$

with integer coefficients and variables $x_1,\cdots,x_n$; does there exist an algorithm $A(\bar{P})$ to determine whether or not (2.17) has a solution $(x_1,\cdots,x_n) \in \mathbb{Z}^n$. By an algorithm $A(\bar{P})$ we mean a finite set of instructions which describes, in a completely deterministic way, how to start from (2.17) and to obtain after a finite number of steps the correct answer to the question: does (2.17) have a solution $(x_1,\cdots,x_n) \in \mathbb{Z}^n$. "At no step in the process should the instructions call for either ingenuity or chance. On the other hand, we do not demand practicality of the method or place any restrictions on time or space needed to carry out the process" [Robinson, p. 80].

In 1970, Y. Matiyasevič proved that there is a $\bar{P}(x_1,\cdots,x_n)$

with no corresponding A(P). Fundamental work had previously been done by M. Davis, H. Putnam, and J. Robinson. Gödel's profound study (1931) asserting the existence of undecidable statements in formal systems set the stage for all of the subsequent work in the field. It is interesting that Pell's equation, e.g., section 2.2.6, and Fibonacci numbers have played a role in the research culminating in Matiyasevič's result. [Davis] is an excellent exposition of the problem, its solution, and its history; and [Chowla] is a study of some interesting related material.

2.2.4 Hypatia and the Arithmetica

Frequently, there are fascinating stories and unanswered questions attached to a book's journey from ancient to modern times; we now give a few remarks on the Arithmetica's trip, cf., [Diophantus, Chapter 2].

Hypatia (370-415), the daughter of Theon of Alexandria, was murdered by Christian fanatics. Theon was the author of the revision of Euclid's Elements from which all subsequent editions emerged. Hypatia was a neo-Platonist and gave lectures on philosophy. Her students included Synesius of Cyrene who became the Bishop of Ptolemais. Their close contact is symbolic of the relation between early Christian spirituality and pagan philosophy. Unfortunately, Hypatia was also a victim of the militant Christian spirit. Hypatia is important to us because of her commentary on the Arithmetica. Tannery has suggested that the remarks by Psellus that we mentioned earlier might have been taken directly from Hypatia's recension of the Arithmetica.

The Arithmetica found its way into Arabian algebra before 1000 A.D.; and it was Regiomontanus (1436-1476) who in 1463, after seeing Cardinal Bessarion's copy of the Arithmetica "according to Planudes" (1260-1310), suggested a translation of it from Greek into Latin. The task was completed in 1575 by Wilhelm Holzmann (1532-1576) of Heidelberg; Holzmann was also called Xylander, the Graecised form of his name. The manuscript that Xylander translated belonged to Andreas Dudicius. Xylander intended also to publish the Greek text of the Arithmetica but died before he was able.

Using yet another Greek manuscript of the Arithmetica as well as Xylander's work, Bachet de Méziriac (1581-1638) published a Latin translation of the Arithmetica in 1621 along with the Greek text and notes. Unfortunately, Bachet not only underestimates Xylander's influence on his own work but actually denigrates the latter's research; luckily, Heath was able to find a copy of Xylander's work and to advertise correctly Xylander's important contribution to scholarship. Bachet also borrowed freely from Bombelli's (1526-1573) algebra text (1572) which included all of the problems from the first four books of the Arithmetica.

It was in the margin of Bachet's book that Fermat wrote his famous claim, Fermat's last theorem, that we discussed in section 1.3.2. Fermat's son published another edition of Bachet's book in 1670; this edition is inferior to Bachet's original edition as far as the Arithmetica is concerned but it contains Fermat's notes which his son collected from the margins of his papa's copy.

2.2.5 Linear Diophantine equations

We shall characterize all solutions $(x_1,x_2) \in \mathbb{Z} \times \mathbb{Z}$ of the equation

$$ax_1 + bx_2 = c, \tag{2.18}$$

where $a,b,c \in \mathbb{Z}$. This equation was not explicitly considered in the Arithmetica, cf., [Diophantus, p. 67]. Since Diophantus allowed solutions $(x_1,x_2) \in \mathbb{Q} \times \mathbb{Q}$, such equations did not have a particular significance for him. [Ore, p. 184] is of the opinion that Diophantus was capable of finding the integral solutions of (2.18).

In any event, the complete characterization of (2.18) for integer solutions was first given by the Indian Brahmagupta (598-660); another Indian, Aryabhata (475-550), had previously made a contribution to the problem. Brahmagupta also worked on Pell's equation which we'll discuss in section 2.2.6.

We'll use the Euclidean algorithm, given in section 1.3.2, to prove

Proposition 2.1 Let $c = 1$ in (2.18) and assume that $(a,b) = 1$. Then there is a solution $(x_1,x_2) \in \mathbb{Z}^2$ of (2.18).

Proof. Let $a > b$ so that by Proposition 1.4 and our assumption on (a,b) we have $r_{n-2} = q_n r_{n-1} + r_n$ and $r_{n-1} = q_{n+1} r_n$ where $r_n = 1 = (a,b)$.

Thus,

$$1 = r_{n-2} - q_n r_{n-1}. \tag{2.19}$$

We have $r_{n-3} = q_{n-1}r_{n-2} + r_{n-1}$ by the Euclidean algorithm; and substituting this in (2.19) we obtain

$$1 = -q_n r_{n-3} + (q_{n-1}q_n + 1)r_{n-2}.$$

Proceeding backwards in this manner we actually construct a solution $(x_1,x_2) \in \mathbb{Z}^2$ of $ax_1 + bx_2 = 1$.

q.e.d.

The generalization of this result that completely settles the situation for a linear equation is

Theorem 2.4 a. The linear equation

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = c, \tag{2.20}$$

with $a_1,\cdots,a_n$, $c \in \mathbb{Z}$, has a solution $(x_1,\cdots,x_n) \in \mathbb{Z}^n$ if and only if the greatest common divisor, $d = (a_1,a_2,\cdots,a_n)$, of the set $\{a_1,\cdots,a_n\}$ divides c.

b. If $n = 2$ in (2.20) and $(t_1,t_2) \in \mathbb{Z}^2$ is a solution (i.e., $(a_1,a_2)|c$), then every solution $(x_1,x_2) \in \mathbb{Z}^2$ of (2.20) is given by

$$x_1 = t_1 + \frac{a_2}{(a_1,a_2)}n \quad \text{and} \quad x_2 = t_2 - \frac{a_1}{(a_1,a_2)}n$$

where n ranges through $\mathbb{Z}$.

2.2.6 Diophantine equations and Diophantine approximation

In Archimedes' Cattle Problem, dealing with the colors of bulls and cows, we have an example of a Diophantine system of seven linear equations in eight unknowns where four of these unknowns, w,x,y,z, must satisfy the conditions $w + x = n^2$ and

$y + z = m(m+1)/2$ for some $m,n \in \mathbb{N}$, e.g., [Archimedes, pp. 324-326]. These equations lead to Pell's equation

$$x^2 - py^2 = 1, \tag{2.21}$$

where in Archimedes' case, $p = 4,729,494$ and there is the side condition that y be a multiple of 9304. Bhaskara, whom we mentioned in section 1.1, solved Pell's equation for some special cases; and, in fact, the Indian school had techniques to deal with special cases of (2.21) as early as 600 A.D.

Theorem 2.6, which solves (2.21), was stated without proof by Fermat in 1657; and the first complete proof was given by Lagrange (1736-1813) in 1768. The algorithms developed by the Indian school to generate solutions did not have the capacity generally to verify if the computed value was in fact a solution. Theorem 2.6 can be proved using continued fractions. We shall give Dirichlet's proof in which he used the so-called pigeon-hole principle, viz., Theorem 2.5.

As we've indicated, John Pell (1610-1685) did not originate study in (2.21); he was given the "nominal" honor in a paper by Euler in 1732-1733.

Theorem 2.5 (Dirichlet) a. Given $\alpha \in \mathbb{R}$. For every positive integer $Q > 1$ there are $p,q \in \mathbb{Z}$, where $1 \leq q \leq Q$, with the property that

$$|q\alpha - p| < 1/Q.$$

b. Given $\alpha \in \mathbb{R}\backslash\mathbb{Q}$. There are an infinite number of relatively prime pairs $(p,q) \in \mathbb{Z} \times \mathbb{Z}$ such that for each pair (p,q) we have

(2.22) $$|q\alpha - p| < 1/q.$$

(there are only a finite number of solutions when $\alpha \in \mathbb{Q}$).

Proof. a. Consider the $Q+1$ numbers $n\alpha - [n\alpha] \in [0,1)$, where $n = 0,1,\cdots,Q$.

Partition $[0,1]$ into Q pieces each having length $1/Q$.

Consequently there are non-negative integers $n_1 < n_2 \leq Q$ such that $|(n_1\alpha - [n_1\alpha]) - (n_2\alpha - [n_2\alpha])| < 1/Q$.

Set $q = n_2 - n_1$ and $p = [n_2\alpha] - [n_1\alpha]$. Thus, $|q\alpha - p| \leq 1/Q$ and, in particular,

$$|\alpha - \frac{p}{q}| < \frac{1}{qQ} \leq \frac{1}{q^2}.$$

b. Suppose $(p_1,q_1),\cdots,(p_k,q_k)$ are relatively prime pairs which are solutions of (2.22).

Since α is irrational, $q\alpha - p \neq 0$ whenever $p,q \in \mathbb{Z}$; and so there is an integer $Q > 1$ such that

(2.23) $$\forall\, j = 1,\cdots,k, \quad \frac{1}{Q} < |\frac{p_j}{q_j} - \alpha|.$$

For this Q we choose relatively prime integers p and q from the proof of a for which $|\alpha - p/q| \leq 1/(qQ)$.

Therefore, $|\alpha - p/q| < 1/(qQ) \leq 1/Q$; and we see that (p,q) is not one of the pairs (p_j,q_j) because of (2.23).

We set $(p_{k+1},q_{k+1}) = (p,q)$.

q.e.d.

Refinements of the above result are found in [Hardy and Wright; Niven].

Dirichlet's theorem tells us that if α is irrational then 0 is a limit point of $\{n\alpha - [n\alpha] : n \in \mathbb{N}\}$; it is then easy to check that $\{n\alpha - [n\alpha] : n \in \mathbb{N}\}$ is dense in $[0,1)$. This latter result with prescribed rates of approximation is the one-dimensional Kronecker theorem. Kronecker's theorem has a deeper multi-dimensional form which is important in dealing with questions about the distribution of primes.

We now solve Pell's equation.

Theorem 2.6 Assume that $p \in \mathbb{N}$ is not a perfect square. There are integers x and y such that $x^2 - py^2 = 1$.

Proof. i. We prove that there is $M > 0$ and there are an infinite number of relatively prime pairs $(x,y) \in \mathbb{Z} \times \mathbb{Z}$, $y > 1$, such that for each pair, $|x^2 - py^2| \leq M$.

Since p is not a perfect square we know that $\sqrt{p}$ is irrational (Proposition 1.1). By Theorem 2.5 b there are an infinite number of relatively prime pairs $(x,y) \in \mathbb{Z} \times \mathbb{Z}$, $y > 1$, such that $|x - \sqrt{p}y| < 1/y$; and, in particular, $|x/y| < \sqrt{p} + 1/y^2 < \sqrt{p} + 1$.

Thus, for any such pair,

$$|x^2 - py^2| = |(x-\sqrt{p}y)(x+\sqrt{p}y)| < \frac{|x+\sqrt{p}y|}{y}$$

$$= \left|\frac{x}{y} + \sqrt{p}\right| < 1 + 2\sqrt{p} = M.$$

ii. Because of part i there is $k \in \mathbb{Z} \setminus \{0\}$ such that $x^2 - py^2 = k$ has an infinite number of solutions $(x,y) \in \mathbb{Z} \times \mathbb{Z}$. Take two such solutions, (x_1,y_1) and (x_2,y_2).

Set $x = \frac{x_1x_2 - py_1y_2}{k}$ and $y = \frac{x_1y_2 - x_2y_1}{k}$. We obtain

$$x^2 - py^2 = \frac{x_1^2x_2^2 + p^2y_1^2y_2^2 - 2px_1x_2y_1y_2}{k^2} - \frac{p(x_1^2y_2^2 + x_2^2y_1^2 - 2x_1x_2y_1y_2)}{k^2}$$

$$= \frac{1}{k^2}(x_1^2(x_2^2 - py_2^2) - py_1^2(x_2^2 - py_2^2)) = \frac{k}{k^2}(x_1^2 - py_1^2) = 1.$$

Thus, it is sufficient to prove that $x,y \in \mathbb{Z}$. This can be done easily by congruences or in a more complicated way using simple algebra.

q.e.d.

It is not à priori clear why Diophantine approximations such as Dirichlet's theorem should have anything to do with the solution of Diophantine equations. The following calculation gives a hint as to how these analytic estimates arise in dealing with discrete algebraic problems. In 1909 the Norweigian mathematician Thue (1863-1922) was responsible for establishing this approach for dealing with binary (two-variable) Diophantine equations. The exposition in [LeVeque, pp. 1-24] provides an interesting survey of this interplay between Diophantine approximations and equations (among other topics) prior to Schmidt's (1972) work.

Consider Diophantine equations having the form

$$(2.24)\quad a_0x^n + a_1x^{n-1}y + a_2x^{n-2}y^2 + \cdots + a_ny^n = c,$$

where $a_0 \neq 0$ and $a_0,\cdots,a_n,\ c \in \mathbb{Z}$. Assuming the existence of some sort of solution, e.g., section 3.2, we factor (2.24) into

$$a_0(x-\alpha_1y)(x-\alpha_2y)\cdots(x-\alpha_ny) = c,$$

and so

$$a_0 y^n \left(\frac{x}{y} - \alpha_1\right)\left(\frac{x}{y} - \alpha_2\right) \cdots \left(\frac{x}{y} - \alpha_n\right) = c.$$

If the given Diophantine equation has infinitely many relatively prime solutions $(x_j, y_j) \in \mathbb{Z}^2$, $j = 1,2,\cdots$, then $\lim_{j\to\infty} |y_j| = \infty$. Consequently,

$$\lim_{j\to\infty} \left|\left(\frac{x_j}{y_j} - \alpha_1\right) \cdots \left(\frac{x_j}{y_j} - \alpha_n\right)\right| = 0.$$

Thus there is an α, say $\alpha = \alpha_1$, for which

$$\lim_{j\to\infty} \left|\alpha - \frac{x_j}{y_j}\right| = 0.$$

2.3 Interlude while the Dark Ages play

2.3.1 Greek mathematical language

Various factors associated with the Roman and Christian ascents to power are responsible for the Greek intellectual, and in particular the Alexandrian mathematical, decline. Before discussing this topic we first ask ourselves if there were any internal (to the Alexandrians) intellectual reasons for this demise. In section 1.5.1 we indicated that an inadequacy in Greek mathematical notation and language could have had an effect. Zeuthen and van der Waerden make the point as follows [van der Waerden, pp. 265-266]: "Theaetetus and Apollonius were at bottom algebraists; they thought algebraically even though they put their reasoning in a geometric dress. Greek algebra was a geometric algebra, a theory of line segments and of areas, not of numbers. And this was unavoidable as long as the requirements of strict

logic were maintained. For "numbers" were integral or, at most, fractional, but at any rate rational numbers, while the ratio of two incommensurable line segments can not be represented by rational numbers. It does honor to Greek mathematics that it adhered inexorably to such logical consistency. But, at the same time, this set bounds for Hellenic algebra. Equations of the first or second degree can be expressed clearly in the language of geometric algebra and, if necessary, also those of the third degree. But to get beyond this point, one has to have recourse to the bothersome tool of proportions. ••• But one can not get any farther; besides, one has to be a mathematician of genius, thoroughly versed in transforming proportions with the aid of geometric figures, to obtain results by this extremely cumbersome method. Anyone can use our algebraic notation, but only a gifted mathematician can deal with the Greek theory of proportions and with geometric algebra."

It is possible that over a long period of time this communication problem, with its growing dependence on the "written roll" (of parchment), took its toll. In the short range, the oral tradition of transmitting results seems to argue against this argument, although obvious problems could arise when stringing together several such brief intervals.

2.3.2 Astronomy, astrology, and mathematical communication

During this period of Greek mathematical decline, say, 47 B.C. - 646 A.D., there was real progress made in Greek astronomy [van der Waerden, p. 265]. It is interesting to note the

importance of astrology during this period and its close relation to astronomy. It is probably true that astrology nurtured astronomy in much the same way as alchemy later influenced chemistry. Alexandrian astrology made predictions using data involving the positions of the sun and moon as well as the five planets in the zodiac. Ptolemy (85-165) wrote the Almagest ("the greatest") which remained a fundamental work for astronomers for a thousand years; in it he uses the approximate value $377/120 = 3.1416$ for π, although this may in fact have been used by Apollonius (260-190). He was also the author of Tetrabiblos ("work in four parts"), a major work on astrology which again made him a man to be read for the next thousand years. For example, medieval medical schools gave courses on mathematical astrology; mercury ruled the liver, venus the genitals, etc. How will present day mathematical sociology be viewed in 800 years? (There was a medical school at Bologna in the twelfth century).

A possible weakness of the Zeuthen-van der Waerden position is the fact that the mathematical language in the astronomical treatises seems to have been sufficiently understood to allow for the asserted progress in astronomy.

If the Zeuthen-van der Waerden conjecture is true then it has an analogue in the eighteenth century when English reluctance to adopt Leibnitz's notation for the calculus, because of the Newton (1642-1727)-Leibnitz controversy, played a role in the subsequent weak mathematical showing by England. Of course the whole issue of mathematical communication in previous times is quite difficult for us to measure; general communication was

more restrictive, there were only a handful of mathematicians, etc.

In any case, the issue of internal, i.e., neither Roman nor Christian, influences on the Alexandrian mathematical decline is interesting. Less speculative is the effect of the Romans and Christians on the Greek mathematical tradition; we shall discuss this in sections 2.3.4 and 2.3.5.

2.3.3 Biographical sketches - Leibnitz (1646-1716) and Wiener (1894-1964)

The work of Leibnitz and Wiener in language and communication is emphasized in these classroom sessions. The calculus was treated in terms of effective mathematical language in our discussion of Leibnitz. Cybernetics was the chief non-biographical topic in the discussion of Wiener; his deep work in mathematical analysis was beyond the range of the course. Besides our usual references we used [Hofmann; Weil] for studying Leibnitz. Wiener's autobiography [Wiener, 1953, 1956], obituary [Wiener, 1966], and book [Wiener, 1950] were used for studying Wiener.

2.3.4 The gray flannel toga

Recall that Archimedes was killed in 212 B.C. during the Roman conquest of Syracuse; this was part of the Punic (i.e., relating to Carthage) pulverization program which saw Carthage essentially destroyed.

In 47 B.C. Julius Caesar (100- 44) set fire to the Egyptian fleet anchored at the Alexandrian harbor. The fire spread to the city and burned the library; an estimated half-million books were

destroyed. The loss was irreparable. Mark Anthony (82-30) partially repaid the city by giving a large book collection to Cleopatra (69-30). At the time of Cleopatra's death the Romans came to Alexandria to stay. Augustus (63 B.C.-14 A.D.), the adopted son of Julius Caesar, ruled the Roman Empire during the period 30 B.C. - 14 A.D. The administrative machine developed during his reign produced an organization of and a stability in the provinces.

There were, of course, uprisings thoughout the empire, including Alexandria, from time to time, and these were dealt with sternly and decisively. One of the probable reasons that Christianity grew during this period was that it offered the helpless suffering masses a glorious afterlife; and in some sense the suffering during one's lifetime could be used to optimize this pursuit. Needless to say the Roman Empire developed an impressive IRS and Department of Defense - an unbeatable combination to stifle intellectual pursuits. [Russell, pp. 276 ff.] has analyzed the cultural relation between the Romans and conquered Greeks.

When the Roman Empire fell in 476 Alexandria could still not rest. In 646 the Moslems conquered Egypt and all of the manuscripts in the library at Alexandria were destroyed under the guiding words of the Arab leader, Omar: "Either the books contain what is in the Koran, in which case we do not have to read them, or they contain the opposite of what is in the Koran, in which case we must not read them."

2.3.5 The gray flannel chasuble

In the same spirit as the above quote by Omar, we have Saint

Augustine's (354-430) sensitive perception: "Whatever knowledge man has acquired outside Holy Writ, if it be harmful it is there condemned; if it be wholesome, it is there contained." The mathematical community more or less got even with Augustine by Georg Cantor's remark to the effect that Augustine, in accepting the sequence of integers as an actual infinity, had made an important mathematical observation, e.g., see [Struik, p. 106] for references; of course, Cantor had serious problems on this point of the mathematical infinite with some of his 19^{th} century mathematical colleagues.

The Roman emperor Constantine, who reigned from 312 to 337, adopted Christianity as the state religion. The powerful spiritual motives sometimes accorded Constantine on this ruling are put in proper perspective when one notes that a large percentage of his soldiers were Christians. Once the Church assumed a position of power it was possible to battle paganism, and consequently, Hellenic mathematics, quite effectively, for over 1000 years, e.g., see [Beckmann, Chapter 8] for a few poignant examples. Of course, one must also try to appreciate the Church's position in this time. Byzantium was a condescending and cultural cousin to lowly Rome for long periods; the barone of Rome chose popes capriciously and often, suggesting that the papal lineage required divine intervention to assure bounded variation; and intervention from the same source and of the same magnitude was apparently necessary to prevent a complete Moslem takeover of Europe.

Exercises for Chapter 2

2.1 Prove that x and y, as defined in part ii of the proof of Theorem 2.6, are integers.

2.2 Let $\mathbb{R}^n$ be Euclidean n-space and let M_n be the maximum number of spheres in $\mathbb{R}^n$ that can touch a fixed one of the same size without overlapping. The fact that $M_2 = 6$ can be verified using seven pennies. Can you convince yourself of Newton's assertion in 1694 that $M_3 = 12$?

2.3 Prove Theorem 2.4.

2.4 Consider the lists of squares and of cubes of positive integers:

1	4	9	16	25	...
1	8	27	64	125	...

It is natural to ask how often a square and cube can differ by 1, by 2, etc. It turns that the square 9 and the cube 8 constitutes the only case when the difference is 1, and that the square 25 and the cube 27 constitutes the only case when the difference is 2. Verify the latter assertion. The solution generally involves the Diophantine equation $x^3-y^2 = 2$ which can be settled using a unique factorization property similar to the one for $\mathbb{N}$ that we discussed in Chapter 1.

2.5 A polyhedron P is a solid figure in $\mathbb{R}^3$ whose boundary consists of a finite number of portions of planes, where the

boundary of each portion is a polygon; these planar portions are the faces of P. For each P, let V,F, and E denote the number of its vertices, faces, and edges, respectively. P is a regular polyhedron if each of its faces has the same number of sides and if the same number of faces come together at each vertex (of P). Euclid's definition of a regular polyhedron seems more specialized (but is not), e.g., [Hilbert and Cohn-Vossen, pp. 290-293].

a. Prove the Descartes-Euler formula for a polyhedron P: $V + F = E + 2$.

b. Use part a to prove that there are precisely five regular polyhedrons and that these polyhedrons are characterized by the information in Figure 11, where f denotes the polygonal shape of a face.

Name	V	F	E	f
Tetrahedron	4	4	6	equilateral triangle
Octahedron	6	8	12	equilateral triangle
Hexahedron (cube)	8	6	12	square
Icosahedron	12	20	30	equilateral triangle
Dodecahedron	20	12	30	regular pentagon

Figure 11

Part b appears in Euclid's Elements and is due to Theaetetus. These solids were known from the time of Plato and assumed an important role in Platonic philosophy, e.g., [Boyer, pp. 94-96; Plato; van der Waerden, p. 100; Waterhouse]. The

dodecahedron was a symbol of the universe for Plato: "God used it for the whole"; it existed long ago in natural form (in Italy) as crystals of pyrite, being used both for dice and religious purposes, cf., [Steinhaus; von Fritz, p. 256]; and it plays a major role in Dalí's (1904-) Last Supper.

2.6 In 1596, Kepler (1571-1630) introduced his model of the solar system using spherical shells and the five regular polyhedrons. The model was both spectacularly unusual and false. In 1604, overcoming tremendous historical and mathematical prejudices, he discovered the true elliptical nature of planetary orbits; but always considered the earlier model with great pride, e.g., [Dyson; Gillispie, Klein; Sternberg, pp. 94-99].

We shall briefly review the main geometrical feature of his polyhedron model. The six planets mercury, venus, earth, mars, jupiter, and saturn were known at Kepler's time; and beginning with saturn, each was farther from the sun than the previous one. Kepler associated the octahedron with venus and mercury, the icosahedron with earth and venus, the dodecahedron with mars and earth, the tetrahedron with jupiter and mars, and the cube with saturn and jupiter. We indicate this association for the case of earth and venus. Kepler let S_e resp., S_v, be the spherical shell formed using the maximum and minimum distance of earth, resp., venus, from the sun; then, letting the inner spherical surface of S_e circumscribe an icosahedron P, he claimed that the outer spherical surface of S_v inscribed P. Kepler's verification for this model involved

an occasionally blasé use of some of Copernicus' (1473-1543) observational data.

It turns out that certain rotations of a sphere circumscribed (and glued) to an icosahedron play a fundamental role in characterizing solutions of quintic equations. F. Klein (1849-1925) was the first to understand this relation; although, earlier, Galois (1811-1823) studied rotations of the icosahedron with regard to his theory of solvability for algebraic equations (Galois theory). We shall return to quintic equations in Chapter 3. As background material we now discuss rotations of the icosahedron.

Let $P \subseteq \mathbb{R}^3$ be an icosahedron, and let L be a line through P. Below, in i, ii, and iii, we list all of the ways of choosing L so that it is possible to turn P about L, and to ensure that P occupies the same exact portion of $\mathbb{R}^3$ at the beginning and end of the turn. Such a motion is a congruence motion.

i. Let L intersect opposite vertices of P;

ii. let L intersect the centers of opposite faces of P;

iii. let L intersect the midpoints of opposite edges of P.

a. Verify that, including the identity rotation of leaving P fixed, there are 60 congruence motions of the icosahedron.

b. Let $X_n = \{1,2,\cdots,n\}$ and let S_n be the set of all surjective functions $f: X_n \longrightarrow X_n$. S_n is a symmetric group. Prove that card $S_n = n!$.

c. Show that the "group" of 60 congruence motions of the icosahedron can be identified with a subset $A_5 \subseteq S_5$ where A_5 has the property that

$$\forall f,g \in A_5, \quad f \circ g \in A_5. \quad \circ$$

A_5 is an alternating subgroup and, as we've indicated, card $A_5 = 60$. It turns out that the dodecahedron can be analyzed in a similar way and can also be identified with A_5. This claim can be comfortably digested after an examination of the data in Figure 11.

2.7 Let us look at Archimedes' technique to compute π. We shall aim at obtaining the inequality $3.24 > \pi$ using a 12 sided circumscribed polygon and the inequality $1.74 > \sqrt{3}$. Archimedes obtained the result we quoted in section 2.1.4.1 by employing the technique we now indicate on 96 sided circumscribed and inscribed polygons.

Consider the triangles ΔDAO and ΔBAO, where $\sphericalangle DAO$ and $\sphericalangle BAO$ are right angles and B is a point on the segment AD.

a. If the segment OB bisects the angle $\sphericalangle AOD$ prove that $|DO|/|AO| = |BD|/|AB|$.

b. Use part a to prove $(|DO| + |AO|)/|AD| = |AO|/|AB|$ when OB bisects the angle $\sphericalangle AOD$.

c. Let $|AD|$ be half the length of the side of a regular hexagon. Verify that this hexagon circumscribes a circle C having radius $r = |AO|$.

d. Let $|AD| = 1$ and consider the situation of part c, so that $|AO| = \sqrt{3}$. Form a 12 sided circumscribed polygon about C and verify that $3.24 > \pi$ by means of part b and by comparing the perimeter of the polygon with r.

Bibliography for Chapter 2

Archimedes, Collected works, translation and commentary by T.L. Heath, Cambridge University Press, 1897.

I.G. Bachmakova, "Les méthodes différentielles d'Archimède", Arch. Hist. Exact Sci. 2 (1964) 87-107.

P. Beckmann, A history of pi, The Golem Press, Boulder, 1971.

C. Boyer, A history of mathematics, J. Wiley and Sons, N.Y. 1968.

S. Chowla, The Riemann hypothesis and Hilbert's tenth problem, Gordon and Breach, N.Y. 1965.

M. Davis, "Hilbert's tenth problem is unsolvable", Amer. Math. Monthly 80 (1973) 233-269.

Diophantus, Collected works, translation and commentary by T.L. Heath, Dover, N.Y., 1964.

F. Dyson, "Mathematics in the physical sciences", Sci. Amer., Sept. 1964.

Euclid, Elements, translation and commentary by T.L. Heath, second edition unabridged, Dover, N.Y. 1956.

H. Eves, The other side of the equation, Prindle, Weber, and Schmidt, Inc., Boston, 1969 and 1971.

C. Gillispie (editor) Dictionary of scientific biography, C. Scribner's Sons, N.Y.

G.H. Hardy and E. Wright, An introduction to the theory of numbers, 4th edition, Oxford University Press, 1960.

T.L. Heath, A manual of Greek mathematics (1931), Dover, N.Y., 1963.

D. Hilbert, "Mathematische Probleme", BAMS 8 (1901-1902) 437-479, English translation.

D. Hilbert and S. Cohn-Vossen, Geometry and the imagination (1932), Chelsea Publishing Company, N.Y., 1956.

J.E. Hofmann, Leibniz in Paris 1672-1676, Cambridge University Press, 1974.

W. LeVeque, editor, Studies in number theory, MAA Studies in Math. 6 (1969).

K. May, Bibliography and research manual of the history of mathematics, University of Toronto Press, 1973.

H. Meschkowski, Ways of thought of great mathematicians, Holden-Day, San Francisco, 1964.

O. Neugebauer, The exact sciences in antiquity, second edition, Dover, N.Y., 1969.

I. Niven, Irrational Numbers, MAA Carus monographs, 1956.

O. Ore, Number theory and its history, McGraw-Hill, N.Y., 1948.

Plato, Timaeus (360 B.C.), Penguin Books Inc., Baltimore, 1965.

J. Robinson, "Diophantine decision problems" Studies in number theory, MAA Studies in Math. 6 (1969) 76-116.

B. Russell, A history of western philosophy, Simon and Schuster, N.Y., 1945.

H. Steinhaus, Mathematical snapshots, Oxford University Press, 1960.

S. Sternberg, Celestial mechanics Part I, W.A. Benjamin, Inc., N.Y., 1969.

D. Struik, A concise history of mathematics (1948), Dover, N.Y.

J. Swift, "Diophantus of Alexandria", Amer. Math. Monthly, 63 (1956) 163-170.

H. Tietze, Famous problems of mathematics, Graylock Press, Baltimore, 1965.

B. van der Waerden, Science awakening, Noordhoff Ltd., Groningen, Holland, 1954.

K. von Fritz, "The discovery of incommensurability by Hippasus of Metapontum" Annals of Math. 46 (1945) 242-264.

W.C. Waterhouse, "The discovery of the regular solids", Arch. Hist. Exact Sci. 9 (1972) 212-221.

A. Weil, Review of Hofmann's "Leibniz" BAMS, 81 (1975) 676-688.

N. Wiener, The human use of human beings (1950), Avon Books, N.Y., 1967.

N. Wiener, Ex-prodigy (1953), MIT Press, 1964.

N. Wiener, I am a mathematician (1956), MIT Press, 1964.

N. Wiener, "Norbert Wiener 1894-1964", BAMS 72 (1966) Number 1, Part 2.

List of characters in alphabetical order (Chapter 2)

Anatolius (-283 A.D.)

Mark Antony (82-30)

Apollonius (260-190)

Archimedes (287-212)

Aryabhata (475-550)

Augustine (354-430)

Augustus (63 B.C.-14 A.D.)

Bachet de Mézeriac (1581-1638)

Bhaskara (1114-1185)

R. Bombelli (1526-1573)

Brahmagupta (598-660)

Julius Caesar (100- 44)

G. Cantor (1845-1918)

Cicero (106- 43)

Cleopatra (69-30)

N. Copernicus (1473-1543)

S. Dalí (1904-)

M. Davis (1928-)

Democritus (460-350)

A. De Morgan (1806-1871)

R. Descartes (1596-1650)

Diophantus of Alexandria (a-b) ≤ (150-350)

P. Dirichlet (1805-1859)

Eratosthenes (275-195)

Euclid (365-275)

Eudoxus of Cnidus (408-355)

L. Euler (1707-1783)

P. Fermat (1601-1665)

É. Galois (1811-1832)

K. Gödel (1906-)

H. Hankel (1839-1873)

D. Hilbert (1862-1943)

Hypatia (370-415 A.D.)

J. Kepler (1571-1630)

F. Klein (1849-1925)

L. Kronecker (1823-1891)

J.L. Lagrange (1736-1813)

J.H. Lambert (1728-1777)

G. Leibnitz (1646-1716)

C.L.F. Lindemann (1852-1939)

Y. Matiyasevič (contemporary)

Metrodorus (c. 500 A.D.)

I. Newton (1642-1727)

J. Pell (1610-1685)

Planudes (1260-1310)

Plato (428-348)

M. Psellus (1018-1080)

Ptolemy (85-165)

H. Putnam (contemporary)

Regiomontanus (1436-1476)

A.H. Rhind (1833-1863)

J. Robinson (contemporary)

W. Schmidt (contemporary)

H. Schubert (1848-1911)

Synesius of Cyrene (student of Hypatia)

Theaetetus (414-369)

Theon of Alexandria (father of Hypatia)

A. Thue (1863-1922)

L. van Ceulen (1540-1610)

N. Wiener (1894-1964)

Xylander (1532-1576)

3. Three mathematical journeys

3.1 The theory of algebraic equations

3.1.1 Complex numbers

The set $\mathbb{C}$ of complex numbers is the set of points (x,y) comprising the plane $\mathbb{R} \times \mathbb{R}$, and we shall use the notation $(x,y) = x + iy = z \in \mathbb{C}$, where $x,y \in \mathbb{R}$.

If $z_j = x_j + iy_j \in \mathbb{C}$, for $j = 1,2$, we define addition in $\mathbb{C}$ as

$$z_1 + z_2 = (x_1+x_2) + i(y_1+y_2) \in \mathbb{C} \tag{3.1}$$

and multiplication in $\mathbb{C}$ as

$$z_1 z_2 = (x_1x_2-y_1y_2) + i(x_2y_1+x_1y_2) \in \mathbb{C}. \tag{3.2}$$

The formula for multiplication is technically meaningful if one thinks of the letter "i" as the symbol "$\sqrt{-1}$", which in turn one blesses with the "property" that "$(\sqrt{-1})^2 = -1$". In any case, $\mathbb{C}$ with the algebraic properties (3.1) and (3.2) is a field with multiplicative unit 1. The set of real numbers $\mathbb{R}$ is a subfield of $\mathbb{C}$ under the map $x \mapsto (x,0) = x + i0$. (Abel was the first to define the notion of a field.) Division in $\mathbb{C}$ takes the form

$$\frac{1}{x+iy} = \frac{1}{x+iy} \cdot \frac{x-iy}{x-iy} = \frac{x}{x^2+y^2} + i\left(\frac{-y}{x^2+y^2}\right)$$

for a given $z = x + iy \in \mathbb{C}$.

If $z = x + iy \in \mathbb{C}$ then $x = \mathrm{Re}\, z$ is the real part of z and $y = \mathrm{Im}\, z$ is the imaginary part of z. The absolute value $|z|$ of $z = x + iy \in \mathbb{C}$ is

$$|z| = (x^2+y^2)^{1/2}.$$

It is not difficult to prove that $|z_1+z_2| \leq |z_1| + |z_2|$ for $z_1, z_2 \in \mathbb{C}$.

If $z = x + iy \in \mathbb{C}$ then

$$z = r(\cos \phi + i \sin \phi),$$

where $r = |z|$, $\cos \phi = x/r$, and $\sin \phi = y/r$; we write $\phi = \arg z$, where "arg" stands for "argument". For a given $z = r(\cos \phi + i \sin \phi) \in \mathbb{C}$ it is easy to verify de Moivre's formula:

$$z^n = r^n(\cos n\phi + i \sin n\phi).$$

Similarly, it is easy to check that

$$z_1 z_2 = r_1 r_2(\cos(\phi_1+\phi_2) + i \sin(\phi_1+\phi_2)),$$

where $z_j = r_j(\cos \phi_j + i \sin \phi_j) \in \mathbb{C}$; and de Moivre's formula obviously follows from this result.

De Moivre's formula was developed by Abraham de Moivre (1667-1754) and Leonard Euler in the first half of the 18^{th} century. The origins of complex numbers stem from the baffling appearance of things like $\sqrt{-2}$ in the honest work of finding zeros (e.g., section 3.1.2) of polynomials $P(x)$ with positive coefficients, in this case $P(x) = x^2 + 2$. Euler was aware that complex numbers were points in the plane since, in trying to solve $x^n-1 = 0$, he considered the solutions, $\omega_k = \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n}$ for $k = 0,\cdots,n-1$, as the vertices of a regular polygon in the plane. Each ω_k is an n-th root of unity. Setting $\omega = \omega_1$ it is clear that

$$\forall\, j = 1,\cdots,n-1, \quad \omega^j = \omega_j$$

and $\omega^n = \omega_0$.

$\mathbb{C}$, with its untidy imaginary past and its mysterious sign $\sqrt{-1}$, was legitimatized once and for all by Gauss in the first part of the 19^{th} century; the Norwegian C. Wessel (1747-1818) and Swiss J.R. Argand (1768-1822) also made fundamental insights into $\mathbb{C}$ during this period, but, from a public relations standpoint, their work had very little impact at the time. We shall come back to Gauss and Argand when we discuss the fundamental theorem of algebra.

3.1.2 Quadratic equations

As we indicated in our discussion of Pythagorean triples, the Babylonians are responsible for the solution of quadratic equations [Neugebauer , Chapter 2; van der Waerden, 1954, Chapter 3]. The quadratic problems that they solved used specific numbers as coefficients, a phenomenon which lasted to the time of Viète (1540-1603); and it seems that they probably accomplished their calculations by means of completing the square.

The Babylonians frequently posed their "quadratic problems" in terms of a pair of simultaneous equations. For example, the following is adapted from the ancient Babylonian text BM (for British Museum) 13901 via [van der Waerden, 1954, p. 69]: I have added the areas of my two squares to obtain A; the side of the second is $\frac{2}{3}$ that of the first plus 5. Thus we have

$$x^2 + y^2 = A \quad \text{and} \quad y = \frac{2}{3}x + 5.$$

Substituting $y = \frac{2}{3}x + 5$ into the first equation gives the quadratic equation

$$(1 + \tfrac{4}{9})x^2 + \tfrac{20}{3}x + (25-A) = 0;$$

and the solution is then correctly determined.

Working with the luxury of $\mathbb{C}$ at our disposal, we say that $x = z \in \mathbb{C}$ is a <u>zero</u> or <u>root</u> of the polynomial

$$(3.3)\quad P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0, \quad a_j \in \mathbb{C},$$

if $P(z) = 0$. If $a_n \neq 0$ in (3.3) then the <u>degree of P</u>, denoted by deg P, is n. We now state and prove the Babylonian theorem

<u>Proposition 3.1</u> Given the polynomial $P(x) = ax^2 + bx + c$, where $a,b,c \in \mathbb{R}$ and $a \neq 0$. Then

$$(3.4)\qquad x = -\frac{b}{2a} \pm \frac{1}{2a}\sqrt{b^2-4ac}$$

are the two zeros of the equation $P(x) = 0$.

<u>Proof</u> $P(x) = 0$ is $x^2 + \frac{b}{a}x = -\frac{c}{a}$, and so

$$x^2 + \frac{b}{a}x + \frac{b^2}{4a^2} = -\frac{c}{a} + \frac{b^2}{4a^2}.$$

Thus, $(x + \frac{b}{2a})^2 = \frac{b^2}{4a^2} - \frac{c}{a}$; and we obtain (3.4).

<u>q.e.d.</u>

The fact that there are two solutions to quadratic equations, three to cubic equations, etc., is easy to prove once we know that such an algebraic equation has at least one zero; we'll prove this fact in section 3.2.3.

3.1.3 Thus spake Algoritmi

There is a general and still open historical problem of determining the influence of Babylonian algebra on Greek mathematics or on Arabic algebra. Whereas there is reasonable evidence that Pythagoras was aware of some Babylonian mathematical contributions, the problem of determining direct Babylonian influence on Diophantus or the Arabic algebraists is difficult, although it certainly seems likely that such influence existed, cf., [van der Waerden, 1954, p. 280]. The Pythagoreans transmuted Babylonian algebra into a geometrical form out of a feeling of logical necessity [van der Waerden, 1954, pp. 125-126]; and the Greeks were quite successful in solving quadratic equations by geometrical means [Heath, pp. 100 ff.; van der Waerden, 1954, pp. 118-124].

In the early part of the 9th century, Muhammad ibn Musa Al-Khwārizmī (Mohammed the son of Moses from Khorezm, part of present-day Russia) (775-845) wrote a systematic treatise, Hisāb al-jabr w'al-muqābala, on the solution of algebraic equations. Robert of Chester (c. 1140) made a Latin translation of this work and "al-jabr" became "algebrae". The Arabic "al-jabr" means "restoration"; and, in fact, a medieval barber called himself an "algebrista" not because he restored hair for the balding but because a standard sideline included setting bones (restoring or reuniting them). (The fact that the barber also did dental work and so had to dig the "calculus" from around teeth is further indication of the nobility of barbering.) Al-Khwārizmī also wrote a book (which is lost) on Hindu numerals

whose Latin translation, found in 1857, begins with: "Spoken has Algoritmi•••"; thus, "Al-Khwārizmī" led to the word "algorithm". The Al-jabr gave geometrical proofs of its algebraic recipes, showing the Greek influence in civilization's intellectual nervousness in optimizing verifiability. These geometric apron-strings on algebra were finally dispensed with by the time of Viéte. Of course Newton later used geometric arguments in his work on mathematical physics and the calculus.

3.1.4 The Italian school

The leading Italian mathematics book at the beginning of the 16^{th} century was the treatise published in 1494 that was written by the Franciscan Luca Pacioli (1445-1510). The algebraic sections contain material on linear and quadratic equations, as well as the opinion that general methods to solve higher order equations, do not exist. It is interesting that the unknown quantity in algebraic equations was called "cosa" (the Italian word for "thing") and this is the origin of the term "cossick art" which became the European name that the theory of equations assumed in subsequent years; actually, the late Latin writers used "res" for the unknown and "cosa" is its translation into Italian.

Gerolamo Cardano's (1501-1576) Ars Magna was printed at Nuremberg in 1545, and, contrary to Fra Luca's expectations, he published general methods for solving both cubic and quartic equations. Actually, the Soviet historian Depman is of the opinion that in 1486 the Grand Inquisitor Torquemada sentenced the Spanish mathematician Valmes to be burned at the stake

because the latter claimed to have found a solution to the quartic; Torquemanda had decided that such a solution must be beyond human understanding, a quality which was not one of his dominant traits.

The Babylonians had actually dealt with cubics and solved some special cases. The Greeks also dealt with cubic equations in their geometric algebra, but in all probability did not make significant forward progress; although [Archimedes] indicates that Archimedes had some expertise on the matter. A major study of cubic equations was made by Omar Khayyám whom tradition buries in 1123. His non-mathematical Rubā'iyyat is, of course, well-known to the general public. He solved many cubic equations with positive zeros by means of geometrical arguments involving the intersection of two conic sections, e.g., [Coolidge, pp. 27-29; Eves; Struik, 1948, pp. 88-94]. These equations arose because of problems similar to that of trisecting the angle (e.g., section 3.3.7) as well as those concerned with constructing regular polygons. Although Omar Khayyám avoided negative zeros in his algebra, these were being confronted to some extent at the time. All of which brings us back to Cardano.

Sometime after 1500, Scipio del Ferro (1465-1526), a professor of mathematics at the University of Bologna, solved the cubic $x^3 + ax = b$ for a and b positive. (Of course, Viète had not yet been born, and del Ferro's coefficients were specific numbers.) In 1535, del Ferro's student, Antonio Maria Florido (1505-), challenged the then well-known mathematician Niccolò Tartaglia (1499-1557) to a problem-solving contest. In fact, Florido had become the heir to del Ferro's solution of the cubic,

and problem-solving contests were an important means of attaining or losing academic positions and intellectual prestige ; printing, invented about 1450, was still a new means of communication and it was standard to keep surreptitiously research results until the proper moment when these results could be used in a problem-solving contest with the purpose of gaining purse, position, or prestige. Tartaglia, who lived in Venice and was born in Brescia, had been quite successful in such challenges.

The battle between Florido and Tartaglia focused on Florido's questions about the cubic (details are provided in [Ore, 1953; Tietze, pp. 213-215]). Spectacularly, Tartaglia was able to answer the cubic challenge, and, being a much stronger mathematician than Florido, actually went beyond del Ferro's results - and emerged the victor. This is where Cardano enters the picture. In 1539, Cardano persuaded Tartaglia to tell him the solution of the cubic, but Tartaglia did this only after Cardano had taken a solemn oath not to disclose the information; in fact, Tartaglia was planning to conquer the hearts of the intellectual world by using his recent research on the cubic as the ultimate result of his projected treatise on algebra. In the Ars Magna Cardano proves results about the cubic and gives proper credit to del Ferro and Tartaglia, although Tartaglia doesn't seem to have been impressed by this business of proper credit. A vicious argument followed since Tartaglia claimed that Cardano had broken his word; although Tartaglia did have ten years to publish his results. In any case, Cardano also made significant further gains concerning the cubic [Ore, 1953; Smith, 1925].

The solution to the quartic is due to Lodovico Ferrari (1522-1565), the run-of-the-mill tempestuous (for example, at 17 during a brawl he lost all the fingers on his right hand) Renaissance genius. Ferrari was the amanuensis of Cardano, eventually became a very rich man, always remained extremely loyal to Cardano, and supposedly was poisoned to death by his sister. During the controversy between Cardano and Tartaglia, Ferrari actually won a debate against Tartaglia.

3.1.5 The cubic and quartic equations

We'll now solve the cubic and quartic equations. The Italian solution of the cubic yielded one zero, and it was Euler (1732) who first completed the calculation by showing how to obtain all three zeros. This latter part is of course easy technically, but required a deeper understanding of the nature of polynomial equations than existed in the first half of the 16^{th} century.

Proposition 3.2 a. The solution of the cubic equation

$$x^3 + a_2x^2 + a_1x + a_0 = 0, \quad a_j \in \mathbb{C}, \tag{3.5}$$

can be reduced to the solution of the cubic equation

$$y^3 + ay + b = 0, \tag{3.6}$$

where $a = a(a_0,a_1,a_2)$, $b = b(a_0,a_1,a_2) \in \mathbb{C}$.

b. The three solutions of (3.6) are given by

$$\begin{aligned} y_1 &= u + v, \\ y_2 &= \omega u + \omega^2 v, \end{aligned} \tag{3.7}$$

and

$$y_3 = \omega^2 u + \omega v,$$

where

$$(3.8) \quad u = \left(-\frac{b}{2} + \left(\frac{b^2}{4} + \frac{a^3}{27}\right)^{1/2}\right)^{1/3}, \quad v = \left(-\frac{b}{2} - \left(\frac{b^2}{4} + \frac{a^3}{27}\right)^{1/2}\right)^{1/3}$$

and ω is the cube root of unity $(-1 + i\sqrt{3})/2$ (the cube roots u and v must have the property that $uv \in \mathbb{R}$).

Proof a. Set $x = y - \frac{a_2}{3}$ and substitute this into (3.5). We obtain

$$\left(y - \frac{a_2}{3}\right)^3 + a_2\left(y - \frac{a_2}{3}\right)^2 + a_1\left(y - \frac{a_2}{3}\right) + a_0$$

$$= \left(y^2 - \frac{2a_2y}{3} + \frac{a_2^2}{9}\right)\left(y + \frac{2a_2}{3}\right) + a_1y - \frac{a_1a_2}{3} + a_0,$$

and so the y^2 terms cancel.

b. i. Let $y = u + v$ in (3.6), so that the problem is changed into one with two unknowns. (3.6) becomes

$$(u^2+2uv+v^2)(u+v) + a(u+v) + b$$

$$(3.9) \qquad = u^3 + v^3 + 3u^2v + 3v^2u + a(u+v) + b$$

$$= u^3 + v^3 + b + (u+v)(3uv+a) = 0.$$

ii. Let $y = y_1$ be a solution to (3.6). We shall prove later in the Fundamental Theorem of Algebra that this is not a vacuous assumption; and, naturally, we can just check that (3.7) and (3.8) provide a solution.

By solving a quadratic equation we can choose u and v so

that $y_1 = u + v$ and

(3.10) $$uv = -a/3$$

(that is, substitute $u = y_1 - v$ into (3.10) to form $v^2 - y_1 v - \frac{a}{3} = 0$, and then solve this quadratic equation). Thus, u and v are determined, and we'll now describe how to write them in terms of a and b.

The constant $-a/3$ in the constraint (3.10) was chosen in light of the non-cubic part of (3.9).

From what we've done we see that u and v must satisfy the system

(3.11) $$\begin{aligned} u^3 + v^3 + b &= 0 \\ 3uv + a &= 0. \end{aligned}$$

iii. Using (3.11) we'll form the quadratic equation whose zeros are u^3 and v^3. In fact, the second equation in (3.11) becomes

(3.12) $$u^3 v^3 = -a^3/27;$$

so that solving for u^3 (resp., v^3) in the first equation of (3.11) and substituting in (3.12) we see that u^3 and v^3 are the solutions of

(3.13) $$x^2 + bx - \frac{a^3}{27} = 0.$$

Thus, solving (3.13) as in Proposition 3.1 we obtain

$$u^3 = -\frac{b}{2} + \frac{1}{2}\sqrt{b^2 + \frac{4a^3}{27}}, \quad v^3 = -\frac{b}{2} - \frac{1}{2}\sqrt{b^2 + \frac{4a^3}{27}}.$$

Taking cube roots and using the definition of y_1 we obtain (3.7) and (3.8).

iv. It is easy to check that y_2 and y_3, as defined in the statement of this result, provide other solutions to (3.6).

q.e.d.

(3.7) (and (3.8)) is Cardano's solution of the cubic equation (3.6).

We shall now give Viète's proof (1591) of Proposition 3.2 which provides a valuable insight in finding explicit solutions to polynomial equations of deg n, $n \geq 5$. We begin with the trigonometric relation

Lemma $\cos 3\alpha = 4\cos^3\alpha - 3\cos\alpha$.

Proof By de Moivre's formula

$$\cos 3\alpha + i \sin 3\alpha = (\cos\alpha + i \sin\alpha)^3$$
$$= \cos^3\alpha - 3\cos\alpha \sin^2\alpha + i(3 \sin\alpha \cos^2\alpha - \sin^3\alpha).$$

We obtain the result by equating real and imaginary parts and using the fact that $\cos^2\alpha + \sin^2\alpha = 1$.

q.e.d.

We shall use the Lemma in section 3.3.7 to prove the impossibility of trisecting certain angles by means of a ruler and compass construction. We now use it in

Trigonometric proof of Proposition 3.2 b. We'll solve (3.6).

From the Lemma we have

$$x^3 - \frac{3}{4}x - \frac{1}{4}\cos 3\alpha = 0, \tag{3.14}$$

where we've set $x = \cos\alpha$.

Write $y = wx$, where y comes from (3.6), where x comes from (3.14), and where w is at our disposal.

Substituting $y = wx$ into (3.6) we obtain

$$x^3 + \frac{a}{w^2}x + \frac{b}{w^3} = 0;$$

and, with (3.14) in mind, we choose $w = \sqrt{-4a/3}$.

Note that we still have α at our disposal.

Choose α so that $-\frac{1}{4}\cos 3\alpha = \frac{b}{w^3}$ (here we are using some elementary facts about complex variables that we shall not verify).

Thus, using our chosen value of w, we have

$$\cos 3\alpha = \frac{-b}{2(-a^3/27)^{1/2}}. \tag{3.15}$$

We solve (3.15) for $\alpha = \alpha(a,b)$ and so compute $x = x(a,b) = \cos\alpha$.

Since $w = w(a)$ and $y = wx$ we have found $y = y(a,b)$ which satisfies (3.6).

q.e.d.

Before going on to the quartic, let us expand on our statement about the importance of the above trigonometric solution of the cubic equation. Trigonometric functions have a single period p, e.g., $\sin z = \sin(z+np)$ where $p = 2\pi$ is the period, $z \in \mathbb{C}$, and $n \in \mathbb{Z}$. As such, trigonometric functions

are the degenerate forms of so-called elliptic functions, which are a class of functions f defined on $\mathbb{C}$ and having two periods, p_1 and p_2:

$$\forall z \in \mathbb{C} \text{ and } \forall n, m \in \mathbb{Z}, \quad f(z) = f(z+mp_1+np_2).$$

It turns out that quintic equations can not in general be solved by methods depending on the extraction of roots (as we did in (3.8)), but they can be solved by means of elliptic modular functions. This was accomplished by Hermite (1822-1905) in 1858, and is analogous to the solution of the cubic by trigonometric functions.

We now give Ferrari's solution of the quartic.

Proposition 3.3 The four solutions of the quartic equation

$$x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 = 0 \tag{3.16}$$

are given by the four solutions of the two quadratic equations

$$x^2 + \frac{a_3}{2}x + \frac{1}{2}y_1 = \pm(ax+b),$$

where a and b are well defined numbers determined in the proof and where y_1 is Cardano's solution of the cubic equation

$$y^3 - a_2y^2 + (a_3a_1-4a_0)y - (a_0(a_3^2-4a_2) + a_1^2) = 0. \tag{2.17}$$

Proof i. We write (3.16) as $x^4 + a_3x^3 = -(a_2x^2+a_1x+a_0)$, and then complete the square on the left hand side by adding $a_3^2x^2/4$ to both sides. We obtain

(3.18) $$\left(x^2 + \frac{a_3 x}{2}\right)^2 = \left(\frac{a_3^2}{4} - a_2\right)x^2 - a_1 x - a_0.$$

To give ourselves some necessary freedom we add $(x^2 + \frac{a_3 x}{2})y + \frac{y^2}{4}$ to both sides of (3.18), where y is a new variable.

Note that as such the left hand side of (3.18) remains a perfect square:

$$\left(x^2 + \frac{a_3 x}{2}\right)^2 + \left(x^2 + \frac{a_3 x}{2}\right)y + \frac{y^2}{4} = \left(x^2 + \frac{a_3 x}{2} + \frac{y}{2}\right)^2.$$

Thus,

(3.19) $$\left(x^2 + \frac{a_3 x}{2} + \frac{y}{2}\right)^2 = \left(\frac{a_3^2}{4} - a_2 + y\right)x^2 + \left(\frac{a_3 y}{2} - a_1\right)x + \left(\frac{y^2}{4} - a_0\right).$$

ii. We shall now show that we can choose y so that the right hand side of (3.19) can be written as the square, $(ax+b)^2$.

Generally, the equation, $Ax^2 + Bx + C = a^2x^2 + 2abx + b^2$ will be valid if $B^2 - 4AC = 0$.

In fact, if $AC = \frac{B^2}{4}$ then

$$(\sqrt{A}\,x + \sqrt{C})^2 = Ax^2 + 2x\sqrt{AC} + C = Ax^2 + Bx + C.$$

Thus, we set $a = \sqrt{A}$ and $b = \sqrt{C}$ where we have

$$A = \left(\frac{a_3^2}{4} - a_2 + y\right), \quad B = \left(\frac{a_3 y}{2} - a_1\right), \quad \text{and} \quad C = \left(\frac{y^2}{4} - a_0\right)$$

from (3.19).

It remains to verify if y can be taken with the property that $B^2 - 4AC = 0$, i.e., if there is y for which

$$(3.20)\qquad \frac{a_3^2y^2}{4} - a_1a_3y + a_1^2 - 4\left(\frac{a_3^2}{4} - a_2 + y\right)\left(\frac{y^2}{4} - a_0\right) = 0.$$

(3.20) is (3.17) and we saw how to find the required $y = y_1$ in Proposition 3.2.

iii. Consequently, form (3.17) and part ii, there are numbers $a,b,y_1 \in \mathbb{C}$, each depending on $a_0,\cdots,a_3$, such that

$$\left(x^2 + \frac{a_3x}{2} + \frac{y_1}{2}\right)^2 = (ax+b)^2.$$

This yields the result.

q.e.d.

Proposition 3.2 and Proposition 3.3 constituted the first clear-cut significant new mathematics that modern Western civilization had produced. The immediate course was now well-defined: solve the quintic equation.

3.1.6 The quixotic quintic

In 1683, the German Ehrenfried Walter von Tschirnhausen (1651-1708), a friend of Leibnitz, showed that for cubic polynomials $P(x)$ there are quadratic polynomials $Q(y) = x$ such that $P(Q(y)) = y^3 + a$, where a is a well-defined constant. Then $y = -a^{1/3}$, $-\omega a^{1/3}$, $-\omega^2 a^{1/3}$ are the three solutions of $P(Q(y)) = 0$, where $\omega \neq 1$ is a cube root of unity; and, hence, $x = Q(-a^{1/3})$, $Q(-\omega a^{1/3})$, $Q(-\omega^2 a^{1/3})$ are the three solutions of $P(x) = 0$.

Tschirnhausen had comparable success with the quartic, and for a long time thought he had transformed a general quintic polynomial $P(x)$ to one having the form $P(Q(y)) = y^5 + a$, cf.,

the opinion of [Tietze, p. 224]. It was Leibnitz who found the error in this latter calculation; and it was subsequently shown, in fact, that the original quintic was transformed into one of the 24^{th} degree. In 1786, the Swedish mathematician E.S. Bring (1736-1798) was able to use a Tschirnhausen transformation to reduce the general quintic equation $P(x) = 0$ to the form $P(Q(y)) = y^5 + ay + b = 0$. When Hermite solved the general quintic polynomial equation in 1858 by means of elliptic modular functions, he begins with this reduced Bring form but attributes it to the Englishman Jerrard (-1863) who published such a reduction in 1834, cf., [Harley; Klein, 1884, pp. 157-158]. Jerrard insisted that his technique reduced the general quintic $P(x) = 0$ to $P(Q(y)) = y^5 + a$ in spite of irrefutable objections to the contrary. For further remarks on Tschirnhausen transformations we refer to [Cajori, 1904, pp. 102-103; 1894, pp. 328-329; Dickson, Chapter 12].

We noted that Hermite solved the general quintic polynomial equation be means of elliptic modular functions. In fact, it can not generally be solved by the "algebraic" operations of addition, multiplication, and taking roots, but requires "transcendental" devices, cf., section 3.3.3. When solutions of a polynomial equation can be found by means addition, multiplication, and taking roots, we say that the equation can be solved by radicals.

In 1771, Joseph-Louis Lagrange of Torino (many of his countrymen from present-day northern Italy still say "Lagrangia" instead of "Lagrange") whom we mentioned in section 2.2.6 published a

profound study on the theory of equations entitled "Réflexions sur la résolution algébrique des équations". The importance of this work in setting the stage for the theory of groups is analyzed in [Pierpont, 1895]. For $\deg P \leq 4$, his method reduced the problem of solving the polynomial equation $P(x) = 0$ to that of considering polynomials of lower degree - the same effect as the Tschirnhausen transformation; for $\deg P = 5$ his technique provided a polynimial Q with $\deg Q = 6$.

Paolo Ruffini (1765-1822) of Modena was an enthusiastic disciple of Lagrange; and in his major mathematical works of 1799 and 1813 (he was also a medical doctor and politician) he used group theoretic notions while trying to show that not every quintic can be solved by radicals. His proof is not conclusive but was patched up in the latter half of the 19^{th} century. E. Bortolotti has written extensively on Ruffini's work, e.g., Ruffini's collected works and the 1928 International Congress of Mathematicians. There is a critical study of Ruffini's theorem due to [Burkhardt], cf., [Ore, 1957]. In 1824, Abel conclusively proved the impossibility of solving an arbitrary quintic by radicals, e.g., [Smith, 1929, pp. 261-266]. Abel's result is complicated and was done without knowledge of Ruffini's work. Ruffini's group theoretic arguments can be used in conjunction with Abel's idea to produce a palatable and elementary proof of the insolubility by radicals of the general quintic [Pierpont, 1896]. Abel had sent Gauss a copy of this result, and the great and grating Gauss had paid no attention.

Hilbert went on to prove that for each $n \geq 5$ there are an

infinite number of polynomials $P(x)$, with $\deg P = n$ and having integer coefficients, for which the equation $P(x) = 0$ can't be solved by radicals; $P(x) = x^5 - 6x + 3$ provides such an example.

3.1.7 Biographical sketches - Abel (1802-1829), Galois (1811-1832), and Lagrange (1736-1813)

Besides [Gillispie] and the references in [May] we also used [Galois; Kiernan]. [Infeld; Ore, 1957; Sarton] provided particularly interesting reading.

3.2 The fundamental theorem of algebra

3.2.1 The number of zeros of a polynomial

The calculations in section 3.1.5 were based on the assumption that solutions to the given cubic and quartic equations did in fact exist; then the formulas we derived exhibited explicit solutions. We shall prove the Fundamental Theorem of Algebra: if $P(x)$ is a polynomial with $\deg P = n \geq 1$ and with complex coefficients then

$$\exists\, \alpha \in \mathbb{C} \text{ such that } P(\alpha) = 0. \tag{3.21}$$

As we shall see, the Fundamental Theorem of Algebra is more of a result in analysis or topology (in particular, the geometry of curves) than algebra. The term "Fundamental Theorem of Algebra" is due to Gauss.

Cardano realized to some extent that if $\deg P = n$ then $P(x)$ must have n zeros. In this regard, there is a basic relationship between the coefficients of $P(x)$ and its zeros.

Viète was one of the first to have some insight into the matter, and shortly afterward the issue was clarified by the Englishman Thomas Harriot (1560-1621) and the Flemish Albert Girard (1590-1633). Girard actually allowed for negative and imaginary zeros, as opposed to Viète and Harriot. He also explicitly asserted that "every algebraic equation has as many solutions as the exponent of the highest term indicates", but he really had some qualifications to this general statement in mind, e.g., [Smith, 1929, p. 292]. A comparison of the contributions of Girard, Harriot, and Viète is made in [Boyer, pp. 334-338; Cajori,1894], cf., [Bosmans; Struik, 1969, pp. 81-87]. Their contribution on this point can be summed up as

Proposition 3.4 Let $P(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be a polynomial with $\deg P = n \geq 1$ and coefficients in $\mathbb{C}$. Assume (3.21) (which we'll prove later).

a. $P(x)$ has the unique representation

$$P(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n), \tag{3.22}$$

where $\{\alpha_1,\cdots,\alpha_n\} \subseteq \mathbb{C}$ is the set of zeros of $P(x) = 0$ ((by uniqueness we mean that if $P(x) = (x-\beta_1)\cdots(x-\beta_m)$ then $m = n$ and that the β's can be arranged so that $\alpha_1 = \beta_1,\cdots,\alpha_n = \beta_n$).

b. The zeros and coefficients of $P(x)$ satisfy the following relations:

$$a_{n-1} = -\sum_{j=1}^{n} \alpha_j,$$

$$a_{n-2} = \sum_{i<j} \alpha_i\alpha_j,$$

$$a_{n-3} = -\sum_{i<j<k} \alpha_i\alpha_j\alpha_k$$

$$\vdots$$

$$a_0 = \pm \alpha_1\alpha_2 \cdots \alpha_n$$

(e.g., $\alpha_1\alpha_2 = \alpha_2\alpha_1$ so that if $n = 3$ then $a_{3-2} = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3$).

Proof b follows from a when we multiply out the expression for $P(x)$ in (3.22) and compare with the given expression.

a. By (3.21) we let $x = \alpha_1$ be a zero of $P(x)$. Dividing, $(x-\alpha_1)|P(x)$, it is clear that we obtain

(3.23) $$P(x) = (x-\alpha_1)P_1(x) + c_1,$$

where $P_1(x)$ is a polynomial with deg $P_1 = n-1$ and $c_1 \in \mathbb{C}$.

Letting $x = \alpha_1$ in (3.23) we have $P(\alpha_1) = c_1$ so that $c_1 = 0$ since $P(\alpha_1) = 0$. Thus

$$P(x) = (x-\alpha_1)P_1(x), \quad \deg P_1 = n-1.$$

We now prodeed in the same way with P_1 and obtain

$$P(x) = (x-\alpha_1)(x-\alpha_2)P_2(x), \quad \text{where } \deg P_2 = n-2.$$

In this way we compute (3.22). We omit the proof of uniqueness.

q.e.d.

It is possible that $\alpha_1 = \cdots = \alpha_m$ in (3.22). In this case, if $\alpha_1 \notin \{\alpha_{m+1},\cdots,\alpha_n\}$ then α_1 is a multiple zero of multiplicity m. Cardano and, later, Newton had observed that if $P(x)$ has real coefficients and if $P(\alpha+i\beta) = 0$, $\alpha,\beta \in \mathbb{R}$ and $\beta \neq 0$, then $P(\alpha-i\beta) = 0$. It was also popular sport to

see how many positive (resp., negative, complex) zeros P might have; for example, Descartes proved that if P is a polynomial with real coefficients then the maximum number of positive zeros of $P(x)$ is the number of changes in sign of the coefficients, e.g., [Uspensky, pp. 121-124]. We illustrate what we mean by the number of changes in sign. Let $a_5 = 1$, $a_4 = -1$, $a_3 = -3$, $a_2 = -5$, $a_1 = 6$, $a_0 = 6$; the sign changes between a_5 to a_4 and between a_2 to a_1. In this case the number of changes in sign of the coefficients is 2. If $a_j = 0$ then there can not be a change of sign counted for either a_{j+1} to a_j or a_j to a_{j-1}. Results such as Descartes' led to a general problem of determining the distribution of zeros of polynomials in $\mathbb{C}$; and this has led to certain aspects of modern algebraic geometry. A 19^{th} century high point on this general problem is due to C. Sturm (1803-1855); Sturm's theorem (1829) allows one to find the exact number of real zeros contained between two given real numbers for equations without multiple zeros, e.g., [Alexandrov, Chapter 4.4; Uspensky, Chapter 7].

The formulas in Proposition 3.4 b led to the study of symmetric polynomials, which along with the theory of permutation groups and the use of so-called resolvents, formed the basis of Lagrange's study of polynomials.

3.2.2 Integration theory and the fundamental theorem of algebra

In 1746, Jean Le Rond D'Alembert (1717-1783) formulated and attempted to prove (3.21). Interest at this time to prove (3.21), and thus obtain the representation (3.22), received an

impetus from the problem of using partial fractions as a technique of integration. In 1702, the Swiss Johann Bernoulli (1667-1748), who was an outspoken critic of the English in the Leibnitz-Newton controversy, claimed that the integral

$$\int \frac{P(x)}{Q(x)}\,dx, \tag{3.24}$$

where P and Q are polynomials, is solved by means of trigonometric and logarithmic functions (and no other "transcendental" functions) as well as quotients of polynomials.

A rational function is a quotient of polynomials, and during the 17^{th} century and early part of the 18^{th} century many attempts were made to integrate both rational and "irrational" functions. In the latter category we include integrals which are used to calculate the arc length of an ellipse and which arose from problems in astronomy. It was natural to approximate the "irrational" functions by rational ones. Without being specific we note that the study of "elliptic integrals" led to a very sizable theory by the mid-19^{th} century, cf., [Dieudonné, pp. 833 ff.]; and it was Hermite's expertise on such matters that led to his solution of the general quintic in terms of elliptic modular functions.

Bernoulli's claim on the evaluation of (3.24) was not universally accepted, and the dispute reduced to the problem of whether or not a polynomial P with real coefficients could be written as a finite product of linear and quadratic polynomials with real coefficients; this representation is of course valid because of (3.21) and Proposition 3.4 a. Thus, if we are given

the rational function P/Q, with $\deg P < \deg Q$, Johann Bernoulli and we have

$$\frac{P(x)}{Q(x)} = \frac{P(x)}{L_1(x) \cdots L_m(x) Q_1(x) \cdots Q_n(x)},$$

where $L_j(x) = a_j x + b_j$, $Q_j(x) = c_j x^2 + d_j x + e_j$, and $a_j, \cdots, e_j \in \mathbb{R}$. Assuming that the L_j and Q_j are all distinct, the method of partial fractions yields

$$\frac{P(x)}{Q(x)} = \sum_1^m \frac{A_j}{L_j(x)} + \sum_1^n \frac{B_j x + C_j}{Q_j(x)}, \tag{3.25}$$

where the $A_j, B_j, C_j \in \mathbb{R}$ can be computed by writing the denominator of the right hand side of (3.25) as $Q(x)$, performing the calculation, and identifying coefficients of this new numerator with those of $P(x)$. The integrals of the terms in the right hand side of (3.25) are then easily computed. For example, if we must compute

$$\int \frac{ax+b}{x^2+cx+d}\, dx,$$

then we let $u = x^2 + cx + d$, set

$$\frac{ax+b}{x^2+cx+d} = \frac{A}{u}\frac{du}{dx} + \frac{B}{u},$$

and solve for A and B obtaining $A = a/2$ and $B = \frac{2b-ac}{2}$; therefore, the desired integral is

$$\frac{a}{2} \log |x^2+cx+d| + \frac{2b-ac}{2} \int \frac{dx}{x^2+cx+d},$$

where the remaining integral can be evaluated in terms of a log or $\tan^{-1}$ by completing the square.

3.2.3 Proof of the Fundamental Theorem of Algebra

Before giving proofs of (3.21) let us recall two properties of continuous real-valued functions. If $K \subseteq \mathbb{C}$ is compact and $f: \mathbb{C} \longrightarrow \mathbb{R}$ is continuous then the least upper bound axiom for $\mathbb{R}$ yields the existence of $\alpha \in K$ such that

$$f(\alpha) = \inf \{f(z): z \in K\}.$$

Similarly, we have the intermediate value theorem for continuous functions $f: \mathbb{R} \longrightarrow \mathbb{R}$: if $f(a) < 0$, $f(b) > 0$, and $a < b$ then there is $\alpha \in (a,b)$ such that $f(\alpha) = 0$.

The following is due to Euler.

Proposition 3.5 Given $P(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ where $n > 1$ is odd and $a_0, \cdots, a_{n-1} \in \mathbb{R}$. Then there is $\alpha \in \mathbb{R}$ such that $P(\alpha) = 0$.

Proof Set $M = 1 + \sum_0^{n-1} |a_j|$ and note that

$$|P(x)-x^n| \leq \sum_0^{n-1} |a_j||x|^j. \tag{3.26}$$

Using the facts that n is odd, the a_j are real, and $M \geq 1$, we obtain (for $x = -M$)

$$P(-M) \leq -M^n + \sum_0^{n-1} |a_j|M^j \leq -M^n + M^{n-1} \sum_0^{n-1} |a_j|$$

$$= -M^n + M^{n-1}(M-1) = -M^{n-1}.$$

Thus, $P(-M) < 0$.

Similarly, we compute (for $x = M$)

$$P(M) \geq M^n - \sum_0^{n-1} |a_j| M^j > M^n - M^{n-1} \sum_0^{n-1} |a_j|$$

$$= M^n - M^{n-1}(M-1) = M^{n-1}.$$

Thus, $P(M) > 0$.

The result follows from the intermediate value theorem.

q.e.d.

Theorem 3.1 (Fundamental Theorem of Algebra) Given a polynomial $P(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ with complex coefficients and $n \geq 1$. Then

(3.21) $\exists\, \alpha \in \mathbb{C}$ such that $P(\alpha) = 0$.

Proof i. We shall first verify that

(3.27) $\exists\, \alpha \in \mathbb{C}$ such that $|P(\alpha)| = \inf \{|P(z)| : z \in \mathbb{C}\}$.

Define $w = \inf \{|P(z)| : z \in \mathbb{C}\}$.

If $|z| = R$ note that

$$|P(z)| \geq R^n(1 - (|a_{n-1}|R^{-1} + \cdots + |a_0|R^{-n});$$

and so $\lim_{|z| \to \infty} |P(z)| = \infty$.

Thus we can choose $R > 0$ with the property that $|P(z)| > w$ when $|z| > R$.

Set $K = \{z : |z| \leq R\}$.

Consequently, since K is compact there is $\alpha \in K$ for which

$$|P(\alpha)| = \inf \{|P(z)| : z \in K\}.$$

By the way we've chosen K we see that

$$\inf \{|P(z)| : z \in K\} = \inf \{|P(z)| : z \in \mathbb{C}\}.$$

Thus, we obtain (3.27).

ii. We shall assume $w \neq 0$ and then find $\beta \in \mathbb{C}$ for which

$$|P(\beta)| < |P(\alpha)| = w. \tag{3.28}$$

(3.28) contradicts (3.27) and so w must be 0. This is (3.21).

iii. Since $w \neq 0$ we can define $Q(z) = P(z+\alpha)/P(\alpha)$. Because $n \geq 1$ we see that Q is not a constant function. Also,

$Q(0) = 1$, and $|Q(z)| \geq 1$ by the definition of α.

The facts that Q is a polynomial and $Q(0) = 1$ allow us to write

$$Q(z) = 1 + b_k z^k + b_{k+1} z^{k+1} + \cdots + b_n z^n \tag{3.29}$$

for some $1 \leq k \leq n$, where $b_k \neq 0$.

iv. By the properties of $\mathbb{C}$, we can choose $\theta \in \mathbb{R}$ for which $-|b_k| = b_k e^{ik\theta}$.

From (3.29) we see that

$$\begin{aligned} &Q(re^{i\theta}) \\ &= 1 + r^k b_k e^{ik\theta} + r^{k+1} b_{k+1} e^{i(k+1)\theta} + \cdots + r^n b_n e^{in\theta} \\ &= 1 - r^k |b_k| + r^k (r b_{k+1} e^{i(k+1)\theta} + \cdots + r^{n-k} b_n e^{in\theta}) \end{aligned}$$

is valid for all $r > 0$.

Take $r > 0$ small enough so that $1 \geq r^k |b_k|$, and without loss of generality assume $k < n$. For such r the triangle inequality yields

$$\begin{aligned} |Q(re^{i\theta})| &\leq 1 - r^k |b_k| + r^k (r|b_{k+1}| + \cdots + r^{n-k}|b_n|) \\ &= |1 - r^k(|b_k| - r|b_{k+1}| - \cdots - r^{n-k}|b_n|)|. \end{aligned} \tag{3.30}$$

Clearly $(|b_k| - r|b_{k+1}| - \cdots - r^{n-k}|b_n|) > 0$ for small $r > 0$ since $b_k \neq 0$.

Consequently, when $r > 0$ is small we obtain (3.28) from (3.30).

q.e.d.

We refer to [Stein] for an easy topological proof of the Fundamental Theorem of Algebra. In fact, by elementary homology theory it can be shown that for each $n \in \mathbb{Z} \setminus \{0\}$ there is no continuous function $f : \{z \in \mathbb{C} : |z| \leq 1\} \longrightarrow \{z \in \mathbb{C} : |z| = 1\} = S^1$ whose restriction to S^1 is defined by $f(z) = z^n$; assuming the negative of (3.21) yields a contradiction to this result.

3.2.4 History of the Fundamental Theorem of Algebra

The first precise statements of (3.21) (although not in the context of $\mathbb{C}$) and Proposition 3.4 a (in terms of real coefficients and linear and quadratic factors) seem to be due to Euler in a letter he wrote to Johann Bernoulli's nephew Nicholas Bernoulli (1687-1759) in 1742. A little later, in 1746, D'Alembert attempted a proof of (3.21); we shall have more to say about D'Alembert's idea in a moment.

In 1749 Euler published his proof of Proposition 3.5, and then proceeded to solve (3.21) for $\deg P = n$ by a series of solutions for special even integers, e.g., [Struik, 1969, p. 102]. There were gaps in this latter stage of the proof which Lagrange attempted unsuccessfully to fill, and of which Gauss gave a critique in his Helmstädt doctoral dissertation of 1799.

It was in this dissertation that (3.21) was first proved correctly, e.g., [Struik, 1969, pp. 115-122], although some

statements concerning the structure of the real numbers and properties of continuous functions were not properly formulated until later; according to his journal, Gauss discovered this proof in October 1797. The idea of this first proof was the basis for the proof of (3.21) that Gauss published in 1849, but this time using the properties of $\mathbb{C}$ more directly, e.g., [Uspensky, pp. 293-297]. In 1814 and 1816 Gauss published two other different proofs of (3.21). Besides the importance of settling (3.21), such proofs dealt with the very important issue of mathematical existence. Both Greek mathematics and algebra from the Babylonians to the 16^{th} century Italians generally viewed mathematical existence in terms of construction; for example, the solution of a quadratic equation was actually exhibited. Gauss was able to verify the validity of (3.21) but was not able to provide a procedure for constructing such a zero. This existential and non-constructive aspect is contained in the proofs of both Proposition 3.5 and Theorem 3.1; in the former it is reflected in the use of the intermediate value theorem and in the latter by the property that continuous functions achieve their minima on compact sets.

Gauss' first proof of (3.21) was geometrical. He wrote the given polynomial P as $P(x+iy) = u(x,y) + iv(x,y)$ where u and v are real-valued functions of two real variables. Then a zero of P is a point of intersection of the curves $u(x,y) = 0$ and $v(x,y) = 0$. Thus, Gauss verified (3.21) by showing that the curves $u = 0$ and $v = 0$ intersect. He also proved Proposition 3.4 a in his dissertation.

His second proof is algebraic except for the use of Proposition 3.5 at the very end of his paper [Smith, 1929, pp. 292-306]. This second proof indicates the essentially analytic side of the fundamental theorem of algebra; for try as he did to solve (3.21) completely algebraically, Gauss had to use the intermediate value theorem to clinch his proof. This second proof also invites a comparison between it and Artin's (1898-1962) proof of (3.21) which uses Galois theory and Proposition 3.5 [van der Waerden, 1931, Section 70] (ie., how close did Gauss come to Galois theory?).

Gauss' third proof of (3.21) is entirely analytic in nature and the techniques anticipate the theory of complex variable. This proof is given in [Meschkowski, pp. 64-69], and an intersecting study of it is found in [Bôcher]. The third proof is closely related to the Argand-D'Alembert proof on which we'll soon comment, to those proofs of (3.21) that involve Liouville's or Rouché's (1832-1910) theorems, e.g., [Ahlfors, p. 122; Hille, volume 1, p. 254], respectively, and to some ostensibly ad hoc proofs, e.g., [Buck, p. 493]. One fact that connects all of these seemingly diverse approaches is the Cauchy integral formula.

After Gauss' first proof the next serious proof seems due to Argand (1806). In order to discuss Argand's contribution it is necessary to give D'Alembert's idea that we mentioned at the beginning of this section and which turns out to be quite sound. D'Alembert's attempted proof of (3.21), properly modernized, consists of two steps. The first step asserts (3.27), and the second, which is called D'Alembert's lemma states that

$$\forall\, \alpha \in \mathbb{C} \text{ for which } P(\alpha) \neq 0,\ \exists\, \beta \in \mathbb{C} \text{ such that}$$

(3.31)

$$|P(\beta)| < |P(\alpha)|.$$

Obviously, (3.31) is (3.28), and these two steps are precisely the way we proved Theorem 3.1. D'Alembert's lemma is a form of maximum modulus principle that is studied in the theory of complex variable. We also note that Gauss' geometrical proof in 1799 actually comes around to the use of (3.27) [Petrova, p. 258]. D'Alembert's attempted proof was not valid, or at the very least it contained gaps, even if we consider the subtle foundational step contained in (3.27) to be more of an axiom than as something to be verified. It has even been suggested that his actual argument depended on (3.21), although [Petrova, p. 257] argues against this. In any case, Argand gave the first valid proof of (3.31). It turns out that Cauchy and Legendre (1752-1833) gave similar, less accurate, and more widely distributed proofs of Theorem 3.1 after Argand's proof; and there is suspicion to the possibility that Legendre knew of Argand's work and did not reference it [Petrova, p. 260].

3.2.5 A constructive fundamental theorem of algebra

We have discussed the existential nature of the proofs of (3.21). For such a basic result it is natural to ask for more in the way of determining a solution.

Galois' theory characterizes those polynomials whose zeros can be found by radicals; and as we mentioned there are fifth degree polynomial equations which are not solvable by radicals. We then noted that quintic equations can be solved by certain

transcendental functions (elliptic modular functions). Such a procedure is aesthetically satisfying and provides insight into the structure of such polynomials.

On the other hand, it is also important to see if a well-defined (denumerable) procedure exists which allows us to construct zeros for a given polynomial equation in a computable way. H. Weyl was able to do this using an intuitionist proof based on a residue argument; whereas in 1940 H. Kneser succeeded in producing a constructive proof based on Argand's proof and an earlier attempt to use Argand's proof by R. Lipschitz (1832-1903). Many facets of complex variable, including the complex variable proof of (3.21), yield to constructive methods, and as we mentioned in section 1.5.3 a systematic treatment is found in [Bishop]. A constructive proof of (3.21) based on arguments of a purely algebraic nature and on assumptions about $\mathbb{R}$ that were stated in purely algebraic terms (although the proof of these assumptions would require analytic methods) was first given by O. Perron (1880-), e.g., [Zassenhaus].

3.2.6 Biographical sketches - Euler (1707-1783) and Gauss (1777-1855)

Besides [Gillispie] and the references in [May] we used [Hall] in our discussion of Gauss; [Scott] has a good description of Gauss' work in number theory. Although noted in [May], I mention for emphasis the definitive account by [Dunnington] and the personal memorial by [von Waltershausen]. Euler's collected works should be mandatory viewing for the course along with selected readings from Truesdell's (1919-) eloquent and

profound analysis of Euler, e.g., [Euler, series secunda, volume II, part 2; Truesdell]. We also mention [Gillings] since it argues convincingly against the dramatic nature of the confrontation between Euler and Diderot (1713-1784).

3.3 Squaring the circle

3.3.1 Statement and origin of the problem

Take a straightedge and compass. With the straightedge we only allow ourselves to draw a straight line between two given points. With the compass we only allow ourselves to draw a circle with a given radius and a given center. Each of these two operations is called a fundamental construction. Any segment constructed by a finite number of fundamental constructions will be called a ruler and compass construction. No other operation is allowed. For example, we do not allow markings on the straightedge to be used in the construction. Consider a circle C with radius having unit length so that the area A_C bounded by C is π. The squaring of the circle problem is to determine if a segment having length $\sqrt{\pi}$ can be constructed by a ruler and compass construction. The terminology, squaring of the circle, is used since A_C is the area of the square with side having length $\sqrt{\pi}$.

The Rhind papyrus states the problem of transforming the unit circle into a square of equal area; the fundamental ruler and compass constraint is not made there. The writer of the papyrus gives the following solution: cut off 1/9 of the diameter and construct a square upon the remainder; the area of this square is the desired answer. Thus,

$$\pi = A_C = (2 - \frac{2}{9})^2 = (\frac{16}{9})^2 \approx 3.16 \; -$$

not bad. Estimating the value of π and the above mentioned problem from the Rhind papyrus are practically equivalent endeavors; and the squaring of the circle can be viewed as a refinement of this problem.

Anaxagoras of Clazomenae (500-428), who is responsible for the correct theory of eclipses (but who still thought the earth was flat), is reported by Plutarch (46 -120) in De exilio to have worked on estimating π while in prison. Anaxagoras was one of the first resident Athenian philosophers [Bochner, pp. 305-306; Russell; van der Waerden, 1954]. Antiphon, a contemporary of Socrates, used the method of inscribing polygons in C to compute π [Heath, pp. 140-141]; and as such it can be argued that he had a basic insight concerning the method of exhaustion. It is to his mathematical credit that he was criticized by Aristotle about this work. None of these Greeks, including Archimedes, Hippocrates of Chios, (460-357) and Apollonius, squared the circle in the precise way that we have demanded, but several of them obtained good information about π as we mentioned in Archimedes' case. [Beckmann; Heath, pp. 143 ff.; Hobson; Klein, 1895, pp. 55 ff.; Tietze, Chapter 5; van der Waerden, 1954, pp. 130 ff.] survey the work of those who have "squared the circle", including those who knew they were not obeying the ruler and compass guidelines as well as those who didn't know.

3.3.2 Constructible numbers

Suppose we are given the complex plane marked only with the points $(0,0)$ and $(0,1)$. A complex number $c = a + ib \in \mathbb{C}$ is constructible if segments of lengths $|a|$ and $|b|$ can be made from ruler and compass constructions. In this case we can find the point $(a,b) \in \mathbb{C}$ in the plane by means of a ruler and compass construction. Let $C \subseteq \mathbb{C}$ be the set of all constructible numbers. By our assumption, $1 \in C$; and we note that $\mathbb{Q}$ is the field generated by 1.

Proposition 3.6 $\mathbb{Q} \subseteq C$ and C is a field.

Proof $1 \in \mathbb{Q} \cap C$ by hypothesis and so it is sufficient to prove that C is a field. Given $\alpha,\beta \in C$; and, without loss of generality, let $\alpha,\beta \geq 0$.

i. We shall construct $\alpha + \beta$.

Draw a straight line and on it use the compass to mark off the lengths $|OA| = \alpha$ and $|AB| = \beta$ (where A is between O and B); then $|OB| = \alpha + \beta$.

ii. We shall construct $\alpha\beta$.

Mark off the lengths $|OA| = \alpha$ and $|OB| = \beta$ where $0 < \sphericalangle AOB < \pi/2$ radians; and mark off the length $|OU| = 1$ on the line determined by OA.

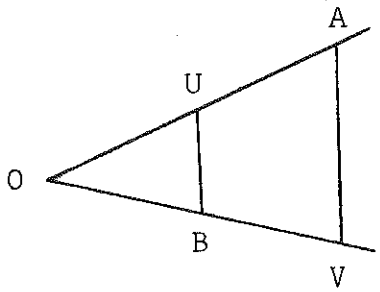


Figure 12

Draw the segment UB and construct the segment AV parallel to UB, where V is on the line determined by OB, e.g., Figure 12.

By the fundamental property of similar triangles,

$$\frac{\alpha}{1} = \frac{|OV|}{\beta}, \quad \text{i.e.,} \quad |OV| = \alpha\beta.$$

iii. Assuming $\beta > 0$ we shall construct α/β.

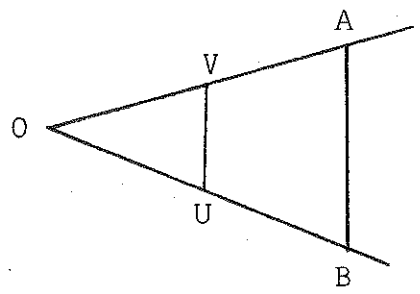


Figure 13

Take OA and OB as in part ii and mark off the length $|OU| = 1$ on the line determined by OB.

Draw the segment AB and construct the segment UV where UV is parallel to AB and V is on the line determined by OA, e.g., Figure 13.

By the fundamental property of similar triangles,

$$\frac{\beta}{1} = \frac{\alpha}{|OV|}, \quad \text{i.e.,} \quad |OV| = \frac{\alpha}{\beta}.$$

q.e.d.

It is conceivable that $\mathbb{Q} = C$.

Proposition 3.7 If $\alpha \in C$ is non-negative then $\sqrt{\alpha} \in C$. In particular $C \setminus \mathbb{Q} \neq \emptyset$ since we know that $\sqrt{2} \notin \mathbb{Q}$.

Proof On a straight line, mark off lengths $|OA| = \alpha$ and $|AB| = 1$ as in Figure 14.

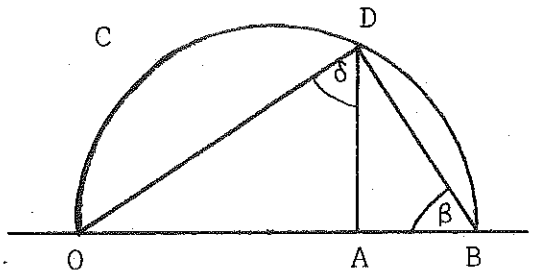


Figure 14

Bisect OB and draw the circle C having diameter $|OB|$.

Let AD be the perpendicular to OB, where D is a point of C.

The angle $\sphericalangle ODB$ is a right angle since the triangle ΔODB is inscribed in a semi-circle.

Consequently, $\sphericalangle ODA = \sphericalangle OBD$, i.e., $\delta = \beta$. This is clear from Figure 14, since we have $\pi = \frac{\pi}{2} + (\frac{\pi}{2} - \delta) + \beta$ in the triangle ΔADB.

Therefore ΔOAD and ΔDAB are similar; and so we compute

$$\frac{\alpha}{|AD|} = \frac{|AD|}{|AB|}, \text{ i.e., } |AD| = \sqrt{\alpha}.$$

q.e.d.

Let $S \subseteq \mathbb{C}$ be the smallest field with the property that if $\alpha \in S$ and $\alpha \geq 0$ then $\sqrt{\alpha} \in S$. We've just proven that $S \subseteq C$. The following result shows that "$\sqrt{\ }$" is the only non-rational operation possible by means of a ruler and compass construction.

Proposition 3.8 $S = \mathbb{C}$.

Proof We must prove that $\mathbb{C} \subseteq S$. The proof is by induction. For the case $n = 0$, we assert that the given points $(0,0)$, $(1,0) \in \mathbb{C}$ are each formed by 0 fundamental constructions. The induction hypothesis is that if $\alpha \in \mathbb{C}$ is formed by at most n fundamental constructions then $\alpha \in S$. Given this hypothesis we'll now prove that if $\alpha \in \mathbb{C}$ is formed by at most $n+1$ fundamental constructions then $\alpha \in S$. The construction of α proceeds in the following way. At the completion of n^{th} step a finite set $\{\alpha_1,\cdots,\alpha_m\} \subseteq \mathbb{C}$ has been formed by fundamental constructions, and because of the induction hypothesis we have $\{\alpha_1,\cdots,\alpha_m\} \subseteq S$. At this point there are three possibilities in which to form $\alpha \in \mathbb{C}$ at the $(n+1)$st step from a fundamental construction given the set $\{\alpha_1,\cdots,\alpha_m\}$. We shall illustrate each of these three possibilities and show that in each case we obtain $\alpha \in S$.

i. Without loss of generality draw the line L_1 through α_1 and α_2, and draw the line L_2 through α_3 and α_4. Let $\alpha \in L_1 \cap L_2$.

We can write L_j as

$$A_j x + B_j y + C_j = 0, \quad j = 1,2, \tag{3.32}$$

where $A_j, B_j, C_j \in S$ by the induction hypothesis. Clearly, α is the solution of the system (3.32); and so $\alpha \in S$ since $A_j, B_j, C_j \in S$.

ii. Let $\alpha \in L_1 \cap C$, where L_1 is as in part i and where C is a circle with center α_3 and with $\alpha_4 \in C$. The equation for C is

$$x^2 + y^2 + 2Dx + 2Ey + F = 0, \tag{3.33}$$

where $D,E,F \in S$ by the induction hypothesis.

Solve for y in the $j = 1$ equation of (3.32), and substitute this value of y in (3.33).

The solution of the resulting quadratic equation in x yields the x-coordinates of points of intersection of L_1 and C.

Similarly, solve for x in the $j = 1$ equation of (3.32) and substitute this x in (3.33).

The solution of the resulting quadratic equation in y yields the y-coordinates of points of intersection of L_1 and C.

These solutions involve square roots and rational operations on numbers in S, and so $\alpha \in S$.

iii. Suppose finally that α is an intersection point of two circles C_1 and C_2 (whose equations are written in the form of (3.33)).

Subtract the second equation from the first to obtain a linear equation which we use with C_1 in a way analogous to the computation in part ii.

Consequently, as in part ii, we see that $\alpha \in S$.

q.e.d.

We now consider Proposition 3.8 in the following framework.

Set $F_0 = \mathbb{Q}$ and take $\alpha \in \mathbb{Q}$ such that $\sqrt{\alpha} \notin \mathbb{Q}$. Let $F_1 \subseteq \mathbb{C}$ be the field of numbers generated by $\sqrt{\alpha}$ and $\mathbb{Q}$, where F_1 depends on α. For any such F_1 and any $\alpha \in F_1$ for which $\sqrt{\alpha} \notin F_1$, let F_2 be the field generated by $\sqrt{\alpha}$ and F_1, where F_2 depends on α. Thus, for each $n \geq 1$ we form a countable family of fields F_n, where each such F_n depends on an F_{n-1} and an $\alpha \in F_{n-1}$ for which $\sqrt{\alpha} \notin F_{n-1}$. F_n is an extension field of F_{n-1} depending on α. Consequently, $\alpha \in C$ if and only if α is in some such F_n; and $\beta \in F_n$ if and only if $\beta = a + b\sqrt{\alpha}$, where $\alpha, a, b \in F_{n-1}$ and $\sqrt{\alpha} \notin F_{n-1}$.

3.3.3 Algebraic and transcendental numbers

$\alpha \in \mathbb{C}$ is algebraic if it is the root of some polynomial equation $P(x) = 0$, where $P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ and each $a_j \in \mathbb{Q}$. If $\alpha \in \mathbb{C}$ is not algebraic then it is transcendental. Let $A \subseteq \mathbb{C}$ be the set of algebraic numbers. Clearly, $\mathbb{Q} \subseteq A$; and $\sqrt{2} \in A$ since $\alpha = \sqrt{2}$ is a zero of the equation $x^2 - 2 = 0$. It turns out that A is a field of numbers [Pollard, p. 37].

Liouville constructed the first transcendental numbers in 1844; his main article on the subject appeared in 1851. In 1873, Georg Cantor proved that A is a countable set and that the set of transcendental numbers is an uncountable set, e.g., section 3.3.5.

Proposition 3.9 $C \subseteq A$.

Proof Take $\alpha \in C$. By our remark at the end of section 3.3.2

on extension fields, we see that α is an element of some F_n.

We shall prove the result using induction on the F_n's.

Suppose $\alpha = a + b\sqrt{\beta} \in F_1$, where $a,b,\beta \in \mathbb{Q} = F_0$ and $\sqrt{\beta} \notin \mathbb{Q}$.

We have $\alpha \in \mathbb{C}$.

Thus, $(\alpha-a)/b = \sqrt{\beta}$ so that $\alpha^2 - (2a)\alpha + (a^2-b^2\beta) = 0$.

Consequently, α is a zero of a polynomial with rational coefficients and hence $\alpha \in A$.

From this procedure we see that if $\alpha \in F_n \subseteq \mathbb{C}$ then it satisfies a quadratic equation whose coefficients are in F_{n-1}.

By induction it is straightforward to check that α satisfies a polynomial equation of degree 2^j whose coefficients are in F_{n-j}, where $0 < j \leq n$.

The result $\alpha \in A$ therefore follows when $j = n$.

q.e.d.

Because of Proposition 3.9 the squaring of the circle problem will be settled in the negative if we show that $\sqrt{\pi}$ is transcendental. Indeed, this is the case as we mentioned in section 2.1.4.3 because of Lindemann's result that $\pi \in \mathbb{C} \setminus A$, a fact asserted long before by James Gregory (1638-1675), cf., [Baker, pp. 3-6]; in fact, if $\sqrt{\pi} \in A$ then $\pi \in A$ since A is a field. At the University of Munich there is a bust of Ferdinand Lindemann, and beneath the engraved name there is the letter π framed in a circle and a square.

Lindemann's proof is not easy and was strongly influenced by Hermite's proof that e is transcendental. Kronecker's remark on Lindemann's work actually runs deeper than it appears but

certainly not less caustic: "Of what use is your beautiful investigation regarding π? Why study such problems since irrational numbers do not exist?" The major result on the general problem of finding specific transcendental numbers is due to C.L. Siegel (1896-) Gelfond, (1906-) and Schneider in 1934, and Baker in 1966. A special case of Siegel's result is: if β is irrational then at least one of $2^\beta, 3^\beta$, or 5^β is transcendental. The Gelfond-Schneider theorem is: let β be an irrational algebraic number and assume that α is an algebraic number not equal to 0 or 1; then α^β is transcendental. Baker's theorem is a far reaching generalization of this result.

Example 3.1 a. e^π is transcendental since $e^\pi = (e^{\pi i})^{\frac{1}{i}} = (-1)^{-i}$.

b. It is not known if the following numbers are irrational: $\pi + e$, π^e, $\pi^{\sqrt{2}}$, $\sum_1^\infty \frac{1}{n^3}$, 2^e, Euler's constant $\gamma = \lim_{n\to\infty} (\sum_{k=1}^n \frac{1}{k} - \log n)$. On the other hand $e\pi$ is irrational. Cambridge folklore has it that G.H. Hardy (1877-1947) would have resigned his position in favor of anyone who proved the irrationality of γ.

Remark With regard to Theorem 2.5 b we now quote the Thue, Siegel, Roth (1925-) theorem (1955): let α be a real algebraic number and let $\delta > 0$; then the inequality

$$0 < |\alpha - \frac{p}{q}| < 1/q^{2+\delta}$$

has only a finite number of solutions $(p,q) \in \mathbb{Z} \times \mathbb{N}$.

3.3.4 The Delian problem

In light of Proposition 3.9 it is natural to ask if $A = C$. The question is answered in the negative since $\sqrt[3]{2} \in A$ ($\sqrt[3]{2}$ is a solution of $x^3 - 2 = 0$), while some elementary properties of cube roots and our characterization of C show that $\sqrt[3]{2} \notin C$, e.g., [Courant and Robbins, pp. 134-135]. This example deals a setback to prayer-oriented solutions of medical problems. In fact, in the face of a devastating plague, the Athenians asked for help at the oracle at Delos. They were advised to double the size of the cubical altar of Apollo. Plato suggested to the Delians that perhaps the oracle was not responding directly to the plague problem but was trying to shame them because of their contempt for geometry. We refer to [Heath, pp. 154-170; van der Waerden, 1954, pp. 159 ff.] for a survey of ancient Greek work on this Delian problem as well as for other possibilities as to its origin. When one decides to use a ruler and compass construction instead of an hammer and saw, the Delian problem is equivalent to finding out whether or not $\sqrt[3]{2}$ is constructible. This follows since the oracle asked a solution to the equation

$$x^3 = 2a^3,$$

where a is the length of a side of Apollo's altar and x is the desired side; consequently, $x = a\sqrt[3]{2}$.

3.3.5 The Cantor diagonal process and transcendental numbers

Georg Cantor's work concerning uniqueness questions in trigonometric series led him to questions about sets and numbers which have affected the mathematical world in a most profound

way, cf., sections 1.2.5 and 1.2.6.

The following remarks and Proposition 3.5 are due to Cantor. A set $S \subseteq \mathbb{C}$ is countably infinite if there is a bijection (i.e., a one-to-one onto function) $f: \mathbb{N} \longrightarrow S$; in this case we write card $S = \aleph_0$ ("card" designates "cardinality"). A finite or countably infinite set $S \subseteq \mathbb{C}$ is countable. If $S \subseteq \mathbb{C}$ is not countable then it is uncountable.

Example 3.2 a. We'll show that card $\mathbb{Q} = \aleph_0$. Without loss of generality consider the set of positive rationals, and identity this set with the points (m,n) having integer coefficients in the first quadrant of the plane. We can draw a path through all of these points as in Figure 15.

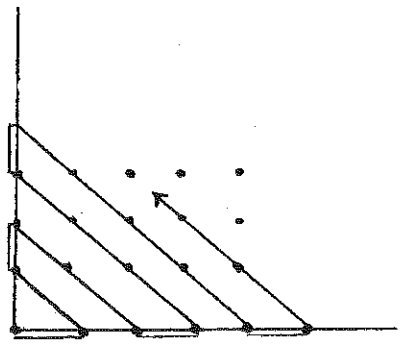


Figure 15

The bijection f is defined by the rule that $f(n)$ is the n^{th} point on the path.

b. We'll show that $\mathbb{R}$ and $\mathbb{C}$ are uncountable. Without loss of generality we'll prove that the set S of points in the

interval $(0,1)$ is uncountable. If card $S \leq \aleph_0$ then $S = \{f(n) : n \in \mathbb{N}\}$ where $f : \mathbb{N} \longrightarrow S$ is a bijection. We designate the decimal expansion of $f(n)$ by $.a_{1,n}a_{2,n}\cdots$; and we shall obtain a contradiction to our countability hypothesis by writing down a decimal $.b_1b_2\cdots$, $b_j \in \{0,1,\cdots,9\}$ which is not equal to any $f(n)$. In fact, we define b_j as

$$b_j = \begin{cases} 1 & \text{for } a_{j,j} \neq 1 \\ 2 & \text{for } a_{j,j} = 1. \end{cases}$$

Let $\mathcal{I}$ be the collection of all polynomials $P(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0$, deg $P \geq 1$, with the property that each a_j is an integer and $\{a_0,\cdots,a_n\}$ is a pairwise relatively prime set.

Proposition 3.10 Card $A = \aleph_0$, and the set of real transcendental numbers is uncountable.

Proof For $P \in \mathcal{I}$ we define $h(P) = n + \sum_0^n |a_j|$; thus, $h(P) \geq 2$.

For $N \geq 2$ we let $\mathcal{I}_N$ comprise those polynomials $P \in \mathcal{I}$ for which $h(P) = N$.

Clearly, each $\mathcal{I}_N$ is a finite set, and $\mathcal{I} = \cup\, \mathcal{I}_N$.

Corresponding to $P(x) = a_nx^n + \cdots + a_0 \in \mathcal{I}_N$ there is a "word" $a_0a_1\cdots a_n$; and we list the words (corresponding to a given N) in dictionary order.

Each $P \in \mathcal{I}$ has a finite number of zeros.

Take $N = 2$. List the finite number of zeros of the first element of $\mathcal{I}_2$, then those of the second, etc., passing over those which had been proviously listed, until the zeros

of the last element of I_2 have been recorded.
Then proceed to I_3, etc.
A is the collection of all such zeros, and so card $A = \aleph_0$.
The result is completed since $\mathbb{R}$ is uncountable.

q.e.d.

3.3.6 Liouville numbers

It is interesting to note that Proposition 3.10 coupled with a slightly fancier proof that $\mathbb{R}$ is uncountable (in fact, one which is the essential part of the proof of the Baire category theorem for $\mathbb{R}$) provide a direct means of computing transcendental numbers. It is not as efficient as Liouville's example that we shall now give, but nonetheless it is direct, thus refuting some of the strong criticism against Cantor at the time that he published Proposition 3.10.

We observed earlier that $\mathbb{Q} \subseteq A$. The degree $d(\alpha)$ of $\alpha \in A$ is the smallest positive integer n for which $P(\alpha) = 0$, where $\deg P = n$ and $P \in I$. Thus, $\mathbb{Q} \setminus \{0\}$ is precisely the subset X of A such that

$$\forall\, \alpha \in X, \quad d(\alpha) = 1.$$

The following should be compared with Theorem 2.5.

Proposition 3.11 Let $\alpha \in A$ be real with $d(\alpha) = n > 1$. Then there is a positive integer Q such that

$$\forall (p,q) \in \mathbb{Z} \times \mathbb{N}, \left|\alpha - \frac{p}{q}\right| > 1/(Qq^n).$$

Proof Take $P \in I$ for which $P(\alpha) = 0$ and $\deg P = n$.

Let Q be a positive integer with the property that $|P'(x)| \leq Q$ if $|\alpha - x| \leq 1$.

By the mean value theorem and the fact that $P(\alpha) = 0$ we have

$$|P(x)| \leq Q|\alpha - x| \tag{3.34}$$

for $|\alpha - x| \leq 1$.

If we take integers p and q, $q > 0$, for which $|\alpha - \frac{p}{q}| > 1$ then we are done since $1 \geq 1/(Qq^n)$.

Choose $p, q \in \mathbb{Z}$, $q > 0$, with the property that $|\alpha - \frac{p}{q}| \leq 1$.

We have $|P(p/q)| \leq Q|\alpha - \frac{p}{q}|$ from (3.34), and so

$$|q^n P(\tfrac{p}{q})| \leq Qq^n|\alpha - \tfrac{p}{q}|. \tag{3.35}$$

Note that P does not have rational roots. In fact, if $P(r) = 0$ for some $r \in \mathbb{Q}$, then $Q(x) = P(x)/(x-r)$ is a polynomial with rational coefficients of degree $n-1$; clearly, $Q(\alpha) = 0$ since α is irrational, and so we obtain a contradiction to the definition of $d(\alpha)$.

Since P does not have rational roots and because deg $P = n$, we see that $q^n P(\frac{p}{q}) \in \mathbb{Z} \setminus \{0\}$.

Thus the left hand side of (3.35) is at least 1.

This yields our result noting that the strict inequality follows from the fact that α is irrational.

q.e.d.

$\alpha \in \mathbb{R}$ is a Liouville number if it is irrational and has the property that

$$\forall\, n \geq 1, \quad \exists\, p_n, q_n \in \mathbb{Z} \text{ such that } |\alpha - \frac{p_n}{q_n}| < 1/q_n^n,$$

where $q_n > 1$. In light of Proposition 3.11 and our desire to find transcendental numbers it is interesting to exhibit a Liouville number.

Example 3.3 We'll prove that $\alpha = \sum_1^\infty (-1)^j/2^{j!}$ is a Liouville number.

i. The fact that α is irrational follows by the same argument that we used to prove that e is irrational. Suppose $\alpha = p/q$ where $p,q \in \mathbb{N}$, and let $n \in \mathbb{N}$ be odd. Clearly, then,

$$(3.36)\quad r_n = 2^{n!}q\left(\frac{p}{q} - \sum_1^n (-1)^j/2^{j!}\right) = 2^{n!}q \sum_{n+1}^\infty (-1)^j/2^{j!} \in \mathbb{N}.$$

Choose such an n so that $1 > q/2^{n+1}$. We compute

$$r_n < 2^{n!}q/2^{(n+1)!} = q/2^{n+1} < 1,$$

which contradicts (3.36).

ii. For each n let $p_n/q_n = \sum_1^n (-1)^j/2^{j!}$, so that $q_n = 2^{n!}$. Then

$$\left|\alpha - \frac{p_n}{q_n}\right| = 2^{-(n+1)!} - 2^{-(n+2)!} + \cdots < 2^{-(n+1)!}$$

$$= (2^{n!})^{-(n+1)} < (2^{n!})^{-n} = 1/q_n^n.$$

Proposition 3.12 Every Liouville number is transcendental.

Proof Let α be a Liouville number and assume that $\alpha \in A$ with $d(\alpha) = n$. Since α is irrational we have $n > 1$.
By Proposition 3.11 there is a positive integer Q such that

$$(3.37)\qquad \left|\alpha - \frac{p}{q}\right| > 1/(Qq^n)$$

for all $(p,q) \in \mathbb{Z} \times \mathbb{N}$.

Choose a positive integer k such that $2^k \geq Q2^n$.

Since α is a Liouville number there are integers p_k, q_k with $q_k > 1$ such that

$$|\alpha - \frac{p_k}{q_k}| < 1/q_k^k. \tag{3.38}$$

Combining (3.37) for $p = p_k, q = q_k$ and (3.38) we obtain $q_k^k < Qq_k^n$.

Thus, $Q > q_k^{k-n} \geq 2^{k-n} \geq Q$, a contradiction.

q.e.d.

Example 3.4 a. $\alpha = \sum_1^\infty 1/10^{j!}$ is a Liouville number.

b. Given a Liouville number α it is possible to generate an uncountable family of transcendental numbers. For example take α as in part a. Then each $\beta = \sum_1^\infty a_j/10^{j!}$ is transcendental, where a_j takes the value 1 or 2.

3.3.7 Trisecting an angle

We now prove that it is impossible to trisect some angles by means of a ruler and compass construction.

Recall from Proposition 3.4 and the fundamental theorem of algebra that we can write the polynomial $P(x) = x^3 + a_2x^2 + a_1x + a_0$ as $(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$, where $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{C}$ are the zeros of $P(x)$; and we easily compute that

$$-a_2 = \alpha_1 + \alpha_2 + \alpha_3. \tag{3.39}$$

Proposition 3.13 Given $P(x) = x^3 + a_2x^2 + a_1x + a_0 = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$ where $a_0, a_1, a_2 \in \mathbb{Q}$ and $\alpha_1, \alpha_2, \alpha_3 \notin \mathbb{Q}$. Then $\alpha_1, \alpha_2, \alpha_3 \notin C$.

Proof Suppose $P(\alpha) = 0$ and $\alpha \in C$.

Then α is in some F_k where F_k is an extension field of some F_{k-1}, F_{k-1} is an extension field of some F_{k-2}, etc.

Without loss of generality, let k be the smallest integer j for which a zero of $P(x)$ belongs to some F_j.

By hypothesis, $\alpha \notin F_0 = \mathbb{Q}$, and we have assumed that $\alpha \notin F_{k-1}$.

We have $\alpha = \beta_1 + \beta_2\sqrt{\beta}$ where $\beta, \beta_i \in F_{k-1}$ and $\sqrt{\beta} \notin F_{k-1}$.

It is a routine (or, perhaps, rootine) calculation with cubics to check that $\alpha' = \beta_1 - \beta_2\sqrt{\beta}$ is also a root of $P(x) = 0$.

If $\beta_2 = 0$ then $\alpha \in F_{k-1}$, a contradiction. Thus, $\alpha \neq \alpha'$.

Because of (3.39), the remaining zero γ of $P(x)$ is

$\gamma = -a_2 - \alpha - \alpha' = -a_2 - 2\beta_1 \in F_{k-1}$ since $a_2 \in \mathbb{Q}$ and $\beta_1 \in F_{k-1}$.

This contradicts our definition of k, and so $\alpha_1, \alpha_2, \alpha_3 \notin C$.

q.e.d.

We now show that it is impossible to trisect the angle having $\pi/3$ radians by means of a ruler and compass construction.

Proposition 3.14 $\cos(\pi/9) \notin C$.

Proof i. From the Lemma in section 3.1.5 we have

$$\cos\phi = 4\cos^3(\phi/3) - 3\cos(\phi/3). \tag{3.40}$$

Letting $\phi = \pi/3$ in (3.40), the problem reduces to proving that

$$8x^3 - 6x - 1 = 0$$

has no constructible solutions.

Setting $y = 2x$, the problem is equivalent to proving that

(3.41) $$y^3 - 3y - 1 = 0$$

has no constructible solutions; and in light of Proposition 3.13 it is sufficient to show that (3.41) has no rational solutions.

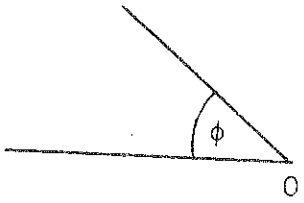
ii. Assume $y = p/q$, $(p,q) = 1$, is a solution of (3.41). Then $p(p^2 - 3q^2) = q^3$ so that $p|q^3$ and hence $p|q$; this contradicts the condition $(p,q) = 1$ unless $p = \pm 1$. Also, $p^3 = q^2(3p + q)$ so that $q|p$; and this is a contradiction unless $q = \pm 1$.

Consequently, the only possible rational solutions of (3.41) are $y = \pm 1$, and these obviously fail.

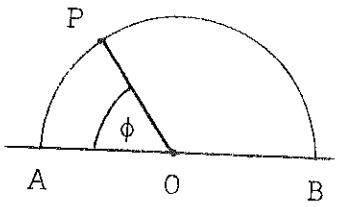
q.e.d.

The above result does not preclude the possibility that one can trisect every angle by a ruler and compass construction plus some seemingly trivial extra help. For example, Descartes was able to effect such a trisection with the additional aid of a fixed parabola.

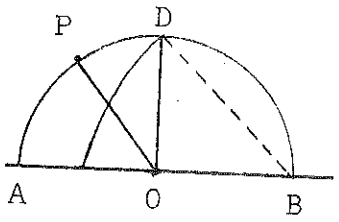
[Tietze, p. 55] records the ruler and compass "approximate trisections" of the German tailor, E. Kopf. One of Kopf's constructions never produces an error of more than $\pi/(43,200)$ radians. The following Kopf construction in Figure 16, although relatively simple, has a maximum error of $\pi/(1080)$ radians.



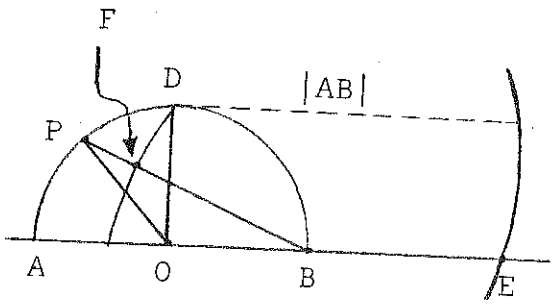
ϕ is the given angle.



AB is a diameter of a circle C_1 with center O.



OD is the perpendicular bisector of AB; and B is the center of the circle C_2 with radius of length $|BD|$.



D is the center of the circle C_3 with radius of length $|AB|$; E is a point on C_3 which intersects AB.

Figure 16

F is the point of intersection of the segment PB with the circle C_2; and the angle $\measuredangle OEF$ is the desired approximation of $\phi/3$.

3.3.8 Squaring in Solitude

E.J. Goodwin, M.D. (not "mathematical doctor"), of Solitude, Posey County, Indiana, wrote House Bill No. 246 for enactment

by the Indiana State Legislature in 1897. In the first section he seems to set $\pi = 16/\sqrt{3}$ [Beckmann, p. 170], and the final section of the proposed bill states:

> In further proof of the value of the author's proposed contribution to education, and offered as a gift to the State of Indiana, is the fact of his solutions of the trisection of an angle, duplication of the cube (Delian problem), and quadrature of the circle (squaring of the circle) having been already accepted as contributions to science by the American Mathematical Monthly, the leading exponent of mathematical thought in this country. And be it remembered that these noted problems had been long since given up by scientific bodies as unsolvable mysteries and above man's ability to comprehend.

The state house of representatives passed the bill by a vote of 67-0. Despite the backing of the State Superintendent of Public Instruction, the state senate postponed action on the bill because of some of the adverse publicity the bill was receiving as well as some eleventh hour mathematical coaching to the senate by Purdue mathematics professor, C.A. Waldo.

Exercises for Chapter 3

1. Reconcile the calculation:

$$i = \sqrt{-1} = \sqrt{\frac{1}{-1}} = \frac{\sqrt{1}}{\sqrt{-1}} = \frac{1}{i} \text{ so that } 1 = -1.$$

2. Let $\{\varepsilon_n > 0 : n = 1, \cdots\}$ be a sequence which tends to 0. Is it true that for each n there is a ruler and compass trisection procedure for every angle that produces a maximum error of ε_n radians (independent of the angle)?

3. Show that any (finite) segment can be trisected by a ruler and compass construction.

4. a. A <u>group</u> G is a pair $(G, \circ)$ with a uniquely defined product $f \circ g \in G$ for each $f, g \in G$ for which

   i. $\exists\, j \in G$ such that $\forall\, f \in G$, $f \circ j = j \circ f = f$;

   ii. $\forall\, f \in G$, $\exists\, g_f \in G$ such that $f \circ g_f = g_f \circ f = j$;

   iii. $\forall\, f, g, h \in G$, $(f \circ g) \circ h = f \circ (g \circ h)$.

   A bijective function $f : X \longrightarrow f(X)$, for some $X \subseteq \mathbb{R}^2$, is <u>homeomorphism</u> if f and f^{-1} are continuous. When $X = S^1 \subseteq \mathbb{R}^2$ is the unit-circle we say that $f(S^1) = C$ is a <u>Jordan curve</u> if $f : S^1 \longrightarrow f(S^1) = C$ is an homeomorphism. The <u>Jordan curve theorem</u> asserts that if $C \subseteq \mathbb{R}^2$ is a Jordan curve then there are two disjoint connected open sets D_e and D_i such that C is the boundary of both D_e and D_i, $\mathbb{R}^2 = C \cup D_e \cup D_i$, $C \cup D_i$ is bounded, and D_e is unbounded.

Verify that the Jordan curve theorem allows us to well-define the direction of a Jordan curve in either the clockwise or counterclockwise sense. An homeomorphism $f : \mathbb{R}^2 \longrightarrow f(\mathbb{R}^2) = \mathbb{R}^2$ is orientation preserving if f preserves the direction of every Jordan curve in $\mathbb{R}^2$. Let G be the set of such orientation preserving homeomorphisms and prove that G is a group where the product "$\circ$" is defined as ordinary composition of functions.

b. Let G be the group of orientation preserving homeomorphisms of $\mathbb{R}^2$ onto itself and let $H \subseteq G$ be a subgroup (i.e., H is a subset of G and $f \circ g \in H$ when $f,g \in H$). A pair $(x,y) \in \mathbb{R}^2 \times \mathbb{R}^2$ is congruent under H to a pair $(x',y') \in \mathbb{R}^2 \times \mathbb{R}^2$ if there is $f \in H$ for which $f(x) = x'$ and $f(y) = y'$. If $B(z) \subseteq \mathbb{R}^2$ designates a disc with center z, we say that a pair $(x,y) \in \mathbb{R}^2 \times \mathbb{R}^2$ is semicongruent under H to a pair $(x',y') \in \mathbb{R}^2 \times \mathbb{R}^2$ if for any discs $B(x)$, $B(y)$, $B(x')$, $B(y')$ there are congruent pairs (under H) $(a,b) \in B(x) \times B(y)$ and $(a',b') \in B(x') \times B(y')$. A metric space X is a pair (X,d), where X is a nonempty set and $d : X \times X \longrightarrow \mathbb{R}$ satisfies:

$$\begin{aligned}
&\forall\, x,y \in X, && d(x,y) \geq 0,\\
&\forall\, x,y \in X, && d(x,y) = 0 \text{ if and only if } x = y,\\
&\forall\, x,y \in X, && d(x,y) = d(y,x),\\
&\forall\, x,y,z \in X, && d(x,z) \leq d(x,y) + d(y,z);
\end{aligned}$$

d is a metric. Verify that ordinary Euclidean length

and hyperbolic length are examples of metrics on $\mathbb{R}^2$; in Exercise 1.6 we defined hyperbolic length for Poincaré's Euclidean model (in the upper half-plane) of hyperbolic geometry. If $(\mathbb{R}^2,d)$ is a metric space then $f \in G$ is an isometry if

$$\forall\, x,y \in \mathbb{R}^2, \qquad d(x,y) = d(f(x),f(y))$$

Using the Jordan curve theorem, Hilbert and Lie (1842-1899) proved the following result, e.g., [Hilbert, 1902, Appendix; 1968, Anhang 4; Fáry]. Let H be a subgroup of G with the following properties:

i. if $(x,y) \in \mathbb{R}^2 \times \mathbb{R}^2$ is semicongruent under H to $(x',y') \in \mathbb{R}^2 \times \mathbb{R}^2$ then (x,y) is congruent under H to (x',y');

ii. there is $x \in \mathbb{R}^2$ such that $H_x = \{f \in H : f(x) = x\}$ is neither H nor the identity map (i.e., H_x is a proper subgroup of H), and

$$H_x(y) = \{z \in \mathbb{R}^2 : \exists f \in H_x \text{ such that } f(y) = z\}$$

is infinite for all $x \neq y$, $x,y \in \mathbb{R}^2$.

Then H is the group of all orientation preserving isometries on $(\mathbb{R}^2,d)$, where d is either Euclidean or hyperbolic length.

Remark The Hilbert-Lie theorem allows for an axiomatic development of geometry in terms of groups; and, in particular, the parallel axiom of Euclidean geometry is characterized by the existence of

normal subgroups of H. The result is in the spirit of the fundamental geometrical research of Riemann and Helmholtz (1821-1894); and can be viewed as a contribution to Hilbert's fifth problem [Hilbert 1901; Montgomery and Zippin, pp. 67-71].

3.5 The Fundamental Theorem of Algebra asserts the existence of zeros for any polynomial $P(x)$ with complex coefficients, and Abel showed that if $\deg P \geq 5$ then the algebraic equation $P(x) = 0$ can't necessarily be solved by radicals. Next, Galois characterized those algebraic equations which can be solved by radicals in terms of certain groups, a term which Galois introduced. In 1858 Hermite used the analytic theory of elliptic functions to obtain solutions of any quintic by means of "modular equations". Abel and Jacobi had developed this theory for a different purpose. Solutions were also given during this period by Brioschi (1824-1897) and Kronecker. [Klein, 1884] reviewed and unified this work on the quintic in terms of the icosahedral group A_5 (introduced in Exercise 2.6). For this exercise, compare Hermite's and Klein's solutions of the quintic. This is a reasonable group (sic) project, and, besides [Klein, 1884] and the references therein, we recommend [Bell, pp. 231-239; Cole; Dickson; Lehner, pp. 6-11]. Hilbert made major analogous progress for polynomial equations $P(x) = 0$, $\deg P > 5$, e.g., [Bell, pp. 236-239; Cole; Segre].

3.6 On March 30, 1796, Gauss made his first first-rate discovery: it is possible to make a ruler and compass construction of

a regular polygon with 17 sides, e.g. [Tietze, Chapter 9]. This result led to his characterization of polygonal constructions: a regular polygon of n sides can be made by a ruler and compass construction if and only if $n = 2^m$ or

$$n = 2^m q_1 \cdots q_j$$

where each $q_i \in P$, $m \geq 0$, and $q_1, q_2, \cdots, q_j$ are different Fermat numbers (defined in Exercise 1.5).

a. Verify that

$$\cos \frac{2\pi}{17} = -\frac{1}{16} + \frac{1}{16}\sqrt{17} + \frac{1}{16}\sqrt{34-2\sqrt{17}} + \frac{1}{8}\sqrt{17 + 3\sqrt{17} - \sqrt{34-2\sqrt{17}} - 2\sqrt{34+2\sqrt{17}}}.$$

b. Use Gauss' results to verify that the trisection of an angle is not necessarily possible by means of a ruler and compass construction.

3.7 Prove that if $a,b \in \mathbb{R}$ are positive then

$$\frac{a+b}{2} \geq \sqrt{ab};$$

and there is equality if and only if $a = b$.

Gauss proved an important relation between the arithmetic/geometric means of this simple but important inequality and the elliptic integrals that are fundamental in astronomy as well as in the study of the quintic. Let $a > b > 0$ and define

$$a_n = \frac{a_{n-1} + b_{n-1}}{2}, \qquad b_n = \sqrt{a_{n-1}b_{n-1}}$$

where $n = 1,2,\cdots$, $a_0 = a$, and $b_0 = b$. Gauss proved that there is a number $M(a,b)$ for which

$$\lim a_n = \lim b_n = M(a,b).$$

He related M with "complete elliptic integrals" by showing that

$$\frac{1}{M(1-x,1+x)} = \frac{1}{\pi}\int_0^{\pi} \frac{dy}{\sqrt{1-x^2\cos^2 y}}.$$

3.8 Fill in the details of the following heuristic proof due to Euler. Note that Proposition 3.4 is used in an intuitive way. The problem is to prove that

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6},$$

cf., Example 3.1b. We begin with the Taylor series,

$$\sin x = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \cdots,$$

so that when $\sin x = 0$ and $x \neq 0$ we have

$$0 = 1 - \frac{y}{3!} + \frac{y^2}{5!} - \frac{y^3}{7!} + \cdots$$

for $y = x^2$. We obtain the result by supposing that this last series has the properties of polynomials listed in Proposition 3.4.

Bibliography for Chapter 3

L. Ahlfors, Complex analysis, 2nd edition, McGraw-Hill, N.Y., 1966.

A.D. Aleksandrov et alii (editors), Mathematics, its content, methods, and meaning, 2nd edition (1956), M.I.T. Press, 1969.

Archimedes, Collected works, translation and commentary by T.L. Heath, Cambridge University Press, 1897.

A. Baker, Transcendental number theory, Cambridge University Press, 1975.

P. Beckmann, A history of pi, The Golem Press, Boulder, 1971.

E.T. Bell, The development of mathematics, 2nd edition.

E. Bishop, Foundations of constructive analysis, McGraw-Hill, N.Y., 1967.

M. Bôcher, "Gauss' third proof of the fundamental theorem of algebra," BAMS 1 (1895) 205-209.

S. Bochner, The role of mathematics in the rise of science, Princeton University Press, 1966.

H. Bosmans, "La théorie des équations dans 'L'invention nouvelle en l'algèbre d'Albert Girard," Mathésis, 41 (1926) 59-67, 100-109, 145-155.

C. Boyer, A history of mathematics, J. Wiley and Sons, N.Y., 1968.

R.C. Buck, Advanced calculus, 2nd edition, McGraw-Hill, N.Y., 1965.

H. Burkhardt, "Die Anfänge der Gruppentheorie und Paclo Ruffini," Zeit. für Math. und Phys. 37 (1892) 121-159 (supplement), Ann. di Mat., 22 (1894) 175-212.

F. Cajori, A history of mathematics, Macmillan, N.Y., 1894,

F. Cajori, An introduction to the theory of equations, (1904) Dover, N.Y., 1969.

F.N. Cole, "Klein's Ikosaeder", Amer. J. Math., 9 (1887) 45-61.

J.L. Coolidge, The mathematics of great amateurs, (1949) Dover, N.Y., 1963.

R. Courant and H. Robbins, What is mathematics? Oxford University Press, 1941.

L.E. Dickson, Modern algebraic theories, (1926), Dover, N.Y.

J. Dieudonné, "The historical development of algebraic geometry", Amer. Math. Monthly, 79 (1972) 827-866.

G.W. Dunnington, Carl Friedrich Gauss (1955) Hafner, N.Y., 1960.

L. Euler, Collected works.

H. Eves, An introduction to the history of mathematics, 3rd edition, Holt, Rinehart, and Winston, N.Y. 1969.

I. Fáry, "On Hilbert's theory of closed group actions", Proc. Conference on Transformation Groups, Springer-Verlag, N.Y. (1968) 419-428.

L. Gaal, Classical Galois theory, 2nd edition, Chelsea, N.Y., 1973.

É. Galois, Écrits et mémoires mathématiques d'Évaristes Galois, preface by J. Dieudonné, Gauthier-Villars er C^{ie}, Paris, 1962.

R. Gillings, "The so-called Euler-Diderot incident", Amer. Math. Monthly, 61 (1954) 77-80.

C. Gillispie (editor), Dictionary of scientific biography, C. Scribner's Sons, N.Y.

T. Hall, Carl Friedrich Gauss, MIT Press, 1970.

R. Harley, "A contribution to the history of the problem of the reduction of the general equation of the fifth degree to a trinomial form", Quarterly J. Math. 6 (1864) 38-47.

T.L. Heath, A manual of Greek mathematics (1931) Dover, N.Y., 1963.

D. Hilbert, Foundations of geometry, 1902 translation, The Open Court Publishing Company, LaSalle, Illinois, 1950.

D. Hilbert, Grundlagen der Geometrie, Teubner, Stuttgart, 1968.

D. Hilbert, "Mathematische Probleme", BAMS 8 (1901-1902) 437-479, English translation.

E. Hille, Analytic function theory, Chelsea, N.Y., 1959.

E.W. Hobson, Squaring the circle (1913) Chelsea, N.Y., 1969.

L. Infeld, Whom the Gods love, McGraw-Hill, N.Y., 1948.

B. Kiernan, "The development of Galois theory from Lagrange to Artin", Arch.Hist. Exact Sci. 8 (1971) 40-154.

F. Klein, Famous problems of elementary geometry (1885) Dover, N.Y., 1956.

F. Klein, The icosahedron and the solution of equations of the fifth degree (1884) Dover, N.Y., 1956.

J. Lehner, Discontinuous groups and automorphic functions, AMS Math. Surveys, 1964.

K. May, Bibliography and research manual of the history of mathematics, U. of Toronto Press, 1973.

H. Meschkowski, Ways of thought of great mathematicians, Holden-Day, San Franscisco, 1964.

D. Montgomery and L. Zippin, Topological transformation groups, John Wiley and Sons, N.Y., 1955.

O. Neugebauer, The exact sciences in antiquity, 2nd edition, Dover, N.Y., 1969.

O. Ore, Cardano the gambling scholar (1953) Dover, N.Y., 1965.

O. Ore, Niels Henrik Abel, U. of Minnesota Press, 1957.

S.S. Petrova, "Sur l'histoire des démonstrations analytiques du théorème fondamental de l'algèbre", Hist. Math. 1 (1974) 255-261.

J. Pierpont, "Lagrange's place in the theory of substitutions", BAMS 1 (1895) 196-204.

J. Pierpont, "On the Ruffini-Abel theorem", BAMS 2 (1896) 200-221.

H. Pollard, The theory of algebraic numbers, MAA Carus monographs, 1950.

B. Russell, A history of western philosophy, Simon and Schuster, N.Y., 1945.

G. Sarton, "Évaristes Galois", Osiris 3, part 1 (1937) 241-259.

J.F. Scott, A history of mathematics, Taylor and Francis, London, 1958.

B. Segre, "The algebraic equations of degrees 5,9,157,..., and the arithmetic upon an algebraic variety", Annals of Math. 45 (1945) 287-291.

D.E. Smith, History of mathematics, volume 2, Ginn and Co., Boston, 1925.

D.E. Smith, A source book in mathematics, volume 1 (1929), Dover, N.Y., 1959.

S. Stein, "The fundamental theorem of algebra", Amer. Math. Monthly 61 (1954) 109.

D. Struik, A concise history of mathematics, (1948) Dover, N.Y.

D. Struik, A source book in mathematics 1200-1800, Harvard University Press, 1969.

H. Tietze, Famous problems of mathematics, Graylock Press, Baltimore, 1965.

C. Truesdell, Essays in the history of mechanics, Springer-Verlag, N.Y., 1968.

J.V. Uspensky, Theory of equations, McGraw-Hill, N.Y., 1948.

B. van der Waerden, Modern algebra, volume 1 (1931), Ungar, N.Y. 1949.

B. van der Waerden, Science awakening, Noordhoff Ltd., Groningen, Holland, 1954.

S. von Waltershausen, Gauss, a memorial (1856) Colorado Springs, 1966.

H. Zassenhaus, "On the fundamental theorem of algebra", Amer. Math. Monthly 74 (1967) 485-497.

List of characters in alphabetical order (Chapter 3)

N. Abel (1802-1829)

M. Al-Khwārizmi (775-845)

Anaxagoras of Clazomenae (500-428)

Antiphon (5th century B.C.)

Apollonius (260-190)

Archimedes (287-212)

J.R. Argand (1768-1822)

Aristotle (384-322)

E. Artin (1898-1962)

A. Baker (contemporary)

Johann Bernoulli (1667-1748)

N. Bernoulli (1687-1759)

E. Bring (1736-1798)

Brioschi (1824-1897)

G. Cantor (1845-1918)

G. Cardano (1501-1576)

A. Cauchy (1789-1857)

J. D'Alembert (1717-1783)

S. del Ferro (1465-1526)

A. de Moivre (1667-1754)

R. Descartes (1596-1650)

D. Diderot (1713-1784)

Diophantus (a-b) ≤ (150-350)

L. Euler (1707-1783)

L. Ferrari (1522-1565)

A. Fiore (1505-)

É. Galois (1811-1832)

C. Gauss (1777-1855)

A. Gelfond (1906-)

A. Girard (1590-1633)

J. Gregory (1638-1675)

G.H. Hardy (1877-1947)

T. Harriot (1560-1621)

H. Helmholtz (1821-1894)

C. Hermite (1822-1905)

D. Hilbert (1862-1943)

Hippocrates of Chios (460-357)

C.G. Jacobi (1804-1851)

G. Jerrard (-1863)

O. Khayyám (1045-1123)

F. Klein (1849-1925)

E. Kopf

H. Kneser (20th century)

L. Kronecker (1823-1891)

J.L. Lagrange (1736-1813)

A. Legendre (1752-1833)

G. Leibnitz (1646-1716)

S. Lie (1842-1899)

F. Lindemann (1852-1939)

J. Liouville (1809-1882)

R. Lipschitz (1832-1903)

I. Newton (1642-1727)

L. Pacioli (1445-1510)

O. Perron (1880-)

Plato (428-348)

Plutarch (46-120)

Pythagoras (570-500)

B. Riemann (1826-1866)

K.F. Roth (1925-)

E. Rouché (1832-1910)

P. Ruffini (1765-1822)

T. Schneider (20th century)

C.L. Siegel (1896-)

Socrates (470-399)

C. Sturm (1803-1855)

N. Tartaglia (1499-1557)

A. Thue (1863-1922)

Torquemada (Grand Inquisitor, 15th century)

C. Truesdell (1919-)

Valmes (15th century)

F. Viète (1540-1603)

E.W. von Tschirnhausen (1651-1708)

C.A. Waldo

C. Wessel (1747-1818)

H. Weyl (1885-1955)