History and philosophy of Mathematics
Course notes, Louis Rowen April, 2010; not for general distribution

CONTENTS

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

(42) Hilbert's third problem
(43) Hilbert's second problem - Foundations of set theory
(44) Zermelo-Frankel axioms
(45) Cardinals
(46) Gödel
(47) Recursive functions and computability
(48) Axiom of Choice
(49) The age of paradoxes
(50) Geometric paradoxes
(51) New directions in the 20th century
(52) Computational mathematics
(53) Complexity theory
(54) The golden age of algebra
(55) Algebraic topology
(56) Algebraic K theory
(57) Physicists classify low-dimensional manifolds
(58)
(59)
(60)
(61)
(62)
(63)

What is mathematics?

Definition from the Random House Dictionary

Mathematics: The systematic treatment of magnitude, relationships between figures and forms, and relations between quantities expressed symbolically.

How does this relate to modern algebraic geometry?

Wikipedia:

"Mathematics is the study of quantity, structure, space, and change. Mathematicians seek out patterns,[2][3] formulate new conjectures, and establish truth by rigorous deduction from appropriately chosen axioms and definitions.[4]

Mathematics is used throughout the world as an essential tool in many fields, including natural science, engineering, medicine, and the social sciences. Applied mathematics, the branch of mathematics concerned with application of mathematical knowledge to other fields, inspires and makes use of new mathematical discoveries and sometimes leads to the development of entirely new mathematical disciplines, such as statistics and game theory. Mathematicians also engage in pure mathematics, or mathematics for its own sake, without having any application in mind, although practical applications for what began as pure mathematics are often discovered.[8]"

Alternative Definition? Mathematics is the use of a given set of assumed facts (axioms) to deduce other assertions by means of accepted methods of inference.

A key difference with other forms of inquiry is that mathematical truth is its independence of time; a proof will always be valid under those axioms.

Wikipedia: "There is debate over whether mathematical objects such as numbers and points exist naturally or are human creations. The mathematician Benjamin Peirce called mathematics "the science that draws necessary conclusions".[5] Albert

Einstein, on the other hand, stated that "as far as the laws of mathematics refer to reality, they are not certain; and as far as they are certain, they do not refer to reality."[6]"

In this course, we do not deal with the interpretation of mathematics, except where it affected mathematical development. Thus the question of whether $2+2=4$ is trivial for us, since we are not concerned about determining when we have 2.

Likewise the difficulty of deducing by strict mathematical rules was observed as early as the ancient Greek Epimenides: Is the sentence " I am lying" true or false?

Problems with definition:

(1) Perhaps the axioms are not comprehensive enough to yield all theorems that we would like to obtain (How do we know this also?)
(2) Perhaps the axioms are inconsistent
(3) How do we know that a proof is true?

Gödel's incompleteness theorem shows that any consistent set of axioms will NEVER suffice to obtain all assertions. There are various famous axioms which have been shown to be independent of the previous ones: Euclid's 5th postulate, Axiom of Choice, Continuum hypothesis, which we shall discuss later.

Examples:

(1) The sphere-packing problem (Kepler's conjecture), Wu-Yi Hsiang (1990), published in International Journal of Mathematics (1993).
(2) Wile's proof of Fermat's Last Theorem (Annals of Math. 1995). His original proof was spotted wrong only after a half year, by a single person.
(3) The Classification (of simple groups). Simple group has no normal subgroups other than itself and $\{e\}$. For an Abelian group, any subgroup is simple. So any simple Abelian group is cyclic (since it has a subgroup generated by any given element). The order is prime; thus the only cyclic Abelian groups are isomorphic to $\mathbb{Z}_p$. So question is what are the finite nonAbelian simple groups, called FNASG for short? Galois knew A_n was simple for $n \geq 5$, and even before Hilbert's time, the classical simple groups (PSL, and those analogously arising from bilinear forms) had been discovered. On the other hand, Mathieu (1860-1867) had found five simple permutation groups. Burnside (1906?) proved that the order of a FNASG has to be divisible by at least 3 distinct prime numbers.

    The problem became mainstream mathematics when, perhaps inspired by Chevalley's work in obtaining simple groups from Lie theory, Brauer (1950's) pushed for a classification, and proved a sample theorem classifying those simple groups for which the centralizer of an element of order 2 is cyclic. Feit-Thompson (1963) proved the order of a FNASG is even. In the 1970's and 1980's, Gorenstein (and Aschbacher) organized a program, apportioning out important cases to a dozen mathematicians, and 15,000 journal pages later, announced there was a proof. Gorenstein started a projected series of 5 volumes which would contain a complete proof from beginning to end, but died in 1992 after publishing only 1 of the 5 volumes. The Classification has since been used in dozens of theorems in group theory and its applications. The only problem is that it turned out that one of the key cases (quasi-thin groups) was not complete. The author (Mason) wrote a 500-page manuscript where somewhere in the middle of the argument he simply stopped, but hardly anyone had paid attention. Aschbacher and

Smith (2004) finally finished this case, and by 2009 it was generally believed that the proof is complete. R. Solomon is now overseeing a project of 12 volumes which hopefully will contain the full proof, but as of now a unified proof has not been written down.

(4) Four-color map problem (Francis Guthrie). Can a map be colored with 4 colors, such that any two adjacent countries have different colors? (Ignoring water) Guthrie asked his brother, who asked De Morgan, who wrote to Hamilton in 23 October 1852.

1879. The British mathematician Kempe published a "proof" in *Amer. J. Math.*. Soon elected as Fellow of the Royal Society of Math. and later knighted.

1880. Peter Guthrie Tait published a *second* "proof."

1890. Percy John Heawood found error in Kempe's proof, but showed 5 colors is enough. He also recognized that Tait's proof is incomplete, but a counterexample to Tait's main claim was only found in 1946 by Tutte.

1960's. Heinrich Heesch discovered reducing algorithms.

1976. W. Haken and K. Appel (U. Illinois at Urbana) reduced to 1482 basic maps (published in Ill. J. Math.) Errors kept cropping up, so Appel and Haken wrote an error-correcting routine, which (until 1989) had taken care of all mistakes which came up.

1997. Robertson, Sanders, Seymour, and Thomas reduced the unavoidable configurations to 633, and streamlined the reduction process by a factor of 10. All in all, they provided a quadratic algorithm to color any map (as opposed to the quartic algorithm by Haken and Appel.)

As we shall see, the great early civilizations (Bablyonians, Egyptians, and Chinese) all had their special contributions to mathematics. Wikipedia: " The systematic study of mathematics in its own right began with the Ancient Greeks between 600 and 300 BC. ... most notably in Euclid's Elements. Mathematics continued to develop, for example in China in 300 BCE, in India in 100 CE, and in Arabia in 800 CE, until the Renaissance, when mathematical innovations interacting with new scientific discoveries led to a rapid increase in the rate of mathematical discovery that continues to the present day."

The mathematics of the ancients

Before starting, let me stress that, for convenience, we use modern notation, including use of symbols for unknown quantities; this is anachronistic, since they were not used until the Arab mathematicians of 1000 years ago.

All of the famous ancient civilizations had well developed mathematical theories, which were utilized for counting and measuring. Uses of numbers in the tora include counting days in creation, calendar, measurements for construction, counting people and animals, and monetary transactions.

The word *geometry* means "measure the earth", and the ancients also wanted to determine the positions of the stars and planets in the sky, since they believed this had an impact on their day-to-day lives. Thus arithmetic, geometry and astronomy (or astrology) became prime forces in the development of mathematics.

Sometime in the beginning of civilization humans began to count both with the notion of ordinal and cardinal. This is reflected in Bereshit, in the account of creation (Vayehi Erev Vayehi Boker, Yom Echad; Vayehi Erev Vayehi Boker,

Yom Sheni (note this is ordinal). One of the crucial advances in counting was a notation for counting. Early systems largely involving gematria, assigning a number value for each letter. This is known to us through midrashim on the tora, and also through Roman numerals, which were used throughout the Greco-Roman world. However, it was extremely difficult to carry out even the most fundamental arithmetic operations: What is DCCCLIX times CCXLVII? In fact, the Roman contribution to mathematics was negligible. Their main fame in this regard was for murdering Archimedes.

By far more advanced were the Babylonians [Mi, p. 48] who invented a "place" system to the base 60 by the year 1900 BCE-1600 BCE. This is called the Old Babylonian period.

They had symbols for the the numbers 1 through 60 but then used transposition to represent numbers greater than 60; for example (in modern notation) 1,15 denotes 75 and 2,15 denotes 135. (Comma is part of the modern representation.) They also had decimal-type notation for fractions. Main problem is that they did not have a 0, so 65 and 3605 would both look like 1,5, whereas we can differentiate between 15 and 105.

Tablet Plimpton 322 (Analyzed by O. Neugebauer and A. Sachs).

One incredible tablet lists 15 solutions to integral sides of right triangles, in decreasing angles (albeit with four numerical errors); they give only the two larger sides, since $a^2 = c^2 - b^2 = (c+b)(c-b)$ can then be calculated easily:

$1, 59$	$2, 49$
$56, 7$	$1, 20, 25$
$1, 16, 41$	$1, 50, 49$
$3, 31, 49$	$5, 9, 1$
$1, 5$	$1, 37$
$5, 19$	$8, 1$
$1, 59$	$2, 49$
$38, 11$	$59, 1$
$13, 19$	$20, 49$
$8, 1$	$12, 49$
$1, 22, 41$	$2, 16, 1$
45	$1, 15$
$2, 41$	$4, 49$
$29, 31$	$53, 49$
56	$1, 46$

In modern notation:

b	c	$\frac{b}{c}$	factors of a
119	169	.704	$2, 3, 5$
3367	4825	.698	$2, 3$
4601	6649	.692	$2, 3, 5$
12709	18541	.6854	$2, 3, 5$
65	97	.6701	$2, 3$
319	481	.6632	$2, 3, 5$
2291	3541	.647	$2, 3, 5$
799	1249	.6397	$2, 3, 5$
481	769	.6255	$2, 3, 5$
4961	8161	.608	$2, 3, 5$
45	75	.6	$2, 3, 5$
161	289	.5571	$2, 3, 5$
1771	3229	.5485	$2, 3, 5$

Note that the sine of the smaller angle ($\frac{b}{c}$) is always decreasing, and the factors of the third side are always from 2,3, and 5. (For example, in the second line. Here $c - b = 1458 = 2 \cdot 3^6$ and $c + b = 8192 = 2^13$.) This later fact is very significant, because it indicates that the calculations were not purely empirical, and also that they had some methods for multiplying by 2,3, and 5. (Since these divide 60, their multiplication tables are far simpler than for the other numbers.) If one works this out using Pythagorean triples, the computations are not that difficult.

Other tablets describe solutions of various linear algebraic equations. See tablet A24194 transcribed in Midonick (pp. 77-83). They also could solve certain equations of the form $a^x = b$, so in this sense knew the rudiments of logarithms.

The Babylonians also were far advanced in using mathematics in astronomy, i.e. to calculate the positions of the heavenly bodies (although their physical concept of the universe was most primitive). Avraham Avinu, who left Babylon around this time, therefore had access to the most advanced mathematical methodology of ancient times. The one disadvantage of the Babylonian approach was that it, like the Egyptian, was very application oriented, and there is no record of the Babylonians studying abstract mathematics.

Egyptian mathematics. The Egyptians had crude arithmetic (based on successive doubling and halving), but developed measurements well enough to build the pyramids. The famous "Moscow papyrus" (Also the "Rhine papyrus") describes the area of the triangle and trapezoid. They also had the formula $(\frac{8}{9}d)^2$ for the area of a circle with diameter d. This makes π to be $4\frac{64}{81} = 3.1604$. (Interesting note: There is a hint in the Bible that π is $3 \times \frac{111}{106}$ which gives the value 3.1415. The hint is that *kav* is spelled *kaveh* when describing the circumference of a circle, which hints the numerical value of kav (106) is replaced by that of kaveh (111). The Egyptians developed triangulation, the division of polygons into triangles in order to measure area (since the area of a triangle is well known). Interestingly enough, this method does not work in 3 dimensions (see discussion of Hilbert's 3rd problem). However, the influence of the ancient Egyptians was limited by their lack of a workable number system.

Chinese mathematics. The Chinese knew how to solve elementary algebraic equations, and already had encoded arithmetic in the legendary text called the K'iu-ch-ang, which by tradition dates from around 2500 BCE.

It is possible that the Chinese were the first with many major discoveries; archeologists found bones with markings, starting with pre-historic times. The Oracle bone script of Shang dynasty (14th to 11th century BCE) has a complete (non-place) decimal numeral system. Further,there are separate symbols for 40,50,60,70,80,90,100,200,300...900, 1000,2000,....9000, 10000, up to 40000. There are indications that the Chinese had a place notation in the "Spring and Autumn" period, from the second half of the 8th century BCE to the first half of the 5th century BCE. Also cf. [OL], which claims that the Chinese book Yi-King (the book of changes) contains a description of a binary positional system with zero. If he was right, the zero is from China.

Unfortunately the emperor Ts'in Shih Huang-Ti declared possession of mathematical works a capital crime, and burned all known books. This greatly reduced their impact on world culture. Chang Tsang (b. 152) resurrected what he could. Discovered remnants (-1000) contain a statement of the Pythagorean theorem! The Chinese were masters in the art of numbers, including magic triangles, powers of numbers, mostly in terms of mystical properties.

The Classical period

The Greeks developed mathematics into a far-reaching science, bringing in applications to mechanical physics, and developing astronomy to heights which would only be matched 1500 years later. Most of our knowledge is based on the historian Procleus (412-485 CE), so there is much uncertainty. However, there are main periods, identified with the mathematical giants of antiquity.

Pythagoras of Samos (-569– -475?, or c. 420 BCE?) is best remembered for stating the Pythagorean Theorem (although it was already known by the Babylonians, and probably also the Chinese and Egyptians). (Classical proofs use similar triangles. Easy proof: Inscribe square of side c into square of side $a + b$.

Pythagoras was perhaps the first person to study numbers as abstract entities. He believed that the essence of matter was contained in numbers. Thus his very important school (the Philosophs), established in Samos (and later in Italy), studied the properties of numbers, often with mystical overtones. They constructed numbers by means of compass and straight edge, in particular rational numbers which can be constructed using parallel lines. In fact, the Greeks, lacking a decent number system, approached most problems geometrically. This is one reason why the Greeks only considered positive numbers. This should be borne in mind throughout the study of ancient Greek mathematics.

Unfortunately one of the students, Hippasus of Metapontum, proved that $\sqrt{2}$ is irrational. For this unspeakable crime he was sentenced to death.

Although Hippasus' proof was geometric, here is a modern algebraic proof: We start with the fact that if a^2 is even then a is even. Suppose $2 = \frac{a^2}{b^2}$ We shall show both a and b are even, and then cancel 2 ad infinitum. But $b^2 = 2a^2$ is even, so b is even, and writing $b = 2c$ we see that $2c^2 = a^2$ is even, implying a is even, as desired. His reward was to be drowned by his colleagues for his blasphemy.

Nevertheless, this awareness of the difference between rational and irrational numbers was a major advance, since it advanced numbers from a mere tool of measurement to an object of learning. It also gave rise to the question of which numbers are constructible by means of compass and straight edge. This gave rise

to a number of constructions:

(1) Constructing a perpendicular (anach) from a given point of a line;
(2) Constructing a perpendicular from a given point outside a line to the line;
(3) Constructing a line parallel to a given line, through a given;
(4) Constructing the product and ratio of two numbers (using similar triangles);
(5) Constructing the square root of a number (since $(1+a)^2-(1-a)^2=4a$.)

Four famous problems involving construction of numbers:

(1) Doubling the cube;
(2) Trisecting the angle;
(3) Squaring the circle;
(4) Constructing a regular n-gon for $n \geq 7$.

Since the square root of any natural number could be constructed, the Greeks of Pythagorus' school knew how to construct roots of quadratic equations.

Although their method was geometric, we express it in algebraic terms, in modern notation. Suppose we want to solve the equation $x^2 = ax+b$. This is equivalent to finding two numbers $x > y$ such that $x - y = a$ and $xy = b$. Putting

$$z = x - \frac{a}{2} = y + \frac{a}{2}$$

yields

$$b = xy = (z + \frac{a}{2})(z - \frac{a}{2}) = z^2 - (\frac{a}{2})^2,$$

so $z = \sqrt{(\frac{a}{2})^2 + b}$. The same argument solves $y^2 + ay = b$. Significantly the Greeks could not solve $x^2 + b = ax$, since they thought geometrically and did not know about negative numbers.

The Pythagoreans had a sworn code of secrecy, and one reason their geometry survived was because they granted an exception to Hippocrates of Chios since he had lost his fortune and needed to make a living teaching geometry. His *Elements* include the squaring of a certain lune (whose argument is rather elementary).

A competing school of Eleatics was founded by Parmenides at Elea (now Velia), a Greek colony in Campania, Italy, in the early fifth century BCE. Other members of the school included Zeno of Elea and Melissus of Samos. Zeno is mostly known for his paradoxes, described below. Plato wrote about this school in the dialogue called the Parmenides, in which Plato describes a visit to Athens at a time when Zeno is "nearly 40" (Parmenides 127b) and Socrates is "a very young man" (Parmenides 127c). Assuming an age for Socrates of around 20, and taking the date of Socrates' birth as 470 BCE, gives an approximate date of birth for Zeno of 490 BCE, and death perhaps at 430 BCE.

The great philosopher Plato was surpassed by many mathematicians, but his school did provide the so-called *Platonic solids*; these are convex polyhedra whose faces are all congruent regular polygons, with the same number of faces meeting at each vertex. For example, the tetrahedron is comprised of four congruent equilateral triangles, and the cube (hexahedron) is comprised of six congruent squares. There are five of these Platonic solids (the others being the octahedron, made of eight equilateral triangles, the icosahedron, made of twelve regular pentagons, and the dodecahedron, made of twenty equilateral triangles, the first four of which were identified respectively in Plato's dialogue Timaeus c.360 B.C. with the four classical elements (fire, earth, air, and water). Although these solids were studied previously

by Pythagoras's school and have been in evidence long before, Plato's contemporary Theaetetus described all five Platonic solids. (We shall give a quick proof later, in the discussion of Euler's formula.)

One of the great early Greek mathematicians was Eudoxos of Cnidus(now Knidos, Turkey), 408 BCE - 355 BCE. Eudoxos was a Greek mathematician and astronomer who contributed to Euclid's Elements. He studied with Archytas who was a disciple of Pythagoras. Then Eudoxos studied at Plato's famous Academy in Athens. But he surpassed Plato in mathematics and established his own school in Cyzicus (Asia minor). After another trip to Athens, he returned to Cnidus, set up an observatory, and wrote two books, the *Mirror* and the *Phaenomena*. The planetary system of Eudoxos is homocentric, involving 27 spheres, and is given in his book, *On velocities* and is described by Aristotle in the latter's Metaphysics. He also wrote a book about the different peoples in the civilized world. He mapped the stars and compiled a map of the known world. Eudoxos is said to have doubled the cube (by means of intersections of curves) and is quoted extensively by Euclid and Aristotle.

Eudoxos introduced the *method of exhaustion*, based on Antiphon's earlier ideas of approximating the area of a circle by inscribing regular polygons with increasing numbers of sides. Eudoxos made Antiphon's theory rigorous and gave rigorous proofs of the theorems, first stated by Democritus, that

1. the volume of a pyramid is one-third the volume of the prism having the same base and equal height; and

2. the volume of a cone is one-third the volume of the cylinder having the same base and height.

The Golden age of Hellenistic Mathematics.

Classical mathematics reached its peak in Alexandria, which was founded by Alexander in 332 BCE to be the capital of the world. Ptolemy I Soter was a Macedonian general under Alexander the Great who became ruler of Egypt (323 BC283 BC) and founder of both the Ptolemaic Kingdom and the Ptolemaic Dynasty. Ptolemy was one of Alexander the Great's most trusted generals, perhaps his half-brother. Ptolemy is reputed to have founded the legendary library. Any traveller to Alexandria had to deposit his books at the library, where they were copied before being returned to him, and soon the library had over 600,000 books. This was a suitable home for the perhaps the world's first university at Alexandria. (Another famous ancient university was in Pergammum, whose library of Pergammum served as the reference center for many geometers. Julius Caesar is reputed to have destroyed the library in Alexandria, in order to subdue Egypt. To impress Cleopatra, Marc Anthony reconstituted the library of Alexandria, by raiding the library of Pergammum;

Euclid (b. 330 BCE) was a prominent mathematician in Athens who accepted the position as head of the mathematics department in Alexandria. His great work is Elements: axiomatic foundation of geometry, included conic sections, and number theory. Other books attributed to him include Data, De Divisionibus (on dividing areas), Optics, and Phaenomena (on the sphere). Euclid also formalized the argument of *reductio ad absurdum*.

Euclid's number theory:

(1) Euclidean algorithm for finding gcd of numbers (book VII, Prop. 1,2);
(2) Infinite number of primes (book IX, Prop. 20);
(3) Properties of primes (if $p|ab$, then $p|a$ or $p|b$, book VII, Prop. 30);

(4) Perfect numbers. We say n is *perfect* if the sum of the divisors of a number $S(n)$ equals 2n. Note that

$$S(p^i) = 1 + p + p^2 + \cdots = \frac{p^{i+1} - 1}{p - 1},$$

and $S(mn) = S(m)S(n)$ if m, n are relatively prime. Thus for $n = \prod p_u^{i_u}$, we have

$$S(n) = \prod \frac{p_u^{i_u+1} - 1}{p_u - 1},$$

and the question of whether a number n is perfect is to determine whether or not $\frac{S(n)}{n} = 2$

$$\prod_{u=1}^{t} \frac{p_u^{i_u+1} - 1}{p_u^{i_u}(p_u - 1)} = 2.$$

For $n = 2^i$, $\frac{S(n)}{n} = \frac{2^{i+1}-1}{2^i} = 2 - \frac{1}{2^i}$, so high powers of 2 are "almost" perfect; this is the basis of the following discussion. Indeed, taking $n = 2^i p$ where $p = 2^{i+1} - 1$ is prime, we have

$$\frac{S(n)}{2n} = \frac{2^{i+1} - 1}{2^i} \frac{p + 1}{p} = \frac{2^{i+1} - 1}{2^i} \frac{2^{i+1} - 1}{2^{i+1} - 1} = 2,$$

so n is perfect. There are 30 known primes of this form, including $q = 2, 3, 5, 7$, and 216091, yielding $3, 7, 31, 127$, and $2^{216091} - 1$.

Conversely, suppose n is perfect. If $p_1 = 2$ and $i = i_1 \geq 1$, then the first factor is $2^{i+1} - 12^i$. In order to arrive at an integer, some other prime p_u has to divide $2^{i+1} - 1$, in which case, writing $j = i_u$, we have

$$S(p^j) \geq \frac{p^j + p^{j-1}}{p^j} = \frac{p + 1}{p} > \frac{2^{i+1}}{2^{i+1} - 1},$$

unless $p = 2^{j+1} - 1$, so $S(n) > 2$ unless $t = 2$ and $p_2 = 2^{i+1} - 1$, and there cannot be no other prime factors. In other words, $n = 2^i p_j$, where $p_j + 1$ is a power of 2.

(ASIDE: Note: that if $p_j = 2^q - 1$ then q must also be prime, since otherwise if $q = rs$ we have $2^{rs} - 1 = (2^r)^s - 1$ is divisible by $2^r - 1$.)

Thus, we have determined all even perfect numbers. However, it is not known if there are an infinite number of them, and even worse, it is not known if there is an odd perfect number.

A similar argument shows that if $p = 2^q + 1$ is prime then q must be a power of 2. (Indeed, writing $q = 2^k s$ for $k \geq 0$ and s odd, then $2^{(2^k)} + 1$ divides $p = 2^q + 1$, contrary to p prime unless $s = 1$. These numbers, called 'Fermat primes,' played an important role later on.

(5) Amiable numbers. These are numbers a, b such that $S(a) = b$ and $S(b) = a$. The example known to Euclid was 220 and 284.

(6) (Book X) There are an infinite number of Pythagorean triples. (The formula for Pythagorean triples is given in his book; also, he gave a direct argument that does not rely on the formula. Indeed, the squares $1, 4, 9, 16, 25, \ldots$ differ by successive odd numbers, $1, 3, 5, 7, 9 \ldots$, so whenever this odd number is a square we will have a Pythagorean triple (in which $c = b + 1$).

Euclid's geometry: Euclid is best known for his formulations of the postulates of geometry, although he relied on Eudoxos and others. In fact, Eudoxos is generally credited with the concept of order in the number system, including the so-called Archimedean postulate. (Eudoxos was also the first to build a mathematical model of the universe, built on an elaborate system of spheres.)

Euclid's notions of point, line, etc. were not relevant to the development of his theory, so these are considered as undefined terms. (See Archimedes below for a definition of a line.) The basic (unprovable) properties of these undefined terms are called *postulates*. The theorems are those properties which can be proved from the postulates, using accepted principles of deduction.

Euclid's fifth postulate:

If a straight line crossing on two straight lines makes the interior angles on the same side less than two right angles, the two straight lines, if extended indefinitely meet on that side on which are the angles less than the two right angles.

In other words, as noted by Proclus, there is only one line through a point parallel to a given line. This postulate was attacked from the outset. For twenty centuries, mathematicians tried to prove this postulate from the others. It seems clear that it is consistent with the other axioms, especially, since Descartes later gave an algebraic model of Euclidean geometry (Affine space). On the other hand, in the 19th century it was shown that there are non-Euclidean models. (Hyperbolic geometry).

Note: Projective space is a model of the other postulates, but fails the basic (assumed) postulate that through every point there exists a line parallel to any given line!

Euclid also gave a complete mathematical description of the Platonic solids in the Elements.

Classical mathematics reached its zenith under Archimedes (287-212), one of the all-time mathematical greats. Two of his mathematical masterpieces were "On the Sphere and Cylinder," and The Sand Reckoner, -216. in the former book, developing Eudoxos' methods further, Archimedes computed volumes and ares of cones and spheres via successive approximation, thus anticipating integral calculus! His way of avoiding limits was to approximate circles by n-polygons enclosing them, noting that if for some function $f(n)$, that $f(\infty) < a$ iff $f(n) < a$ for suitably large n; this gives him a bound from above, and likewise, approximating a circle by inscribed polygons, he can bound f from below. In this way he calculated the surface of a sphere of radius r to be $4\pi r^2$ and the volume to be $\frac{4}{3}\pi r^3$.

He also explicitly defined a straight line as the shortest distance between two points, and likewise a plane to be the surface having the smallest area of any surface whose boundary is a given set of (coplanar) lines.

He claims to have solved $\frac{a-x}{b} = (\frac{c}{x})^2$ (which would be equivalent to solving the cubic equation!) by means of intersections of conics, and he discovered the discriminant of the cubic equation (to be discussed later). (His methods were rigorous, but in this case he referred the reader to a later portion of the book which either was never written or was lost, but finished by Eutocius in his commentary); also see discussion of Omar Khayyam below).

Archimedes also proposed the famous cattle problem, which showed that he could solve equations involving huge numbers.

From Wikipedia, the free encyclopedia: Archimedes' cattle problem (or the problema bovinum or problema Archimedis) ... Attributed to Archimedes, the problem

involves computing the number of cattle in a herd from a given set of restrictions. The problem was discovered by Gotthold Ephraim Lessing in a Greek manuscript containing a poem of forty-four lines, in the Herzog August Library in Wolfenbuttel, Germany in 1773.

The problem remained unsolved for a number of years, due partly to the difficulty of computing the huge numbers involved in the solution. The general solution was found in 1880 by A. Amthor; he gave the exact solution using exponentials and showed that it was about $7.76 \times 10^2 06544$ cattle. The decimal form is too long for humans to calculate exactly, but multiple precision arithmetic packages on computers can easily write it out explicitly.

On his tomb is engraved a sphere inscribed in a cylinder; he computed their relative volumes, which he considered one of his great achievements. He also developed three-dimensional curves such as the spiral, and applied them in inventions (the water screw).

Archimedes utilized the *Archimedean postulate* of the real numbers, that given x, y there is always n such that $nx > y$, although nowadays Eudoxos is generally credited for discovering this (in the form that any for any number x there is an integer $n > x$).

Archimedes discovered the laws of displacement while in the bath, in order to help the Syracusan king determine that a crown claimed to be made of pure gold was actually a fake, since it was only gold plated over silver.

Archimedes was killed by the Romans during the fall of Syracuse. (For good reasons - his inventions, inspired by geometric notions, included the triple pulley and multiple levers which enabled the Syracuse army to haul huge weights against Roman ships, and he focused sunlight via prisms to set the ships on fire. delayed their advance by 3 years). This is probably the greatest impact the Romans had on mathematics.

Conon of Samos - Friend of Archimedes, Died early but proposed classical questions, for example:

Given a sphere construct a cone or cylinder of same volume

Divide volume of sphere into two parts according to a given ratio of their volumes.

Divide volume of sphere into two parts according to a given ratio of their areas.

All of these are impossible, but he also proposed the question: Find a planar figure with same area as surface of sphere. (Possible, since this is constructing a figure with area $\frac{4}{3}\pi$, so a circle with radius $\frac{2}{\sqrt{3}}$ suffices.)

Aristarchus of Samos, during the golden period, proposed the heliocentric theory in his lost work *On the sizes and distances of the sun and moon*, which by its title must have been steeped in mathematics. (Quoted by Archimedes (sand reckoner, -216) and Ptolemy (Syntaus), Plutarch (On the Face in the Moon) His assumptions are a bit off – he assumes that the moon reflects full light at when it is half full. From this, he concludes that the distance of the sun from the earth is only 18 to 20 times that of the distance of the moon from the earth. This calculation was improved by Eratosthenes (-275)

He seems to have understood continued fractions. This is because he estimates $\frac{7921}{4050}$ as $\frac{88}{45}$ which is the beginning of the expansion of

$$1 + \frac{1}{1 + \frac{1}{21 + \frac{1}{2 + \cdots}}}$$

and he estimates $\frac{71755875}{61550073}$ as $\frac{43}{37}$ which is the beginning of the expansion of

$$1 + \frac{1}{6 + \frac{1}{6+\cdots}}$$

As pointed out by a student in the course, perhaps he had some other way of making the calculations, since $\frac{7920}{4050} = \frac{88}{45}$.

Appolonius of Perga (-262 to -190), born in Ionis, now in modern Turkey, and died in Alexandria) codified the works on conics, with great sophistication (tangents to conics, such as a circle tangent to three given circles, normal lines, harmonic quadruples, asymptotes, focal properties of spherical and parabolic mirrors, pencils of lines).

The twilight of the classical period

Many of the mathematical advances at this time were related to astronomy, especially movements of the planets, which required spherical geometry. Since it was believed the sun moves around the earth, the calculations were extremely intricate. Interestingly, trigonometry (both 2- and 3-dimensional, studied in terms of chords) developed under Menelaus (first century) and Ptolemy (2nd century) to the extent that he could calculate the sophisticated epicyclic motion required under his theory of planetary motion. Ptolemy also mastered the stereographic projection. This is, perhaps, the most geometric of the projections, obtained by rotating a line passing through one point of a sphere to project onto the plane tangent at the other end.

The great mathematician of the late Hellenistic period, Diophantus, continuing the tradition of Pythagoras and Euclid, codified the theory of numbers. Strangely enough, we do not know exactly when he lived. He is not quoted by Nicomachus or Theon of Smyrna, so he probably was born after 130. On the other hand, Theon of Alexandria (c. 365) quotes him, and Theon's daughter Hypatia preserved part of his masterpiece "Arithmetica" (13 books) in her commentary. Thus Diophantus probably wrote the Arithmetica around 300. Diophantine equations (polynomial equations with rational solutions) and Fermat's Theorem. One thing we know about Diophantus was his age when he died, because of a famous epitaph on his tomb (described in the Paletine anthology written 100 years after his death), composed by a friend in terms of a Diophantine equation. (One sixth of his life was in childhood; after a twelfth more he grew a beard; after a seventh more he married; 5 years later a son was born, who lived to be half his father's total life; he died four years after his son.

A sample question solved in "Arithmetica," Book V: To find three squares such that the sum of their squares is a square. In other words, solve

$$a^4 + b^4 + c^4 = d^2.$$

(Solution: $\frac{144}{25}$, 9, 16; or in integers, $a = 12, b = 15, c = 20, d = 481$.) This should be compared with Euler's problem described below.

In Book II, Diophantus discovered a geometric way to solve the Pythagorean triples, probably making him the first person to have a proof that all Pythagorean triples have this form. First of all, dividing through by z, we need to find rational numbers x, y such that $(\frac{x}{z})^2 + (\frac{y}{z})^2 = 1$, or, in geometric terms, we want the rational

solutions on the unit circle $\mathcal{C}$ (described by $x^2 + y^2 = 1$). First one starts with a "trivial" solutio. Take a line $x = 1 - ty$ passing through $(1, 0)$, where t varies in $\mathbb{Q}$. In other words, we are rotating a ruler around the point $(1, 0)$ and looking for the other intersection point with $\mathcal{C}$.

This point (x, y) satisfies $(1 - ty)^2 + y^2 = 1$. Solving, one gets the equation

$$1 - 2ty + t^2y^2 + y^2 = 1;$$

cancelling y yields $y = \frac{2t}{t^2+1}$; $x = \frac{1-t^2}{t^2+1}$. Writing $t = -\frac{v}{u}$ yields $y = \frac{2uv}{u^2+v^2}$; $x = \frac{u^2-v^2}{u^2+v^2}$.) Multiplying through by $u^2 + v^2$ yields the famous Pythagorean triples.

Diophantus also studied different properties of Pythagorean triples, including triangles for which the two shorter sides differ by 1. Then $u^2 - v^2 = 2uv \pm 1$, so $(u - v)^2 = 2v^2 \pm 1$; continue by infinite descent. Examples: 3,4,5; 20, 21, 29. Note that this is the reverse problem for that studied by Euclid.

The following Diophantine equation is very significant: Find a rational solution to the equation $y(6 - y) = x^3 - x$, other than the obvious solutions $x \in \{\pm 1, 0\}$. Here is a geometric solution: $(-1, 0)$ also lies on the line $x = ty - 1$; the other intersection point satisfies $6y - y^2 = t^3y^3 - 3t^2y^2 + 2ty$. For $t = 3$, this becomes

$$-y^2 = 27y^3 - 27y^2,$$

which degenerates to the linear equation $27y = 26$, or

$$y = \frac{26}{27}; \qquad x = \frac{17}{9}.$$

Diophantus must have seen that any equation of this form (cubic in x and square in y) with a "trivial" solution, has another solution obtained by intersecting its curve with a suitable line. Such a curve $y^2 = q(x)$ with $\deg q = 3$ is called an *elliptic curve*, and has played an extremely important role in mathematics since 1950.

Note: One of the students in my class, Ron Held, solved Diophantus' equation in a few minutes, using elementary properties of integers to arrive at the solution $x = -9$ and $y = 30$. Later, using the same methods, he came up with $x = -9$ and $y = 30$ or -24; $x = -35$ and $y = -204$ or 210; $x = -37$ and $y = -222$ or 228; But these solutions presumably would not be available to Diophantus, since, in each case, $x < 0$.

Pappus (4th cent.), Theon.

Hypatia (370 CE? – 415 CE), Theon's daughter, and perhaps the first great female mathematician, wrote commentary on six books of Diophantus' 13-volume Arithmetica. She also edited the third book of her father's commentary on Ptolemy's Almagest, as well as her father's commentary on Euclid's Elements, and simplified Apollonius's Conics. Hypatia was lynched by a Christian mob, and this symbolizes the death of Classical mathematics.

Proclus (412 – 485), and Eutocius (480–540) mastered many of the Classical works, but did not add much to them. It would be over 1000 years before Western mathematics reached this plateau again.

What happened to Classical mathematics? There was the general fall of culture with the fall of Classical civilization, which in the early middle ages was often identified with heathenism. The library of Alexandria, symbol of Classical knowledge,

was sacked by Christians (389), and then by Moslems (642). Caliph Omar's infamous quote: If it is against the Koran it should be burned and if it is for the Koran it is superfluous and thus should be burned.

However, this does not explain why the last great mathematical advance in classical Europe came several hundred years earlier. Here is another hypothesis: The great philosophical minds missed the mark when considering basic physical principles.

The Hellenist mathematicians could not progress further in number theory without a reasonable number system. The great philosopher Aristotle had opposed the notion of 0, since one cannot divide by it.

Geometry was saddled with the Herculean task of supplying the computations for an untenable physical theory: Aristotle's theory required continuous force to keep an object in motion, together with his geocentric theory of the universe The physical theory of motion requiring a mover had no mathematical basis, and thus there was no need for development of the theory of functions. The reliance on the circle diverted attention from other conics such as the ellipse, and removed incentive for discovering differential calculus (which may have been natural considering the Greeks' understanding of tangents, but which also relies on limits).

Likewise, mathematics was dominated by philosophy in astronomy, where the geocentric theory, featuring spheres, was adopted by Aristotle and led to great efforts in putting everything in terms of epicenters etc. This was done with high accuracy by Ptolemy, but again diverted attention from non-spherical geometry. The greatest computational minds were needed to calculate the unnecessarily complicated orbits of the heavenly bodies. In other words, philosophical constraints most likely put the brakes on mathematical development.

Another stumbling block: Zeno's paradoxes, as reported by Aristotle (quoted from Wikipedia):

Achilles and the tortoise (Physics VI:9, 239b15) In a race, the quickest runner can never overtake the slowest, since the pursuer must first reach the point whence the pursued started, so that the slower must always hold a lead.

(Physics VI:9, 239b10) That which is in locomotion must arrive at the half-way stage before it arrives at the goal.

(Physics VI:9, 239b5) If everything when it occupies an equal space is at rest, and if that which is in locomotion is always occupying such a space at any moment, the flying arrow is therefore motionless.

Before 212 BC, Archimedes had developed a method to derive a finite answer for the sum of infinitely many terms that get progressively smaller. But Zeno's paradoxes, pointing out the logical difficulties with limits, may have stifled the development of this theory (for 2000 years.)

Hebrews. Elaborate astronomical calculations which enabled them to calculate their sophisticated solar-lunar calendar; traditionally ascribed to Rabbi Akiva?.

India

As advanced as Greek mathematics became, it was apparently in India that 0 and the negative numbers were discovered. (Perhaps these were discovered earlier in China, but if so, these discoveries were lost.) A copper plate from Gujarat, India mentions the date 595, written in a decimal place value notation, although there is

doubt as to its authenticity. Decimal numerals recording the years 683 have also been found in stone inscriptions in Indonesia and Cambodia.

Bakhshali manuscript, written on birch bark. Although the manuscript was written in the ninth century, its contents are considered to be from a much earlier time, because it uses the sloka measure which was replaced in 500 by the arya measure. Also the arithmetic is written in Sarada script in the ancient Gatha dialect, which was replaced by Sanskrit. Finally the currencies mentioned are the dinara and dramma, which were from the Classical period (dinar and drakhma). (This also shows the influence of the Greeks and Romans on Indian mathematics.) The modern concensus puts the date after 2nd century BCE and up to the 3rd century. Major innovations: Use of $\cdot$ for the numeral 0 (and also for an unspecified unknown), and negative numbers.

Indians also introduced sine notation into trigonometry, replacing the chords of the Greeks. The Surya Siddhanta (c. 400) (authorship unknown) contains the roots of modern trigonometry. This ancient text uses the following as trigonometric functions for the first time:

Sine (Jya), cosine (Kojya), arc sine (Otkram jya), Ttangent. secant The Hindu cosmological time cycles, copied from an earlier work, give: The average length of the sidereal year as 365.2563795 days, only 1.4 seconds longer than the modern value of 365.2563627 days; the average length of the tropical year as 365.2421756 days, only 2 seconds shorter than the modern value of 365.2421988 days. Later Indian mathematicians such as Aryabhata made references to this text, and there were later Arabic and Latin translations.

Aryabhata (b. 476) wrote the Aryabhatiya (c. 499) in Kusumapura above the Ganges; interested in astronomy. He knew to take square roots, cube roots, solve quadratic equations, compute sines, and sum powers of numbers.

Brahmagupta (b. 598) Head of Ujjain astronomical observatory. and expert in astronomical calculations. Wrote Brahmasphutatidd'hanta (628) which reviewed much of the classical mathematics, including planar geometry, set out rules of arithmetic (including negative numbers). Interestingly, he attacked Aryabhata's work.

Bhascara Acharya (The Learned, 1114-1185?) Head of Ujjain astronomical observatory. Wrote Sidd'hanta siromani. Contains permutations, rules of arithmetic and solving equations over $\mathbb{Q}$, as well as solutions of various Diophantine equations in several unknowns (using colors to designate the unknowns), and a diagram indicating the proof of the Pythagorean theorem.

Golden age of Islamic mathematics. The Muslims of Baghdad collected Greek works from Byzantium and also were influenced by the Indians, who had the most active current tradition. The Arabs quickly became the world leaders in mathematics, with no competition from the rest of the Western world.

Mohammed Ben-Musa Al-Khowarizmi was a great astronomer and expert in trigonometry, but his most famous work is Al–jabr w'al mugahala (825), which lent its name to the subject of Algebra. ("Algebra" means *rectification*, i.e. transposition of equal parts on both sides of an equation.) In it, he invented algebraic notation (x is the indeterminate), and found the algebraic solution for quadratic equations, by means of completing the square. In other words, if we have to solve $x^2 + 10x = 39$, we take a square $x + 5$ units long. Then the area is $x^2 + 5x + 5x + 25 = 64$, so $x + 5 = 8$, i.e., $x = 3$. This work was quoted directly or

indirectly for over 700 years.

Abu'l Hasan Ahmad ibn Ibrahim Al-Uqlidisi wrote the earliest surviving book on the positional use of the Arabic numerals, around 952, especially notable for its treatment of decimal fractions.

Abu Wefa (1000) knew the sine theorem, and the Islamics had sine and cosine tables; sophistication continued until Al-Kashi (1400), who used the law of cosines, and computed π to 16 places in the decimal system. The Islamics also could extract n-th roots by iteration. At this time, most Europeans did not even use decimal notation!

Omar Khayyam (d. 1123 or 1132) the famous Islamic poet and scholar, provided a solution to the equation $x^3 + b^2x = 2b^2c$, displaying it as the intersection of the parabola $x^2 = by$ with the circle $(x - c)^2 + y^2 = c^2$. Indeed if $x^2 = by$ then $x^2 - 2cx = -\frac{x^4}{b^2}$, so cancel x and solve. (Although there could be four points of intersection of these two curves, one of them, $(x, y) = (0, 0)$ dropped out in the reduction to the cubic, so we are left with at most three solutions.) Note the parallel to the (geometric) parametric method used by Diophantus. The reason that this does not enable one to construct the root of a cubic is that the parabola is not constructible via our strict rules.

Omar Khayyam also studied Euclid's fifth postulate, noting that its negation would lead to hyperbolic space (although he tried to prove this would lead to a contradiction); likewise he had the beginnings of projective geometry.

The dark ages in Western Europe. The mathematics in Western Europe during this period was truly in a "dark age," with nothing remotely comparable to The Greco-Indian school.

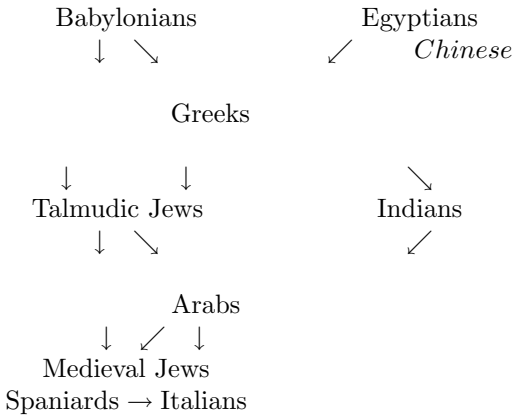
Abraham bar Hiyya was a Spanish Jewish mathematician and astronomer, working in Barcelona, who wrote Hibbur ha-Meshihah ve-ha-Tishboret (Treatise on Measurement and Calculation), translated into Latin by Plato of Tivoli as *Liber Embadorum* in 1145. This book is the earliest treatise on Arab algebra written in Europe, and contains the complete solution of the general quadratic. He had the Hebrew title 'Ha-Nasi,' meaning 'the leader,' but he is also known by the Latin name Savasorda which comes from his 'job description' showing that he held an official position in the administration in Barcelona.

For the most part, the best Westerners could do was translate Arabic texts. Leonardo of Pisa (c.1170-c. 1245), otherwise known as Fibonacci, was the leading Medieval mathematician in Europe. He wrote Liber Abaci (1202) which advocated use of the Hindu-Arabic decimal notation, but took time to be accepted.

Alphonso the Wise, king of Castile, assembled an academy at Toledo (c. 1250), largely composed of Jews who utilized astronomical calculations to refine their calendar, and these techniques spread through Europe.

Immanuel ben Jacob Bonfils (1350?) Decimal notation. (Largely of historical value, since manuscript was lost for years)

Ancient, Classical, and Medieval periods:



The Renaissance

Although the renaissance gets its name from the rebirth of Hellenistic influence, the mathematicians also benefited from the interim advances of the Indians (the non-positive integers) and the Muslims.

Solution of algebraic equations of degree ≤ 4. Perhaps the leading mathematical advances in the Renaissance was in algebraic equations. With the well-known solution of quadratic equations by " completing squares," the next step was the cubic equation $x^3 + ax^2 + bx + c = 0$. Replacing x by $x + \frac{a}{3}$, one can eliminate the coefficient of x^2, so the general form of the cubic is

$$x^3 = bx + c. \tag{1}$$

In general, when solving the equation

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$$

of degree n, one may assume the coefficient of x^{n-1} is 0. Indeed, let $y = x + \frac{a}{n}$. then $x = y - \frac{a_{n-1}}{n}$, so

$$\begin{aligned} x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} = y^n - n\frac{a_{n-1}}{n}y^{n-1} + \frac{n(n-1)}{2}\left(\frac{a_{n-1}}{n}\right)^2 y^{n-2} + \cdots \\ + a_{n-1}(y^{n-1} - (n-1)\frac{a_{n-1}}{n}y^{n-2} + \cdots) \\ + y^{n-2} + \cdots \\ = y^n + (\frac{(n-1)}{2n}(a_{n-1})^2 - \frac{n-1}{n}a_{n-1} + 1)y^{n-2} + \cdots \end{aligned}$$

Chuquet wrote an important text, Triparty en la science des nombres. Despite special cases proved by the Arabs, as late as 1494 Pacioli claimed the general solution of $x^3 + mx = n$ will be as impossible as the quadrature of a circle.

In 1515 Scipione del Ferro (1465–1526) obtained a solution, which he kept secret so that he could challenge others to solve specific equations. (This might sound

strange, until we consider recent attempts by the NSA to suppress papers on factorizing prime numbers.) In 1535 Niccolo Fontana (1500–1557, known as Tartaglia, "the stutterer") solved the cubic in time to beat such a challenge, and he confided his solution to Cardano, who in 1539 proceeded to publish the solution in his great work *Ars Magna*, which he credited to del Ferro; namely the solution to (1) is

$$x = \sqrt[3]{\sqrt{(\frac{c}{2})^2 - (\frac{b}{3})^3} + \frac{c}{2}} + \sqrt[3]{\sqrt{(\frac{c}{2})^2 - (\frac{b}{3})^3} - \frac{c}{2}}.$$

Note that one can get a real root from this solution precisely when $27c^2 - 4b^3$ is positive; this is called the *discriminant*. The idea in Cardano's solution to (1) was to reduce to an equation of lower degree. Namely writing $x = \sqrt[3]{t} + \sqrt[3]{u}$ for t, u to be determined, one gets

$$x^3 = t + u + 3(\sqrt[3]{t} + \sqrt[3]{u})\sqrt[3]{tu},$$

so plugging into (1) yields

$$(t + u - c) + (\sqrt[3]{t} + \sqrt[3]{u})(3\sqrt[3]{tu} - b) = 0.$$

Matching parts yields

$$t + u = c, \qquad tu = (\frac{b}{3})^3,$$

Substituting $u = t - c$ yields

$$t(t - c) = (\frac{b}{3})^3, \tag{2}$$

a quadratic equation which can be solved for t (and thus for u), and thus which provides x. Equation (2) is called the "resolvent" equation for the cubic.

Even though Cardano's method gives a formula, it is by no means as "clean" as the quadratic formula, in the sense that sometimes it is extremely difficult to recognize the solution (as in the equation $x^3 + x = 2$) and other times, the formula misses the only (real) solution, as in the equation $x^3 + 16x = 64$. (Also, the formula applied to the equation $x^3 + 16 = 12x$ produces -4 instead of 2), These difficulties were discussed in length in Cardano's book.

This method of solving via a resolvent equation was so powerful that Cardano's student Lodovico Ferrari solved the general quadric

$$x^4 + px^2 + qx + r = 0$$

in a similar manner. Taking a quantity u to be determined, one has

$$(x^2 + \frac{p}{2} + u)^2 = -qx - r + (\frac{p}{2})^2 + 2ux^2 + pu + u^2.$$

If the right hand side is a polynomial in x then we can take square roots and solve. But, completing the square, its square root must be

$$\sqrt{2u}x - \frac{q}{2\sqrt{2u}},$$

yielding

$$-r + (\frac{p}{2})^2 + pu + u^2 = \frac{q^2}{8u},$$

or

$$8u^3 + 8pu^2 + (2p^2 - 8r)u - q^2 = 0.$$

This cubic equation, called the *resolvent cubic*, can be solved by Cardano's formula. Although Cardano included Ferrari's solution in *Ars Magna*, he felt uncomfortable with equations of degree higher than 3, because this seemed unnatural, exceeding the dimensions in nature. Nevertheless, the mere fact Cardano treated fourth powers showed that algebra was freeing itself from the geometric constraints which had shackled the Greeks.

Algebra in the years 1550–1625.

As noted above, Cardano's formula has the difficulty that sometimes it produces the "wrong" root or an unrecognizable root. Even worse, when the resolvent quadratic has no real roots, one cannot find the real root of the cubic without passing to complex numbers. Thus, complex numbers were a necessary consequence of Cardano's formula (despite Cardano's discomfort with non-real solutions), and indeed appear in full flower in Rafaele Bombelli's 1572 book on algebra. Bombelli seems to be the first major mathematician after the early Greeks to consider the continuity of the real numbers. This sophisticated concept is necessary for his method of determining a root of a polynomial via successive approximation. Nevertheless, progress was faster in studying precise solutions than approximating in the real (or complex) number system, which had to wait for methods from calculus.

Franois Vieta, or Viète (1540-1603) and Simon Stevin (1548-1620) rediscovered and popularized decimal notation; Viète also used letters for symbolic computations in *Introduction to the Analytic Art* (1591) distinguishing between unknowns (designated by vowels) and parameters (consonants). Thus Viète was the first to deal with polynomials. Viète (1595) solved van Roomen's challenge from 1593:

$$\begin{aligned} A =& 45x - 3795x^3 + 95634x^5 - 1138500x^7 + 7811375x^9 - 34512075x^{11} \\ &+ 105306075x^{13} - 232676280x^{15} + 384942375x^{17} - 488494125x^{19} \\ &+ 483841800x^{21} - 378658800x^{23} + 236030652x^{25} - 11769100x^{27} \\ &+ 46955700x^{29} - 14945040x^{31} + 3764565x^{33} - 740259x^{35} \\ &+ 111150x^{37} - 12300x^{39} + 945x^{41} - 45x^{43} + x^{45}. \end{aligned}$$

If $f_n(X) = \sum_{i=0}^{[n/2]} (-1)^i \frac{n}{n-i} \binom{n-i}{i} x^{n-2i}$ then

$$2\sin(n\alpha) = (-1)^{(n-1)/2} f_n(2\sin\alpha).$$

Thus given $2\sin(45\alpha)$ one wants to find $2\sin\alpha$. How do you do this? First divide by 2, take the arc sine, divide by 15, and take the sine.

With Napier's invention of logarithms in 1614, all the arithmetical tools for computation were in place.

Europe was poised for its great revolution in mathematics, in which Western Europe grabbed the reins, leaving Islamic and Hindu mathematics far behind.

Astronomy in the Renaissance.

With the development of mathematical techniques, mathematicians turned again to the skies, to try to find a workable system to calculate orbits of the stars and planets (which according to the Aristotelian-Ptolemaic theory all moved around the world). The first person to present an alternative quantitative theory was Nikolas Copernicus (1473-1543). His system of the universe was designed to simplify computations (although it still needed epicycles since he was stuck on circular orbits; in fact he increased the number of epicycles from Ptolemy's 40 to 48).

Johannes Kepler (1571-1630). Kepler's 3 laws:

The orbits are elliptical;

the area swept out from a focus of the orbit is proportional to the time;

for any satellite of a fixed body, the ratio of the square of the period of the orbit to the mean radius cubed is constant.

Kepler and Copernicus were mathematicians in the sense that their careers were devoted mostly to curve-fitting. However, Kepler's great contribution was that by presenting reasonably shaped orbits, people could start considering the velocity of the planet, and Kepler's last two laws deal with this.

By the beginning of the 17th century, European mathematics was on its feet, and strong enough that Galileo Galilei (1564-1642) could assert that scientific truth is the supreme test for a physical theory (although this brought him into conflict with the Inquisition). Galileo was largely responsible for the development of physics along mathematical principles.

Cartesian geometry. Galileo's quest for scientific truth paved the way for the great French mathematician Descartes (1596-1650) who invented analytic geometry, bringing the mysteries of geometry down to earth. In 1637 he published *Discours de la mthode*, which enabled one to study all the obscure theorems of geometry in terms of algebra. Descartes used the term the term "imaginary" for expressions involving square roots of negative numbers, although he thought any such solution is nonexistent. (Thus he did not think that one could arrive at a real solution via an imaginary one.) Fermat had anticipated him in private correspondence. Also, they saw the interplay between curves and algebraic equations, the foundation of modern algebraic geometry. In particular it was now a trivial matter to calculate slopes of secants, and to describe limits, a concept which seems to have escaped the later Greeks, perhaps because of their preoccupation with Zeno's paradoxes. In short, the modern properties of the real numbers were finally available to mathematicians.

Probability. Apparently at the invitation of some gamester friends, Pascal (1623-1662) who, in 1654, with the help of his friend Fermat, developed the theory of probability, a subject completely outside the realm of classical mathematics.

Pierre Fermat. Who was this person involved in the two great theories of the 17th century? Pierre Fermat (1601- 1665) was a French jurist (in Toulouse) who only did mathematics as an avocation. Perhaps Fermat's most famous contributions were to number theory. Bachet had translated Diophantus' *Arithmetica* in 1621, thereby reviving the theory of Diophantine equations. Fermat discovered methods of proving by means of infinite descent, which is equivalent to present-day mathematical induction. He found a new amicable pair (as did his friend Descartes) and studied prime numbers. He proved that any prime number of the form $4n + 1$

is a sum of two squares, and studied primes of the form $2^{2^k}+1$, called *Fermat primes*. (Actually, his only recorded mistake was that he thought these numbers are all prime, whereas Euler showed $k = 5$ provides a counterexample.)

Fermat's Last Theorem. Diophantus's discussion of Pythagorean triples must have aroused Fermat's imagination. Fermat wrote in the margin of his copy of *Arithmetica* that he had a "marvellous demonstration" that there are no natural numbers $a, b, c, n,\ n > 2$, such that $a^n + b^n = c^n$, but which the margin is too narrow to contain. Elsewhere, for $n = 4$, Fermat did write down the proof, by infinite descent. In honor of Fermat's manifold contributions to mathematics and the sublimity of the conjecture, it is called "Fermat's Last Theorem," or FLT for short.

The Calculus. Kepler (1615) had devised a method of infinitesimals, but it was up to Newton (1642-1726) and Leibniz (1646-1716) to change the face of mathematics forever. The great influx in curves that could be studied via Cartesian coordinates gave rise to the study of tangents to curves. Fermat was the first to describe a tangent to a point P as the limit of secants as the second point approaches P. Leibniz and Newton, building on Fermat's work on differentials and by finding areas through summations (as done by the ancients, updated by Wallis and Isaac Barrow, Newton's mentor), found that integration is the inverse of differentiation. Newton's great work, *Philosophiae naturalis principia mathematica*, appeared in 1687. Newton also discovered binomial expansion for rational powers. Calculus still was not on a rigorous foundation, and it remained for Robin (1735) and MacLaurin (1742) to carry out this task, whereas later Weierstrass introduced the famous $\delta - \epsilon$ proofs which still confound students.

Cauchy (1829) founded the theory of calculus in a complex variable, and Riemann and Lebesgues furthered the study of multi-dimensional calculus. in the 1950's, Robinson finally carried out Leibniz idea of using infinitesimal numbers (rather than limits) in "nonstandard analysis," and these ideas were formulated in a Calculus text by Keisler (1970).

The Bernoulli family. One of the great mathematical families of the late Renaissance early classical period was the Bernoulli's, among whom the following members are prominent:

Jakob Bernoulli (1654–1705; also known as James or Jacques) after whom Bernoulli numbers are named, Nicolaus Bernoulli (1662–1716), Johann Bernoulli (1667–1748; also known as Jean), Nicolaus I Bernoulli (1687–1759), Nicolaus II Bernoulli (1695–1726), Daniel Bernoulli (1700–1782), developer of Bernoulli's principle and the St. Petersburg paradox, Johann II Bernoulli (1710–1790; also known as Jean), Johann III Bernoulli (1744–1807; also known as Jean), Jakob II Bernoulli (1759–1789; also known as Jacques).

The climax of the classical period

Euler (1707–1783).

Euler, born in Basel, Switzerland, received private lessons from Johann Bernoulli, and completed his dissertation in 1726. Blind in one eye for most of his adult life, Euler was the jewel of the crown of Catherine the Great, residing in St. Petersburg (1733-1741 and 1766-1783), and was director of mathematics at the Berlin academy

from its inception (1744-1766) and head of the Berlin Academy from 1759. In 1771 Euler lost his sight in his other eye, and wrote half his papers by memory!

Euler secured his reputation by finding beautiful formulas relating to classical mathematics. Euler proved that $2^{2^5}+1$ is *not* prime (by producing its prime factors), contrary to a conjecture of Fermat, and also found 62 amicable pairs.

Euler treated complex numbers as computable entities, and was the first to publish explicitly De Moivre's formula

$$(\cos\theta + i\sin\theta)^n = \cos(n\theta) + i\sin(n\theta).$$

This important formula, which essentially makes plane trigonometry an exercise, has its roots in Cotes (1722). Taking $n\theta = 2k\pi$ for $k \in \mathbb{N}$, this also shows that $\rho_n = e^{\frac{2k\pi i}{n}} = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$ is an n-root of 1. In particular, one can construct (complex) cube roots of 1.

De Moivre's formula is best understood in terms of the unit complex circle; one can define the primitive n-root ρ_n of 1 by subdividing the unit circle into n equal arcs. He solved Fermat's Last Theorem (1753) for $n = 3$ by means of expanding the number system to $\mathbb{Z}[\rho_3]$, where ρ_3 is a primitive cube root of 1. His method is by infinite descent reminiscent of number-theoretic the proof of Pythagorean triples given above; the first step is to factor $c^n - b^n$ over $\mathbb{Z}[\rho_n]$.

Let us review the basics of Euler's proof. Consider $a^p + b^p = c^p$ for p an odd prime. We may assume a, b, and c are relatively prime Thus $a^p = c^p - b^p$. Let ρ be a primitive p-root of 1. We work in the extension ring $\mathbb{Z}[\rho]$. Thus

$$a^p = \prod_{i=0}^{p-1}(c - \rho^i b).$$

For $p = 3$, we have

$$a^3 = (c-b)(c-\rho b)(c-\rho^2 b). \tag{1.1}$$

We define the norm of a number

$$N(u+\rho v) = (u+\rho v)(u+\overline{\rho} v) = u^2 - uv + v^2.$$

Then the gcd of the $c - \rho^i b$ is at most $1-\rho$, so comparing factorizations, we see that each factor on the right side must be a cube times some power of $1-\rho$ times some invertible element of $\mathbb{Z}[\rho]$. Thus

$$c - \rho^i b = d_i u_i (1-\rho)^{k_i},$$

and one can get an equation generalizing Equation (1.1), of smaller norm. (Details can be found in the book of Hardy and Wright on number theory.) Thus, one concludes by infinite descent that there is no equation by induction.

(Some hidden requirements: $\mathbb{Z}[\rho_3]$ is a unique factorization domain, with precisely six invertible elements – the roots of unity, which are $\pm\rho^i$ for $0 \le i \le 2$.)

At the same time Euler proposed a new conjecture: $a^4 + b^4 + c^4 = d^4$ has no natural solutions. However, in 1988 Noam Elkies found the following example:

$$2682440^4 + 15365639^4 + 18796760^4 = 20615673^4.$$

The Zeta function.

Define the Zeta function $\zeta(z) = \sum_{n\geq 1} \frac{1}{n^z}$. This is often called the Riemann Zeta function because of Riemann's famous 1859 paper to be discussed below, but in fact Euler studied it for integral values of z in two celebrated papers in 1734 (for z positive) and 1749 (for z negative). We focus on the 1734 paper, since its results are easier to describe. Euler observed

$$\zeta(s) = \prod_{p \text{ prime}} (1 + p^{-s} + p^{-2s} + \dots) = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}}$$

as p runs over the prime numbers, thereby making the first of many important connections between the Zeta function and number theory. (This instantly reproves Euclid's theorem about there being infinitely many prime numbers, since an easy argument shows that in the series for $\zeta(1)$, the sum of the $2^m + 1$ term through the 2^{m+1} term is greater than

$$2^m \frac{1}{2^{m+1}} = \frac{1}{2},$$

implying that the series does not converge; it also gives an indication of the distribution of prime numbers.) Euler also proved that

$$\zeta(2) = 1 + \frac{1}{4} + \frac{1}{9} + \dots = \frac{\pi^2}{6},$$

and in both papers he tied the Zeta function in to the Bernoulli numbers.

Topological problems and invariants.

A topologist is sometimes defined as a person who does not know the difference between the coffee cup and the doughnut. (Both have a single hole, and there is a continuous transformation from one to the other. Often in proving the impossibility of doing something, one wants to calculate a number which contains key information about the problem, and showing that the existence of a solution would give rise to a different number. For example, can one cover the "mutilated checkerboard" (opposite corners cut out) with dominoes? No, because there are more black squares than white.

The Konigsburg bridge problem. This question was whether a certain collection of bridges could be traversed in such a way as to cross each bridge exactly once, without breaking the route. Its solution is another very simple application of invariants. In a connected graph, at most two vertices have odd degree. (Proof, any vertex inside the path has one edge entering and one leaving, so only the two ends of the path can add an odd degree to the vertex.)

Euler's formula. Considering topological problems such as this led Euler to a profound discovery. In any connected planar map made up of polygons,

$$v - e + f = 1,$$

where v, e, f stand respectively for total number of vertices (kodkodim), edges (kshatot), and faces (peiot) of the polygons. For example, for the n-gon we have $e = v = n$ and $f = 1$. Counting the "unbounded" face makes $v-e+f = 2$.) This can be proved easily by triangularization. Namely, one sees easily that triangularizing

does not change the number, and so we may assume all our polygons are triangles. Now the result is obvious for a single triangle, where $3-3+1=1$, and any new triangle adds two vertices, three edges, and one face, thereby adding $2-3+1=0$. One way of interpreting this fact is that $v-e+f$ is an invariant of the sphere, and indeed any surface has its own *Euler invariant*.

For example, the torus has Euler invariant 0. This might be seen easiest by subdividing it into four rectangles, involving 4 vertices and 8 edges; thus we get $4-8+4=0$.

One application of Euler's formula is a quick topological proof that there are only five Platonic solids. Suppose p is the number of vertices of each polygon in a given Platonic solid (which is also the number of edges of each polygon), and q dually is the number of polygons touching a given vertex. Note that $p, q \geq 3$. Also,

$$e = \frac{fp}{2}; \qquad v = \frac{fp}{q}.$$

Hence, substituting in Euler's formula and dividing through by fp gives

$$\frac{1}{q} - \frac{1}{2} + \frac{1}{p} = \frac{2}{fp},$$

implying $\frac{1}{q} + \frac{1}{p} > \frac{1}{2}$. This is impossible when both $p, q \geq 4$, so either $p = 3$ or $q = 3$. If $p = 3$ then $q \geq 6$ is impossible, so we conclude that either $p = 3$ with $3 \leq q \leq 5$ or $q \leq 3$ with $3 \leq p \leq 5$. Thus, we have at most five integral solutions for (p, q), and each one provides a solution for f and a Platonic solid:

$$(3,3),(f=4); \quad (4,3),(f=6); \quad (3,4),(f=8); \quad (5,3),(f=12) \quad (3,5),(f=20).$$

Lagrange (1736-1813).

Joseph-Louis Lagrange was the mathematical conduit into the 19th century, and, although born in Turin, Italy, was a protege of Euler, in the sense that he was in frequent contact with Euler, improved some of Euler's results, and Euler promoted Lagrange's career at several key stages. (On the other hand, he refused Euler's offer of a professorship at Berlin until Euler retired, perhaps feeling that there was not room for him as long as Euler was there. In 1766 Lagrange became the mathematics director of the Berlin academy.) Lagrange's first major contributions (1760's) were in the theory of variations and probability. While at Berlin, he made major contributions in astronomy and the three-body problem, and won many prizes from the French Academy of Sciences.

Lagrange developed Lagrange interpolation to fit polynomials to a given set of data, and also (1770) noted that if we adjoin the roots of a polynomial f of degree n to $\mathbb{Q}$, the transformations (now called automorphisms) permute the roots, and thus can be identified with a subgroup of permutations of S_n, whose order divides $n!$ (Lagrange's Theorem). In case this subgroup is cyclic of degree n, Lagrange found a method of solving the polynomial by radicals (called *Lagrange resolvents*). Lagrange also built on a theorem of Fermat, proving that every number is a sum of four squares.

In 1787 Lagrange accepted a position as a permanent member of the French Academy of Sciences, and in 1788 published his tract on analytic mechanics. Lagrange was fairly apolitical, and so survived the French revolution; in fact a special exception was made for him when all foreign scientists were fired under the Reign of Terror. At the end of his life he was honored by Napoleon.

Waring's problem. In the margin of a book about Lagrange's theorem, Waring (1770) claimed without proof that every integer is a sum of 9 cubes, 19 fourth powers, etc. The assertion that for any k, there is a number $g(k)$ such that any number is a sum of $g(k)$ k-powers, became known as Waring's problem, and was proved much later by Hilbert (1909), with an elegant solution later by Hardy and Littlewood. The precise determination $g(3) = 9$ was found by Wieferich in 1909. Liouville showed $g(4) \leq 53$, but $g(4) = 19$ was only proved in 1986 by Balasubramanian et al. Chen (1964) proved $g(5) \leq 37$.

Mathematics at the beginning of the nineteenth century

The first half of the 19th century saw the final resolution of the problems of antiquity, the precise formulation of the real numbers and complex numbers, and also the flowering of calculus. There is one mathematician whom we should single out.

Gauss (1777-1855). Carl F. Gauss was the greatest mathematician of the 19th century, often ranked together with Archimedes and Newton as the leading three mathematicians ever. In his dissertation Gauss constructed the regular 17-gon, thereby solving a two-thousand year old problem.

Gauss also constructed complex numbers rigorously, thereby enabling him to discover the fundamental theorem of algebra (1799). An example of Gauss' complex number system: The *Gaussian integers* $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$.

Fact: Suppose $p \in \mathbb{Z}$ is prime. Then either p is prime in $\mathbb{Z}[i]$ or else $p = N(a + bi) = a^2 + b^2$ for suitable $a, b \in \mathbb{Z}$, where N denotes the complex norm. Proof: If p is not prime then some $a + bi$ divides p, for $a, b \neq 0$. Then $N(a + bi)$ divides $N(p) = p^2$ in $\mathbb{Z}$. This implies $N(a + bi) = p$, as desired.

Now one can prove that p is prime iff p has the form $4n+3$. This yields Fermat's theorem that an odd prime number p is a sum of two squares iff p has the form $4n + 1$.

Continuing with complex numbers, Gauss then determined the cyclotomic polynomials (1801), i.e., the minimal polynomials of complex roots of 1.

Note: The use of ordered pairs to denote the complex plane was first published by William Rowan Hamilton in the Theory of Algebraic Couples (1835). Thus the notion of complex numbers was fully developed by the mid-19th century.

Gauss proved the surprising quadratic reciprocity law (1801), anticipated by Euler and Legendre: A number a is a *quadratic residue* modulo p if $a \equiv b^2 \pmod{p}$ for some b not divisible by p. Suppose p, q are odd primes. Define the *Legendre symbol* $\left(\frac{p}{q}\right)$ to be 0 if q divides p, 1 if p is a quadratic residue mod q, and -1 otherwise. Gauss proved that

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}},$$

and $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Gauss also proposed non-Euclidean geometry (unpublished), studied convergence of series (1812), and discovered Gaussian curvature (1828) in differential geometry, and found the method of least squares for fitting lines to data (together with Legendre).

One topic which Gauss did *not* contribute to directly was FLT, although he was responsible for encouraging Sophie Germain in this direction, for some time.

Impossibility of solving equations, and group theory.

The 19th century witnessed the solution to the classical question of solving any equation of degree n in terms of radicals. Earlier mathematicians had thought that the Cardano-Ferrari method could be generalized, and indeed Tschirnhaus (1683) proposed a reduction to a radical equation by changing variables via polynomial substitutions of smaller degree. However, his method was seen by Leibniz to require solving a "resolvent" equation of degree 6, for $n = 5$, so is useless. Nevertheless Tschirnhaus transformations are an important tool in the theory of polynomials. As noted eariler, Lagrange (1770) recognized the roots of a polynomial generate a number system that can be studied in terms of permutations of the roots. Ruffini (1799) published two volumes establishing the nonsolvability of equations of degree 5, but his work of 500 pages was complicated and had mistakes, and was not generally accepted. Abel (1824) gave a much more streamlined proof, solving this ancient question. But Galois (1832), at the age of 19, realized in full the deep connection between field extensions and groups (of automorphisms), and proved that the solvability of a polynomial is equivalent to an intrinsic problem of the corresponding group, called *solvability*. The alternating groups A_n are simple for $n \geq 5$ and thus not solvable. This explains the nonsolvability of polynomials of degree ≥ 5 in general (and in fact gives a verifiable criterion for the solvability of each particular polynomial). Unfortunately, Galois's manuscript which he submitted to the Academy was rejected because of sloppy exposition, and many mathematicians did not grasp the proof. Galois himself became embroiled in a political-romantic feud which ended in his being killed in a dual in 1832. We thank Liouville for going over the manuscript and publishing it with details in 1843. This revolutionized algebra, and gave a completely new point of view for looking at finite groups.

Indeed, the theory of field extensions already available at 1800 easily disposes of the other classical problems (squaring the circle, doubling the cube, trisecting the angle), which all have negative solutions for the same reason, namely that the degree of a constructible number must be a power of 2. (Specifically one must check the three numbers $\sqrt[3]{2}, \arccos \frac{\pi}{9}$, and π). Gauss' work (1801) on cyclotomic polynomials shows that the regular n-gons can be constructed precisely for the values $n = 2^u p_1 \dots p_t$, where $p_1, \dots, p_t$ are Fermat primes (discussed earlier), but the classification of Fermat primes remains open to this day. Strictly speaking, the impossibility of the squaring of the circle had to wait until 1882, when Lindemann proved the transcendence of π.

Cauchy (1789-1857). Perhaps second only to Gauss in the 19th century is the mathematician Augustin-Louis Cauchy. His family were refugees from Paris (to Arcueil) in the French revolution. In 1814 he gave a rigorous memoir on integration. Finally the real numbers were understood. The prime example of this new level of sophistication is Bolzano's theorem (1817) that every polynomial with a positive value and a negative value also has a root. (In particular every polynomial of odd degree over the reals has a root.) Only with Cauchy (1821) were the real numbers understood well enough to describe the limit process in calculus on a truly rigorous footing. (Cauchy sequences.) Cauchy introduced the calculus of complex variables (1829).

Thus, by the mid-nineteenth century, both the real numbers and complex numbers had reached their modern form.

Furthermore, Laplace developed sophisticated tools to advance classical celestial

mechanics (1799-1825).

Dirichlet (1805-1859) proved, among other theorems, that every arithmetic series $a + bn : n \in \mathbb{Z}$ with a, b relatively prime contains infinitely many prime numbers.

Fermat's Last Theorem revisited. We end our account of the 19th century with the history of two problems whose histories occupied much of the 19th and 20th century. The first was referred to by Hilbert in his famous Paris address in 1900, but was not in the list because it was so well known.

FLT is considered the epitomical problem in mathematics for several reasons: The simplicity of its statement, the great mathematicians drawn to it, and the great mathematical concepts which emerged from it. Two major prizes were dedicated to it: The French Academy (which finally awarded the prize to Kummer for showing how hard it is to solve FLT!) and the Wolfskehl prize (in gratitude to the problem which prevented a suicide). As we stated earlier, Fermat had written a proof for $n = 4$, and Euler for $n = 3$, as we observed before.

It is then easy to reduce the problem to n prime ≥ 5. Euler's proof also gives a hint as to how to attack the general conjecture.

Ingredients: Unique factorization in $\mathbb{Z}[\rho]$ to carry out the factorization arguments; use of norm to enable the induction; a finite number of invertible elements in order to be able to handle the different cases.

The history during the first half of the 19th century is rather colorful.

(1) (letter 1800? to Gauss) Sophie Germain proved that if n and $2n + 1$ are prime then any solution satisfies $n|abc$.
(2) 1825 Legendre and Dirichlet solved $n = 5$, based on Germain's work
(3) 1840's Gabriel Lam $n = 7$.
(4) 1 March 1847. Lam and Cauchy announced they were about to solve FLT, and submitted sealed envelopes.
(5) 24 May 1847 Liouville read a letter of Ernst Kummer which showed that $\mathbb{Z}[\rho_n]$ is not a unique factorization domain for $n = 37$, so all methods used until then must fail! (Kummer had already determined in 1844 that there are primes for which the factorization in the domain of cyclotomic integers is non-unique. He thought that $p = 23$ is the first such prime, but had an error in his computation.) Worse more, the number of irregular primes is infinite. In this sense, the Fermat-Euler-Lam-Cauchy approach to FLT was refuted.

    On the other hand, Kummer's work led to the theory of ideals. Over the next hundred years, many individual prime exponents in FLT were eliminated, but no unified program was conceived to attack all primes, for 100 years.
(6) 1956 Taniyama-Shimura conjecture: Every elliptic curve arises from a modular form.
(7) 1983 Using differential geometry (examining the surface $x^n + y^n = 1$ and its rational solutions), Faltings proved that FLT has only a finite number of solutions.
(8) 1984 Frey claimed the elliptic curve. $y^2 = x^3 - (a^n - b^n)x^2 - a^n b^n$ could not arise from a modular form, and thus would be a counterexample to the Taniyama-Shimura conjecture.
(9) 1986 Ribet (with Mazur's help) verified Frey's claim.
(10) 1988 Miyaoka claimed he proved FLT by making Falting's method explicit.

(11) May, 1993 After 7 years intensive work, Wiles announced proof of Taniyama-Shimura conjecture (and thus FLT), by modifying the Kolyavagin-Flach method. Paper submitted to *Inventiones*, where it is subdivided into chapters and sent to separate referees.
(12) 23 Aug. 1993 Katz finds an error in the proof of his chapter.
(13) 25 Oct. 1994 Patched up proof with result on Hecke algebras joint with Taylor.

Noneuclidean geometry. Another ancient question to fall was the independence of Euclid's fifth postulate from Euclid's other axioms of plane geometry. Gauss, Bolyai (1831-2), and Lobachevski(1826-9) produced non-Euclidean geometries. However, Riemann (1854) revolutionized the subject by redefining straight lines in terms of geodesics, which are defined locally (in terms of differentials). Thus, space could intrinsically be curved, which gives rise to easy models of hyperbolic geometry (which is non-Euclidean), and gave the mathematical foundation for Einstein's theory of relativity.

Later nineteenth century developments

We see that by 1850 many of the old issues in geometry, polynomial equations, constructibility, and number theory, had been settled, and celestial mechanics had reached a plateau. New directions of research were indicated.

Riemann (1826-1866). One of the mathematicians most influential in issuing in the modern era of mathematics was Georg Friedrich Bernhard Riemann, a student of Gauss in the latter's old age. We already discussed Riemann's 1854 paper redefining geometry. Riemann also used his ideas to put integration on a much more solid footing.

In 1859 Riemann exploited Euler's formula concerning the Zeta function, to get a good estimate for the number of primes between 1 and n (approximately $\sum_{m=2}^{n} \frac{1}{\log(m)}$). Also Riemann considered the zeta function as a complex function in ζ; noting that the first 10 zeroes that he computed have real part $\frac{1}{2}$, Riemann conjectured that every complex zero must have real part $\frac{1}{2}$. This conjecture was recognized to have far-reaching consequences in number theory (see Hilbert's 8th problem), and subsequently the Zeta function was attached to Riemann's name.

Vector spaces and their transformations.

Hamilton extended the complex numbers in 1843 to get a 4-dimensional version of the complex numbers called the *quaternions*, which however are not commutative.

Cayley (1869) developed geometry in n dimensions, by means of vector spaces and their transformations (which are *matrices*). Incidentally, Hamilton had searched for ten years for a 3-dimensional extension of the reals that contains the complex numbers $\mathbb{C}$. But if it has dimension m as a vector space over $\mathbb{C}$, it must have dimension $2m$ over $\mathbb{R}$, so if Hamilton had known about vector spaces, he would have seen at once to look at four-dimensional examples! Matrices quickly took on a life of their own, for example the Hamilton-Cayley Theorem and Frobenius' Theorem, and took new significance in 1869-1871 during the Franco-Prussian war, when the young Felix Klein (1849-1925) and Sophus Lie (1842-1899) discussed how groups of transformations are the key to geometry. This led to Klein's famous Erlangen program (1872), where he defined all geometries in terms of suitable groups of transformations, thereby redefining geometry in terms of actions of groups on sets.

Lie meanwhile had travelled to Italy with a suitcase full of notes, and was promptly arrested by the French as a suspected spy in the Franco-Prussian War. In jail he had time to go over his notes, and upon release he created the theory of Lie groups, published in 1893.

Cantor (1845-1918) and Infinite sets.

Perhaps the most striking development was the work of Georg Cantor in the theory of transfinite numbers, as expounded in his book (1895-97). The 1:1 equivalences of sets are called *cardinals*.

A set can be in 1:1 correspondence with a subset; Dedekind was the first mathematician who identified such sets as the infinite sets. This is demonstrated popularly in **Hilbert's hotel** demonstrating equality of two different (infinite) ordinals, . Countable = cardinality of first limit ordinal, denoted $\aleph_0$.

Cantor proved (with his famous diagonalization trick) that if $\aleph$ is a cardinal, then $2^{\aleph} > \aleph$, so we have an infinite number of infinite cardinals. In fact there are "too many" infinite cardinals to form a set. In particular the collection of ordinals is not a set. We need this important fact in the sequel.

Cantor showed that there are different, noncommensurate levels of infinity, and that although the rational numbers are dense in the reals, their levels of infinity differ. On the other hand, Cantor also discovered infinite nowhere dense subsets in the interval $[0, 1]$. (At each step, remove the middle third of each segment that remains. What remains are real numbers whose expansion in base 3 are comprised only of the digits 0 and 2, which is clearly uncountable.) In this way, Cantor divorced set theory from topology, and certainly impressed Hilbert, whose first problem, the Continuum hypothesis is due to Cantor: Are there any levels of infinity strictly between that of the integers and that of the reals? Nevertheless, Cantor was not appreciated suitably by the general mathematical community, and died in a mental hospital.

Another development in the foundations of mathematics was Peano's postulates (1889), providing a rigorous basis for mathematical induction, now one of the most common forms of proof.

We end our account of the 19th century with the history of a problem whose solution took 100 years.

The Four-color problem.

This problem has had a checkered history, often considered a puzzle for amateurs rather than mainstream mathematics. After inspiring some topological foundations relating to what we mean by "country" and "border," the problem quickly reduces to a combinatorial question based on Euler's formula, which produces a fast and elegant solution for the 5-color problem (which Haywood found in 1890). Thus by 1900 the whole thrust of the problem was to reduce the bound from 5 to 4.

Indeed, some of its main contributors were not mathematicians, as reflected by terminology: The minimal counterexample was called a *minimal criminal*. This skepticism reached its extreme in Minkowski, who said it was not proved because only "third-rate mathematicians" had attempted its solution. But he retracted, and later said "Heaven is angered by my arrogance." G. Birkhoff and Oyestein Ore gave the problem respectability in this century.

The proof by Appel and Haken has raised new doubts as to the value of the problem in mathematical development. Indeed, rather than introducing fundamental new ideas, its solution does not produces new mainstream mathematics, but rather

involves a series of seemingly ad hoc reductions to a thousand or so cases, which were disposed of by the computer. As such it is a triumph for computer science, but its impact on mathematics has been much less significant than Hilbert's problems.

Note that the four-color problem or five-color problem on the plane is equivalent to the same question on the sphere, since we could easily add one "unbounded" country surrounding everything on the map.

We make a series of reductions, using induction on the number of countries; assume we have a minimal "criminal."

(1) One can assume that there are no vertices or "final edges." Thus each country can be drawn as a polygon, whose edges correspond precisely to the borders with the other countries.
(2) Each vertex has degree at most 3. (Otherwise, at each boundary create a tiny new polygonal country. If one succeeds in coloring this new map, one could color the original map by erasing the tiny new countries.)
(3) Two important properties: Each edge signifies the border of precisely two countries. Also, the degree of a vertex is the number of edges emanating from it, which is also the number of countries reaching that vertex.
(4) The key to the mathematics is Euler's formula $v - e + f = 1$. If a vertex has degree 2, then we disregard it, and combine the two edges emanating from it, to produce a "bent edge". Each "bent edge" still borders precisely two countries. (Since we have removed 1 each from v and from e, Euler's formula still remains valid.) Thus we may assume that each vertex has degree 3. This means $3v = 2e$ in Euler's formula, so multiplying Euler's formula by 3 yields
$$-e + 3f = 3.$$
(5) If n_C denotes the number of countries bordering C, then $\sum n_C = 2e$, since we could count the bordering countries as twice the number of borders. Noting that the number of countries is f, we have $\sum_C 6 = 6f$, and thus
$$-\sum_C n_C + \sum_C 6 = -\sum_C n_C + 6f = 6,$$
or $\sum_C (6 - n_C) = 6$. This key formula shows $6 - n_C$ is positive for some C, i.e., some country has 5 or fewer neighbors.
(6) One is done if there is a country C having 4 or fewer neighbors. For 4 neighbors, one erases two opposing borders, colors the map by induction, redraws the borders, and then, noting we have only used 3 colors for C's neighbors, we color C with the remaining color. For up to 3 neighbors one just erases one border and uses the same argument. Thus every country has $n_C \geq 5$.
(7) The same argument already proves the 5-color theorem. Namely, suppose the country C has five neighbors C_1, C_2, C_3, C_4, C_5; one may assume that C_2 and C_4 do not touch. Make one country from C, C_2, C_4. Color the map by induction; now we have used one color for C_2 and C_4, and at most 1 for each of the other 3 countries, leaving a spare color for C.
(8) (Digression) For surfaces of genus 1 or greater, such as the torus, one can still apply this method to prove a 6-color theorem. Namely, for $n_C = 6$ one could erase 3 nonadjacent borders.

(9) Likewise, the same argument as in (5) enables one to assume there is no cycle of 3 countries.

To prove the 4-color theorem, one seems to need an elaborate system of redrawing maps to change configurations to better configurations. (This is called "discharging.") Maps which cannot be so altered are called "unavoidable configurations," and these often require checking by the computer. Even worse, the computer seems to be needed to perform the discharging procedure.

Hilbert (1862-1943)

David Hilbert himself was a colorful figure. After finishing his thesis (under Hurwitz and Lindemann)(and defending it together with questions in mathematical physics and philosophy) Hilbert moved to Leipsig to study with the master geometer, Felix Klein.

Hilbert's first great breakthrough was in invariant theory. Recall that the determinant and trace of an $n \times n$ matrix A remain unchanged under a change of indices, and more generally, if $f_A = \lambda^n + \sum_{i=1}^n \alpha_i \lambda^i$ is the characteristic polynomial, then each α_i remains unchanged. (Note that $a_1 = -\operatorname{tr}(A)$ and $\alpha_n = (-1)^n \det(A)$.) Since a change of indices corresponds to an action of a permutation, we could define an action of the permutation group S_n on the algebra of matrices, and define the S_n-*invariants* to be those quantities which are independent of the action of S_n. Newton's formulas imply that any S_n-invariant of a matrix A belongs to the algebra generated by $\alpha_1, \dots, \alpha_n$. For example, the invariant $\operatorname{tr}(A^2)$ equals $\operatorname{tr}(A)^2 - 2\det(A)$. More generally, one could define G-invariants of matrices for any subgroup G of S_n, and ask whether the algebra of invariants is affine (finitely generated as an algebra). This had been the major question in invariant theory at the end of the nineteenth century, and many papers had been written for individual groups, by constructing the generators.

In 1888 Hilbert proved his famous basis theorem, that any ideal of a ring of polynomials in finitely many indeterminates is finitely generated, which yields a positive answer to this question. Hilbert's proof was remarkable in that it was totally nonconstructive, and did not give a clue as to how to find the explicit generators. As such, it created a scandal, (Gordon's famous reaction: This is not mathematics - it is theology!) But Klein backed him, and a new concept of algebra began to emerge. Soon thereafter, Hilbert proved his famous Nullstellensatz, and when Klein became director of Gottingen, Klein brought Hilbert along in 1895. Hilbert turned to number theory, and wrote his famous tract which included Hilbert's extension of Gauss reciprocity and many important algebraic results. Then he turned to geometry and cleaned up Euclidean geometry in his book Foundations of Geometry (1899), describing the axiomatic system with such great precision as to permit the understanding of nonEuclidean geometries. Thus, Hilbert's work before 1900 led him to question the nature of the axiomatic framework of mathematics.

Hilbert was to produce great work after 1900 (Solution of Waring's problem, Hilbert spaces, and so forth), and as his influence in Gottingen increased, Hilbert helped make it the mathematical center of the world. He worked for its mathematical welfare, overcoming discriminations of all sort. (He brought in Grommer, a very religious Jew, and Emmy Noether, the first female professor in Gottingen. (Hilbert's famous comment to silence those who were shocked that a woman should enter the halls of the Senate - The Senate is not a bathhouse.) But even Hilbert

could not protect his beloved Gottingen from the Nazi onslaught. When the Nazi minister of education asked Hilbert in 1933 how Gottingen was faring now that Gottingen had been cleansed of Jews, Hilbert replied, "Gottingen is now cleansed of mathematics." By now Hilbert was over 70, and stayed in Germany until he died, but he kept his moral integrity intact.

Hilbert's problems (Paris meeting, 1900). Classical mathematics (including calculus) had largely run its course by the end of the nineteenth century. The problems of antiquity had been solved modulo a question about Fermat primes, the different non-Euclidean geometries were in place, and calculus (even of several variables) was on a firm footing. Accordingly it was natural to request Hilbert, acknowledged at age 38 to be the greatest living mathematician at that time, to list problems for the upcoming century. If his objective was to stimulate research into the twentieth century, Hilbert was immensely successful - most of his problems were answered at least in part (details given in square brackets in the list), and indeed paved the way for much of the research of the twentieth century. Skipping the four-color problem, Hilbert started his address by acknowledging the still unsolved Fermat's Last Theorem, but did not discuss it further because it was so well known. Hilbert proceeded with the following list:

(1) Continuum hypothesis [Cantor's problem, solved by Paul Cohen]. The cardinality of $\mathbb{N}$ is denoted $\aleph_0$.

Cantor proved (with his famous diagonalization trick) that if $\aleph = \text{card})(S)$, then the cardinality of the set of subsets of S is $2^{\aleph} > \aleph$, but this leaves open the question, Is there any cardinal between $\aleph_0$ and $2^{\aleph_0}$?

(2) The consistency and independence of the axioms of set theory. [Answered by Gödel with his compactness and incompleteness theorems]
(3) Can any two tetrahedra of the same base and same height be subdivided into congruent tetrahedra, or combined with congruent tetrahedra to form two polyhedra which can be subdivided into congruent tetrahedra? [Solved by Dehn]
(4) What geometries can be defined using the sole axiom that the shortest distance between two points is a straight line?
(5) Is every locally Euclidean group of transformations a Lie group?
(6) Axiomatic development of the laws of physics.
(7) Transcendence of various numbers, for example $e^{i\pi x}$ when x is irrational algebraic. Or geometrically, in an isosceles triangle if the ratio of angles is irrational algebraic, then is the ratio of the sides transcendental? [Gel'fond-Schneider Theorem : If a, b are algebraic and b irrational then a^b is not algebraic.]
(8) Riemann conjecture: Do all the complex zeroes of the Zeta function have real part $\frac{1}{2}$? How does this affect the distribution of prime numbers? [Deligne proved it for varieties over a finite field, but this remains the most significant open problem on the list.] Is $\zeta(3)$ transcendental?
(9) Can quadratic reciprocity laws be generalized to prime powers?
(10) Is there an algorithm to solve diophantine equations? [No, answered by ??]
(11) Is there a method of solving quadratic equations in several indeterminates (rational solutions)? [Yes, answered by ??]
(12) Can one generalize Kronecker's Theorem that any abelian number field can be obtained by adjoining roots of 1? [Inspired by Jugendtraum (letter from

Kronecker to Dedekind in 1880) This relates to elliptic curves.]

(13) Are there polynomials of degree 7 which are impossible to solve by means of continuous functions in two parameters? (Specifically $x^7 + ax^3 + bx^2 + cx + 1 = 0$.) [Degree 5 and 6 functions can be reduced by means of Tschirnhaus transformations; answer given by]

(14) If $R = F[a_1, \dots, a_n]$ is an affine domain with field of fractions K, and if k is a subfield of K then is $R \cap k$ affine? In particular what if k is the fixed subfield of K under a group of automorphisms? [There are counterexamples of Nagata (1959).]

(15) Put Schubert's enumerative calculus (of geometric configuations) on a rigorous footing. [Schubert made some amazing claims which have never been verified or disproved. For example in 1879 Schubert claimed that there are 666,841,048 quadric surfaces tangent to 9 given quadric surfaces in space.]

(16) Topology of algebraic curves and surfaces

(17) Can every positive definite form be expressed as the quotient of two quadratic forms? [Answered in the affirmative by E. Artin (1926) using the Artin-Shreier theory of real closed fields.]

(18) In n-dimensional Euclidean space is there only a finite number of different groups of motions with a compact fundamental region? [Bieberbach (1910) proved this, giving rise to theory of tiling. Heesch found tiling by a polygon which is not a fundamental domain.]

(19) Are the solutions to regular problems (i.e. Lagrangians) in the calculus of variations always analytic?

(20) What are the boundary values of elliptic partial differential equations?

(21) The existence of linear differential equations having prescribed monodromic group.[Deligne (1970) solved it.]

(22) Uniformization of analytic relations by means of automorphic forms. [Answered in the affirmative by Poincar and Koebe (1913).]

(23) Extensions of the calculus of variations [This problem is the one most developed in his article, but less explored in the literature.]

Hilbert's third problem. This problem by Hilbert was solved by Dehn (1900) almost as soon as Hilbert posed it, although [Bo] claims that the first readable proof was written by Kagan (1903). The 2-dimensional case was known essentially by the ancients, who certainly knew how to cut a triangle into pieces which reassemble to a rectangle of the same base and half the height, thereby yielding the area of the triangle as $\frac{1}{2}bh$. We say two polygons are *equidecomposable* if they can be subdivided (through a finite number of cuts) into a finite number of congruent polygons; here is a proof in stages that any two polygons having the same area are equidecomposable:

(1) Any two given rectangles having the same area are equidecomposable. (Proof: Superimpose them and then run a diagonal from the top left to bottom right. One thereby obtains a common shape (pentagon) plus two triangles in each rectangle, congruent pairwise. Indeed, the two pairs of triangles are similar. Thus it suffices to prove that the areas of the similar triangles are equal. Since the sum of the areas is the same, it suffices to prove that the area S_1 of the upper left triangle T_1 equals the area S_2 of the lower right triangle T_2, or equivalently, letting S_3 be the area of the large lower left triangle, we need $\frac{S_1}{S_3} = \frac{S_2}{S_3}$. If the two rectangles have respective bases b_i and heights h_i,

$i = 1, 2$, then the triangle t_1 has height $h_2 - h_1$ and the triangle t_2 has base $b_2 - b_1$. Given $b_1 h_1 = b_2 h_2$ it follows that

$$\frac{b_2 - b_1}{b_2} = \frac{h_1 - h_2}{h_1}$$

so

$$\frac{S_1}{S_3} = \left(\frac{b_2 - b_1}{b_2}\right)^2 = \left(\frac{h_1 - h_2}{h_1}\right)^2 = \frac{S_2}{S_3},$$

and thus T_1 and T_2 are congruent (and likewise for the other pair of triangles). Thus triangle can be slid down, and the other moved to fill the gap.

(2) Any triangle is equidecomposable to a rectangle. Run a parallel halfway up the base, and slice the upper triangle along the height. This will enable you to put them together in a rectangle.

(3) Any two polygons of the same area are equidecomposable. Indeed, slice one into triangles, and rearrange it into rectangles; then each rectangle is equidecomposable to a rectangle with a given base, say 1, by (1), so we can put them together to one big rectangle; we conclude with (1) again.

We have proved that any polygon can be cut and reassembled to a rectangle with base 1 and some height h; then we could *define* the area to be h. This definition of area is fast, intuitive, and does not depend on any limit process. Thus, it would be nice to have an analogue in three dimensions, which would enable us to define volume.

Hilbert suspected that there is no such decomposition in higher dimensions, based on the evidence that in the preceding 2000 years nobody had produced a direct computation of the volume of tetrahedra; all proofs use limits.

Bricard had proposed a theorem in 1896 which would have yielded the solution to Hilbert's third problem. However there was an unfilled gap, so the problem was posed.

Before proceeding let us pause and use Archimedes' formula $V = \frac{1}{3}Bh$ to compute the volume of a regular tetrahedron, i.e. formed by equilateral triangles, each having edge of length 1. Then each median in the base has length $\frac{\sqrt{3}}{2}$, so the base has area $B = \frac{\sqrt{3}}{4}$. The altitude from the top meets the three medians $\frac{2}{3}$ of the way across, so is part of a right angle triangle whose base is $\frac{\sqrt{3}}{6}$ and whose hypotenuse is $\frac{\sqrt{3}}{2}$, so the altitude itself is

$$h = \frac{\sqrt{3}}{2}\sqrt{1 - \frac{1}{9}} = \frac{\sqrt{3}}{2}\frac{\sqrt{8}}{3} = \frac{\sqrt{2}}{\sqrt{3}},$$

and thus the volume is

$$\frac{1}{3}Bh = \frac{1}{3}\frac{\sqrt{3}}{4}\frac{\sqrt{2}}{\sqrt{3}} = \frac{\sqrt{2}}{12}.$$

But notice that we relied on a formula which does not have a proof without limits.

Dehn's negative solution to Hilbert's third problem relies on the clever use of an invariant associated to any polyhedron.

Recall the *dihedral angle of an edge* at the intersection of two planes is the angle formed by the two normal vectors taken in the planes. This is clearly the same at

any point of the edge. Dehn was probably inspired by the fact that the dihedral angle of the edge of a regular tetrahedron has cosine

$$\frac{\sqrt{3}}{6}/\frac{\sqrt{3}}{2} = \frac{1}{3},$$

as seen in the previous paragraph; on the other hand the dihedral angles of the right-angled pyramid are $\frac{\pi}{2}$ and $\frac{\pi}{4}$.

Lemma. *Let $\theta = \arccos \frac{1}{3}$. Then $\frac{\theta}{\pi}$ is not rational.*

Proof. Otherwise, say $\theta\pi = \frac{p}{q}$ for p, q integers, $q > 0$. Then $\cos(\frac{p\pi}{q}) = \frac{1}{3}$, i.e. letting $\theta = \frac{p\pi}{q}$,

$$\cos\theta = \frac{1}{3}; \qquad \cos q\theta = \pm 1.$$

This is false, for we claim by induction on q that $\cos q\theta = \frac{a_q}{3^q}$ where 3 does not divide a_q. Indeed, for $q = 2$, $\cos 2\theta = 2\cos^2\theta - 1 = -\frac{8}{9}$; for $q = 3$,

$$\cos 3\theta + \cos\theta = 2\cos 2\theta\cos\theta = -\frac{16}{27},$$

implying $\cos 3\theta = -\frac{16}{27} + \frac{1}{3} = -\frac{7}{27}$. In general one concludes with the formula

$$\cos(q+1)\theta + \cos(q-1)\theta = 2\cos q\theta\cos\theta.$$

By induction,

$$\cos(q-1)\theta = \frac{a_{q-1}}{3^{q-1}}; \qquad 2\cos q\theta\cos\theta = \frac{2a_q}{3^{q+1}},$$

implying

$$\cos(q+1)\theta = \frac{2a_q - 9a_{q-1}}{3^{q+1}},$$

as desired.

Thus the dihedral angle $\alpha = \arccos\frac{1}{3}$ is linearly independent of π, and we need an invariant under equidecomposability which can differentiate between polyhedra with dihedral angles $\arccos\frac{1}{3}$ and those with angles which are rational multiples of π. Here is Dehn's candidate. We can define a $\mathbb{Q}$-linear function $f\colon \mathbb{R} \to \mathbb{R}$ by $f(\pi) = 0$ and $f(\alpha) = 1$.

Given a $\mathbb{Q}$-linear function $f\colon \mathbb{R} \to \mathbb{R}$ such that $f(\pi) = 0$, we define the *Dehn function* $g(A)$ on a polyhedron A with sides $\ell_1 \dots \ell_p$ and corresponding dihedral angles $\alpha_1, \dots, \alpha_p$ to be $\sum \ell_i f(\alpha_i)$. It is not hard to see that if a polyhedron A is cut into two polyhedra A_1 and A_2, then the Dehn function on A is the sum of the Dehn functions on A_1 and A_2. This is seen by examining the two possibilities for a cut.

CASE I. The cut is made through an edge (not at a vertex). The contribution at the edge ℓ_i (cut say into edges ℓ_{i1} and ℓ_{i_2} was originally $\ell_i f(\alpha_i)$ and after the cut is the sum of $\ell_{i1} f(\alpha_i)$ and $\ell_{i2} f(\alpha_i)$, which is $(\ell_{i1} + \ell_{i1}) f(\alpha_i)$, the same as before. On the other hand, any new face in A_1 has an opposite face at A_2, so in computing the Dehn function one has merely added terms

$$\ell f(\alpha) + \ell f(\pi - \alpha) = \ell f(\pi) = 0.$$

This proves that $g(A) = g(A_1) + g(A_2)$.

CASE II. The cut is made through a vertex. Now the original dihedral α_i is divided into α_{i1} and α_{i2}, whose contributions $\ell_i f(\alpha_{i1})$ and $\ell_i f(\alpha_{i2})$ sum to $\ell_i f(\alpha_i)$, the original contribution from that edge. The contributions from new edges cancel as before, so again we get $g(A) = g(A_1) + g(A_2)$.

An easy induction shows that the Dehn function is additive, in the sense that if there is a decomposition $A = \sum A_i$ then $g(A) = \sum g(A_i)$. Consequently if A, B are equidecomposable polyhedra then $g(A) = g(B)$. We have sketched the proof of

Dehn's Theorem. *Suppose A, B have different values under a Dehn function. Then A, B are not equidecomposable*

In particular, since the cube has Dehn number 0 but is the disjoint union of two congruent right tetrahedra, we see the Dehn number of the right tetrahedron is 0.

Corollary. *The regular tetrahedron and right-angled tetrahedron are not equidecomposable.*

Proof. We define a $\mathbb{Q}$-linear function $f\colon \mathbb{R} \to \mathbb{R}$ by $f(\pi) = 0$ and $f(\alpha) = 1$. We saw $g(\text{right-angled tetrahedron}) = 0$, but if P is a regular tetrahedron with side m then $g(P) = 6m \neq 0$.

In fact, Sydler (1965) proved that two polyhedra A, B of the same area are equidecomposable iff for *every* Dehn function f we have $g(A) = g(B)$. [Bo] uses a proof of Jessen (1968), which still is quite difficult.

Hilbert's second problem - Foundations of set theory. Already by Hilbert's time the more refined techniques of mathematics were beginning to lead to a disturbing number of paradoxes. For example, surely there should be some largest level of infinity, but Cantor's work shows this is impossible in the mathematical framework. Thus Hilbert's second problem could be viewed as a plea to the mathematical community to establish foundations for mathematical before the impending earthquake. (Little did he know that this work would bring on the earthquake.)

Peano gave postulates for $\mathbb{N}$ which serve as the basis for mathematical induction, but in the early 20th century this was put in the framework of more general axiomatic system for set theory (Hilbert-Bernays-von Neumann-Gödel). $=$, $\in$, $\{\ :\ \}$ are primitives. Reversing our initial intuition, we say a *set* is a member of some class. Thus the *universe* $\mathcal{U} = \{x : x = x\}$ is not a set, but all members of $\mathcal{U}$ are sets. We permit the usual operations on classes $(\ , \cap, \cup, \emptyset)$, and the axiom of subsets. One can prove that if S is a set then so is its *power set* $\mathcal{P}(S)$, which is the set of subsets of S, also denoted 2^S. One can define an *ordered pair* (x, y) as the set $\{x, \{x, y\}\}$, and thus define a relation as a set of ordered pairs, and a function as a relation f which is single-valued (i.e. if $(x, y), (x, z) \in f$ then $y = z$.

Since $2^{\aleph} > \aleph$, we have an infinite number of infinite cardinals. In fact this yields *Cantor's paradox*: There are "too many" infinite cardinals to form a set (since 2 to its power would be greater.)

An easier way to state this difficulty is via *Russell's paradox*, which is closely related to described above: Call a set *extraordinary* if it is a member of itself; otherwise it is *ordinary*. Is the set of ordinary sets ordinary or extraordinary? (This paradox shows that you cannot name a set as a collection of certain elements.)

Bertrand Russell (Bertrand Arthur William Russell, 3rd Earl Russell, 18 May 1872 2 February 1970) went on to write **Principia Mathematica** (three volumes

– 1910, 1912, 1913) with Whitehead, but always felt something was missing; his paradox indicated that self-referential sentences will always throw in a monkey-wrench. Frege ignored this and wrote tomes about foundations of mathematics, using self-reference. This led Russell to write his famous letter to Frege, saying how much he appreciated the latter's book, but that he had one little question to ask:

In a small town, a barber shaves all those and only those who do not shave themselves. Russell's question: Who shaves the barber?

In order to avoid Russell's paradox, we have

Regularity axiom. *(Skolem (1923) and von Neumann (1925)).*
For any $S \neq \emptyset$ there is $x \in S$ such that $x \cap S = \emptyset$.

Proposition. *$S \notin S$ for all sets S.*

Proof. Consider the singleton $\{S\}$.

Corollary. *For any sets S, T one has either $S \notin T$ or $T \notin S$.*

Proof. Consider the doubleton $\{S, T\}$.

Zermelo-Frankel axioms.

Zermelo (1908) and A. Fraenkel (1922-23) determined the set-theoretic axioms on which most mathematical proofs are based:

(1) Set existence (There is a set)
(2) Extensionality (Two sets with the same elements are equal)
(3) Foundation = Regularity axiom
(4) Pairing (For any two sets there is a set of two elements, whose members are precisely the two original sets.)
(5) Union of sets is a set
(6) Comprehension Scheme (Any subclass of elements of a set satisfying a given formula defines a subset.)
(7) Replacement Scheme: Any class of elements defined by a function constitutes a set.
(8) Power set (defined above).
(9) Axiom of infinity (defined presently).

One way to avoid intrinsic contradictions is to restrict one's definition of sets. The ZF axioms lead us to define the *ordinal numbers*. We start with the *finite ordinals*:

$$\mathbf{0} = \emptyset, \quad \mathbf{1} = \{\emptyset\} = \{\mathbf{0}\}, \quad \mathbf{2} = \{\{\emptyset\}, \emptyset\} = \{\mathbf{1}\} \cup \mathbf{1}, \quad \ldots,$$

$$\ldots, \quad \mathbf{n+1} = \{\mathbf{n}\} \cup \mathbf{n}, \quad \ldots$$

It is clear that the ordinals are well-ordered, insofar as each ordinal is a member of each subsequent ordinal, and not vice versa (because of the corollary above).

To proceed further we need

Axiom of infinity. *There is a nonempty set S containing 0 satisfying $x \cup \{x\} \in S$ whenever $x \in S$.*

It follows at once that $\cup\mathbf{n}$ is a subset of this set, which is called ω. This is the first infinite ordinal, and we can keep on going. In general given an ordinal ω write

$\omega^+ = \{\omega\} \cup \omega$; an ordinal is a *limit ordinal* if it is the set of ordinals less than itself. In general, a set S is an *ordinal* if $\in$ is transitive (i.e., the member of a member is a member).

Transfinite induction means that a property is proved for an ordinal ω if it can be proved for 0, and given the property on a given set of ordinals it is also true for their successor and union (i.e., the limit ordinal formed from them). Indeed, this is immediate from the definition of ω.

Gödel.

When Russell posed his famous paradoxes, although it shook up mathematicians, they seemed to be metamathematical and perhaps could be glossed over by strict language which forbad self-referencing. But the man who almost singlehandedly remade logic, over a space of 10 years, was Kurt Gödel (1906–1978), born in Brno, Austria-Hungary (which became Czechoslovakia).

Gödel's completeness theorem (1929). Any consistent infinite system of axioms has a *model* of not greater cardinality, i.e., some system that satisfies all the given axioms without a contradiction.

Consequently, if a statement p cannot be proved from S, there is a model satisfying both S and the negation of p, i.e., in which p is false.

Nonetheless. In 1930 Gödel proved his two incompleteness theorems.

The first is that for any set of axioms concerning arithmetic, there always will be a sentence about the natural numbers that can be neither proved nor disproved. The idea is very simple. Since the set of symbols used in formulating sentences is finite, one can enumerate them (say, alphabetically). Some of these sentences can be proved, and others cannot.

Gödel's incompleteness theorem goes back to the Greeks' knowledge that language necessarily contains internal contradictions. ("This statement is false.") One needs to modify it to "This statement is unprovable." Gödel succeeded in formulating such a paradox in arithmetic.

Gödel's second incompleteness theorem goes even further and asserts that one cannot prove that any axiomatic system containing all sentences holding in the arithmetic of natural numbers is consistent.

Although not Jewish, Gödel was attacked by Nazis for looking like a Jew and sympathizing with them, and immigrated to the US in 1940. Already in the 1930's Gödel had repeatedly visited the Institute for Advanced Studies in Princeton, and inspired the work to be described now.

Recursive functions and computability.

These difficulties arise from self-referencing. This still left open the question of treating concrete questions in arithmetic in a stricter framework which does not permit self-referencing, a subject of intense investigation in Princeton in the 1930's. First one has to specify which sentences are admissible. These were proposed by Church (1903-1995), but, building on work of Herbrand, Gödel preferred a different definition, now known as recursive functions. (Defining $f\colon \mathbb{N} \to \mathbb{N}$ in terms of values of a given finite number of functions $h_1, \ldots, h_m$ already defined on $1, \ldots, n-1$). These definitions were proved in 1935 by Church and his students Kleene (1909-1994) and Rosser (in Princeton) to be equivalent, leading to **Church's Thesis** that all meaningful assertions in arithmetic could be formulated in these terms.

A set is **recursively enumerable** if it is the range of a recursive function. This could be interpreted as the set of "solutions" to a certain mathematical system,

so it is important to know whether or not a certain number m is contained in a recursively enumerable set S. The problem is that although as soon as we display $m = f(n)$ we know $m \in S$, what happens if $m \notin S$? We only find out after an infinite number of steps. Thus we define S to be **recursive** if both S and $\mathbb{N} \setminus S$ are recursively enumerable. For such a set S, for any natural number n, we can determine after a finite number of steps whether or not $n \in S$.

Thus the provability of statements in arithmetic is seen to be similar to the question of whether or not all recursively enumerable sets are recursive.

However, one still has the assertion, discovered by the Princeton group in 1934:

Theorem. *There exists a recursively enumerable set which is not recursive.*

Indeed, one can list the recursive functions as $f_1, f_2, \ldots$, say first according to the physical length of the sentence used to define them, and then alphabetically. Now define the function f by $f(n) = f_n(n)$. Let S be the range, i.e., $m \in S$ iff $m = f_n(n)$ for some n. This set is recursively enumerable. We claim S cannot be recursive. For otherwise there would be a recursive function g such that $m \notin S$ iff $m = g(t)$ for some t. Write $g = f_n$ Then $f_n(n) \in S$ by definition of S, but $f_n(n) = g(n) \notin S$, by definition of g, contradiction.

This proof does not contain self-referencing, since there is a perfectly reasonable algorithm for listing the recursive functions and then defining f accordingly. The same idea was discovered independently in 1936 by Turing (1912-1954), when he was going through the presumably routine process of trying to define the essence of an artificial calculating machine. (He defined the idealized "Turing machine," which consisted of a finite number of states and the ability to move a tape back and forth and make or erase marks depending on the state. Intuitively, the provable statements should be those which can be verified by a suitably programmed Turing machine, but he demonstrated along the lines above that there always will be true result that cannot be programmed. Today Turing machines are used in most expositions on recursiveness.

Turing's life was also greatly affected by the World War. He was leader of the team that succeeded in decoding the German Enigma machine (1938). However, his personal life did not match the norms encoded into British law, and he was humiliated to the point that he finally poisoned himself.

Axiom of Choice.

Even before Gödel was showing that any system of axioms is incomplete, questions were being raised as to which set-theoretic axioms depend on others. A *choice function* is a function f which satisfies $f(x) \in x$ for every member x of the domain of f. One axiom which was shown to be independent of the others is the following: For any set $\mathcal{S}$ there is a choice function with domain $\mathcal{S}$, in other words a function $f\colon \mathcal{S} \to \cup S_i$ sending S_i to an element of S_i, for each $i \in I$.

This might seem self-evident, but has some far-reaching consequences.

Theorem. *Any set S is in 1:1 correspondence with an ordinal.*

Proof. By transfinite induction one can build a 1:1 function from each ordinal into S, so if one could proceed forever one would have a 1:1 function from all ordinals to S, contrary to the fact the the collection of ordinals is not a set. Thus this process must stop, which means for some ordinal our 1:1 function is onto.

For example, we say a set is *well-ordered* if every subset has a minimal element. Any ordinal obviously is well-ordered, so the axiom of choice implies that every set is well-ordered (with respect to an appropriate order).

Another application: a totally ordered set is also called a *chain*.

Theorem. *For any set S, any subchain is contained in a maximal subchain of S.*

Proof. Order the elements by means of the previous theorem; keep on adding one element at a time (using a choice function) until one is done.

Immediate consequences:

(1) Banach maximality principle. If every chain in a collection of sets $\mathcal{S}$ is bounded (under containment) by a member of $\mathcal{S}$, then $\mathcal{S}$ contains a maximal set.
(2) minimality principle. If every chain in a collection of sets $\mathcal{S}$ is bounded below by a member of $\mathcal{S}$, then $\mathcal{S}$ contains a minimal set.
(3) Kuratowski lemma. Every chain in a partially ordered set is contained in a maximal chain.
(4) Zorn's lemma. If every chain in a partially ordered set has an upper bound, then the set has a maximal element.
(5) Tarski proved that $|S|^2 = |S|$ implies the axiom of choice, but Sageev (1973) showed that $2|S| = |S|$ does *not* imply the axiom of choice.

(1) implies (2) was discovered by Zermelo (1908). In fact, during the subsequent 20 years, it was seen that the Hausdorff maximality principle to prove the axiom of choice, so that we have the following additional equivalence:

(1) Axiom of choice
(2) Each set can be well ordered.
(3) Hausdorff maximality principle

Hilbert's first problem - The continuum hypothesis. Paul Cohen (1958?) proved this is independent of the other axioms of set theory, by building one model where it holds and another in which it does not. His method, which involves constructing models whose ordinals have varying properties (and thus the continuum hypothesis holds in one such model but not in another), is called *forcing*, and revolutionized mathematical logic in the mid-twentieth century. Another burst in this field was provided by nonstandard analysis, involving infinitesimal quantities which finally justified Leibniz' approach to calculus.

Hilbert's tenth problem. The failure of algorithms in many aspects of arithmetic led Post in 1944 to suspect that there is no algorithm to solve Diophantine equations. First of all, in view of Lagrange's theorem that every natural number is a sum of squares, every Diophantine equation over $\mathbb{Z}$ can be reduced to a Diophantine equation over $\mathbb{N}$, so it suffices to consider Diophantine equations over $\mathbb{Z}$.

Crossing the barrier of the Iron Curtain, Martin Davis, Julia Robinson, and Yuri Matiyasevich (1954) proved that every recursively enumerable set is Diophantine.

If there were an algorithmic method to solve Diophantine equations, then there would be an algorithmic method to check whether or not an element is in a recursively enumerable set, i.e., if the recursively enumerable set is recursive, which is impossible. Hence Hilbert's tenth problem has a counterexample!

Review of independence of various axioms of set theory.

(1) Axiom of Infinity

(2) Axiom of Choice (equivalent to the well-ordering of the ordinals, and to $|S|^2 = S$)
(3) Continuum hypothesis
(4) Gödel's incompleteness theorem
(5) Turing machine (recursively enumerable versus recursive)

The age of paradoxes

The 19th century had witnessed the erection of some of the great edifices of mathematics, groups and matrices. This development continued throughout the 20th century, with ever more sophisticated techniques pushing methods further and further. However, by the beginning of the 20th century, some of the structure had begun to crack at the foundations. We already noted the paradoxes of Cantor and Russell and how they were bypassed. However, deeper paradoxes emerged in the coming decades.

Geometric paradoxes. The axiom of choice is used so often in mathematics that it is hard to imagine how we could live without it. Nevertheless, if we accept it we have to live with at least one result which would make us uncomfortable: Things began to unravel when Hausdorff (1912) partitioned the 2-sphere into two parts each of which is congruent to the original sphere. This was refined to:

Banach-Tarski paradox. *Any sphere can be cut with a finite number of cuts into parts which can be reassembled to a sphere of twice the size.*

The underlying idea of the paradox was an observation which can be traced back to Galileo, that one can divide the set of natural numbers $\mathbb{N}$ into two sets each in 1:1 correspondence to $\mathbb{N}$, namely the odd integers and the even integers. (In fact, Galileo's observation does not rely on the axiom of choice, and the true nature of the paradoxes might lie in the fact that nature does not act pointwise.)

Since Klein had reformulated geometry in terms of actions of groups on sets, it remained to make this partition compatible to group actions. Recall a *group action* on a set S is defined formally as an operation $G \times S \to S$ satisfying $1s = s$ and $(ab)s = a(bs)$ for $a, b \in G$, $s \in S$. Intuitively, the elements of the group act as 1:1 transformations on the set S.

Suppose a group G acts on a set S. We say that a subset E of S is *G-paradoxical* if there are disjoint subsets $A_{i,j}$ of E and $\sigma_{ij} \in G$ such that

$$S = \cup_i \sigma_{i1}(A_{i1}) = \cup_i \sigma_{i2}(A_{i2}).$$

Lemma. *$\mathbb{Z}$ is paradoxical under the set of 1:1 transformations from $\mathbb{Z}$ to itself.*

Proof. (i) We partition $2\mathbb{Z}$ into $4\mathbb{Z} \cup 4\mathbb{Z}+2$, and partition $2\mathbb{Z}+1$ into $4\mathbb{Z}+1 \cup 4\mathbb{Z}+3$. Now there are transformations of $\mathbb{Z}$ sending $4\mathbb{Z}$ to $2\mathbb{Z}$, or sending $4\mathbb{Z}+2$ to $2\mathbb{Z}+1$, or sending $4\mathbb{Z}+1$ to $2\mathbb{Z}$, or sending $4\mathbb{Z}+3$ to $2\mathbb{Z}+1$, so we have the paradoxical action. □

A different sort of example: Any group G acts on itself by taking the group operation on the left.

Incidentally, the fact that an arbitrary infinite set S is paradoxical under the group of bijections means $2|S| = |S|$.

Proposition. *The circle S^1 is countably paradoxical under the group of rotations.*

Proof. Let σ_m denote the rotation by m radians. Say two points are equivalent if one can be rotated to the other by some σ_m. Let $A = \{\sigma_m : m \text{ odd}\}$ and $B = \{\sigma_m : m \text{ even}\}$. Define a set S_0 by choosing one element from each equivalence class of S^1. Then $S^1 = \cup\sigma_i S_0 = AS_0 \cup BS_0$, but

$$S^1 = \cup\sigma_i S_0 = \cup\sigma_i\sigma_{2i-1}^{-1}(\sigma_{2i-1}S_0) = \cup\sigma_i\sigma_{2i}^{-1}(\sigma_{2i}S_0).$$

Although this paradox relied heavily on the axiom of choice, one can also obtain paradoxes without it. Let us isolate the principle behind the next set of paradoxical actions. The **free semigroup** is the semigroup of formal words, where multiplication is juxtaposition. We say a the free semigroup A on x, y acts *disjointly* on a point s of S if for each $v, w \in A$ we have

$$xvs \neq yws$$

(Thus the free semigroup acts disjointly on itself.)

Proposition. *Suppose G contains a free semigroup A acting disjointly on a point s of set S. Then the action of G on As is paradoxical.*

Proof. $As = x^{-1}xAs = y^{-1}yAs$.

Theorem(Sierpinski-Mazurkiewicz Paradox). *The real plane $\mathbb{R}^2$ contains a nonempty paradoxical subset (under isometries).*

Proof. Take $u = e^{i\theta}$ transcendental. The rotation $z \mapsto uz$ and the translations $z \mapsto z + 1$ generate a free semigroup acting disjointly on the origin. (To see this, write x for the rotation $z \mapsto uz$ and y for the translation $z \mapsto z + 1$. Let $m_1, n_1, m_2, n_2, \ldots, m_t$ to denote that one applies x m_t times, and then y n_{t-1} times, and then x m_{t-1} times, and then y n_{t-2} times, and so forth. (We do not apply y at the beginning since $y(0) = 0$.) Then 0 is sent to m_t, and then to $u^{n_t}m_t$, and then to $u^{n_t}m_t + m_{t-1}$, and then to $u^{n_{t-1}}(u^{n_t}m_t + m_{t-1}) = u^{n_{t-1}+n_t}m_t + u^{n_{t-1}}m_{t-1}$, and so forth. Thus $m_1, n_1, m_2, n_2, \ldots, m_t$ sends 0 to

$$u^{n_1+\cdots+n_{t-1}+n_t}m_t + u^{n_1+\cdots+n_{t-1}}m_{t-1} + \cdots + m_1.$$

Since u is transcendental, these are all different, corresponding to polynomials in u which have constant term m_1, so the action on 0 is disjoint. □

Corollary. *For any Lebesgues measure on $\mathbb{R}^{(2)}$ there is some unmeasurable set.*

Note this paradox did not rely on the axiom of choice. This idea can be extended to get the Banach-Tarski paradox. First note that the group of rotations SO_n has a free subgroup G generated by two matrices

$$\phi_1 = \begin{pmatrix} \frac{1}{3} & -\frac{2\sqrt{2}}{3} & 0 \\ \frac{2\sqrt{2}}{3} & \frac{1}{3} & 0 \\ 0 & 0 & 1 \end{pmatrix}; \qquad \phi_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{3} & -\frac{2\sqrt{2}}{3} \\ 0 & \frac{2\sqrt{2}}{3} & \frac{1}{3} \end{pmatrix}$$

Indeed, to check that no nontrivial word w in ϕ_1, ϕ_2 equals 1, after conjugating by a suitable power of ϕ_2 and ϕ_1, one may assume the word ends in ϕ_1. But then $w(1, 0, 0) = \frac{1}{3^k}(a, b\sqrt{2}, c)$ for some k, with b not divisible by 3. □

(The first such construction was found by Hausdorff(1914). This example is due to Swierczkowski.) In fact Tits (1972) proved a deep theorem that any subgroup of GL_n is either solvable or contains a free nonabelian subgroup.

Theorem(Hausdorff Paradox). *There is a countable subset $D \subset \mathrm{SO}_3$ which when removed from S^2 yields a SO_3-paradoxical set.*

Proof. Each rotation in the free subgroup G (defined above) of SO_3 has exactly 2 fixed points, and the free group is clearly countable since it is generated as a semigroup by four elements. Taking D to be the set of all of these points, it is clear that G acts freely on $S^2 \setminus D$, so $S^2 \setminus D$ is SO_3-paradoxical $\square$

Thus the Banach-Tarski paradox will be achieved by reducing this countable set D to the empty set. This is done by using some of the ideas in Hilbert's 3rd problem.

If G acts on a set S and $A, B \subset S$ we say B is *G-equidecomposable* to A if A, B can be partitioned into the same finite number of G-congruent pieces, i.e. $A = \cup_{i=1}^n A_i$, $B = \cup_{i=1}^n B_i$, and $\sigma_i A_i = B_i$ for $1 \leq i \leq n$. Clearly G equidecomposability is an equivalence relation (although more pieces may be required), and any set G-equidecomposable to a G-paradoxical set is also G-paradoxical.

We need a classical result from set theory.

Theorem(Banach-Shroeder-Bernstein). *If A is G-equidecomposable to a subset of B and B is G-equidecomposable to a subset of A then A is G-equidecomposable to B.*

Proof. Two Hilbert Hotel arguments intertwined. Let $f\colon A \to B$ and $g\colon B \to A$ be the 1:1 maps producing the G-equidecomposability, and $C_0 = A$, $D_0 = B$, and inductively $C_i = g(D_{i-1})$ and $D_{i+1} = f(C_i)$. Let $A_\infty = \cap_i A_i$ and $B_\infty = \cap_i B_i$. Then clearly $f(A_\infty) = B_\infty$, so f restricts to a 1:1 onto function $f_\infty : A_\infty \to B_\infty$. Moreover f restricts to a 1:1 onto function $f_i : C_{2i} \setminus C_{2i+1} \to D_{2i+1} \setminus D_{2i+2}$ and g restricts to a 1:1 onto function $g_i : D_{2i} \setminus D_{2i+1} \to C_{2i+1} \setminus C_{2i+2}$ whose inverse we call $\hat{f}_i : C_{2i+1} \setminus C_{2i+2} \to D_{2i} \setminus D_{2i+1}$. Piecing together these maps shows that the f_i, $\hat{f}_i$, and f_∞ shows that A is G-equidecomposable to B. $\square$

Theorem. *If D is a countable subset of S^2, then the sets S^2 and $S^2 \setminus D$ are SO_3-equidecomposable.*

Proof. Since D is countable, there is a line ℓ through the origin that misses D. Furthermore there is a rotation ρ around ℓ of some angle θ degrees such that

$$\rho^m(D) \cap D = \emptyset, \quad \text{for all} \quad m \in \mathbb{Z},$$

and thus $\rho^m(D) \cap \rho^n(D) = \emptyset$ for all m, n. Taking $\bar{D} = \cup_{i \in \mathbb{N}} \rho^i(D)$, we have

$$S^2 = \bar{D} \cup (S^2 \setminus \bar{D}) \sim \rho(\bar{D}) \cup (S^2 \setminus \bar{D}) = S^2 \setminus D.$$

$\square$

Using the radial decomposition, we conclude that the unit ball $B \setminus (0,0,0)$ is SO_3-paradoxical, so we need to prove $B \setminus (0,0,0)$ is SO_3-equidecomposable to B. Take a rotation in space of infinite order of $(0, 0, \frac{1}{2})$ missing the origin, and use the same tricks as above.

Although the proof above of the Banach-Tarski paradox requires an uncountable number of rotations, one can prove S^2 is paradoxical iff G has a free subgroup of rank 2 (i.e. G nonsolvable). Unknown if can preserve Baire property.

Another paradox which seemed to arise in analysis is that Banach's definition of dimension sometimes gives fractional dimensions. (However, in the later 20th century Mandelbrot exploited this fact to introduce the theory of fractals.)

New directions in the 20th century

Aside from his prophetic excursion into foundations, Hilbert dealt largely with natural extensions of the nineteenth century. However, certain developments in the twentieth century have brought on a new direction.

Computational mathematics

Computation had been featured in mathematics since the Babylonians, but took on a new turn with the invention of computational machines. We discussed Turing machines above, and despite the early philosophical setbacks, there have been huge strides in computer science.

Turing invented cryptography (1938) and broke the German Enigma Machine. Turing machine gave the theoretical basis for computer science.

Complexity theory.

Michael Rabin: Probabilistic algorithm for testing primes , based on testing converse of Fermat's Little Theorem, namely test whether $a^{n-1} \equiv 1 \pmod{p}$ for enough tests for a such that the probability of p being nonprime is as small as you want.

Udi Shamir: One-way codes. Namely take two large primes p_1, p_2 (found by Rabin's test) and take $n = p_1 p_2$. Take some number m. Given a number a compute some function $\pmod{n}$ of m and a, linear in a, and publicize the result. Then only someone who knows the factorization of n can reverse this function. Given some number

Big question: How can one factor a number? (If we could do this in polynomial time in $\log n$ then we could crack the Shamir code.

Best idea for factorizing: If one can find $a \not\equiv \pm 1$ such that $a^2 \equiv 1 \pmod{n}$ then $a^2 - 1 = (a+1)(a-1)$ is divisible by n, whereas $\gcd(a+1, a-1)) = 2$, so

$$n = \gcd(a-1, n)\gcd(a+1, n)$$

is a factorization. Thus one needs to find such an a, and the object is to compute a large number of squares. Thus far nobody has succeeded in a polynomial time (in $\log n$) algorithm to do this. However, in 2002, Agrawal, Kayal, and Saxena of the Indian Institute of Technology found an algorithm in polynomial time (in $\log n$) to check whether a number is prime. Peter Schor found a polynomial time algorithm to factor a number using quantum computers, once they are created. Thus again mathematics precedes its scientific application.

The golden age of algebra.

Many of Hilbert's problems were related to algebra, and the first half of the twentieth century saw the formal development of algebraic structures: Abstract groups (Burnside's book (1903), and other algebraic structures (Wedderburn, Brauer, Noether, Artin, Levitzki, Jacobson, Albert, Hasse, Witt.) The center of algebra started in Germany, especially in Hilbert's beloved Gottingen, but the Nazi boot left its strong imprint on mathematics in the first half of the 20th century. The most obvious effect was to move the center of mathematics from Europe (particularly Germany) to the US. Of special note is Emil Artin (1898-1962), the solver of two of Hilbert's problems (elaborate). His wife was Jewish, so he left Germany for Notre Dame, and then taught in Indiana and Princeton, finally returning to Germany at the end of his life, well after the war. One of the few algebraists remaining

in Nazi Germany was Hasse (1898-1979), who although personally gracious to Jews such as Albert, accepted the Nazi regime and suffered in his career after the war.

The algebraization of analysis was achieved by Cartan and Jacobson in the development of Lie algebras.

The algebraization of geometry was achieved by Noether, Zariski

The next step, in the middle of the twentieth century was the categorization of topology and algebra by Cartan, Eilenberg, Grothendieck, Gabriel

Algebraic topology.

Some of the most important developments of the twentieth century were in algebraic topology. Smale (1950's) proved the remarkable theorem that there is a continuous deformation of the sphere to invert itself, and (1960) proved one of Poincar's conjectures, that the only manifolds homologically equivalent to spheres are spheres themselves. Atiyah-Singer index theorem.

Bott periodicity

Algebraic K theory. Quillen, Suslin, Bass,

Physicists classify low-dimensional manifolds. Witten, Donaldson

The Millennium Problems

References

Boltianskii V.G., *Hilbert's Third Problem (trans. by Silverman)*, V.H. Winston, Washington D.C..
Browder (ed.), *Mathematical developments arising from Hilbert Problems Proceedings of Symposia in Pure Mathematics XXVIII*, Amer. Math. Soc..
History of the theory of numbers.
Fritsch R. and Fritsch G., *The Four-color theorem*, Springer.
Hofstadter, *Bach, Gödel, and Escher, an Eternal Braid*.
Kapinski L.C., *Robert of Chester's Latin translation of the Algebra of al-Khowarizmi*, University of Michigan, MacMillan Press.
Kelley J., *General Topology*, Van Nostrand University series in higher mathematics.
Koestler, Arthur, *The Sleepwalkers,*, Macmillan, New York.
Midonick H., *The Treasury of Mathematics*, Philosophical library.
Fu-His, The Sage of Ancient China, Jerusalem.
Singh S., *Fermat's Last Theorem*, BBC.
Fermat's Last Theorem.
Tignol J.-P., *Galois' Theory of algebraic equations*, Longman.
Wagon, *The Banach-Tarski Paradox*, Cambridge University Press.
Yandel B., *The Honors Class: Hilbert's Problems and their solvers*, AK Peters.