Notes on the Great Theorems

Leon M. Hall
Department of Mathematics and Statistics
University of Missouri - Rolla
1987

...ignorance of the roots of the subject has its price - no one denies that modern formulations are clear elegant and precise; it's just that it's impossible to comprehend how anyone ever thought of them.

-M. Spivak

Table of Contents

Acknowledgement

Sources for the material are given in the bibliography, but I want to especially express my thanks to Professor William Dunham, of Hanover College, whose article in the *American Mathematical Monthly* crystallized my concept of this course, and who graciously provided a copy of the *Mathematics Supplement* that he developed for his own great theorems course. Several sections are modifications, to varying degrees, of sections from his *Mathematics Supplement*.

Introduction

The quote from M. Spivak could well illustrate one of the reasons that, despite the increasing prominence of mathematics in today's world, most people just plain don't like it. Mathematicians must accept a large part of the responsibility for this state of affairs, and make efforts to increase general awareness of and appreciation for mathematics. This course is one attempt to shed light on some of the important "roots of the subject", and will thus be somewhat different from the usual mathematics course in that, while the details of the mathematics itself will certainly not be neglected, there will be two other important components of the course. First is an historical/biographical emphasis. Mathematics has been, and continues to be, a major cultural force in civilization, and mathematicians necessarily work within the context of their time and place in history. Since only a few episodes and personalities can be highlighted in a course like this, it should be kept in mind that major results in mathematics come about not as isolated flashes of brilliance, but after years (or even centuries) of intellectual struggle and development. Second is an attempt to provide some insight into the nature of mathematics and those who create it. Mathematics is a living, dynamic and vast discipline. The American Mathematical Society's 1979 subject classification contains 61 basic classifications having approximately 3400 subcategories, and it has been estimated that the number of new theorems published yearly in mathematics journals is in excess of 100,000. It is hoped that this course will give the student some perspective on mathematics as a whole, and also provide some insight on how mathematics has developed over the years. The principal objective of the course, however, is that the student gain an understanding of the mathematics itself. In these notes, statements and proofs of theorems are often given in a form as close as possible to the original work. In practically all fields of scholarship, a valuable piece of advice is to *read the classics*, but this is not heard as much in mathematics as in some other areas. For one thing, the mathematics of previous generations is often difficult to read and not up to modern standards of rigor. Nevertheless, by reading primary sources, much valuable insight into a subject can be gained, and this is true for mathematics as well as other fields. The effort required is justified by the benefits.

Deciding which theorems to include has been a major part of the preparation of this course, and the final list is bound to reflect personal taste. Among the guidelines used to make the choices were accessibility to students with a calculus background, variety in the branches of mathematics represented, inclusion of the "superstars" in mathematics, and the intellectual quality of the results. After some thought, it was decided that being able to cover the complete proof of a theorem was important but not necessary. Thus, a few topics, such as Gödel's theorem, are included with considerable discussion, but whose proofs require more mathematics than can reasonably be expected from the students at this stage in their mathematical development.

Finally, a few words to the students about what is expected of them with respect to the proofs of the theorems. Memorization of the proofs should not be a primary goal, although you may find that a certain amount of memorization occurs as a by-product as you work toward the main goal, which is <u>understanding</u>. An effective way to study mathematics is to read the material three times (at least); the first time read only the definitions and the statements of the theorems to get an idea of the mathematical setting; next re-read the material, this time scanning the proofs, but not checking all the details, in order to see what general techniques are used; finally, with pencil and paper ready at hand, read everything carefully, making sure you fully understand the logical path chosen by the mathematician to construct the proof. In many of the proofs in these notes details or steps have been omitted in some places. Whenever this occurs, <u>the student is expected to supply the missing parts</u>. Often, but not always, a statement such as "details are left to the student" helps identify gaps in the arguments. Understanding the great theorems of mathematics will certainly require effort, concentration, and discipline on the part of the student; after all, these theorems do represent pinnacles of mathematical thought. Those who persevere and gain an understanding of these theorems will, however, also gain a sense of personal satisfaction that comes from being able to comprehend some of the masterpieces of mathematics.

The Pythagorean Theorem

In right angled triangles, the square on the side subtending the right angle is equal to the squares on the sides containing the right angle.

Prop. I.47, Euclid's Elements

The Pythagorean Theorem may well be the most famous theorem in mathematics, and is generally considered to be the first great theorem in mathematics. Pythagoras lived from about 572 B.C. until about 500 B.C., but "his" theorem appears to have been known to the Babylonians at least a thousand years earlier, and to the Hindus and Chinese of Pythagoras' time. However, no proofs are given in these early references, and it is generally accepted that Pythagoras or some member of his school was the first to give a proof of the theorem. The nature of Pythagoras' proof is not known, and there has been much conjecture as to the method he used. Most authorities feel that a dissection proof such as the following was most likely.

Denote the legs and hypotenuse of the given right triangle by a, b, and c, and form two squares, each having side a+b, as in Figure 1. Dissect these squares as shown, noticing that each dissection includes four triangles congruent to the original triangle. The theorem follows by subtracting these four triangles from each square. An important part of this proof is the assertion that the central figure in the second dissection is indeed a square. Can you prove this? What geometry is required?

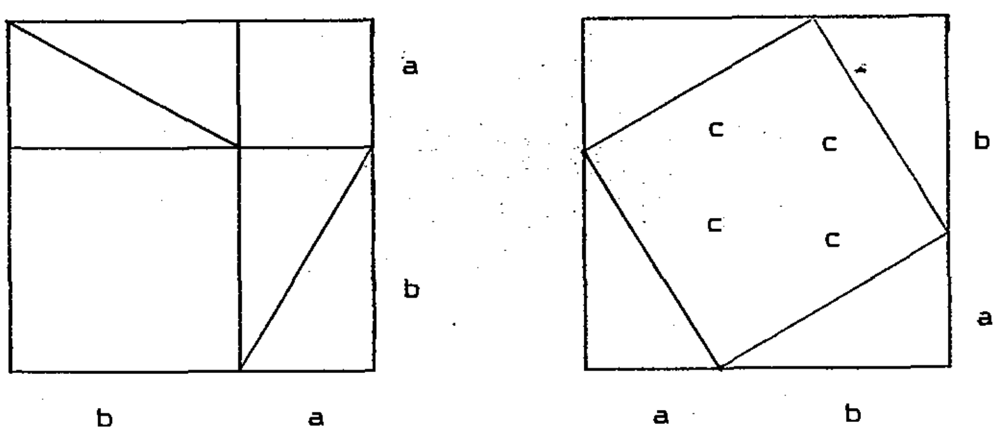


Figure 1

In addition to its claims as the first and most famous of the great theorems of Mathematics, the Pythagorean Theorem is also probably the theorem with the most proofs. E. S. Loomis has collected 370 proofs of this theorem in his book, *The Pythagorean Proposition*. Two more proofs will be given here, the first by James A. Garfield, done when he was a member of the House of Representatives in 1876 (five years before he became the 20th President of the United States), and the second by Euclid in his *Elements*, written about 300 B.C.

James A. Garfield's Proof: Denote the legs and the hypotenuse of the right triangle by a, b, and c, and form the trapezoid shown in Fig. 2. Compute the area of the trapezoid in two ways, directly using the usual formula, and as the sum of the areas of the three right triangles into which the trapezoid can be dissected. Equating these and simplifying gives:

$$(a + b)(a + b)/2 = ab/2 + ab/2 + c^2/2$$
$$a^2 + 2ab + b^2 = 2ab + c^2$$
$$a^2 + b^2 = c^2.$$

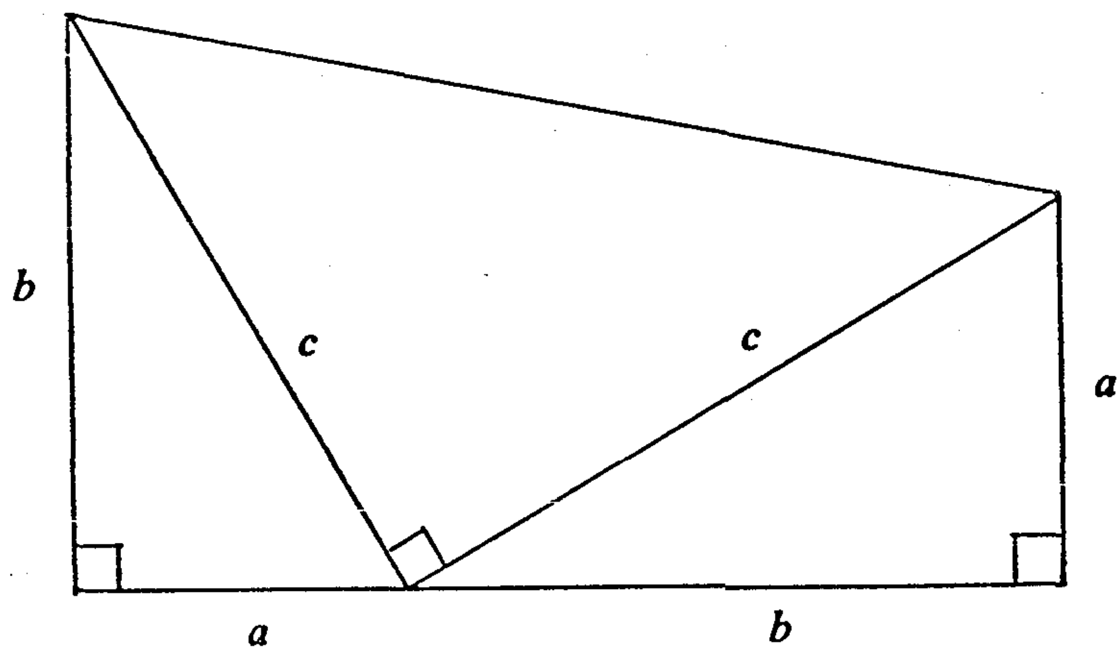


Figure 2

Euclid's Proof: The Pythagorean Theorem is proposition 47 in Book I of Euclid's *Elements* and the proof refers to some of the earlier propositions. These should be looked up by the interested reader. Details should also be filled in.

Suppose ΔABC is a right triangle with $\angle BAC = 90^{\circ}$. Construct the squares BDEC on BC, AGFB on AB, and AHKC on AC (by I.46). Through point A draw AL parallel to BD, and also draw lines FC and AD (by I.31 and Post. 1). See Figure 3.

Now, $\angle BAC = 90^{\circ}$ and $\angle BAG = 90^{\circ}$, so GAC is a straight line (by I.14).

$\angle DBC$ and $\angle FBA$ are right angles, and thus are equal. Adding $\angle ABC$ to both yields $\angle DBA = \angle FBC$. Furthermore, AB = FB and BD = BC, and so triangles ABD and FBC are congruent (by I.4).

Now, triangle ABD and rectangle BDLM share the same base and lie within the same parallels, and so the area of the rectangle is twice the area of the triangle. The same reasoning applies to triangle FBC and rectangle (square) ABFG since it was shown above that GAC is a straight line. (I.41 is used here.)

However, the congruence of triangles proved above leads us to the fact that the areas of BDLM and ABFG are equal.

The above reasoning should now be repeated to arrive at the fact that the areas of MLEC and ACKH are equal. (The student should draw appropriate auxiliary lines and fill in the details.)

For notational convenience, the area of a figure will be indicated by the vertex-notation of the figure, i.e., area(ABC) = ABC. Thus, BDLM = ABFG and MLEC = ACKH. Adding these yields

BDLM + MLEC = ABFG + ACKH

which becomes

$$BCED = ABFG + ACKH$$

and the theorem is proved.

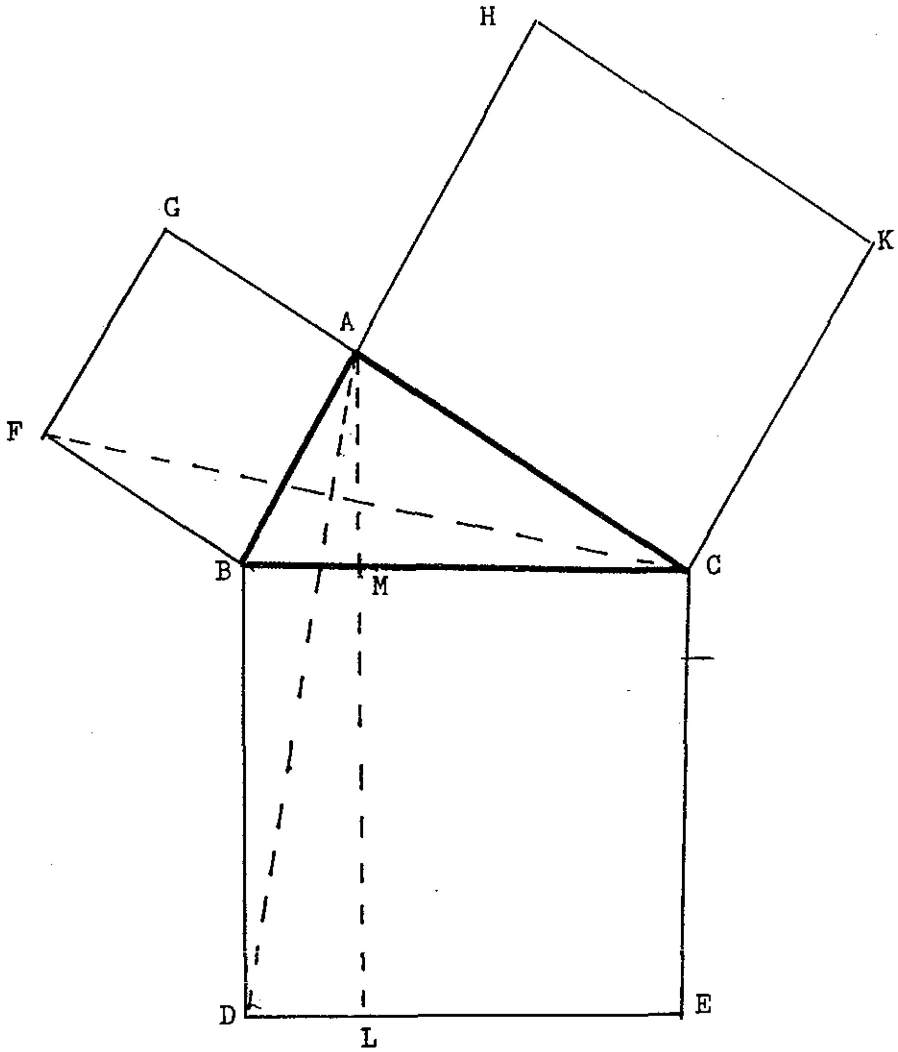


Figure 3

In some modern textbooks, many of the exercises following the proof of the Pythagorean Theorem require not the theorem itself, but the still unproved converse. To Euclid's credit, in the *Elements* the proposition immediately following the Pythagorean Theorem is its converse. Prove the following.

> If in a triangle, the square on one of the sides be equal to the squares on the remaining two sides of the triangle, the angle contained by the remaining two sides of the triangle is right.

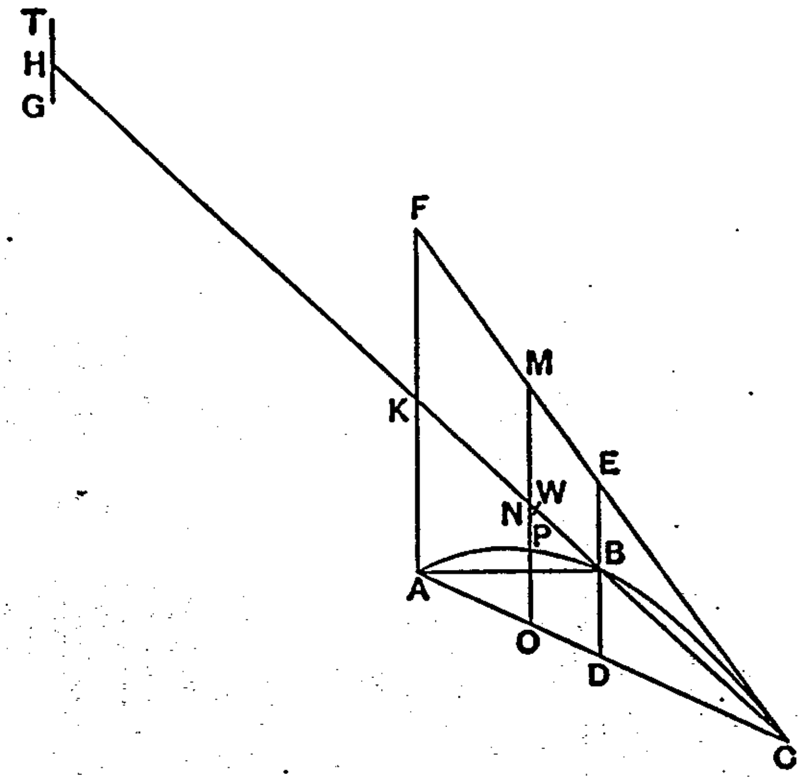
Hint: If in triangle ABC, ∠BAC is to be proved to be a right angle, construct a ⊥ to AC at A, extending to D, such that AD = AB. Then prove triangles ABC and ADC congruent.

> Let ABC be a segment of a parabola bounded by the straight line AC and the parabola ABC, and let D be the middle point of AC. Draw the straight line DBE parallel to the axis of the parabola and join AB, BC. Then shall the segment ABC be $\frac{4}{3}$ of the triangle ABC.
>
> Proposition 1 from the *Method* of Archimedes.

The greatest mathematician of antiquity was Archimedes of Syracuse, who lived in the third century B.C. His work on areas of certain curvilinear plane figures and on the areas and volumes of certain curved surfaces used methods that came close to modern integration. One of the characteristics of the ancient Greek mathematicians is that they published their theorems as finished masterpieces, with no hint of the method by which they were evolved. While this makes for beautiful mathematics, it precludes much insight into their methods of discovery. An exception to this state of affairs is Archimedes' *Method*, a work addressed to his friend Eratosthenes, which was known only by references to it until its rediscovery in 1906 in Constantinople by the German mathematical historian J. L. Heiberg. In the *Method*, Archimedes describes how he investigated certain theorems and became convinced of their truth, but he was careful to point out that these investigations did not constitute rigorous proofs of the theorems. In his own (translated) words: "Now the fact here stated is not actually demonstrated by the argument used; but that argument has given a sort of indication that the conclusion is true. Seeing then that the theorem is not demonstrated, but at the same time suspecting that the conclusion is true, we shall have recourse to the geometrical demonstration which I myself discovered and have already published." This section will give both Archimedes' investigation, from the *Method*, and the rigorous proof, from his *Quadrature of the Parabola,* of the proposition above. The arguments given below are from T. L. Heath's *The Works of Archimedes*, which is a translation "edited in modern notation".

Proposition 1 from the *Method* is stated at the beginning of this section, and the following investigation refers to Figure 1.

From A draw AKF parallel to DE, and let the tangent to the parabola at C meet DBE in E and AKF in F. Produce CB to meet AF in K, and again produce CK to H, making KH equal to CK.



ED = ½ FA by similar △
so 4BD = FA

Figure 1

Consider CH as the bar of balance, K being its middle point.

Let MO be any straight line parallel to ED, and let it meet CF, CK, AC in M, N, O and the curve in P.

Now, since CE is a tangent to the parabola and CD the semi-ordinate,

$$EB = BD\ ;$$

"for this is proved in the Elements (of Conics)." (by Aristaeus & Euclid)

Since FA, MO, are parallel to ED, it follows that

$$FK = KA, \quad MN = NO.$$

Now, by the property of the parabola, "proved in a lemma,"

$MO : OP = CA : AO$ (Cf. *Quadrature of the Parabola*, Prop. 5)

$= CK : KN$ (Euclid, VI. 2)

$= HK : KN.$

Take a straight line TG equal to OP, and place it with its centre of gravity at H, so that TH = HG; then, since N is the centre of gravity of the straight line MO, and MO : TG = HK : KN, it follows that TG at H and MO at N will be in equilibrium about K. (*On the Equilibrium of Planes*, I. 6, 7)

Similarly, all other straight lines parallel to DE and meeting the arc of the parabola, (1) the portion intercepted between FC, AC with its middle point on KC and (2) a length equal to the intercept between the curve and AC placed with its centre of gravity at H will be in equilibrium about K.

Therefore K is the centre of gravity of the whole system consisting (1) of all the straight lines as MO intercepted between FC, AC and placed as they actually are in the figure and (2) of all the straight lines placed at H equal to the straight lines as PO intercepted between the curve and AC.

And, since the triangle CFA is made up of all the parallel lines like MO, and the segment CBA is made up of all straight lines like PO within the curve, it follows that the triangle, placed where it is in the figure, is in equilibrium about K with the segment CBA placed with its centre of gravity at H.

Divide KC at W so that CK = 3KW; then W is the centre of gravity of the triangle ACF; "for this is proved in the books on equilibrium" (Cf. *On the Equilibrium of Planes*, I. 5). Therefore

$$\Delta ACF : (\text{segment } ABC) = HK : KW = 3 : 1.$$

Therefore $\text{segment } ABC = \frac{1}{3}\,\Delta ACF.$

But $\Delta ACF = 4\,\Delta ABC.$ Equal bases, heights ratio 1:4

Therefore $\text{segment } ABC = \frac{4}{3}\,\Delta ABC.$

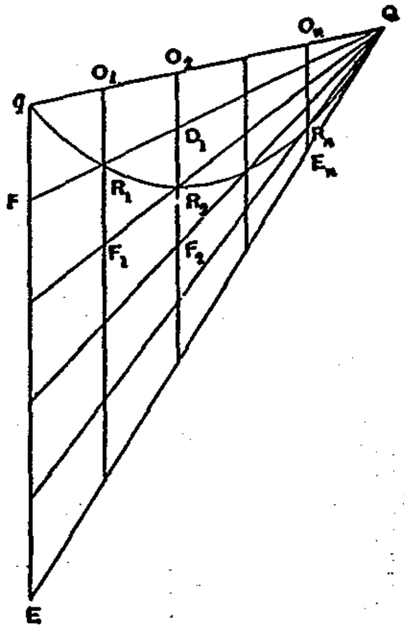
The statement by Archimedes that this is not a proof is found at this point in the *Method*. The mathematically rigorous proof, contained in Propositions 16 and 17 of *Quadrature of the Parabola*, will now be given. Be on the lookout for things like Riemann sums.

Prop. 16. Suppose Qq to be the base of a parabolic segment, q being not more distant than Q from the vertex of the parabola. Draw through q the straight line qE parallel to the axis of the parabola to meet the tangent Q in E. It is required to prove that

$$(\text{area of segment}) = \frac{1}{3}\,\Delta EqQ.$$

The proof will employ the method of exhaustion, a technique much used by Archimedes, and will take the form of a double *reductio ad absurdum*, where the assumptions that the area of the segment is more than and less than $\frac{1}{3}$ the area of the triangle both lead to contradictions.

I. Suppose the area of the segment greater than $\frac{1}{3}$ ΔEqQ. Then the excess can, if continually added to itself, be made to exceed ΔEqQ. And it is possible to find a submultiple of the triangle EqQ less than the said excess of the segment over $\frac{1}{3}$ ΔEqQ.



Let the triangle FqQ be such a submultiple of the triangle EqQ. Divide Eq into equal parts each equal to qF, and let all points of division including F be joined to Q meeting the parabola in $R_1, R_2, \ldots, R_n$ respectively. Through $R_1, R_2, \ldots, R_n$ draw diameters of the parabola meeting qQ in $O_1, O_2, \ldots, O_n$ respectively.

Let O_1R_1 meet QR_2 in F_1, let O_2R_2 meet QR_1 in D_1 and QR_3 in F_2, let O_3R_3 meet QR_2 in D_2 and QR_4 in F_3, and so on.

We have, by hypothesis,

$$\Delta FqQ < (\text{area of segment}) - \frac{1}{3}\,\Delta EqQ,$$

or,

$$(\text{area of segment}) - \Delta FqQ > \frac{1}{3}\,\Delta EqQ \qquad (\alpha)$$

Now, since all the parts of qE, as qF and the rest, are equal, $O_1R_1 = R_1F_1$, $O_2D_1 = R_2F_2$, and so on; therefore

$$\begin{aligned}\Delta FqQ &= (FO_1 + R_1O_2 + D_1O_3 + \ldots)\\ &= (FO_1 + F_1D_1 + F_2D_2 + \ldots + F_{n-1}D_{n-1} + \Delta E_nR_nQ) \qquad (\beta)\end{aligned}$$

But

$$(\text{area of segment}) < (FO_1 + F_1O_2 + \ldots + F_{n-1}O_n + \Delta E_nO_nQ).$$

Subtracting, we have

$$(\text{area of segment}) - \Delta FqQ < (R_1O_2 + R_2O_3 + \ldots + R_{n-1}O_n + \Delta R_nO_nQ),$$

whence, *a fortiori*, by (α),

$$\frac{1}{3}\,\Delta EqQ < (R_1O_2 + R_2O_3 + \ldots + R_{n-1}O_n + \Delta R_nO_nQ).$$

But this is impossible, since [Props. 14,15]

$$\frac{1}{3}\,\Delta EqQ < (R_1O_2 + R_2O_3 + \ldots + R_{n-1}O_n + \Delta R_nO_nQ).$$

Therefore

$$(\text{area of segment}) > \frac{1}{3}\,\Delta EqQ$$

cannot be true.

II. If possible, suppose the area of the segment less than $\frac{1}{3}\,\Delta EqQ$.

Take a submultiple of the triangle EqQ, as the triangle FqQ, less than the excess of $\frac{1}{3}\Delta EqQ$ over the area of the segment, and make the same construction as before.

Since $\Delta FqQ < \frac{1}{3}\,\Delta EqQ$ - (area of segment), it follows that

$$\Delta FqQ + (\text{area of segment}) < \frac{1}{3}\,\Delta EqQ < (FO_1 + F_1O_2 + \ldots + F_{n-1}O_n + \Delta E_nO_nQ)$$

[Props. 14, 15] Subtracting from each side the area of the segment, we have

$$\Delta FqQ < (\text{sum of spaces } qFR_1,\ R_1F_1R_2,\ \ldots,\ E_nR_nQ)$$

$$< (FO_1 + F_1D_1 + \ldots + F_{n-1}D_{n-1} + \Delta E_nR_nQ),\ \textit{a fortiori};$$

which is impossible, because, by (β) above,

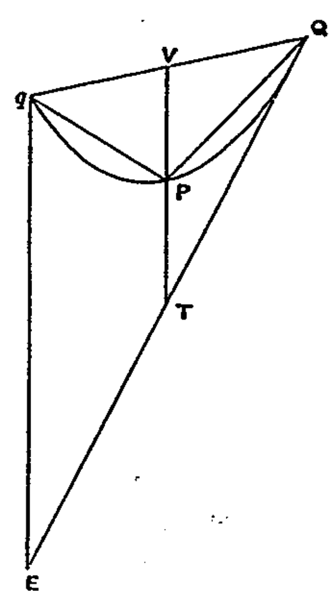
$$\Delta FqQ = FO_1 + F_1D_1 + \ldots + F_{n-1}D_{n-1} + \Delta E_nR_nQ.$$

Hence the area of the segment cannot be less than $\frac{1}{3}\,\Delta EqQ$.

Since the area of the segment is neither less nor greater than $\frac{1}{3}\,\Delta EqQ$, it is equal to it.

Proposition 17. It is now manifest that the area of any segment of a parabola is four-thirds of the triangle which has the same base as the segment and equal height.

Let Qq be the base of the segment, P its vertex. Then PQq is the inscribed triangle with the same base as the segment and equal height.



Since P is the vertex of the segment, the diameter through P bisects Qq. Let V be the point of bisection.

Let VP, and qE drawn parallel to

it, meet the tangent at Q in T, E respectively.

Then, by parallels, qE = 2VT, and PV = PT, [Prop. 2] so that VT = 2PV.

Hence $\Delta EqQ = 4\Delta PQq$. But by Prop. 16, the area of the segment is equal to $\frac{1}{3}\,\Delta EqQ$.

Therefore (area of segment) $= \frac{4}{3}\,\Delta PQq$.

In case readers were not sure what Archimedes meant by the terms *base, height,* and *vertex* in the above work, he defines them immediately *after* Prop. 17. "In segments bounded by a srtaight line and any curve, I call the straight line the **base**, and the **height** the greatest perpendicular drawn from the curve to the base of the segment, and the **vertex** the point from which the greatest perpendicular is drawn."

The General Solution of the Cubic Equation

> Cube the third part of the number of "things", to which you add the square of half the number of the equation, and take the root of the whole, that is, the square root, which you will use, in the one case adding the half of the number which you just multiplied by itself, in the other case subtracting the same half, and you will have a "binomial" and "apotome" respectively; then subtract the cube root of the apotome from the cube root of the binomial, and the remainder from this is the value of the "thing".
>
> from Girolamo Cardano's *Ars Magna*, (Nurnburg, 1545)

Certainly one of the great theorems of mathematics is the quadratic formula, but its origins cannot be pinned down to a specific time, place, or person. The ancient Babylonians of about 2000 B.C. were apparently aware of an equivalent of the quadratic formula, and the method of completing the square on which the formula is based. The case of cubic equations is considerably more difficult, and while some special cases of cubic equations were solved by the Babylonians and others, including Archimedes, the solution of the general cubic was not known until much later. In the eleventh century the Persian poet-mathematician Omar Khayyam devised a geometric solution of cubic equations, and about 500 years later Italian mathematicians were able to get an algebraic solution of both cubic and quartic equations. The interested student can find a discussion of both these methods in *Great Moments in Mathematics (before 1650)* by Howard Eves. Here, the algebraic solution will be developed.

The actual solution technique will be applied to cubic equations of the form $x^3 + mx = n$, or "depressed cubics" which lack a second degree term. As will be seen presently, any cubic can be converted to this form.

A useful result is the following identity:

$$(a-b)^3 + 3ab(a-b) = a^3 - b^3.$$

The student should prove this by expanding and simplifying the left side. If $x = a-b$, the above identity corresponds to the depressed cubic

$$x^3 + 3abx = a^3 - b^3,$$

which suggests choosing a and b so that

$$m = 3ab, \text{ and } n = a^3 - b^3.$$

The solution of these two equations for a and b is

$$a = \sqrt[3]{(n/2) + \sqrt{(n/2)^2 + (m/3)^3}} \quad \text{and} \quad b = \sqrt[3]{-(n/2) + \sqrt{(n/2)^2 + (m/3)^3}}$$

from which one root, $x = a-b$, can be found. The cubic now can be factored into a linear factor and a quadratic factor, and the other solutions found by the quadratic formula. The student should verify the above formulas for a and b.

A general cubic of the form $ax^3 + bx^2 \; cx + d = 0$ can be "depressed" by means of the substitution $x = z - b/3a$, giving

$$z^3 + \left[-\frac{b^2}{3a^2} + \frac{c}{a} \right] z = \left[-\frac{2b^3}{27a^3} + \frac{bc}{3a^2} - \frac{d}{a} \right].$$

<u>Some</u> <u>Examples</u>:

1. $3x^3 - 5x^2 - x - 2 = 0$. Here a=3, b=-5, c=-1, and d=-2, so the substitution $x = z + 5/9$ yields

$$z^3 - \frac{34}{27} z = \frac{871}{729}$$

where now $m = -\frac{34}{27}$ and $n = \frac{871}{729}$, and so (a calculator is handy for the arithmetic) $z = 1.44444$, to five decimals. Thus $x = 2$, and the equation can be factored as $(x-2)(3x^2 + x + 1)$,and the other two roots are seen to be complex (but in the 16th century complex numbers were poorly understood).

2. $x^3 - 63x = 162$. This cubic is in depressed form with $m = -63$ and $n = 162$. The numbers a and b turn out to be

$$a = \left[81 + 30\sqrt{-3} \right]^{1/3} \quad \text{and} \quad b = \left[-81 + 30\sqrt{-3} \right]^{1/3}.$$

This presented problems for the 16th century mathematicians, and this situation came to be known as the "irreducible case". The irreducible case will occur whenever the three roots of the cubic are all real and different from zero. In the given example it can be shown that one of the cube roots of $81 + 30\sqrt{-3}$ is $-3 + 2\sqrt{-3}$, and that one of the cube roots of $81 - 30\sqrt{-3}$ is $-3 - 2\sqrt{-3}$. Thus, $a - b = -6$, which is indeed a root of the given cubic.

Algebraic and Transcendental Numbers

Given any distinct algebraic numbers $\alpha_1, \alpha_2, \ldots, \alpha_m$, the equation

$$\sum_{j=1}^{m} a_j e^{\alpha_j} = 0$$

is impossible in algebraic numbers $a_1, a_2, \ldots, a_m$ not all zero.

(F. Lindemann, 1882)

Probably the first crisis in Mathematics came with the discovery of irrational or incommensurable numbers, such as $\sqrt{2}$. The early Greeks, in the fifth or sixth century BC, were the first to realize that there are points on the number line which do not correspond to any rational number. In fact, it is now known that there are "more" irrationals than rationals. The concept of "more" as applied to infinite sets will be treated in another chapter.

The set of real numbers can also be divided into <u>algebraic</u> and <u>transcendental</u> numbers.

<u>Definition:</u> A number α is algebraic if α satisfies an equation of the form

$$x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n = 0,$$

in which the coefficients a_i are rational numbers.

Notice that all rational numbers are algebraic, as well as numbers like $\sqrt{2}$

.

<u>Definition:</u> A number is transcendental if it is not algebraic.

Thus, all transcendental numbers are irrational, but it was not known until 1844 whether any transcendental numbers actually existed! In that year Liouville constructed not only one, but an entire class of nonalgebraic real numbers, now known as Liouville numbers. About thirty years later, Cantor was able to prove that transcendental numbers exist and have the same cardinality as the real numbers (without exhibiting any transcendental numbers!). In 1873 C. Hermite proved that the number e is transcendental, and in 1882 F. Lindemann, basing his proof on Hermite's, was able to show that π is also transcendental. These are both great theorems, and the proof below of the transcendence of e is based on work of A. Hurwitz, published in 1893.

In order to prove the main result, the following preliminary lemma is convenient.

Lemma: If $h(x) = f(x)g(x)/n!$ where $f(x) = x^n$ and $g(x)$ is a polynomial with integer coefficients, then $h^{(j)}(0)$, the jth derivative of h evaluated at x=0, is an integer for $j=0,1,2,\ldots$. Also, the integer $h^{(j)}(0)$ is divisible by $(n+1)$ for all j except possibly j=n, and in case $g(0)=0$ the exception is not necessary.

Proof: (For those who are wondering what this lemma has to do with the transcendence of e, notice that it involves polynomials with integer coefficients, the kinds of things associated with algebraic numbers.) By calculating the first two or three derivatives of h and using induction it can be seen that

$$h^{(j)}(x) = \frac{1}{n!}\sum_{m=0}^{j} \binom{j}{m} f^{(m)}(x)\, g^{(j-m)}(x)$$

where $\binom{j}{m}$ represents the mth binomial coefficient of order j. Since $f(x) = x^n$ and since g can be expressed as $\Sigma_{i=0}^{k} c_i x^i$ with $c_0, c_1, \ldots, c_k$ integers, it follows that

$$f^{(m)}(0) = \begin{cases} 0 \text{ if } m \neq n \\ n! \text{ if } m = n \end{cases} \quad \text{and} \quad g^{(j-m)}(0) = \begin{cases} c_{j-m}(j-m)! \text{ if } j-m \leq k \\ 0 \quad \text{if } j-m > k \end{cases}$$

Noting that k is the degree of g, there are 4 cases:

(1) $\underline{j < n:}$ $f^{(m)}(0) = 0$ for $m = 0,1,\ldots,j$, so $h^{(j)}(0) = 0$.

(2) $\underline{j = n:}$ $h^{(n)}(0) = \frac{1}{n!} f^{(n)}(0)\, g(0) = c_0$.

(3) $\underline{j = n+s,\ s = 1,2,\ldots k:}$ $h^{(j)}(0) = \frac{1}{n!}\binom{n+s}{n} n!\, g^{(s)}(0)$

$$= \frac{(n+s)!}{n!} c_s .$$

(4) $\underline{j > n+k:}$ $h^{(j)}(0) = 0$.

Clearly, $h^{(j)}(0)$ is an integer in each case, and is divisible by $(n + 1)$ in all except case (2). If $g(0) = c_0 = 0$, then the result in case (2) is also divisible by $(n + 1)$. The proof of the lemma is complete.

Theorem: e satisfies no relation of the form

$$a_m e^m + a_{m-1} e^{m-1} + \ldots + a_1 e + a_0 = 0$$

with integer coefficients not all 0.

Proof: The idea of the proof will be to assume that e *does* satisfy such a relation, and arrive at a logical impossibility, or contradiction. In this case, the contradiction will be that a certain number is a non-zero integer, but also has absolute value less than 1.

There is no loss of generality in assuming that a is nonzero.

For an odd prime p (to be specified later) define the polynomial

$$h(x) = \frac{x^{p-1}(x-1)^p(x-2)^p\ldots(x-m)^p}{(p-1)!}$$

which has degree mp+p-1 and notice that the lemma is applicable to not only h(x), but also to h(x+1), h(x+2),..., and h(x+m). Also define

$$H(x) = h(x) + h'(x) + h''(x) + \ldots + h^{(mp+p-1)}(x)$$

and notice that $h^{(mp+p-1)}(x) = (mp+p-1)!/(p-1)!$, a constant. Now

$$(e^{-x}H(x))' = e^{-x}H'(x) - e^{-x}H(x) = e^{-x}(H'(x) - H(x))$$
$$= -e^{-x}h(x)$$

so that

$$a_i\int_0^i e^{-x}\, h(x)\, dx = -a_i\int_0^i (e^{-x}H(x))'\, dx$$
$$= -a_i\Big[e^{-i}H(i) - H(0)\Big].$$

Now multiply by e^i and sum from i=0 to m :

$$\sum_{i=0}^{m} a_i e^i\int_0^i e^{-x}\, h(x)\, dx = H(0)\sum_{i=0}^{m} a_i e^i - \sum_{i=0}^{m} a_i\, H(i).$$

Now, assuming that e does satisfy the equation in the theorem, the first term on the left is 0, and using the definition of H, the above equation becomes :

$$(*)\qquad \sum_{i=0}^{m} a_i e^i\int_0^i e^{-x}\, h(x)\, dx = -\sum_{i=0}^{m}\sum_{j=0}^{mp+p-1} a_i\, h^{(j)}(i).$$

Looking first at the right side, the lemma can be applied to h(x), h(x+1), h(x+2),..., and h(x+m) to get, (for j = 0,1,...,mp+p-1) $h^{(j)}(0)$, $h^{(j)}(1),\ldots, h^{(j)}(m)$ are all integers and are all divisible by p except possibly $h^{(p-1)}(0)$. However,

$$h^{(p-1)}(0) = (-1)^p(-2)^p\ldots(-m)^p$$

and if p is chosen so that $p > m$ and also $p > |a_0|$ then

1) $h^{(p-1)}(0)$ is not divisible by p, and
2) every term in the double sum above is a multiple of p except the term $-a_0h^{(p-1)}(0)$.

Therefore the right side of (*) represents a nonzero integer.

Turning to the left side now,

$$\left|\sum_{i=0}^{m} a_i e^i\int_0^i e^{-x}\, h(x)\, dx\right| \le \sum_{i=0}^{m}\left| a_i e^i\int_0^i e^{-x}\, h(x)\, dx\right|$$

$$\le \sum_{i=0}^{m} |a_i| \; e^{i} \; i \; 1 \; \frac{m^{mp+p-1}}{(p-1)!}$$

$$\le \sum_{i=0}^{m} |a_i| \; m \; e^{m} \; \frac{m^{mp+p-1}}{(p-1)!}$$

$$\le \sum_{i=0}^{m} |a_i| \; e^{m} \; \frac{(m^{m+2})^{p-1}}{(p-1)!} \; ,$$

where it is necessary to require $p > m+2$ for the last inequality. The expression $\frac{(m^{m+2})^{p-1}}{(p-1)!}$ above is the p-th term in the series for $e^{m^{m+2}}$, which is a convergent series of constants, and so the p-th term can be made arbitrarily small by choosing p large enough. This means that the left side of (*) can be made smaller than 1 in absolute value, contradicting that the right side is a nonzero integer. This completes the proof.

Lindemann's theorem, stated at the beginning of this section, replaces the integer exponents $0,1,\ldots,m$ by algebraic numbers $\alpha_1,\ldots,\alpha_m$. The transcendence of π then follows from observing that, if π were algebraic then $i\pi$ would also be algebraic and the equation

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

would be impossible. However, this formula is one of the best-known in mathematics and is certainly true, so π must be transcendental.

The Three Famous Problems of Antiquity

1. The duplication of the cube.
2. The trisection of an angle.
3. The quadrature of the circle.

These are all construction problems, to be done with what has come to be known as *Euclidean tools*, that is, straightedge and compasses under the following rules:

- o With the straightedge a straight line of indefinite length may be drawn through any two distinct points.
- o With the compasses a circle may be drawn with any given point as center and passing through any given second point.

To expand on the problems somewhat, the duplication of the cube means to construct the edge of a cube having twice the volume of a given cube; the trisection of an angle means to divide an arbitrary angle into three equal parts; the quadrature of the circle means to construct a square having area equal to the area of a given circle.

The importance of these problems stems from the fact that all three are unsolvable with Euclidean tools, and that it took over 2000 years to prove this! Also, these are the problems that seem to attract amatuer mathematicians who, not believing the proofs of the impossibility of these constructions, (and the proofs are ironclad!) expend much effort on "proofs" that one or more of these is indeed possible. Trisecting the angle is the favorite. Many of these attempts do produce very good approximations, but, as will be seen, cannot be exact.

Interestingly enough, the results needed to show that the three problems are impossible are not geometric, but rather are algebraic in nature. The two pertinent theorems are:

THEOREM A: The magnitude of any length constructible with Euclidean tools from a given unit length is an algebraic number.

THEOREM B: From a given unit length it is impossible to construct with Euclidean tools a segment the magnitude of whose length is a root of a cubic equation having rational coefficients but no rational root.

Notice that while Theorem A says any constructible number is algebraic, Theorem B says not all algebraic numbers are constructible. The proofs of these theorems will be postponed while the three famous problems are put to rest now.

Duplication of the cube: Let the edge of the given cube be the unit of length, and let x be the edge of the cube having twice the volume of the given cube. Then $x^3 = 2$. Since any rational root of this equation must have as numerator a factor of 2 and as denominator a factor of 1 the equation has no rational roots. Thus, according to Theorem B, x is not constructible.

Trisection of the angle:
Some angles, such as 90°, can be trisected, but if it can be shown that some angle cannot be trisected, then the general trisection problem will have been proved impossible. Here it will be shown that a 60° angle cannot be trisected. Recall the trigonometric identity

$$\cos\theta = 4\cos^3(\tfrac{\theta}{3}) - 3\cos(\tfrac{\theta}{3})$$

and take $\theta = 60^\circ$ and $x = \cos(\frac{\theta}{3})$. The identity becomes

$$8x^3 - 6x - 1 = 0$$

and, as above, any rational root must have a factor of -1 as numerator and a factor of 8 as denominator. A check of the possibilities again shows that, by Theorem B, x is not constructible. It remains to show that the trisection of a 60° angle is equivalent to constructing a segment of length $\cos 20^\circ$. In Figure 1 the radius of the circle is 1 and $\angle BOA = 60^\circ$. If the trisector OC can be constructed, then so can segment OD, where D is the foot of the perpendicular from C to OA. But OD = x.

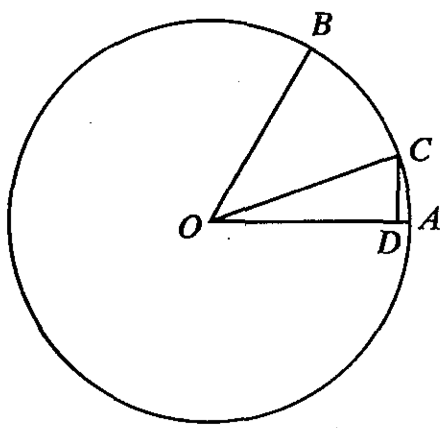


Figure 1

The student should prove the following theorem on the rational roots of a polynomial, which was used in both of the above proofs.

THEOREM C: If a polynomial equation

$$a_0x^n + a_1x^{n-1} + \quad + a_{n-1}x + a_n = 0$$

with integer coefficients a_0, $a_1, \ldots, a_n$ has a reduced rational root b/c, then b is a factor of a_n and c is a factor of a_0.

<u>The quadrature of the circle</u>: In the proof of Theorem A it will be seen that the constructibility of a number a is equivalent to the constructibility of $\sqrt{a}$. Thus, if the radius of the given circle is 1, the required square must have side $\sqrt{\pi}$, but π was shown earlier to be transcendental, and so cannot be constructed, by Theorem A.

<u>Proof of Theorem A</u>: Any Euclidean construction consists of some sequence of the following steps:

1. drawing a straight line between two points,
2. drawing a circle with a given center and a given radius,
3. finding the intersection points of two lines, a line and a circle, or two circles.

Further, every construction problem involves certain given geometric elements a, b, c, ... and requires that certain other elements x, y, z, ... be found. The conditions of the problem make it possible to set up one or more equations whose solutions allow the unknown elements to be expressed in terms of the given ones. At this point the student should show that, given segments of length a, b, and 1, segments of length a+b, a-b, ab, a/b and $\sqrt{a}$ can be constructed. These turn out to be the basic operations. Assume that a coordinate system and a unit length are given, and that all the given elements in the construction are represented by rational numbers. Since the sum, difference, product, and quotient (dividing by 0 is of course excluded) of two rational numbers is another rational number, the rational numbers form a <u>closed set</u> under the 4 arithmetic operations. Any set which is closed with respect to these 4 fundamental operations is called a <u>field</u> and the field of rational numbers will be denoted by Q_0. If two points $P_1(x_1,y_1)$ and $P_2(x_2,y_2)$ are given, then the equation of the line through them is

$$(y_2-y_1)x + (x_1-x_2)y + (x_2y_1-x_1y_2) = 0$$

or

$$ax + by + c = 0.$$

Clearly, a, b, and c are rational. The equation of a circle with radius r and center (h,k) is

$$x^2 + y^2 - 2hx - 2ky + h^2 + k^2 - r^2 = 0$$

or

$$x^2 + y^2 + dx + ey + f = 0$$

where d, e, and f are rational. Now, finding the intersection of two lines involves rational operations on the coefficients of the variables, and finding the intersection of two circles or of a circle and a line involves the extraction of square roots in addition to the 4 rational operations. Thus, a proposed Euclidean construction is possible <u>if and only if</u> the numbers which define the desired elements can be derived from the given elements by a finite number of rational operations and extractions of square roots.

If a unit length is given, then all rational numbers can be constructed, and if k is a rational number, $\sqrt{k}$ and $a + b\sqrt{k}$ can be constructed if a and b are in Q_0 (rationals). If $\sqrt{k}$ is not in Q_0 then all numbers of the form $a + b\sqrt{k}$ forms a new field Q_1. (The student should prove this.) In fact, Q_1 contains Q_0 as a subfield. Next, all numbers of the form $a_1 + b_1\sqrt{k_1}$ where a_1 and b_1 are in Q_1 and k_1 is also in Q_1, but $\sqrt{k_1}$ is not in Q_1 also form a field, Q_2, which contains Q_1 as a subfield. In this way a sequence of fields Q_0, $Q_1, \ldots, Q_n$ can be formed with the following properties:

(i) Q_0 is the rationals

(ii) Q_k is an extension of Q_{k-1}, $k = 1,2,\ldots,n$

(iii) Every number in Q_k , $k = 0,1,\ldots,n$ is constructible

(iv) For every number constructible in a finite number of steps, there exists an integer N such that the constructed number is in one of the fields $Q_0,\ldots,Q_N$.

Since the members of the field Q_k are all roots of polynomials having degree 2^k and rational coefficients, it follows that all constructible numbers are algebraic. This proves Theorem A.

Proof of Theorem B: Consider the general cubic with rational coefficients

$$x^3 + px^2 + qx + r = 0$$

and having no rational roots. Assume that one of the roots is constructible, say x_1. Then x_1 is in Q_n for some integer $n > 0$, where Q_n is one of the fields constructed in the proof of Theorem A. Also assume that none of the roots belong to Q_k, $k < n$. Thus,

$$x_1 = a + b\sqrt{k}$$

where a, b, and k belong to Q_{n-1}. Substituting $x_1 = a + b\sqrt{k}$ into the cubic yields

$$s = a^3 + 3ab^2k + pa^2 + pb^2k + qa + r = 0$$

and

$$t = 3a^2b + b^3k + 2pab + qb = 0.$$

(The student should fill in the details.) Now if $a - b\sqrt{k}$ is substituted into the left side of the cubic, the left side becomes $s - t\sqrt{k}$ and is zero. This means that $x_2 = a - b\sqrt{k}$ is also a root of the cubic. To get the third root, write the cubic as

$$(x - x_1)(x - x_2)(x - x_3) = 0$$

and expand. The coefficient of x^2 turns out to be $-(x_1 + x_2 + x_3)$ which is equal to p. This and the fact that $x_1 + x_2 = 2a$ gives

$$x_3 = -2a - p$$

which means that x_3 belongs to Q_{n-1}, a contradiction. This completes the proof of Theorem B.

Newton's Binomial Theorem and Some Consequences

"Fractions are reduced to infinite series by division; and radical quantities by extraction of the roots, by carrying out those operations in the symbols just as they are commonly carried out in decimal numbers. These are the foundations of these reductions: but extractions of roots are much shortened by this theorem,

$$(P + PQ)^{m/n} = P^{m/n} + \frac{m}{n} AQ + \frac{m - n}{2n} BQ + \frac{m - 2n}{3n} CQ + \frac{m - 3n}{4n} DQ + \text{etc.}$$

where $P + PQ$ signifies the quantity whose root or even any power, or the root of a power, is to be found; P signifies the first term of that quantity, Q the remaining terms divided by the first, and m/n the numerical index of the power of $P + PQ$, whether that power is integral or (so to speak) fractional, whether positive or negative." From the letter of June 13, 1676, written by Isaac Newton to Henry Oldenburg (secretary of the Royal Society).

The patterns of the coefficients obtained when expanding a binomial raised to an integer power, such as $(a + b)^n$, were known to the Arabs of the 13th century, and the array

$$\begin{array}{ccccccccccc} & & & & & 1 & & & & & \\ & & & & 1 & & 1 & & & & \\ & & & 1 & & 2 & & 1 & & & \\ & & 1 & & 3 & & 3 & & 1 & & \\ & 1 & & 4 & & 6 & & 4 & & 1 & \\ 1 & & 5 & & 10 & & 10 & & 5 & & 1 \\ & & & & & \cdots\cdots & & & & & \end{array}$$

called Pascal's triangle was known to mathematicians in the 16th century, about 100 years before Pascal! In 1665, Newton expressed this binomial expansion formally as follows:

$$(P + PQ)^{m/n} = P^{m/n} + \frac{m}{n} P^{m/n}Q + \left(\frac{m - n}{2n}\right)\frac{m}{n} P^{m/n}Q^2 + \\ + \left(\frac{m - 2n}{3n}\right)\left(\frac{m - n}{2n}\right)\frac{m}{n} P^{m/n}Q^3 + \ldots$$

(Do you see what the A, B, C,... are in the introduction?), which, after cancelling the common factor $P^{m/n}$ from both sides, gives

$$(1 + Q)^{m/n} = 1 + \frac{m}{n} Q + \frac{\frac{m}{n}(\frac{m}{n} - 1)}{2!} Q^2 + \ldots + \frac{\frac{m}{n}(\frac{m}{n} - 1)(\frac{m}{n} - 2)\ldots(\frac{m}{n} - k+1)}{k!} Q^k + \ldots$$

which is the general form of the Binomial Theorem as it is known today.

Newton's great insight was not only the formal expansion of this expression, but also the conviction that it remained valid for fractional and negative exponents, cases in which the expansion takes the form of an infinite series. For example,

$$\frac{1}{(1+x)^2} = (1+x)^{-2} = 1 + (-2x) + \frac{(-2)(-3)}{2!}x^2 + \frac{(-2)(-3)(-4)}{3!}x^3 + \ldots$$
$$= 1 - 2x + 3x^2 - 4x^3 + 5x^4 - \ldots\ .$$

Newton "checked" this result by cross-multiplying the expression by $(1+x)^2$ to get 1. Another example done by Newton was

$$\sqrt{1+x} = (1+x)^{1/2} = 1 + \frac{1}{2}x + \frac{(1/2)(-1/2)}{2!}x^2 + \frac{(1/2)(-1/2)(-3/2)}{3!}x^3 + \ldots$$
$$= 1 + \frac{1}{2}x + \frac{1}{8}x^2 + \frac{1}{16}x^3 + \frac{5}{128}x^4 + \frac{7}{256}x^5 + \ldots ,$$

which he checked by squaring the right side to get $1 + x$.

The power and usefulness of the Binomial Theorem were most apparent when Newton used it along with his newly invented Calculus. The next two examples, the first involving integration and the second differentiation, illustrate the interaction between the Binomial Theorem and Calculus.

Newton's Approximation of π

By definition, π is the ratio of the circumfrence of a circle to its diameter. By Newton's time the value of π was known to 39 decimal places, which seems like not much progress, but the work involved required a good deal of geometric insight and literally years of work. Newton, armed with the Binomial Theorem and Calculus, made the problem much, much simpler.

He began with the circle having center $(\frac{1}{2},0)$ and radius $\frac{1}{2}$. The equation for the upper semicircle is easily seen to be $y = \sqrt{x - x^2}$. Let B be the point $(\frac{1}{4},0)$ and draw DB $\perp$ AC. Newton then attacked the area A_1 in two different ways.

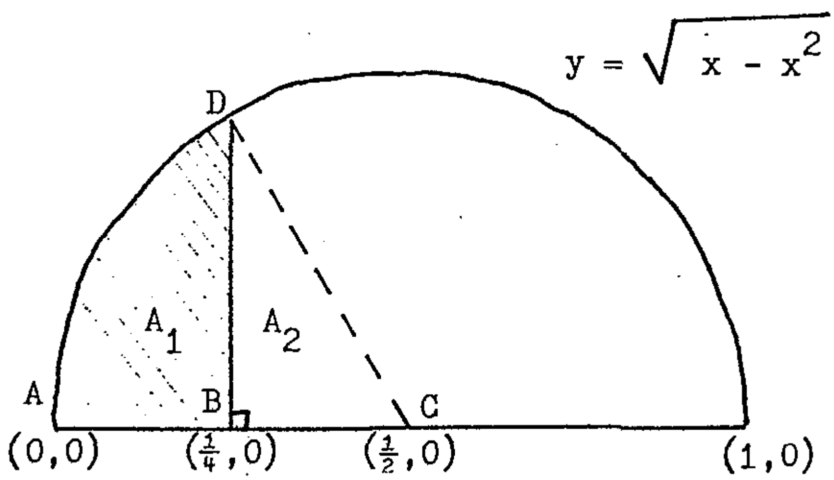


Figure 1

First, he used the Binomial Theorem and Calculus as follows:

$$\sqrt{x - x^2} = \sqrt{x}\ (1 - x)^{1/2}$$
$$= \sqrt{x}\ (1 - \tfrac{1}{2}x - \tfrac{1}{8}x^2 - \tfrac{1}{16}x^3 - \tfrac{5}{128}x^4 - \tfrac{7}{256}x^5 - \dots)$$
$$= x^{1/2} - \tfrac{1}{2}x^{3/2} - \tfrac{1}{8}x^{5/2} - \tfrac{1}{16}x^{7/2} - \tfrac{5}{128}x^{9/2} - \tfrac{7}{256}x^{11/2} - \dots .$$

So, $A_1 = \int_0^{\frac{1}{4}} \sqrt{x - x^2}\ dx$

$$\approx \int_0^{\frac{1}{4}} (x^{1/2} - \tfrac{1}{2}x^{3/2} - \tfrac{1}{8}x^{5/2} - \dots - \tfrac{7}{256}x^{11/2})\ dx = 0.076773207.$$

Next, using geometry, Newton calculated as follows:

In triangle DBC, with area A_2, notice that $\cos\theta = .5$ and so $\theta = \frac{\pi}{3}$. Thus, the length of DB is $\frac{1}{4}\sqrt{3}$, and $A_2 = \frac{1}{32}\sqrt{3}$.

Further, since the area of the sector ADC is to the area of the full circle as θ is to 2π, the area of sector ADC is $\frac{\pi}{24}$. Thus,

$$A_1 = \frac{\pi}{24} - \frac{1}{32}\sqrt{3} \approx 76773207$$

and so

$$\pi \approx 3.141595074$$

which is correct to 5 places. Newton carried the binomial expansion out to 22 terms, and found π accurate to 16 places in a few hours using this technique.

"Newton's Method"

Newton devised a quick method, which is still used today, to approximate solutions of equations. The technique again uses the binomial theorem and calculus. (The student should look up Newton's method in a modern Calculus book.) Here, a specific example will be presented before looking at the more general case.

Consider finding the roots of the cubic equation

$$f(x) = x^3 - 2x - 5 = 0.$$

Denote the exact solution by x^*, so that $f(x^*) = 0$, and begin with a first guess, or approximation to x^*, say $x = 2$. Clearly this is not the exact solution since $f(2) = -1$ rather than 0, but the essence of the method is to successively improve this guess.

Let $p = x^* = 2$ represent the error in the guess, so that

$$0 = f(x^*) = f(2+p) = p^3 + 6p^2 + 10p - 1.$$

Newton then reasoned that if 2 is a good approximation to x^*, then p will be small, and the terms of degree 2 and higher in p can be neglected, giving

$$0 \approx 10p - 1 \quad \text{or} \quad p \approx 0.1.$$

Since $x^* = 2 + p$, the next approximation should be $x = 2.1$, and the process can be repeated. Note that $f(2.1) = 0.061$, which is getting closer to 0. Now let $q = x^* - 2.1$, and get, as before,

$$0 = q^3 + 6.3q^2 + 11.23q + 0.061$$

which gives, upon discarding all but the linear and constant terms,

$$q \approx -0.0054.$$

Thus the revised approximation to the solution is

$$x^* \approx 2.0946.$$

One more application of this procedure gives

$$x^* \approx 2.095447375$$

which is correct to 9 decimal places. (The student should compare this with the method of section 4.)

Newton's method can be applied to the problem of finding the roots of any differentiable function, not just polynomials. The next part gives a general derivation for a general polynomial, and the student (and his/her calculus book) can supply the proof for a general function.

Consider the equation

$$0 = f(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n.$$

Again, let x^* be the exact solution, so that $f(x^*) = 0$, and denote the approximation by x, with $p = x^* - x$ also as before. Then

$$0 = f(x^*) = a_0 + a_1(x+p) + a_2(x+p)^2 + \dots + a_n(x+p)^n$$

$$= a_0 + a_1(x+p) + a_2(x^2 + 2px + p^2) + \dots +$$

$$a_n(x^n + nx^{n-1}p + \frac{n(n-1)}{2!} x^{n-2}p^2 + \dots + nxp^{n-1} + p^n)$$

by the binomial theorem. Now collect terms according to powers of p.

$$0 = (a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n) + p(a_1 + 2a_2 x + \dots + na_n x^{n-1}) + \dots$$

$$+ p^n a_n$$

$$= f(x) + pf'(x) + \text{terms involving } p^2 \text{ or higher.}$$

So, if the terms of degree two and higher are dropped, an approximation for p is

$$p \approx - \frac{f(x)}{f'(x)} .$$

The value of p can be regarded as a correction term for the guess x, so that the next approximation would be

$$x + p \approx x - \frac{f(x)}{f'(x)} .$$

This is the modern form of Newton's method.

Newton's own comment on this was : "I do not know whether this method of resolving equations is widely known or not, but certainly in comparison with others is both simple and suited to practice. Its proof is evident from the mode of operation itself, and in consequence is easily recalled to mind when needed."

> I shall now show that the general problem of quadratures can be reduced to the finding of a line that has a given law of tangency (declivitas), that is, for which the sides of the characteristic triangle have a given mutual relation.
>
> Gottfried Wilhelm Leibniz, *Acta Eruditorum* (1693), 385-392.

There are two forms of the Fundamental Theorem of Calculus usually given in today's textbooks. Briefly, they are as follows :

- $\frac{d}{dx}\int_a^x f(x)\,dx = f(x)$, and
- If the derivative of F(x) is f(x), then $\int_a^b f(x)\,dx = F(b) - F(a)$.

Either form asserts that the processes of differentiation and integration are *inverse operations* (under certain hypotheses, which are not restrictive), that is, each "undoes" the other. Mathematicians before Newton and Leibniz were aware of this inverse relationship, and the first proof is generally attributed to Isaac Barrow, who gave a *geometric* proof of the following theorem in 1669 in his *Lectiones opticae et geometricae*.

Theorem : Let ZN be any curve of continually increasing ordinate and (to render the figure less cluttered) lying below the axis VM (see figure 1) and let R be a given line segment. Let VL be a curve such that if an arbitrary ordinate cuts ZN, VM, and VL in F, E, D, respectively, the rectangle of dimensions ED and R has an area equal to that of VEFZ. Finally, let T on VM be such that FE : ED = R : TE. Then TD is the tangent to the curve VL at D.

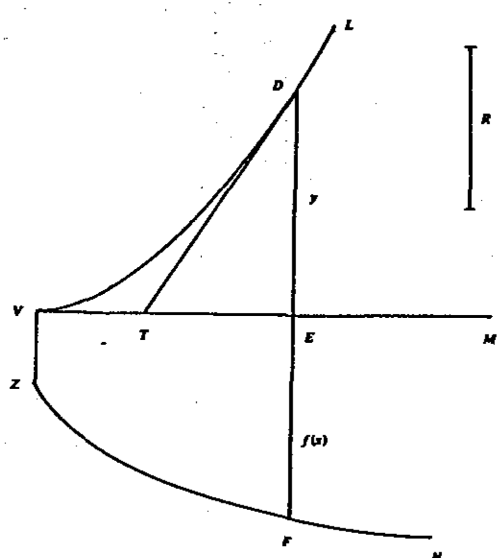


Figure 1

Barrow's proof was purely geometric, and can be found in Struik. Assuming the theorem to be true, take VM to be the x-axis with origin at V. Then set FE = f(x) and ED = y. Taking R as a unit segment, the theorem says that

$$y = (ED)(R) = \text{area VEFZ} = \int_0^x f(x)\, dx,$$

and

$$\frac{dy}{dx} = \text{slope of curve VL at D} = \frac{ED}{TE} = \frac{FE}{R} = f(x).$$

It now follows that

$$\frac{d}{dx}\int_0^x f(x)\, dx = f(x),$$

which is, of course, the fundamental theorem of calculus.

Barrow, who, by the way, was one of Newton's professors at Cambridge, was not able to make very much use of the above theorem, mostly due to his relatively cumbersome geometric approach. Newton and Leibniz, however, took an algebraic approach, and were able to use the theorem to obtain formal rules for integration from corresponding formal rules for differentiation, a point of view still used today. The proof that follows, while given in modern notation, was given, essentially, by both Newton and Leibniz in the late 1600s.

Let f(x) be a continuous, nonnegative function for all values of x in the interval $a \le x \le b$, and consider the definite integral

$$\int_a^b f(x)\, dx.$$

By the definition of the definite integral, this can be interpreted as the area bounded by the curve $y = f(x)$, the x-axis, and the vertical lines at x=a and x=b. See Figure 2.

Now consider the area above, but with the vertical line at x=b replaced by a vertical line at a general x from the interval $a \le x \le b$, and call this area, which clearly depends on x, A(x). Note also that A(a) = 0, a fact which will be used later. The heart of the proof will be to use the definition of the derivative to find the derivative of A(x). Thus, let x be increased by an amount Δx, and denote the corresponding increase in A(x) by ΔA. The area ΔA (see Figure 2 again) has a value that is between the values of the areas of two other rectangles, namely the rectangles having base Δx and heights

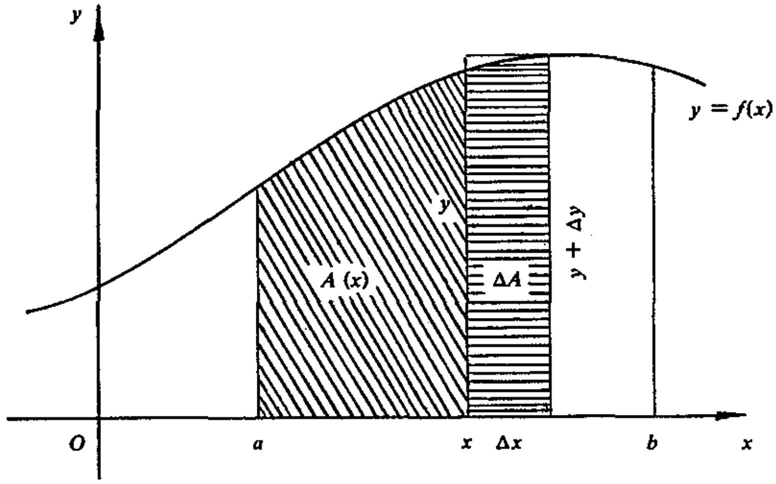


Figure 2

y_{min} and y_{max} , where y_{min} and y_{max} are the minimum and maximum values of f(x) in the x-interval from x to x+Δx. Thus

$$(y_{min})(\Delta x) \leq \Delta A \leq (y_{max})(\Delta x).$$

Since f is continuous, it is possible to find a value $\bar{y}$ between y_{min} and y_{max} so that

$$\Delta A = \bar{y}\Delta x.$$

As $\Delta x \to 0$, $\bar{y} \to y$, and since $\bar{y} = \frac{\Delta A}{\Delta x}$ this means

$$\lim_{\Delta x \to 0} \frac{\Delta A}{\Delta x} = y = f(x).$$

The derivative of the function A(x) is therefore the original integrand f(x).

Functions having the same derivative can differ by a constant, however, so if F(x) is a function whose derivative is also f(x), then

$$A(x) = F(x) + C.$$

To evaluate C, recall that A(a) = 0, so that 0 = F(a) + C or C =-F(a). Thus,

$$A(x) = F(x) - F(a),$$

and the original integral is simply A(b) = F(b) - F(a), or

$$\int_a^b f(x)\, dx = F(b) - F(a),$$

where F(x) is any function having f(x) as its derivative.

Calculus, with integration simplified by the fundamental theorem, has had such a great impact, not only on the development of mathematics, but on the progress of civilization, that it has become a necessary component of technical education today, and is beneficial in many nontechnical fields as well.

Leibniz said of Newton, "Taking mathematics from the beginning of the world to the time when Newton lived, what he did was much the better half.", and inscribed on Newton's tomb are the words, "Mortals, congratulate yourselves that so great a man has lived for the honor of the human race.". However, Newton said of himself that, "If I have seen farther than others, it is because I have stood upon the shoulders of giants.".

Prime Numbers

The Prime Number Theorem : The number of primes not exceeding x is asymptotic to $\frac{x}{\log x}$. Conjectured by C. F. Gauss in 1791, (when he was 15), proved independently by J. Hadamard and C. J. de la Vallee Poussin in 1896.

The Prime Number Theorem has been called the most amazing result yet found about the prime numbers, and is a truly remarkable result which, in addition to its own merits, is notable because of its relation to one of the famous still-unsolved problems in mathematics, the Riemann Hypothesis. The interested student who knows some complex analysis can learn more in advcanced books such as Edwards. There are many interesting properties that prime numbers posess, or appear to posess. One of the attractions of the theory of numbers is that it is both very elementary and very difficult; it is elementary in that it deals with simple mathematical objects, the integers, but the problems and techniques are difficult. However, in spite of being difficult to prove, the theorems of number theory are usually easily stated. Some of the unsettled questions about primes include: Are there infinitely many primes of the form n^2+1? Is there always a prime between n^2 and $(n+1)^2$? Are there infinitely many *Fermat primes*, that is, primes of the form $2^{2^n}+1$?

One of the first properties of prime numbers which *has* been proved is that there exist infinitely many primes. Euclid gave a proof of this which is simple and elegant:

> Suppose there is a largest prime, and that all the primes up to this largest prime are known. Then a complete finite listing of the primes is possible in ascending order:
>
> $$2,3,\ldots,p_n.$$
>
> Now consider the integer
>
> $$N = (2*3*\ldots*p_n) + 1$$
>
> formed by adding 1 to the product of "all" the primes. Obviously, N is larger than the largest prime p_n, and N is not divisible by any of the primes $2,3,\ldots p_n$ (because there will always be a remainder of 1). N is either a prime itself or it isn't. If N is a prime, then it is a prime greater than p_n, and if N is not a prime, then it must be divisible by a prime greater than p_n. Both possibilities show the existence of a prime greater than the previously assumed largest

prime, p_n, and this argument guarantees that the list of primes never ends.

With the aid of modern compitational power the list of primes has been extended quite far, but there seems to be little pattern or regularity in the list! However, the apparent chaos is lessened somewhat if, instead of looking at individual properties of primes, they are considered "in the aggregate". For instance, make (computer aided) a large list of primes, and then count to see how many there are up to a given point. The function $\pi(x)$ is defined to be the number of primes less than or equal to x, and is a measure of the distribution of the prime numbers. If, for some x, $\pi(x)$ is found, then a natural thing to do would be to compute the value of $\frac{\pi(x)}{x}$, which is the fraction of the numbers up x that are primes. Actually, it is more useful to compute the reciprocal of the above fraction, and some results are given below.

x	$\pi(x)$	$\frac{x}{\pi(x)}$	first difference
10	4	2.5	-
100	25	4.0	1.5
1,000	168	6.0	2.0
10,000	1,229	8.1	2.1
100,000	9,592	10.4	2.3
1,000,000	78,498	12.7	2.3
10,000,000	664,579	15.0	2.3
100,000,000	5,761,455	17.4	2.4
1,000,000,000	50,847,534	19.7	2.3
10,000,000,000	455,052,512	22.0	2.3

The most significant part of this table is the last column, which is consistently about 2.3. Most mathematicians, upon seeing this, would eventually think of the number $\log_e 10 = 2.30258\ldots$, and on the basis of this evidence the conjecture

$$\pi(x) \approx \frac{x}{\log_e x}$$

naturally follows. (The student should try to see how the above formula emerges from the table.) Gauss probably did something like this. The more formal meaning of "≈" in this setting is that $\pi(x)$ is *asymptotic to* $\frac{x}{\log x}$ which means

$$\lim_{x \to \infty} \frac{\pi(x)}{(x/\log x)} = 1.$$

This is the famous Prime Number Theorem. The proofs of Hadamard and de la Vallee Poussin both involve the Riemann zeta function, and are slightly beyond the scope of this course, although anyone who knows some of the principles of complex function theory could probably understand them. The interested student is referred to Edwards' book. Proofs exist that avoid the Riemann zeta function, but the required "buildup" would take too long. (See, for instance Hardy and Wright.)

Since the Riemann zeta function is so much involved with the Prime Number Theorem, a short digression on the zeta function will be made here. First define the function $\Pi(z)$, which is almost the same as the gamma function, by

$$\Pi(z) = \int_0^\infty e^{-x} x^z \, dx, \quad \mathcal{R}e(z) > 1.$$

Next, let $\int_{+\infty}^{+\infty}$ indicate a path of integration which begins at $+\infty$, moves to the left down the positive real axis, circles the origin once in the positive (counterclockwise) direction, and returns up the positive real axis to $+\infty$. With these definitions, Riemann's zeta function can be defined as

$$\zeta(z) = \frac{\Pi(-z)}{2\pi i} \int_{+\infty}^{+\infty} \frac{(-x)^z \, dx}{x(e^x - 1)} .$$

It can be shown that the function defined by this formula is analytic (has a convergent Taylor series) at every point of the complex z-plane except for a simple pole at $z = 1$. If z is restricted to real values greater than one, there is a much simpler formula for $\zeta(z)$, viz.,

$$\zeta(z) = \sum_{n=1}^{\infty} \frac{1}{n^z} ,$$

sometimes known as Dirichlet's function. Riemann himself said that he considered it "very likely" that the complex zeros of $\zeta(z)$ all have real part equal to $\frac{1}{2}$, and the experience of his successors has been the same- it is "very likely" that this is true, but no one has been able to prove it. This is the famous Riemann Hypothesis, that if $\zeta(z) = 0$ then $\mathcal{R}e(z) = \frac{1}{2}$. The Riemann Hypothesis still awaits a proof, but, fortunately, it was not needed to prove the Prime Number Theorem.

Returning to the Prime Number Theorem, the expression $\frac{x}{\log x}$, while a fairly simple approximation to $\pi(x)$, is not really very close to $\pi(x)$ until x becomes extremely large, so there has been interest among mathematicians in improving the estimate. Of course, this comes at the price of a more complicated approximant. One of the best approximations to $\pi(x)$ involves the Dirichlet form of the zeta function as follows:

$$R(x) = 1 + \sum_{k=1}^{\infty} \frac{1}{k\zeta(k+1)} \frac{(\log x)^k}{k!} .$$

The following table gives an adea of how good an approximation R(x) is compared to $\frac{x}{\log x}$.

x	$\pi(x)$	$\frac{x}{\log x}$	R(x)
100,000,000	5,761,455	5,428,681	5,761,552
200,000,000	11,078,937	10,463,629	11,079,090
300,000,000	16,252,325	15,369,409	16,252,355
400,000,000	21,336,326	20,194,906	21,336,185
500,000,000	26,355,867	24,962,408	26,355,517
600,000,000	31,324,703	29,684,689	31,324,622
700,000,000	36,252,931	34,370,013	36,252,719
800,000,000	41,146,179	39,024,157	41,146,248
900,000,000	46,009,215	43,651,379	46,009,949
1,000,000,000	50,847,534	48,254,942	50,847,455

Students should get out their calculators and see how close they can come to the numbers in the last two columns.

Euler and Fermat

The Little Fermat Theorem: If p is a prime and p is not a factor of a, then p is a factor of $a^{p-1}-1$. Proposed in 1640 by Fermat, proved in 1736 by Euler.

Pierre de Fermat was one of the great mathematicians of the 17th century, and, indeed of all time. He had a habit, however, of not furnishing proofs of his results. The best known example of this is probably what is now called "Fermat's Last Theorem", which states that if n is an integer greater than two, there are no positive integer values of x, y, and z such that $x^n + y^n = z^n$. This was written in the margin of one of Fermat's mathematics books, and he says that he had found a "truly marvelous" proof, but one "which this margin is too narrow to contain". If Fermat did in fact have a proof, it was indeed "truly marvelous", because no general proof has yet been found! As of 1979 the theorem had been established for all n < 30,000, so some progress has been made.

Two other conjectures of Fermat were settled by the Swiss mathematician Leonhard Euler, who was the most prolific mathematician who ever lived. Euler's collected works contain 886 books and papers, and his mathematical research during his lifetime averaged about 800 pages a year. One of the conjectures of Fermat was proved, and the other was shown to be false.

Euler's proof of Fermat's Little Theorem:

Euler arrived at a proof of Fermat's Little Theorem, stated above, by means of a sequence of results.

<u>Theorem A</u>: If p is prime, and a is any integer, then

$$(a + 1)^p - (a^p + 1)$$

is evenly divisible by p.

<u>Proof</u>: Using the binomial theorem to expand $(a + 1)^p$, the above expression is equal to

$$pa^{p-1} + \frac{p(p-1)}{2!} a^{p-2} + \ldots + pa$$

or

$$p\left[a^{p-1} + \frac{p-1}{2!} a^{p-2} + \ldots + a \right].$$

The student should show that, since p is a prime, the term in the brackets above is an integer. Therefore, p is a factor of

$(a + 1)^p - (a^p + 1)$.

<u>Theorem</u> <u>B</u>: If p is a prime and if $a^p - a$ is evenly divisible by p, then so is $(a + 1)^p - (a + 1)$.

<u>Proof</u>: By Theorem A and the hypothesis, p divides both $a^p - a$ and $(a + 1)^p - (a^p + 1)$, and so p must divide the sum of these expressions. The student can check that the sum is $(a + 1)^p - (a + 1)$.

The next theorem asserts that the divisibility hypothesis of Theorem B is always satisfied.

<u>Theorem</u> <u>C</u>: If p is a prime and a is any integer, then p is a factor of $a^p - a$.

<u>Proof</u>: The proof is by induction. As the student can easily check, the theorem is true for $a = 1$. Knowing this, apply Theorem B with $a=1$ to get that p divides $(1 + 1)^p - (1 + 1) = 2^p - 2$ to establish Theorem C for $p=2$. But now Theorem B can be applied with $a = 2$ and so p divides $(2 + 1)^p - (2 + 1) = 3^p - 3$. In general, assume that Theorem C holds for $a = n$. Then, by Theorem B, p divides

$$(n + 1)^p - (n + 1),$$

and Theorem C is thus true for $a = n + 1$ as well. This shows that p divides $a^p - a$ for any integer a.

With these preliminaries, Fermat's Little Theorem easily follows.

<u>Fermat's</u> <u>Little</u> <u>Theorem</u>: If p is prime and p is not a factor of a, then p <u>is</u> a factor of $a^{p-1} - 1$.

<u>Proof</u>: By Theorem C, p is a factor of

$$a^p - a = a(a^{p-1} - 1)$$

and since p is prime and does not divide a, p must divide $a^{p-1} - 1$. This completes the proof.

Euler's Refutation of a Conjecture of Fermat:

Another of Fermat's conjectures, as he stated it in 1640, was "I have found that numbers of the form $2^{2^n} + 1$ are always prime numbers and have long since signified to analysts the truth of this theorem."

It seems that Fermat had checked this for n = 1, 2, 3, and 4, and for these values, $2^{2^n}+1$ is equal to 5, 17, 257, and 65,537, which, as the student can verify, are all primes. For n=5,

$$2^{2^5} = 4,294,967,297$$

which Euler proved is not prime in 1732, thus disproving Fermat;s conjecture. As will be seen, the smallest prime factor of this number is not extremely large, but is large enough that the brute force method of factorization is impractical. Euler's technique was both ingenious and systematic. His reasoning follows.

First, Euler considered an <u>even</u> integer a and an <u>odd</u> prime p not a factor of a. He then tried to determine the nature of this prime <u>if</u> p divides $a^{2^n}+1$.

<u>Case 1</u>: If n=0, then $a^{2^n}+1 = a + 1$, which is odd since a was assumed to be even. p also must be odd, so for some integer k, p = 2k + 1.

<u>Case 2</u>: If n=1, then $a^{2^n}+1 = a^2+1$, and as in Case 1 any prime dividing a^2+1 must be odd. The prime p thus has either the form 4k + 1 or the form 4k + 3. Suppose p = 4k + 3. Since a is not a multiple of p, the Little Fermat Theorem guarantees that p divides

$$a^{p-1} - 1 = a^{(4k+3)-1} - 1 = a^{4k+2} - 1.$$

Euler then observed that p cannot also divide $a^{4k+2}+1$, since it would then also have to divide the difference

$$a^{4k+2}+1 - (a^{4k+2}-1) = 2$$

which is impossible for an odd prime. $a^{4k+2}+1$, however, can be factored into a product with one factor of a^2+1, as the student can check. Thus, since p cannot divide $a^{4k+2}+1$, it cannot divide a^2+1 either, and so the possible prime divisors of a^2+1 must have the form 4k + 1.

<u>Case 3</u>: If n=2, then $a^{2^n}+1 = a^4+1 = (a^2)^2+1$, and by Case 2 any prime divisor must have the form 4k + 1. Looking at this in terms of multiples of 8, 4k + 1 can be of the form 8k + 1 or 8k + 5. By reasoning similar to Case 2, p = 8k + 5 can be eliminated (the student should check this), leaving p = 8k + 1 as the only choice.

By now, Euler had figured out the pattern (have you?) and determined that if a is even and p is an odd prime, then:

if p divides $a + 1$, then $p = 2k + 1$,

if p divides $a^2 + 1$, then $p = 4k + 1$,

if p divides $a^4 + 1$, then $p = 8k + 1$,

if p divides $a^8 + 1$, then $p = 16k + 1$,

if p divides $a^{16} + 1$, then $p = 32k + 1$,

if p divides $a^{32} + 1$, then $p = 64k + 1$,

etc

In general, this says that

if p divides $a^{2^n} + 1$, then $p = (2^{n+1})k + 1$.

If $a=2$, which is certainly even, this is the type of expression Fermat was talking about in his conjecture. The first unverified case of Fermat's conjecture occurs if $a=2$ and $n=5$, so Euler knew that the only possible prime factors of $2^{2^5} + 1 = 2^{32} + 1$ must look like $64k + 1$. There are not an overwhelming number of primes of this form, and the fifth one Euler tried, corresponding to $k=10$, was 641, which does indeed divide $2^{32} + 1$. This represents a huge improvement over checking all the primes, one at a time, by hand, because 641 is the 114th prime and in the 18th century all calculations were done by hand! The student should verify that for $k=1$ to 9, $64k + 1$ either is not prime or does not divide $2^{32} + 1$.

Any function defined in the interval $(-\pi,\pi)$ can be represented in that interval by a series of the form

$$\frac{1}{2}a_0 + \sum_{n=1}^{\infty}(a_n \cos nx + b_n \sin nx),$$

where the a's and b's are suitable real numbers. From Joseph Fourier's presentation to the French Academy of Sciences, December 21, 1807.

When Joseph Fourier presented his paper on the diffusion of heat to the Institut de France (French Academy of Sciences) in 1807, the secretary for mathematical and physical sciences was the astronomer Jean Baptiste Joseph Delambre, who asked Lagrange, Laplace, Lacroix, and Monge (all mathematicians) to examine the paper. Three of these four apparantly were satisfied with Fourier's work, but the fourth, Lagrange, strongly disagreed with several features, especially the series results like the one above, and the paper was rejected. However, to encourage Fourier, the Academy made the problem of heat propagation the subject of a grand prize to be awarded in 1812. Fourier submitted a revised paper in 1811 which won the prize, but this too was criticized for lack of rigor, and so was not published by the Academy. Not until 1824, when Fourier himself became secretary of the Academy, was his 1811 paper published in the Academy's *Memoires*.

If a function f(x) can be represented as above, and if termwise integration from $-\pi$ to π is allowed, then the values of the coefficients in the series are given by the formulas

$$a_n = \frac{1}{\pi}\int_{-\pi}^{\pi} f(x)\cos(nx)\,dx \quad \text{and} \quad b_n = \frac{1}{\pi}\int_{-\pi}^{\pi} f(x)\sin(nx)\,dx.$$

The student should derive these formulas, which make use of the *orthogonality* of the sine and cosine functions over the interval $(-\pi,\pi)$. Today, these values of a_n and b_n are known as the *Fourier coefficients* of the function f(x), and the trigonometric series

$$\frac{1}{2}a_0 + \sum_{n=1}^{\infty}(a_n \cos nx + b_n \sin nx)$$

with these coefficients is called the *Fourier series* for f(x). Of course, the big question is : Does the Fourier series for f actually converge to the function values of f(x) for x in $(-\pi,\pi)$? Fourier's claim was that the answer was "yes" for <u>any</u> f(x), and this was the point on which he was most criticized by Lagrange and others. Actually, neither Fourier nor his critics were entirely correct, but time has vindicated Fourier more. The following theorem was proved by the German mathematician Peter Gustav Lejune Dirichlet in 1829.

> <u>Dirichlet's Theorem</u>: If in the closed interval $[-\pi,\pi]$ f(x) is single-valued and bounded, has only a finite number of discontinuities, and has only a finite number of maxima and minima, then the Fourier series of f(x) converges to f(x) at all points where f(x) is continuous and to the average of the right-hand and left-hand limits of f(x) at each point where f(x) is discontinuous.

Notice that this theorem gives *sufficient* conditions for convergence of the Fourier series, but not *necessary* conditions. More general sufficient conditions have been found, but so far no conditions are known to be *both* necessary and sufficient. Dirichlet's conditions are good enough to handle many of the periodic functions that arise in physics and engineering, and his theorem is often found in textbooks dealing with Fourier series.

To get his results, Fourier did not use the orthogonality of the trigonometric functions, but instead went through an incredible series of formal manipulations to arrive at the formulas for the coefficients in his series. He began, dealing with the sine series for an arbitrary function, by expanding each sine function in a power series (the usual Taylor series), and then rearranging the terms to get a power series for his "arbitrary" function. But the importance of Fourier's results is due to his claim that functions that *don't necessarily have* Taylor series expansions can be represented by Fourier series, so the method is suspect already. Undaunted, Fourier proceeded to find the coefficients in this (nonexistent) power series usung two more inconsistent assumptions, and obtained an answer involving division by a divergent infinite product! At this point Fourier had "proved" that all the coefficients in the series representing the arbitrary function vanish, which can only lead to the conclusion that the function is identically zero, a conclusion Fourier had no intention of drawing. Thus, he worked some more on the formula, and after some more formal manipulations arrived at the simple result above. If this was the end of the matter, Fourier would not be particularly famous today, for the same formula had been derived 30 years earlier by Euler, although this was unknown to Fourier. (Incidentally, after getting the formula for the coefficients, both Euler and Fourier realized that the result could have been easily obtained using the orthogonality of the sines.) Euler believed that *only* functions given everywhere by a single analytic expression could be represented by a sine or cosine series, however, and did not extend his formula for the coefficients beyond these special cases. Fourier, on the other hand, was the first to observe that the formula for the coefficients and the orthogonality derivation remain valid for any graph which bounds a definite area, and to Fourier this meant any graph at all.

The concept of a "function" is thus one of the ideas of mathematics which was greatly influenced by Fourier's work. Before him, there was a distinction between "function" and "graph". It was agreed that every function had a graph, but that every graph represents a function was not accepted by analysts before Fourier. Thus, a graph defined piecewise by several different formulas did not represent a function to, say, Euler. One of the things Dirichlet did before proving his theorem discussed above was to give a clear, explicit definition of a function . Today, when mathematicians and engineers construct the Fourier series for generalized functions such as the Dirac delta function, divergent series or integrals are encountered, but formal manipulations (in the spirit of Fourier!) have meaning in the context of new theories that are descendents of Fourier's work.

For more detail about Fourier and his work, the interested student should consult the references by Grattan-Guinness and by Langer. Grattan-Guinness contains a very slightly edited version of Fourier's work, in French, with commentaries in English. Langer gives a survey of Fourier series, and is intended to be "readable for students who in mathematics have gone but little beyond a good course in the calculus."

Cantor's Theorem

The set of all real numbers between 0 and 1 can not be put into a one-to-one correspondence with the natural numbers, $\mathbb{N}$.

If M is any set and if $\mathcal{P}(M)$ denotes the set whose elements are all the subsets of M, then M can not be put into a one-to-one correspondence with the set $\mathcal{P}(M)$.

Georg Cantor

Infinity. The concept of an infinite set has been a problem for mathematicians, philosophers, and others for centuries. Zeno, Aristotle, Galileo, Gauss, Cauchy, and many others have struggled with the idea of infinity, and one of the difficulties non-mathematicians today have with mathematics is that when a topic involving infinity comes up, it seems to them that "common sense" often has flown out the window. The paradoxes of Zeno of Elea (which the student should look up) are perhaps the first place where some of the difficulties are indicated. Aristotle distinguished between the *actually* infinite and the *potentially* infinite and was of the opinion that only the potentially infinite could exist. The idea of using a one-to-one correspondence to "compare" infinite quantities is a very old one, but since two line segments of unequal length, or the set of positive integers and the set of squares of positive integers can be put into ono-to-one correspondences, common sense takes a beating. Galileo knew these two examples, and partly because of them he rejected the idea of comparing infinities. Gauss cautioned against "the use of an infinite quantity as an actual entity", and the fact that a part can be put into one-to-one correspondence with the whole (which is characteristic of infinite sets) seemed contradictory to Cauchy.

Toward the end of the nineteenth century, the first truly mathematical treatment of infinite sets was done by Georg Cantor, who exploited the old idea of one-to-one correspondence to give a firm basis for "counting" with infinities. Cantor introduced the following definition:

> Two sets M and N are equivalent (or of the same cardinality) if it is possible to put them by some law in such a relation to one another that to every element of each one of them corresponds one and only one element of the other.

Let $\mathbb{N} = \{1,2,3,4,...\}$ be the set of natural, or counting, numbers. It is not difficult to show (and the student should do so) that $\mathbb{N}$ is equivalent to, among others, the following sets:

{2,4,6,8,10,...}, the even natural numbers,

{...,-3,-2,-1,0,1,2,3,...}, the integers,

{1,4,9,16,25,...}, the squares of the integers.

Cantor used the set ℕ as a prototype for his first *transfinite* cardinal number. He said that any set equivalent to ℕ would be called *countably infinite* and introduced the notation $\aleph_0$ (aleph-zero) to represent the number of objects in a countably infinite set. The word *denumerable* is sometimes used instead of countably infinite today.

The next question naturally was: Are all infinite sets countably infinite? Notice that Cantor's work provides a way to test a set for this property, if the one-to-one correspondence can be found, or proved not to exist. A likely candidate for uncountability was the set ℚ of rational numbers, since there are infinitely many rationals between any two natural numbers. However, it turns out that ℚ is equivalent to ℕ ! This can be seen by writing the set ℚ as shown and following the arrows to get the correspondence with ℕ. (Note that any fraction which has already appeared is skipped.)

0	1	-1	2	-2	3	-3	....
	$\frac{1}{2}$	$-\frac{1}{2}$	$\frac{2}{2}$	$-\frac{2}{2}$	$\frac{3}{2}$	$-\frac{3}{2}$	....
	$\frac{1}{3}$	$-\frac{1}{3}$	$\frac{2}{3}$	$-\frac{2}{3}$	$\frac{3}{3}$	$-\frac{3}{3}$	....
	$\frac{1}{4}$	$-\frac{1}{4}$	$\frac{2}{4}$	$-\frac{2}{4}$	$\frac{3}{4}$	$-\frac{3}{4}$	....
	$\frac{1}{5}$	$-\frac{1}{5}$	$\frac{2}{5}$	$-\frac{2}{5}$	$\frac{3}{5}$	$-\frac{3}{5}$	....
	$\frac{1}{6}$	$-\frac{1}{6}$	$\frac{2}{6}$	$-\frac{2}{6}$	$\frac{3}{6}$	$-\frac{3}{6}$	....

ℕ :	1	2	3	4	5	6	7	8	9	10	11	12	...
	↑↓	↑↓	↑↓	↑↓	↑↓	↑↓	↑↓	↑↓	↑↓	↑↓	↑↓	↑↓	
ℚ :	0	1	$\frac{1}{2}$	1	2	$-\frac{1}{2}$	$\frac{1}{3}$	$\frac{1}{4}$	$-\frac{1}{3}$	-2	3	$\frac{2}{3}$	...

Thus, Cantor was able to match the sets ℕ and ℚ according to his definition, and the somewhat surprising but inescapable conclusion is that there are as many rational numbers as there are positive integers. Cantor also proved that the set of *algebraic* numbers (recall Chapter 5) is countable, and the student should look up this proof.

There is, however, an infinite set which is not equivalent to ℕ, and this is the subject of Cantor's first great theorem.

Theorem: The set of all real numbers between 0 and 1 can not be put into a one-to-one correspondence with $\mathbb{N}$; instead, this set is uncountably infinite.

Proof: The proof uses a method that has come to be known as *Cantor's diagonal process* and is by *reductio ad absurdum.* Thus, the first step is to assume that there is a one-to-one correspondence between $\mathbb{N}$ and (0,1). This means that all the numbers in (0,1) can be listed in a sequence, say $\{r_1, r_2, r_3, r_4, r_5, \ldots\}$. Also, each r_i has a unique representation as a nonterminating decimal. (In order to write rational numbers as nonterminating decimals, recall that, for instance, $\frac{1}{2}$ can be written as .49999... instead of .5000... .) The sequence of r_i's can thus be displayed as follows:

$$r_1 = 0.a_{11}a_{12}a_{13}a_{14}\ldots$$
$$r_2 = 0.a_{21}a_{22}a_{23}a_{24}\ldots$$
$$r_3 = 0.a_{31}a_{32}a_{33}a_{34}\ldots$$
etc.

The symbol a_{ij} represents the digit in the jth decimal place of r_i, and therefore is one of the digits 0,1,2,3,4,5,6,7,8, or 9.

Cantor next constructed a real number b between 0 and 1 which does not appear on the list. One way to define such a b would be as follows:

Let $b = 0.b_1b_2b_3b_4b_5\ldots$, where b_k is chosen to be different from a_{kk}, the kth digit of r_k. This can be done in many ways, such as defining b_k to be

$$b_k = \begin{cases} 7 \text{ if } a_{kk} \text{ is } 0,1,2,3, \text{ or } 4, \\ 3 \text{ if } a_{kk} \text{ is } 5,6,7,8, \text{ or } 9. \end{cases}$$

The number b, defined this way, is clearly between 0 and 1, but it cannot be one of the r_k's because b differs from r_1 in the first decimal place, from r_2 in the second decimal place, from r_3 in the third decimal place, and so on. But this is a contradiction since it was assumed that all the numbers between 0 and 1 were among the r_k's. Therefore, there cannot be a one-to-one correspondence between $\mathbb{N}$ and (0,1), and thus the set of real numbers between 0 and 1 is not countably infinite.

Cantor, in discovering a "bigger" infinity than $\aleph_0$, defined a new cardinal number, c, (for *continuum*) to represent the cardinality of any set which could be put into a one-to-one correspondence with (0,1). This led to several new results, such as:

- $\aleph_0 < c$,
- $\mathbb{R}$, the set of all real numbers, has cardinality c,
- $\mathbb{R}\times\mathbb{R}$, the set of all points in the plane, has cardinality c, at which point Cantor is reported to have said, "I see it, but I do not believe it!".

Also, as is almost always the case in mathematics, Cantor's result led to more questions, the two principal ones being:

- Are there any infinities strictly between $\aleph_0$ and c?
- Are there any infinite numbers larger than c?

Cantor believed that the answer to the first question was "no", and this conjecture has come to be known as the *Continuum Hypothesis*. The Continuum Hypothesis has never been proved, and, as will be seen in the next chapter, is in fact unprovable using standard set theory. Cantor did succeed in answering the second question, and his result is the great theorem which bears his name.

Cantor's Theorem: If M is any set, and if $\mathcal{P}(M)$ denotes the set whose elements are all the subsets of the original set M, then M can not be put into a one-to-one correspondence with the set $\mathcal{P}(M)$.

Proof: $\mathcal{P}(M)$ is called the *power set* of M, and is also denoted by the notation 2^M, since for finite sets, if M has m elements, $\mathcal{P}(M)$ will have 2^m elements, as the student should verify. The general proof is again by contradiction, so assume there is a one-to-one correspondence between M and $\mathcal{P}(M)$. To help illustrate this, suppose M={a,b,c,d,...} and the correspondence is given by:

M		$\mathcal{P}(M)$
a	$\leftrightarrow$	{b,c}
b	$\leftrightarrow$	{d}
c	$\leftrightarrow$	{a,b,c,d}
d	$\leftrightarrow$	$\emptyset$
e	$\leftrightarrow$	M
f	$\leftrightarrow$	{a,c,f,g}
	etc.	

A new set B is now defined as follows:

"B is the set that consists of each element of M that is not a member of the subset (from $\mathcal{P}(M)$) to which it is matched."

To clarify this definition, notice that in the above example a, b, and d would be members of B, but c, e, and f would not.

Of course, B is a subset of M, and so it must correspond to some element of M in the one-to-one correspondence which is assumed. For definiteness, assume B corresponds to the element y in M. Now either y is an element of B or it isn't. If y is in B, then the definition of B asserts that y is not an element of the set with which it is matched, but that set is B! This is a contradiction. But if y is not in B, then y does not belong to the set with which it is matched, and so y is, by definition, in B! Again, this is a contradiction. The one-to-one correspondence assumed between M and $\mathcal{P}(M)$ thus can not exist, and the theorem is proved.

As a consequence of this theorem, Cantor has opened the door to an infinite heirarchy of infinities. If $\mathbb{R}$ denotes the real numbers, having cardinality c, then $\mathcal{P}(\mathbb{R})$ has cardinality greater than c, $\mathcal{P}(\mathcal{P}(\mathbb{R}))$ has cardinality greater still, and so on.

Gödel's Theorem

> For any consistent formal system F which contains the natural number system there are undecidable propositions in F; that is, there are propositions S in F such that neither S nor not-S is provable in F.
>
> Godel's Incompleteness Theorem

> For any consistent formal system F which contains the natural number system, the consistency of F cannot be proved in F.
>
> Kurt Godel, 1931

At the end of the nineteenth century, much work in the foundations of mathematics dealt with axiomatics and axiomatization with a goal being to make very clear exactly what did and what did not constitute a proof. (See especially 2, 6, and 7 on the reading list.) One of the major works was *Principia Mathematica* by Bertrand Russell and Alfred North Whitehead, in which they attempted to develop all of mathematics from the notions of logic and sets. In an axiomatization of a mathematical system, the following general pattern is adhered to:

- There are a number of technical terms, such as elements, relations among elements, operations performed on elements, etc., which are chosen as *undefined terms*.

- There are a number of statements about the undefined terms which are chosen as accepted, but unproved, statements. These are the *axioms*.

- All other technical terms are defined by means of previously introduced terms.

- All other statements are logically deduced from previously accepted or established statements. These are the *theorems*.

Thus, everything is in terms of a formal system, where things are expressed using a fixed vocabulary according to a fixed grammar, and theorems are obtained from axioms according to fixed rules. *Principia Mathematica* was an attempt to evolve all of mathematics in one system.

An axiomatic system is *consistent* if it contains no contradictory statements. For example, number theory would be inconsistent if both the statement "2 is a prime number" and the statement "2 is a composite number" were theorems in number theory. Knowing whether an axiomatic system is or is not consistent is thus an important objective, and the question of the consistency of a major part of classical mathematics can be reduced to the question of the consistency of either the natural number system (with Peano's axioms) or set theory (with the Zermelo-Fraenkel axioms). Therefore the consistency of the natural numbers (ordinary arithmetic) received much study.

A set of axioms is called *complete* if it is impossible to add another axiom that is independent (not provable from) the given set and also consistent with the given set (without the need to introduce new undefined terms). Gödel's result, now known as Gödel's Incompleteness Theorem, says that the natural number system cannot be both consistent and complete. Another of his results, given above, is that one of the unprovable theorems of the natural number system is the consistency of the system!

One of the consequences of Gödel's work is that a distinction must be made in mathematics between the two concepts of *truth* and *provability within an axiom system*. There are true, but unprovable, statements! For example, consider the following:

This sentence is not provable (in axiom system X).

There are two possibilities - the sentence is provable or it isn't. If it is provable, then it is true, and what it says is true, but it says that it is *not* provable. This is an obvious contradiction and leads to mathematical chaos. Thus, the only alternative is that indeed the sentence is not provable, as it is saying. So the sentence must be true!

As can be seen in the above example, Gödel's theorem involves the idea of *self-reference*, an idea which has fascinated many people (not only mathematicians) throughout history. Douglas R. Hofstadter has done more than anyone else to explain Gödel's theorem to a general audience, and the interested student can find out more in his article in Campbell and Higgins (this article can also be found in the March 1982 issue of the *Two-Year College Mathematics Journal*, which contains another article about Gödel as well.), or, for the truly ambitious, his book *Godel, Escher, Bach; An Eternal Golden Braid* (New York: Basic Books, 1979; Vintage Books, 1980).

Reading List

(R) = On reserve in the Library, (H) = Available from Prof. Hall

1. *Historical Topics for the Mathematics Classroom.* Introductory material in Chapters II and IV through VIII, Capsules 9, 14-18, 23, 26, 27, 44-46, 50-53, 55, 58, 67, 71 77, 82, 84, 85, 91, 98, 104-106, 109, 111. (R),(H)

2. *Mathematical Thought from Ancient to Modern Times,* Morris Kline. Chapters 8, 13, 17, 18, 26, 43, 51. (R)

3. *Mathematics in Western Culture*, Morris Kline. Chapters X, XV, XXV. (R)

4. *A Source Book in Mathematics, 1200-1800*, D.J. Struik, Ed. Chapter I, secs. 6, 9; Chapter III, sec 11; Chapter V, pp. 270-291 and 383-386. (R)

5. *Foundations of Euclidean and Non-Euclidean Geometry*, Ellery B. Golos. Part 3, Non-Euclidean Geometry. (R)

6. *The Mathematical Experience*, Philip J. Davis and Reuben Hersh. Chapter 5, Selected Topics in Mathematics. (R),(H)

7. *Mathematics - People, Problems, Results*, Douglas M. Campbell and John C. Higgins, Eds. Volume I, pp. 239-288 (see also the appendix), Volume II, pp. 183-208. (R)

8. *Fourier Series*, R.E. Langer. (Slaught Memorial Paper, *American Mathematical Monthly,* 1947) (R),(H)

Reading List Assignment

- Each student must read two (2) of the above eight items and write a paper (2 to 4 pages, typed, doublespaced) on each one read.
- The first paper is due October 9.
- The second paper is due December 4.
- The papers should contain a summary of what was read, together with the student's reactions, criticisms, impressions, etc.

Bibliography

(R) = On reserve in the Library, (H) = Available from Prof. Hall

Archibald, Raymond Clare: *Outline of the History of Mathematics*, Slaught Memorial Paper, *American Mathematical Monthly*, Supplement to Vol. 56, pp. 1-114 (1949).(R),(H)

Ayoub, Raymond: *An Introduction to the Analytic Theory of Numbers*. Providence: American Mathematical Society 1963.(R)

Bell, Eric Temple: *Men of Mathematics*. New York: Simon and Schuster 1937. (R)

Bold, Benjamin: *Famous Problems of Mathematics, A History of Constructions with Straight Edge and Compasses*. New York: Van Nostrand Reinhold Company 1969. (R)

Bollobás, Béla, Ed.: *Littlewood's miscellany*. Cambridge: Cambridge University Press 1986. (H)

Boyer, Carl B.: *A History of Mathematics*. New York: John Wiley and Sons, Inc. 1968. (R),(H)

Campbell, Douglas M. and Higgins, John C., Eds.: *Mathematics, People Problems, Results* (3 Vols). Belmont: Wadsworth International 1984. (R)

Cardano, Girolamo: *The Great Art*, (translated and edited by T. Richard Witmer). Cambridge: The M.I.T. Press 1968. (R)

Davis, Philip J. and Hersh, Reuben: *The Mathematical Experience*. Boston: Birkhäuser Boston 1981. (R),(H)

Dickson, Leonard E.: *First Course in the Theory of Equations*. New York: John Wiley and Sons, Inc. 1922. (R)

Dunham, William: *The Great Theorems of Mathematics - Mathematics Supplement*. Hanover: Department of Mathematics, Hanover College 1983. (H)

Edwards, H.M.: *Riemann's Zeta Function*. New York: Academic Press 1974. (R)

Eves, Howard W.: *In Mathematical Circles* (2 Vols.). Boston: Prindle, Weber & Schmidt, Inc. 1969. (R)

Eves, Howard W.: *Mathematical Circles Revisited*. Boston: Prindle, Weber and Schmidt, Inc. 1971. (R)

Eves, Howard W.: *Mathematical Circles Adieu*. Boston: Prindle, Weber and Schmidt, Inc. 1977. (R)

Eves, Howard W.: *A Survey of Geometry, Vol. 1*. Boston: Allyn and Bacon 1963. (R) (Unfortunately, Vol. 2 is not in the UMR Library (yet).)

Eves, Howard W.: *An Introduction to the History of Mathematics, 3rd ed.* New York: Holt, Rinehart and Winston 1969. (R)

Eves, Howard W.: *Great Moments in Mathematics (Before 1650)*. The Mathematical Association of America 1980. (R)

Eves, Howard W.: *Great Moments in Mathematics (after 1650)*. The Mathematical Association of America 1981. (R)

Eves, Howard and Newsom, Carroll V.: *An introduction to the Foundations and Fundamental Concepts of Mathematics*. New York: Holt, Rinehart and Winston 1961. (R)

Golos, Ellery B.: *Foundations of Euclidean and Non-Euclidean Geometry*. New York: Holt, Rinehart and Winston 1968. (R)

Grattan-Guinness, I.: *Joseph Fourier 1768-1830*. Cambridge: The M.I.T. Press 1972. (R)

Greenberg, Marvin Jay: *Euclidean and Non-Euclidean Geometries, Development and History*. San Francisco: W.H. Freeman and Company 1980. (R)

Hardy, G.H. and Wright, E.M.: *An Introduction to the Theory of Numbers*. Oxford: Oxford University Press 1979. (R)

Heath, T.L., Ed.: *The Works of Archimedes*. New York: Dover 1912. (R)

Herivel, John: *Joseph Fourier, the Man and the Physicist*. Oxford: Clarendon Press 1975. (R)

Hobson, E.W. *et al.*: *Squaring the Circle and Other Monographs*. Chelsea Publishing Co. (R)

Kline, Morris: *Mathematics in Western Culture.* New York: Oxford University Press 1953. (R)

Kline Morris: *Mathematical Thought from Ancient to Modern Times.* New York: Oxford University Press 1972. (R)

Langer, R.E.: *Fourier's Series,* Slaught Memorial Paper, *The American Mathematical Monthly,* Supplement to Vol. 54, pp. 1-86 (1947). (R),(H)

Meschkowski, Herbert: *Ways of Thought of Great Mathematicians* (translated by John Dyer-Bennet). San Francisco: Holden-Day, Inc. 1964. (R)

National Council of Teachers of Mathematics: *Historical Topics for the Mathematics Classroom, Thirty-first Yearbook.* Washington: National Council of Teachers of Mathematics 1969. (R),(H)

Nagel, Ernest and Newman, James R.: *Goedel's Proof.* New York: New York University Press 1964. (R)

Newman, James R.: *The World of Mathematics (4 Vols.).* New York: Simon and Schuster 1966. (R),(H)

Niven, Ivan: *Numbers: Rational and Irrational.* Washington: The Mathematical Association of America 1961. (R)

Niven, Ivan: *Irrational Numbers.* The Mathematical Assosiation of America 1963. (R)

Smith, David Eugene: *A Source Book in Mathematics.* New York: McGraw-Hill Book Company, Inc. 1929. (R)

Struik, D.J.: *A Source Book in Mathematics, 1200-1800.* Cambridge: Harvard University Press 1969. (R)