Classifications of Number Theory

1. Introduction

Number theory (or) **arithmetic** is a branch of pure mathematics devoted primarily to the study of the integers, more specifically the properties of positive integers. Number theorists study prime numbers as well as the properties of objects made out of integers (e.g., rational numbers) or defined as generalizations of the integers (e.g., algebraic integers).

The positive integers are man's first mathematical creation. The first scientific approach to study of integers, i.e., the true origin of the theory of numbers, is attributed to the Greeks. Around 600BC, Pythagoras and his disciples made through study of integers. Euclid, Diaphanous, Fermat, Euler, Gauss, Goldbach, Dirichlet and Ramanujan were among the main contributors of the theory of the numbers.

Integers can be considered either in themselves or as solutions to equations (Diophantine geometry). Questions in number theory are often best understood through the study of analytical objects (e.g., the Riemann zeta function) that encode properties of the integers, primes or other number-theoretic objects in some fashion (analytic number theory). One may also study real numbers in relation to rational numbers, e.g., as approximated by the latter (Diophantine approximation).

The older term for number theory is arithmetic. By the early twentieth century, it had been superseded by "number theory". (The word "arithmetic" is used by the general public to mean "elementary calculations"; it has also acquired other meanings in mathematical logic, as in Peano arithmetic, and computer science, as in floating point arithmetic.) The use of the term *arithmetic* for number theory regained some ground in the second half of the 20th century, arguably in part due to French influence. In particular, *arithmetical* is preferred as an adjective to *number-theoretic*.

About the positive integers(natural numbers) kronecker once remarked "God created the natural numbers and all the rest is the work of man". Number theory is an art enjoyable and pleasing to everybody. In this project we shall discuss some classifications of number theory. They are

1. Elementary number theory
2. Algebraic number theory
3. Analytic number theory
4. Geometric number theory
5. Computational number theory

What is Number Theory?

Number theory is the study of the set of positive numbers:
1, 2, 3, 4, 5, 6 . . .

We will especially want to study the relationship between different sorts of
Numbers.

Since ancient times, people have separated the whole numbers
Into variety of different types. Here are some familiar and not-so-familiar
Examples:

Odd 1, 3, 5, 7, 9, 11. . .

Even 2, 4, 6, 8, 10. . .

Square 1, 4, 9, 16, 25, 36 . . .

Cube 1, 8, 27, 64, 125 . . .

Prime 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31 . . .

Composite 4, 6, 8, 9, 10, 12, 14, 15, 16 . . .

1 (modulo 4) 1, 5, 9, 13, 17, 21, 25 . . .

Triangular 1, 3, 6, 10, 15, 21,….

Perfect 6, 28, 496 . . .

Many of these types of numbers are undoubtedly already known to us.

A number is called triangular if that number of pebbles can be arranged in a triangle, with one pebble at the top, two pebbles in the next row, and so on. A number is perfect if the sum of all of its divisors, other than itself, adds back up to the original number.

Some Typical Number Theoretic Questions:

The main goal of number theory is to discover interesting and unexpected
Relationships between different sorts of numbers and to prove that these relationship
are true.

In this section we will describe a few typical number theoretic problems, some of which we will eventually solve, some of which have known solutions too difficult for us to include, and some which remain unsolved to this day.

(a) Sums of Squares I

Can the sum of two squares be a square? The answer is clearly “YES”;

For example: 3, 4,5 and 5,12,13 are Pythagorean triple is a set of three integers x, y and z such that (a Pythagorean $x^2 + y^2 = z^2$)

(b) Sums of Higher Powers
Can the sum of two cubes be a cube? Can the sum of two fourth powers be a fourth power? In general, can the sum of two nth powers be an nth Powers? The answer is "NO". The famous problem, called Fermat's Last Theorem, was first posted by Pierre de Fermat in the 17th century, but was not completely solved until 1994 by Andrew Wiles. Wiles' proof used sophisticated mathematical techniques which we will not be able to describe in detail.

Fermat's Last Theorem

Fermat stated in the margin of his copy of Diophantus Arithmetician :

"It is impossible to write a cube as a sum of two cubes, a fourth power as a sum of two fourth powers and in general any powers beyond the second as a sum of two similar powers,for this I have discovered a wonderful proof but the margin is too small to contain it ".

This theorem can be stated as

The Diaphantive equation

$$x^n + y^n = Z^n$$

has no integral solution for n>2 other than the trivial solution in which x or y is zero.

This theorem is know as Fermat's last theorem remainded a challenge for mathematical community for a long time. In June 1993 a mathematician Andrew Wales of Princton University claimed to prove this theorem .The Whole mathematics world is excited today because this theorem defind the best minds of several generations of mathematicians.It is one of the important theorems.For the recognition of its importance,a German mathematician estabilished a prize of 100000 DM in 1908 for offering a correct published proof.

History of Fermat Last Theorem

1.1640, Fermat himself proved the case n=4

2.1770, Euler proved the case n=3;(Gauss also gave a proof)

3.1825,Dirichlet,Legender,proved FLT for n=5

4.1832,Dirichlet treated successfully the case n=14

5.1839,lame prove the case n=7

6.1847,Kummer proved FLT in the case, when the exponent is a regular prime .But it is not known even today, wheather there are infinitely many sophie Germain primes or regular primes.

7.1983,Falting gave a proof of mordell's conjecture .

8.1986,Frey-Ribet –scrre :shimuray –Taniyama-weil conjecture implies FLT.

9.1994,Andrew wiles :proof of S-T-W conjector for semi stable elliptic curve.

2. History

Fig 2

The positive integers are undoubtedly man's first mathematical creation. It is hardly possible to imagine human beings without the ability to count, at least within a limited range .Historical record shows that as early as 5700BC the ancient Sumerians kept a calendar, so they must have developed some form of arithmetic.

By 2500BC the Sumerians had developed a number system using 60 as a base. This was passed on to the Babylonians, who became highly skilled calculators. Babylonians clay tablets containing elaborate mathematical tables have been found, dating back to 2000BC.

When ancient civilization reached a level which proved leisure time to ponder about things, some people began to speculate about the nature and mysticism or numerology and even today numbers such as 3,7,11 and 13 are considered as omens of good or bad luck.

Numbers were used for keeping records and for commercial transactions for over 5000 years before anyone thought of studying numbers themselves in a systematic way. The first scientific approach to the study of integers, that is, the true origin of the theory Of numbers, is generally attributed to the Greeks. Around 600 BC Pythagoras and his disciples made rather thorough studies of integers. The Pythagoreans also linked numbers with geometry .They introduced the idea of polygonal numbers: Triangular numbers, square numbers, pentagonal numbers, etc .The reason for this geometrical Nomenclature is clear when the numbers are represented by dots arranged in the form of triangles, Squares, pentagons , etc., as shown in Figure

Triangular:

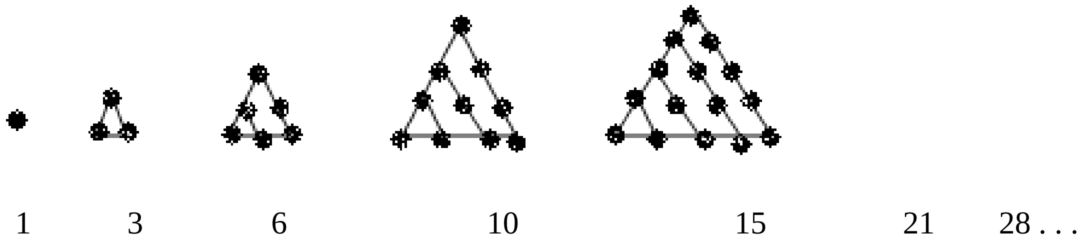


Fig 2.1

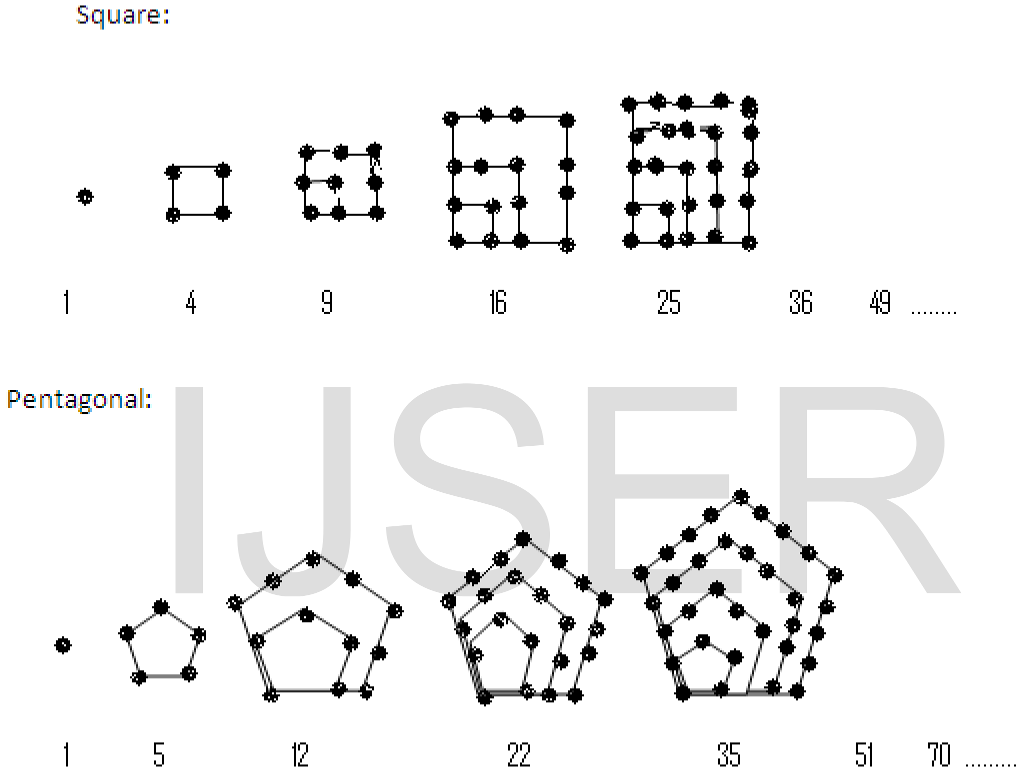


Fig 2.3

Another link with geometry came from the famous theorem of Pythagoras which states that in any right triangle the square of the length of the hypotenuse is the sum of the lengths of the two legs (see figure 1.2). The Pythagoreans were interested in right triangles whose sides are integers, as in figure1.3. Such triangles are now called Pythagorean triangles. The corresponding triple of numbers(x, y, z) representing the lengths of the sides is called a Pythagorean triple.

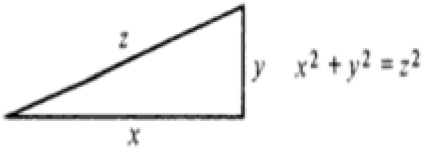


Fig 2.4

A Babylonian tablet has found, dating from about 1700BC, which contains an extensive of Pythagorean triples, some of the numbers being quite large. The Pythagorean triples, some of the numbers being quite large. The Pythagoreans were the first to give a method for determining infinitely many triples. In modern notation it can be described as follows

Let n be any odd number greater them 1, and let

x = n, $y=\frac{1}{2}(n^2\text{-}1)$, $z=\frac{1}{2}(n^2+1)$.

The resulting triple (x ,y ,z) will always be a Pythagorean triple with z=y+1. Here are some examples:

x	3	5	7	9	11	13	15	17	19
y	4	12	24	40	60	84	112	144	180
z	5	13	25	41	61	85	113	145	181

There are other Pythagorean triples besides these;

For example:

x	8	12	16	20

y 15 35 63 99

z 17 37 65 101

In these examples we have z=y+2.plato (430-349bc) found a method for determining all the triples; in modern notation they are given by the formulas

$$x=4n, \quad y=4n^2-1, \quad z=4n^2+1$$

Around 300BC an important event occurred in the history of mathematics. The appearance of Euclid's elements, a collection of 13 books, transformed mathematics from numerology into a deductive science. Euclid was the first to present mathematical facts along with rigorous proofs of these facts.

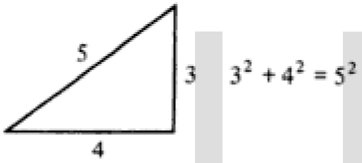


Fig 2.5

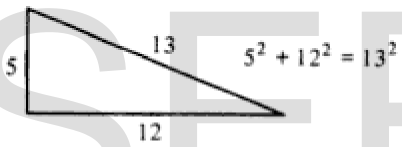


Fig 2.6

There of the thirteen books were devoted to the theory of numbers (books vii ,ix ,and x).in book ix Euclid proved that there are infinitely many primes. His proof is still taught in the classroom today. In book x he gave a method for obtaining all Pythagorean triples although he gave no proof that his method did, indeed, give them all. The method can be summarized by the formulas

$$x=t(a^2-b^2), \quad y=2tab, \quad z=t(a^2+b^2),$$

Where t ,a, and b ,are arbitrary positive integers such that a>b, a and b have no prime factors in common, and one of a or b is odd, the other even.

Euclid also made an important contribution to another problem posed by the Pythagoreans-that of finding all perfect numbers. The number 6 was called a perfect number because 6=1+2+3, the sum of all its proper divisors (that is, the sum of all divisors less than 6).Another example of a perfect number is 28 because 28=1+2+4+7+14 and 1,2,4,7 and 14 are the divisors of 28 less than

28.The Greeks referred to the proper divisors of a number as its “ part”. They are called 6 and 28 perfect numbers because in each case the number is equal to the sum of all its parts.

In Book IX , Euclid found all even perfect numbers. He proved that an even number is perfect if it has the form

$2^{p-1}(2^{p}-1)$, where both p and 2^{p}-1 are primes.

Two thousand years later, Euler proved the converse of Euclid’s theorem. That is, every even perfect number must be of Euclid’s type .For example, for 6 and 28 we have

6=$2^{2-1}(2^{2}-1)$ =2.3 and 28= $2^{3-1}(2^{3}-1)=4.7$.

The first five even perfect numbers are

6,28,496,8128 and 33,550,336

Perfect numbers are very rare indeed .At the present time (1983) only 29 perfect numbers are known. They Correspond to the following values of p in Euclid’s formula:

2,3,5,7,13,17,19,31,61,89,107,127,521,607,1279,2203,2281,3217,4253,4432,9689,9941,11,213,19,937,21,701,23,209,44,497,86,243,132,049

Numbers are of the for $2^{p}-1$,where p is a prime, are now called Mersenne numbers and are denoted by M_p in honor of Mersenne .who studied them in 1644.It is known that M_p is prime for the 29 primes listed above and composite for all values of p<44,497.For the following primes.

P= 137,139,149,199,227,257

Although M_p is composite, no prime factor of M_p is known. No odd perfect numbers are known; it is not even known if any exist .But if any do exist they must be very large; in fact greater than 10^{50}.

We turn now to a brief description of the history of the theory of numbers since Euclid’s time.

After Euclid in 300 BC no significant advances were made in number theory until about AD 250 when Another Greek mathematician, Diophantus of Alexendria, published 13 books, six of which have been preserved. This was the first Greek work to make systematic use of Algebraic symbols. Although his algebraic notation seems awkward by present day standards, diophantus was able to solve certain algebraic equations involving two or three unknowns. Many office problems originated from number theory and it was natural for him to seek integer solutions of equations. Equations to be solved with integer values of the unknowns are now called Diophantine equations. And the study of such equations is known as Diophantine analysis.

The equation $x^2 + y^2 = z^2$ for Pythagorean triples is an example of a Diophantine equation. After Diophantus, not much progress was made in the theory of numbers until the 17th century, although there is some evidence that the subject begin to flourish in the far east-especially in India-In the period between AD 500 and AD1200.

In the 17th century the subject was revived in western Europe, largely through the efforts of the remarkable French mathematician, Pierre de Fermat (1601-1665), who is generally acknowledged to be the father of the modern number theory. Fermat derived much of his inspiration from the works of Diophantus. He was the first to discover really deep properties of the integers. For example, Fermat proved the following surprising theorems.

Every integer is either a triangular number or a sum of 2 or 3tringular numbers ;every integer is either a square or a sum of 2, 3 or 4 squares ; Every integer is either pentagonal number or the sum of 2, 3, 4 or 5 pentagonal numbers, and so on.

Fermat also discovered that every prime number of the form 4n+1 such as 5, 13, 17, 29, 37, 41, etc., is a sum of two squares. For example,

$5=1^2+2^2,\ 13 = 2^2+3^2,\ 17 = 1^1+4^2,\ 29 = 2^2+5^2, 37 = 1^2+6^2,\ 41 = 4^2+5^2$

Shortly after Fermat’s time, the names of Euler (1707-1783), Lagrange(1736-1813), Legendre(1752-1833), Gauss(1777-1855), and Dirichlet(1805-1859) became prominent in the further development of the subject.

The first text book in number theory was published by Legendre in 1798. Three years later Gauss published Disquisitions arithmetic, a book which transforms the subject into a systematic and beautiful science. Although he made a wealth of contributions to other branches of mathematics, as well as to other sciences, Gauss himself considered his book on number theory to be his greatest work. We conclude this introduction with a brief mention of some outstanding unsolved problems concerning prime numbers.

1. (Goldbach's problem) is there an even number > 2 which Is not the sum of two primes?
2. Is there an even number > 2 which is not the difference of two primes?
3. Are there infinitely many twin primes?
4. Are there any infinitely many Mersenne primes, that is, primes of the form $2^p - 1$ Where P is prime?
5. Are there any infinitely many composite mersenne numbers?
6. Are there any infinitely many Fermat primes, that is, primes of the form 2^{2n}+1?
7. Are there any infinitely many composite Fermat numbers?
8. Are there any infinitely many primes of the form $x^2 + 1$,where x is an integer? (it is known that there are infinitely many of the form x^2+y^2, and of the form x^2+$y^2 + 1$,and of the form $x^2 + y^2$+$z^2 + 1$).
9. Are there any infinitely many primes of the firm $x^2 + k$,(k given)?
10. Does there always exist at least one prime between $n^2$and $(n + 1)^2$ For every integer n≥ 1?
11. Does there always exist at least one prime between $n^2$and $n^2 + n$ for every integer n>1?
12. Are there any infinitely many primes whose digits (in base 10) are all ones?(here are two examples(11 and 11, 111, 111, 111, 111, 111, 111, 111).

The professional mathematician is attracted to number theory because of the way all the weapons of modern mathematics can be brought to bear on its problems. As a matter of fact, many important branches of mathematics had their origin in number theory. For example, the early attempts to prove the prime number theorem stimulated the development of the theory of the functions of a complex variable, especially the theory of entire functions.

Attempts to prove that the Diophantine equation $x^2 + y^2 = z^2$ has no nontrivial solution if n≥ 3 (Fermat's conjecture) led to the development of Algebraic number theory, one of the most active areas of modern mathematical research. The conjecture itself seems unimportant compared to the vast amount of valuable mathematics that was created by those working on it (A. Wiles announced a proof of Fermat's conjecture in 1994).

3.Elementary Number Theory

Elementary number theory involves divisibility among integers , the division "algorithm", the Euclidean algorithm (and thus the existence of greatest common divisors), elementary properties of primes (the unique factorization theorem, the infinitude of primes), congruence's (and the structure of the sets $\mathbf{Z}/n\,\mathbf{Z}$ as commutative rings), including Fermat's little theorem and Euler's theorem extending it. "elementary" number theory usually includes classic and elegant results such as Quadratic Reciprocity; counting results using the Möbius Inversion Formula (and other multiplicative number-theoretic functions); and even the Prime Number Theorem, asserting the approximate density of primes among the integers, which has difficult but "elementary" proofs. Other topics in elementary number theory - The solutions of sets of linear congruence equations, The Chinese Remainder Theorem (or) solutions of single binary quadratic equations ,Pell's equations and continued fractions, or the generation of Fibonacci numbers or Pythagorean triples - turn out in retrospect to be harbingers of sophisticated tools and themes in other areas.

For example, many questions in number theory may be posed as Diophantine equations equations to be solved in integers without much preparation. Catalan's conjecture are 8 and 9 the only consecutive powers? (asks for the solution to $x^{a} - y^{b} = 1$ in integers), the Four Squares Theorem (every natural number is the sum of four integer squares) simply asserts that $x^2 + y^2 + z^2 + w^2 = n$ is solvable for all *n*. But the attempt to solve these equations requires rather powerful tools from elsewhere in mathematics to shed light on the structure of the problem. Even the *possibility* of analyzing Diophantine equations , Hilbert's tenth problem , suggests the use of mathematical logic, Matijasevic's negative solution of that problem guarantees number theorists will never find a complete solution to their analyses! Naturally there is significant overlap, and a single question from elementary number theory often requires tools from many branches of number theory.

The branch of number theory that investigates properties of the integers by elementary methods. These methods include the use of divisibility properties, various forms of the axiom of induction and combinatorial arguments. Sometimes the notion of elementary methods is extended by bringing in the simplest elements of mathematical analysis. Traditionally, proofs are deemed to be non-elementary if they involve complex numbers. Usually, one refers to elementary number theory the problems that arise in branches of number theory such as the theory of divisibility, of congruences, of arithmetic functions, of indefinite equations, of partitions, of additive representations, of the approximation by rational numbers, and of continued fractions. Quite often, the solution of such problems leads to the need to go beyond the framework of elementary methods.

Many results obtained previously by P. Fermat, L. Euler, J.L. Lagrange, and others, and also the Chinese remainder theorem, can be stated and proved simply in the language of the theory of congruences. One of the most interesting results of this theory is the quadratic reciprocity law.

3.1 Fermat

Pierre de Fermat (1601–1665) never published his writings in particular, his work on number theory is contained almost entirely in letters to mathematicians and in private marginal notes, He wrote down nearly number of proofs in number theory .He did make repeated use of mathematical induction, introducing the method of infinite descent.One of Fermat's first interests was perfect numbers (which appear in Euclid, *Elements* IX) and amicable numbers, this led him to work on integer divisors, which were from the beginning among the subjects of the correspondence (1636 onwards) that put him in touch with the mathematical community of the day. He had already studied Bachet's edition of Diophantus carefully; by 1643, his interests had shifted largely to Diophantine problems and sums of squares (also treated by Diophantus).

He wrote about his own famous conjecture " I have a truly wonderful proof but the margin is too small to contain it. "

3.1.1 Fermat's achievements in arithmetic

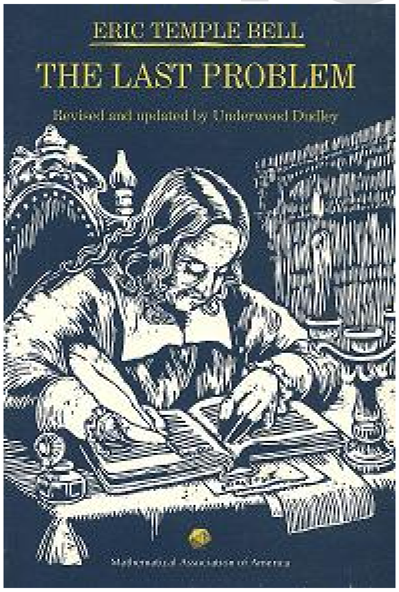
- Fermat's little theorem (1640), stating that, if a is not divisible by a prime p, then $a^{p-1} \equiv 1 (mod\ p)$
- If a and b are co prime, then $a^2+b^2$is not divisible by any prime congruent to -1 modulo 4, *and* Every prime congruent to 1 modulo 4 can be written in the form a^2+b^2. These two statements also date from 1640, in 1659, Fermat stated to Huygens that he had proven the latter statement by the method of descent. Fermat and Frenicle also did some work (some of it erroneous or non-rigorous) on other quadratic forms.
- Fermat posed the problem of solving $x^2 - Ny^2 = 1$ as a challenge to English mathematicians (1657). The problem was solved in a few months by Wallis and Brouncker. Fermat considered their solution valid, but pointed out they had provided an algorithm without a proof (as had Jayadeva and Bhaskara, though Fermat would never know this.) He states that a proof can be found by descent.

- Fermat developed methods for (doing what in our terms amounts to) finding points on curves of genus 0 and 1. As in Diophantus, there are many special procedures and what amounts to a tangent construction, but no use of a secant construction.
- Fermat states and proves (by descent) in the appendix to **Observations on Diophantus** (Obs. XLV) that $x^4 + y^4 = z^4$ has no non-trivial solutions in the integers. Fermat also mentioned to his correspondents that $x^3+y^3=z^3$ has no non-trivial solutions, and that this could be proven by descent.
- Fermat's claim ("Fermat's last theorem") to have shown there are no solutions to $x^n + y^n = z^n$ for all $n\geq3$ (a fact completely beyond his methods) appears only in his annotations on the margin of his copy of Diophantus, he never claimed this to others and thus would have had no need to retract it if he found any mistake in his supposed proof.

3.1.2 The Quest to Solve the World's Most Notorious Mathematical Problem

In 1963 a 10-year old boy borrowed a book from his local library in Cambridge, England. The boy was Andrew Wiles, a schoolchild with a passion for mathematics, and the book that had caught his eye was 'The Last Problem' by the mathematician Eric Temple Bell. The book recounted the history of Fermat's Last Theorem, the most famous problem in mathematics, which had baffled the greatest minds on the planet for over three centuries.

There can be no problem in the field of physics, chemistry or biology that has so vehemently resisted attack for so many years. Indeed E.T. Bell predicted that civilization would come to an end as a result of nuclear war before Fermat's Last Theorem would ever be resolved. Nonetheless young Wiles was undaunted. He promised himself that he would devote the rest of his life to addressing the ancient challenge.


ERIC TEMPLE BELL
THE LAST PROBLEM
Revised and updated by Underwood Dudley
Mathematical Association of America

Pierre De Fermat

The 17th century mathematician Pierre de Fermat created the Last Theorem while studying Arithmetica, an ancient Greek text written in about AD 250 by Diophantus of Alexandria. This was a manual on number theory, the purest form of mathematics, concerned with the study of whole numbers, the relationships between them, and the patterns they form.

The page of Arithmetica which inspired Fermat to create the Last Theorem discussed various aspects of Pythagoras' Theorem, which states that:

In a right-angled triangle the square of the hypotenuse is equal to the sum of the squares on the other two sides.

Soon after his death in 1906, the Wolfskehl Prize was announced, generating an enormous amount of publicity and introducing the problem to the general public

Fermat's little theorem is the basis for the Fermat primality test and is one of the fundamental results of elementary number theory. The theorem is named after Pierre de Fermat, who stated it in 1640. It is called the "little theorem" to distinguish it from Fermat's last theorem

3.1.3 Fermat's little Theorem

Statement: Let p be prime, and suppose $p \nmid a$, then $a^{p-1} \equiv 1(mod\, p)$.

Proof: Consider the integers a ,2a,………….(p -1)a

Reduce mod p to the standard system of residues {1,…….p-1},

(then apply Wilson's theorem.)

There are p - 1 numbers in the set {a ,2a,………….(p-1) a}

Show that they're distinct mod p.

Suppose that 1≤ $j\,, k \leq p - 1$, and

$aj \equiv ak(mod\, p)$,

$p\backslash aj - ak \equiv a(j - k)$,

so $p\backslash a$ (or). $p \backslash j - k$

Since the first case is ruled out by assumption ,$p\backslash j - k$.

But since 1≤ j, k ≤ p-1, this is only possible if j=k.

Thus, {a ,2a,………(p-1)a } are p-1 distinct numbers mod p.

If reduce mod p, get the numbers in {1,……..,p-1}.

Hence, a.2a……….(p-1) a≡ 1.2………..(p-1) (mod p)

$(p-1)!\, a^{p-1} \equiv (p-1)!\, (mod\, p)$

On the other hand, another application of Wilson's theorem shows that

a.2a…….. $(p-1)a \equiv a^{p-1}(p-1)! \equiv -a^{p-1}(mod\, p)$

So $-a^{p-1} \equiv -1(mod\, p)$,

- (or) $a^{p-1} \equiv 1(mod\, p)$.

3.1.4 Converse of Fermat's little theorem

The converse of Fermat's little theorem is not generally true, as it fails for Carmichael numbers. However, a slightly stronger form of the theorem is true, and is known as Lehmer's theorem.

The theorem is as follows

If there exists an a such that

$a^{p-1} \equiv 1(mod\, p)$ an for all prime q dividing $p-1$

$a^{(p-1)/q} \neq 1(mod\, p)$ $t$hen p is prime.

This theorem forms the basis for the Lucas–Lehmer test, an important primality test

3.2 Different Proofs of Fermat's little theorem

Fermat's little theorem states that $a^p \equiv a(mod\, p)$

for every prime number p and every integer a

Simplifications

Some of the **proofs of Fermat's little theorem** given below depend on two simplifications.

The first is that we may assume that a is in the range $0 \leq a \leq p - 1$. This is a simple consequence of the laws of modular arithmetic; we are simply saying that we may first reduce a modulo p.

Secondly, it suffices to prove that

$$a^{p-1} \equiv 1(mod\, p) \qquad (1)$$

for a in the range $1 \leq a \leq p - 1$. Indeed, if (1) holds for such a, multiplying both sides by a yields the original form of the theorem,

$$a^p \equiv a(mod\, p)$$

On the other hand, if a equals zero, the theorem holds trivially.

3.2.1 Proof by counting necklaces

This is perhaps the simplest known proof, requiring the least mathematical background. It is an attractive example of a combinatorial proof (a proof that involves counting a collection of objects in two different ways).

The proof given here is an adaptation of Golomb's proof.

To keep things simple, let us assume that a is a positive integer. Consider all the possible strings of p symbols, using an alphabet with a different symbols. The total number of such strings is a^p, since there are a possibilities for each of p positions (see rule of product).

For example, if $p = 5$ and $a = 2$, then we can use an alphabet with two symbols (say A and B), and there are $2^5 = 32$ strings of length five:

AAAAA , AAAAB , AAABA , AAABB , AABAA, AABAB, AABBA, AABBB,
ABAAA, ABAAB, ABABA, ABABB, ABBAA, ABBAB, ABBBA, ABBBB,
BAAAA, BAAAB, BAABA, BAABB, BABAA, BABAB, BABBA, BABBB,
BBAAA, BBAAB, BBABA, BBABB, BBBAA, BBBAB, BBBBA, BBBBB.

ISSN 2229-5518

We will argue below that if we remove the strings consisting of a single symbol from the list (in our example, AAAAA and BBBBB), the remaining $a^{p} - a$ strings can be arranged into groups, each group containing exactly p strings. It follows that $a^{p} - a$ is divisible by p.

Necklaces

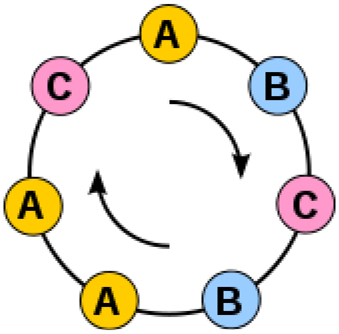


Fig 3.2.1
Necklace representing seven different strings (ABCBAAC, BCBAACA, CBAACAB, BAACABC, AACABCB, ACABCBA, CABCBAA)

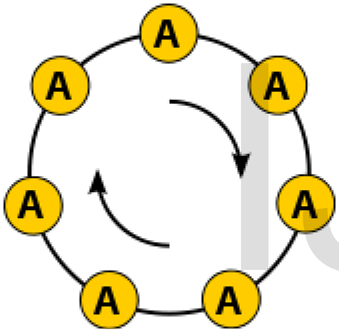
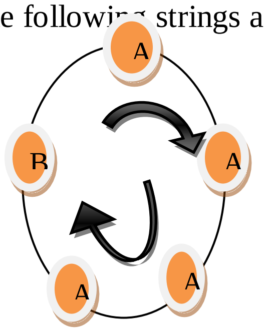


Fig 3.2.2
Necklace representing only one string (AAAAAAA)

Let us think of each such string as representing a necklace.

That is, we connect the two ends of the string together, and regard two strings as the same necklace if we can rotate one string to obtain the second string;

in this case we will say that the two strings are **friends**. In our example, the following strings are all friends:



AAAAB, AAABA, AABAA, ABAAA, BAAAA.

Similarly, each line of the following list corresponds to a single necklace.

AAABB, AABBA, ABBAA, BBAAA, BAAAB,
AABAB, ABABA, BABAA, ABAAB, BAABA,
AABBB, ABBBA, BBBAA, BBAAB, BAABB,

ABABB, BABBA, ABBAB, BBABA, BABAB,
ABBBB, BBBBA, BBBAB, BBABB, BABBB,
AAAAA,
BBBBB.

Notice that in the above list, some necklaces are represented by five different strings, and some only by a single string, so the list shows very clearly why $32 - 2$ is divisible by 5.

One can use the following rule to work out how many friends a given string *S* has

If S is built up of several copies of the string T, and T cannot itself be broken strings down further into repeating strings, then the number of friends of S(including S itself) is equal to the length of T

For example:

suppose we start with the string *S* = "ABBABBABBABB", which is built up of several copies of the shorter string *T* = "ABB". If we rotate it one symbol at a time, we obtain the following three strings:

ABBABBABBABB,
BBABBABBABBA,
BABBABBABBAB.

There aren't any others, because ABB is exactly three symbols long, and cannot be broken down into further repeating strings.

Using the above rule, we can complete the proof of Fermat's little theorem quite easily, as follows. Our starting pool of a^p strings may be split into two categories

- Some strings contain *p* identical symbols. There are exactly *a* of these, one for each symbol in the alphabet. (In our running example, these are the strings AAAAA and BBBBB.)
- The rest of the strings use at least two distinct symbols from the alphabet. If we try to break up such a string *S* into repeating copies of a string *T*, we find that because *p* is prime, the only possibility is that *T* is already the whole string *S*. Therefore, the above rule tells us that *S* has exactly *p* friends (including *S* itself).

The second category contains $a^p - a$ strings, and they may be arranged into groups of *p* strings, one group for each necklace. Therefore $a^p - a$ must be divisible by *p*, as promised.

3.2.2 Proof using group theory

This proof requires the most basic elements of group theory.

The idea is to recognize that the set $G = \{1, 2, \ldots., p - 1\}$, with the operation of multiplication (taken modulo p), forms a group. The only group axiom that requires some effort to verify is that each element of G is invertible. Taking this on faith for the moment, let us assume that a is in the range $1 \le a \le p - 1$, that is, a is an element of G. Let k be the order of a, so that k is the smallest positive integer such that

$$a^k \equiv 1(mod\, p)$$

By Lagrange's theorem, k divides the order of G, which is $p - 1$, so $p - 1 = km$ for some positive integer m. Then

$$a^{p-1} \equiv a^{km} \equiv (a^k)^m \equiv 1^m \equiv 1(mod\, p)$$

3.2.3 Proof using the binomial theorem

This proof uses induction to prove the theorem for all integers $a \ge 0$.

The base step, that $0^p \equiv 0$ (mod p), is true for modular arithmetic because it is true for integers. Next, we must show that if the theorem is true for $a = k$, then it is also true for $a = k+1$. For this inductive step, we need the following lemma.

Lemma: For any prime p,

$$(x + y)^p \equiv x^p + y^p(mod\, p)$$

An alternative way of viewing this lemma is that it states that

$$(x + y)^p = x^p + x^p$$

for any x and y in the finite field **GF**(p).

Postponing the proof of the lemma for now, we proceed with the induction.

Proof:

Assume $k^p \equiv k$ (mod p), and consider $(k+1)^p$. By the lemma we have

$$(k + 1)^p \equiv k^p + 1^p\ (mod\, p)$$

Using the induction hypothesis, we have that $k^p \equiv k$ (mod p); and, trivially, $1^p = 1$. Thus

$$(k + 1)^p \equiv k + 1\ (mod\, p)$$

which is the statement of the theorem for *a* = *k*+1.

In order to prove the lemma, we must introduce the binomial theorem, which states that for any positive integer *n*,

$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^{n-i} y^i$$

where the coefficients are the binomial coefficients,

$$\binom{n}{i} = \frac{n!}{i!(n-i)!}$$

described in terms of the factorial function, *n*! = 1×2×3×⋯×*n*.

Proof of lemma. The binomial coefficients are all integers and when 0 < *i* < *p*, neither of the terms in the denominator includes a factor of *p*, leaving the coefficient itself to possess a prime factor of *p* which must exist in the numerator, implying that

$$\binom{p}{i} \equiv 0 (mod\, p) \quad ,0 < i < p.$$

Modulo p, this eliminates all but the first and last terms of the sum on the left-hand side of the binomial theorem for prime *p*.

The primality of *p* is essential to the lemma, otherwise, we have examples like

$$\binom{4}{2} = 6,$$

which is not divisible by 4.

3.2.4 Proof using dynamical systems

This proof uses some basic concepts from dynamical systems.

We start by considering a family of functions, $T_n(x)$, where *n* ≥ 2 is an integer, mapping the interval [0, 1] to itself by the formula

$$T_n(x) = \{ \begin{array}{cc} \{nx\} & 0 \le x < 1 \\ 1 & x = 1, \end{array}$$

Lemma 1.

For any *n* ≥ 2, the function $T_n(x)$ has exactly *n* fixed points.

Proof.

There are three fixed points in the illustration above, and the same sort geometrical argument applies for any $n \geq 2$.

Lemma 2.

For any positive integers n and m, and any $0 \leq x \leq 1$,

$$T_m(T_n(x)) = T_{mn}(x)$$

In other words, $T_{mn}(x)$ is the composition of $T_n(x)$ and $T_m(x)$.

Proof. The proof of this lemma is not difficult, but we need to be slightly careful with the endpoint $x = 1$. For this point the lemma is clearly true since

$$T_m(T_n(1)) = T_m(1) = 1 - T_{mn}(1)$$

So let us assume that $0 \leq x < 1$. In this case,

$$T_n(x) = \{nx\} < 1.$$

so $T_m(T_n(x))$ is given by

$$T_m(T_n(x)) = \{m\{nx\}\}$$

Therefore, what we really need to show is that

$$\{m\{nx\}\}=\{mnx\}$$

To do this we observe that $\{nx\} = nx - k$, where k is the integer part of nx; then

$$\{m\{nx\}\}=\{mnx-mk\}=\{mnx\}$$

since mk is an integer.

Now let us properly begin the proof of Fermat's little theorem, by studying the function $T_a{}^p(x)$. We will assume that a is positive. From Lemma 1, we know that it has a^p fixed points. By Lemma 2 we know that

$$T_{a^p}(x) = \underbrace{T_a(T_a(\cdots T_a(x)\cdots))}_{p\text{ times}},$$

so any fixed point of $T_a(x)$ is automatically a fixed point of $T_a{}^p(x)$.

We are interested in the fixed points of $T_a{}^p(x)$ that are *not* fixed points of $T_a(x)$. Let us call the set of such points S. There are $a^p - a$ points in S, because by Lemma 1 again, $T_a(x)$ has exactly a

fixed points. The following diagram illustrates the situation for a = 3 and p = 2. The black circles are the points of S, of which there are $3^2 - 3 = 6$.

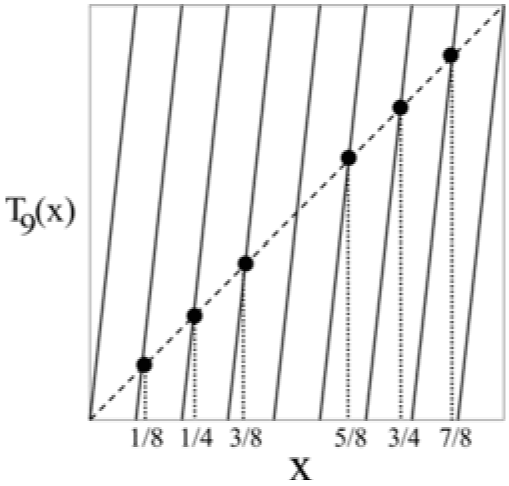


Fig 3.2.4 (c)

The main idea of the proof is now to split the set S up into its **orbits** under T_a. What this means is that we pick a point x_0 in S, and repeatedly apply T_a(x) to it, to obtain the sequence of points

$$x_o, T_a(x_o), T_a(T_a(x_0)), T_a\left(T_a(T_a(x_o))\right), \ldots \ldots \ldots ....$$

This sequence is called the orbit of x_0 under T_a. By Lemma 2, this sequence can be rewritten as

$$x_0. T_a(x_o), T_{a^2}(x_0), T_{a^3}(x_0), \ldots \ldots ..$$

Since we are assuming that x_0 is a fixed point of $T_a{}^p(x)$, after p steps we hit $T_a{}^p(x_0) = x_0$, and from that point onwards the sequence repeats itself.

However, the sequence *cannot* begin repeating itself any earlier than that. If it did, the length of the repeating section would have to be a divisor of p, so it would have to be 1 (since p is prime). But this contradicts our assumption that x_0 is not a fixed point of T_a.

In other words, the orbit contains exactly p distinct points. This holds for every orbit of S. Therefore, the set S, which contains $a^p - a$ points, can be broken up into orbits, each containing p points, so $a^p - a$ is divisible by p.

3.2.5 Proof using the Multinomial expansion

The proof is a very simple application of the Multinomial formula which is brought here for the sake of simplicity.

$$(x_1 + x_2 + \cdots + x_m)^n = \sum_{k_1, k_2, \ldots\ldots, k_m} \binom{n}{k_1, k_2, \ldots\ldots, k_m} (x_1^{k_1} x_2^{k_2} \ldots \ldots \ldots . x_m^{k_m}$$

The summation is taken over all sequences of nonnegative integer indices k_1 through k_m such the sum of all k_i is n.

Thus if we express *a* as a sum of 1s (ones), we obtain

$$a^p = \sum_{k_1,k_2,\dots\dots k_a} \binom{p}{k_1,k_2,\dots\dots\dots k_a}$$

Clearly, if *p* is prime, and if k_j not equal to *p* for any *j*, we have

$$\binom{p}{k_1,k_2,\dots\dots k_a} \equiv 0(mod\, p)$$

and

$$\binom{p}{k_1,k_2,\dots\dots k_a} \equiv 1(mod\, p)$$

if k_j equal to *p* for some *j*

Since there are exactly *a* elements such that $k_j = p$the theorem follows.

3.2.6 Wilson's Theorem and Fermat's Theorem

- *Wilson's theorem says that p is prime if* and only if $(p-1)! \equiv 1(mod\, p)$.
- *Fermat's theorem* says that if p is prime and $p \not| a$, then $a^{p-1} \equiv 1(mod\, p)$.
- Wilson's theorem and Fermat's theorem can be used to reduce large numbers with respect to a give modulus and to solve congruences. They are also used to prove other results in number theory --- for example, those used in cryptographic applications.

3.3 Chinese Remainder Theorem

The **Chinese remainder theorem** is a result about congruences in number theory and its generalizations in abstract algebra. In its basic form, the Chinese remainder theorem will determine a number *n* that when divided by some given divisors leaves given remainders.

The original form of the theorem, contained in a third-century AD book The Mathematical Classic of Sun Zi by Chinese mathematician Sun Tzu and later generalized with a complete solution called *Da yan shu*in a 1247 book by Qin Jiushao, the *Shushu Jiuzhang* Mathematical Treatise in Nine Sections) is a statement about simultaneous congruences

Statement :

Suppose n_1, n_2, …, n_k are positive integers which are pair wise co prime. Then, for any given sequence of integers a_1,a_2, …, a_k, there exists an integer x solving the following system of simultaneous congruence's.

$$\begin{aligned} x &\equiv a_1(mod\, n_1) \\ x &\equiv a_2(mod\, n_2) \\ &. \\ &. \\ &. \\ x &\equiv a_k(mod\, n_k) \end{aligned}$$

, all solutions x of this system are congruent modulo the product, $N = n_1 n_2 \ldots n_k$.

Hence $x \equiv y \pmod{n_i}$for all $1 \leq i \leq k$, if and only if $x \equiv y \pmod{N}$.

3.4 Leonhard Euler

The interest of Leonhard Euler (1707–1783) in number theory was first spurred in 1729, when a friend of his, the amateur Goldbach pointed him towards some of Fermat's work on the subject. This has been called the "rebirth" of modern number theory, after Fermat's relative lack of success in getting his contemporaries' attention for the subject.

Euler's work on number theory includes the following

- Proofs for Fermat's statements. This includes Fermat's little theorem (generalised by Euler to non-prime moduli); the fact that $p=x^2+y^2$if and only if $p\equiv 1 \; mod \; 4$, initial work towards a proof that every integer is the sum of four squares (the first complete proof is by Lagrange (1770), soon improved by Euler himself), the lack of non-zero integer solutions to $x^4+y^4=z^2$ (implying the case *n=4* of Fermat's last theorem, the case *n=3* of which Euler also proved by a related method).

- Pell's equation, first misnamed by Euler. He wrote on the link between continued fractions and Pell's equation.
- First steps towards analytic number theory. In his work of sums of four squares, partitions, pentagonal numbers, and the distribution of prime numbers, Euler pioneered the use of what can be seen as analysis (in particular, infinite series) in number theory. Since he lived before the development of complex analysis, most of his work is restricted to the formal manipulation of power series. He did, however, do some very notable (though not fully rigorous) early work on what would later be called the Riemann zeta function.
- Quadratic forms : Following Fermat's lead, Euler did further research on the question of which primes can be expressed in the form x^2+Ny^2, some of it prefiguring quadratic reciprocity.
- Diophantine equations. Euler worked on some Diophantine equations of genus 0 and 1. In particular, he studied Diophantus's work; he tried to systematise it, but the time was not yet ripe for such an endeavour algebraic geometry was still in its infancy.

3.4 Diophantine Equation

In mathematics, a **Diophantine equation** is an indeterminate polynomial equation that allows the variables to take integer values only. Diophantine problems have fewer equations than unknown variables and involve finding integers that work correctly for all equations. In more technical language, they define an algebraic curve, algebraic surface, or more general object, and ask about the lattice points on it.

The word Diophantine refers to the Hellenistic mathematician of the 3rd century, Diophantus of Alexandria, who made a study of such equations and was one of the first mathematicians to introduce symbolism into algebra. The mathematical study of Diophantine problems Diophantus initiated is now called "Diophantine analysis". A linear Diophantine equation is an equation between two sums of monomials of degree zero or one.

While individual equations present a kind of puzzle and have been considered throughout history, the formulation of general theories of Diophantine equations (beyond the theory of quadratic forms) was an achievement of the twentieth century.

3.4.1 Examples of Diophantine Equations

In the following Diophantine equations, *x*, *y*, and *z* are the unknowns, the other letters being given are constants.

$ax + by = 1$	This is a linear Diophantine equation (see the section "Linear Diophantine equations" below).

$x^n + y^n = z^n$ For n = 2 there are infinitely many solutions (x, y ,z): the Pythagorean triples. For larger integer values of n, Fermat's Last Theorem states there are no positive integer solutions (x, y, z).

$x^2 - Ny^2 = \pm 1$ (Pell's equation) which is named after the English mathematician John Pell. It was studied by Brahmagupta in the 7th century, as well as by Fermat in the 17th century.

$\frac{4}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}$ The Erdős–Straus conjecture states that, for every positive integer $n \geq 2$, there exists a solution in x, y, and z, all as positive integers. Although not

3.5 Quadratic reciprocity law

The relation

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

connecting the Legendre symbols

$\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$

for different odd prime numbers $p$and q. There are two additions to this quadratic reciprocity law, namely:

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$$

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

C.F. Gauss gave the first complete proof of the quadratic reciprocity law, which for this reason is also called the Gauss reciprocity law.

It immediately follows from this law that for a given square-free number d, the primes $p$for which $d$is a quadratic residue modulo $p$ly in certain arithmetic progressions with common difference $2|d|$or $4|d|$. The number of these progressions is $\phi\,(2|d|)\,/\,2$or $\phi\,(4|d|)\,/\,2$,

where $\phi\,(n)$is the Euler function. The quadratic reciprocity law makes it possible to establish factorization laws in quadratic extensions $\mathbf{Q}(\sqrt{d})$of the field of rational numbers, since thfactorization into prime factors in $\mathbf{Q}(\sqrt{d})$of a prime number that does not divide $d$depends on whether or not $x^2 - d$is reducible modulo p.

4. Algebraic number theory

Algebraic number theory is a major branch of number theory which studies algebraic structures related to algebraic integers. This is generally accomplished by considering a ring of algebraic integers O in an algebraic number field K/Q, and studying their algebraic properties such as factorization, the behaviour of ideals, and field extensions. In this setting, the familiar features of the integers such as unique factorization need not hold. The virtue of the primary machinery and L-functions is that it allows one to deal with new phenomena and yet partially recover the behaviour of the usual integers.

A number α is called an algebraic number if it is a root of the algebraic equaction f(x)=$a_0$$\mathrm{x}^{\mathrm{n}}$+$a_1$$\mathrm{x}^{\mathrm{n-1}}$+….+$a_n$=0 where ai are integers.The number α is called an algebraic number of degree n if f(x)is an irreducible polynomial of degree n. if $a_{0=}1$ then α is called an algebraic integer.In algebraic number theory the algebraic integers or algebraic integral ring are studied.Natural numbers are algebraic integers of degree 1.

The non-algebraic numbers are called transcendental numbers.The ideal class group of O is a measure of how much unique factorization of elements fails; in particular, the ideal class group is trivial if, and only if, O is a unique factorization domain.

4.1 Factoring prime ideals in extensions

Unique factorization can be partially recovered for O in that it has the property of unique factorization of ideals into prime ideals (i.e. it is a Dedekind domain). This makes the study of the prime ideals in O particularly important. This is another area where things change from Z to O: the prime numbers, which generate prime ideals of Z (in fact, every single prime ideal of Z is of the form (p):=pZ for some prime number p,) may no longer generate prime ideals in O. For example, in the ring of Gaussian integers, the ideal 2Z[i] is no longer a prime ideal; in fact

2Z[i]$= ((1+i)Z[i])^2$.

On the other hand, the ideal 3Z[i] is a prime ideal. The complete answer for the Gaussian integers is obtained by using a theorem of Fermat's, with the result being that for an odd prime number p

pZ[i] is a prime ideal if p=3(mod 4)

pZ[i] is not a prime ideal if p=1(mod 4).

Generalizing this simple result to more general rings of integers is a basic problem in algebraic number theory. Class field theory accomplishes this goal when K is an abelian extension of Q(i.e.a Galois extension with abelian Galois group).

4.2 Primes and places

An important generalization of the notion of prime ideal in O is obtained by passing from the so-called ideal-theoretic approach to the so-called valuation-theoretic approach. The relation between the two approaches arises as follows. In addition to the usual absolute value function $|\cdot| : Q \rightarrow R$, there are absolute value functions $|\cdot|_p : Q \rightarrow R$ defined for each prime number p in Z, called p-adic absolute values. Ostrowski's theorem states that these are all possible absolute value functions on Q (up to equivalence). This suggests that the usual absolute value could be considered as another prime.

Aprime of an algebraic number field K (also called a place) is an equivalence class of absolute values on K. The primes in K are of two sorts: P-adic absolute values like $|\cdot|_p$, one for each prime ideal Pof O, and absolute values like |·| obtained by considering K as a subset of the complex numbers in various possible ways and using the absolute value $|\cdot| : C \rightarrow R$. A prime of the first kind is called a finite prime (or finite place) and one of the second kind is called an infinite prime (or infinite place). Thus, the set of primes of Q is generally denoted { 2, 3, 5, 7, ..., ∞ }, and the usual absolute value on Q is often denoted $|\cdot|_\infty$ in this context.

number of real (respectively, complex) primes is often denoted r_1 (respectively, r_2). Then, the total number of embeddings $K \rightarrow C$ is r_1+2r_2 (which, in fact, equals the degree of the extension K/Q).

4.3 Local fields

Completing a number field K at a place w gives a complete field. If the valuation is Archimedean, one gets R or C, if it is non-Archimedean and lies over a prime p of the rational, one gets a finite extension K_w / Q_p: a complete, discrete valued field with finite residue field.

This process simplifies the arithmetic of the field and allows the local study of problems. For example the Kronecker–Weber theorem can be deduced easily from the analogous local statement. The philosophy behind the study of local fields is largely motivated by geometric methods. In algebraic geometry, it is common to study varieties locally at a point by localizing to a maximal ideal. Global information can then be recovered by gluing together local data. This spirit is adopted in algebraic number theory. Given a prime in the ring of algebraic integers in a

4.4 Major results

4.4.1 Finiteness of the class group

One of the classical results in algebraic number theory is that the ideal class group of an algebraic number field K is finite. The order of the class group is called the class number, and is often denoted by the letter .

4.4.2 Dirichlet's unit theorem

Dirichlet's unit theorem provides a description of the structure of the multiplicative group of units $O^\times$ of the ring of integers O. Specifically, it states that $O^\times$ is isomorphic to $G \times Z^r$, where G is the finite cyclic group consisting of all the roots of unity in O, and $r = r_1 + r_2 - 1$ (where r_1 (respectively, r_2) denotes the number of real embeddings (respectively, pairs of conjugate non-real embeddings) of K). In other words, $O^\times$ is a finitely generated abelian group of rank $r_1 + r_2 - 1$ whose torsion consists of the roots of unity in O.

4.5 Algebraic number field

In mathematics, an algebraic number field (or simply number field) F is a finite (and hence algebraic) field extension of the field of rational numbers Q. Thus F is a field that contains Q and has finite dimension when considered as a vector space over Q.

- The study of algebraic number fields, and, more generally, of algebraic extensions of the field of rational numbers, is the central topic of algebraic number theory.

4.5.1 Definition

The notion of algebraic number field relies on the concept of a field. Fields consists of a set of elements together with two operations, namely addition, and multiplication, and some distributivity assumptions. A prominent example of a field is the field of rational numbers, commonly denoted Q, together with its usual operations of addition etc.

An algebraic number field (or simply number field) is a finite degree field extension of the field of rational numbers. Here its dimension as a vector space over Q is simply called its degree.

Examples

1) Cyclotomic field

   $Q(\zeta_n)$, $\zeta_n = \exp(2\pi i / n)$
   is a number field obtained from Q by adjoining a primitive nth root of unity ζ_n. This field contains all complex nth roots of unity and its dimension over Q is equal to $\varphi(n)$, where φ is the Euler totient function.

2) The real numbers, R, and the complex numbers, C, are fields which have infinite dimension as Q-vector spaces, hence, they are not number fields. This follows from the uncountability of R and C as sets, whereas every number field is necessarily countable.
3) The set Q^2 of ordered pairs of rational numbers, with the entrywise addition and multiplication is a two-dimensional commutative algebra over Q. However, it is not a field, since it has zero divisors.
4) $(1, 0) \cdot (0, 1) = (1 \cdot 0, 0 \cdot 1) = (0, 0)$.

4.6 Bases for number fields

4.6.1 Integral basis

An integral basis for a number field F of degree n is a set $B = \{b_1, \dots b_n\}$ of n algebraic integers in F such that every element of the ring of integers O_F of F can be written uniquely as a Z-linear combination of elements of B; that is, for any x in O_F we have $x = m_1b_1 + \dots + m_nb_n$,where the m_i are (ordinary) integers.

It is then also the case that any element of F can be written uniquely as $m_1b_1 + \dots + m_nb_n$,where now the m_i are rational numbers. The algebraic integers of F are then precisely those elements of F where the m_i are all integers.

Working locally and using tools such as the Frobenius map, it is always possible to explicitly compute such a basis, and it is now standard for computer algebra systems to have built-in programs to do this.

4.6.2 Power basis

Let F be a number field of degree n. Among all possible bases of F (seen as a Q-vector space), there are particular ones known as power bases, that are bases of the form

$$B_x = \{1, x, x^2, ..., x^{n-1}\}$$

for some element x ∈ F. By the primitive element theorem, there exists such an x, called a primitive element. If x can be chosen in O_F and such that B_x is a basis of O_F as a free Z-module, then B_x is called a power integral basis, and the field F is called a monogenic field. An example of a number field that is not monogenic was first given by Dedekind. His example is the field obtained by adjoining a root of the polynomial $x^3 - x^2 - 2x - 8$.[3]

Example

Consider F = Q(x), where x satisfies $x^3 - 11x^2 + x + 1 = 0$. Then an integral basis is $[1, x, 1/2(x^2 + 1)]$, and the corresponding integral trace form.

The "3" in the upper left hand corner of this matrix is the trace of the matrix of the map defined by the first basis element (1) in the regular representation of F on F. This basis element induces the identity map on the 3-dimensional vector space, F. The trace of the matrix of the identity map on a 3-dimensional vector space is 3.

The determinant of this is 1304 = 2^3 163, the field discriminant; in comparison the root discriminant, or discriminant of the polynomial, is 5216 = 2^5 163.

4.7 Galois theory

Évariste Galois (1811–1832)

In mathematics, more specifically in abstract algebra, Galois theory, named after Évariste Galois, provides a connection between field theory and group theory. Using Galois theory, certain problems in field theory can be reduced to group theory, which is in some sense simpler and better understood.

Originally Galois used permutation groups to describe how the various roots of a given polynomial equation are related to each other. The modern approach to Galois theory, developed by Richard Dedekind, Leopold Kronecker and Emil Artin, among others, involves studying automorphisms of field extensions.

Galois theory originated in the study of symmetric functions the coefficients of a monic polynomial are (up to sign) the elementary symmetric polynomials in the roots. For instance, $(x - a)(x - b) = x^2 - (a + b)x + a\ b$, where 1, $a + b$ and $a\ b$ are the elementary polynomials of degree 0, 1 and 2 in two variables.

This was first formalized by the 16th century French mathematician François Viète, in Viète's formulas, for the case of positive real roots. In the opinion of the 18th century British mathematician Charles Hutton,[2] the expression of coefficients of a polynomial in terms of the roots (not only for positive roots) was first understood by the 17th century French mathematician Albert Girard; Hutton writes.

The first person who understood the general doctrine of the formation of the coefficients of the powers from the sum of the roots and their products. He was the first who discovered the rules for summing the powers of the roots of any equation.

First example

4.7.1 A quadratic equation

Consider the quadratic equation

$$x^2 - 4x + 1 = 0.$$

By using the quadratic formula, we find that the two roots are

$$A = 2 + \sqrt{3}$$
$$B = 2 - \sqrt{3}.$$

Examples of algebraic equations satisfied by *A* and *B* include

$$A + B = 4,$$

and

$$AB = 1.$$

Obviously, in either of these equations, if we exchange *A* and *B*, we obtain another true statement. For example, the equation $A + B = 4$ becomes simply $B + A = 4$. Furthermore, it is true, but far less obvious, that this holds for *every* possible algebraic equation with rational coefficients relating the *A* and *B* values above (in any such equation, swapping *A* and *B* yields another true equation). To prove this requires the theory of symmetric polynomials.

(One might object that *A* and *B* are related by the algebraic equation $A – B - 2\sqrt{3 = 0}$, which does *not* remain true when *A* and *B* are exchanged. However, this equation does not concern us, because it does not have rational coefficients; in particular, $- 2\sqrt{3}$ is not rational).

We conclude that the Galois group of the polynomial $x^2 - 4x + 1$ consists of two permutations: the identity permutation which leaves *A* and *B* untouched, and the transposition permutation which exchanges *A* and *B*. It is a cyclic group of order two, and therefore isomorphic to Z/2Z.

A similar discussion applies to any quadratic polynomial $ax^2 + bx + c$, where *a*, *b* and *c* are rational numbers.

- If the polynomial has only one root, for example $x^2 - 4x + 4 = (x-2)^2$, then the Galois group is trivial; that is, it contains only the identity permutation.
- If it has two distinct *rational* roots, for example $x^2 - 3x + 2 = (x-2)(x-1)$, the Galois group is again trivial.
-

Second example

Consider the polynomial

$$x^4 - 10x^2+1,$$

which can also be written as

$$(x^2-5)^2 - 24.$$

We wish to describe the Galois group of this polynomial, again over the field of rational numbers. The polynomial has four roots.

A $=\sqrt{2} + \sqrt{3}$

B $=\sqrt{2 -} \sqrt{3}$

C $=-\sqrt{2} + \sqrt{3}$

D $=-\sqrt{2} - \sqrt{3}$.

There are 24 possible ways to permute these four roots, but not all of these permutations are members of the Galois group.

The members of the Galois group must preserve any algebraic equation with rational coefficients involving *A*, *B*, *C* and *D*. One such equation is

$$A + D = 0.$$

However, since

$$A + C = 2\sqrt{3} \neq 0,$$

the permutation

$$(A, B, C, D) \rightarrow (A, B, D, C)$$

is not permitted (because it transforms the valid equation $A + D = 0$ into the invalid equation

$A + C = 0$).

Another equation that the roots satisfy is

$$(A+B)^2 = 8$$

This will exclude further permutations, such as $(A, B, C, D) \rightarrow (A, C, B, D)$.

Continuing in this way, we find that the only permutations (satisfying both equations simultaneously) remaining are

$(A, B, C, D) \rightarrow (A, B, C, D)$
$(A, B, C, D) \rightarrow (C, D, A, B)$
$(A, B, C, D) \rightarrow (B, A, D, C)$
$(A, B, C, D) \rightarrow (D, C, B, A)$,
and the Galois group is isomorphic to the Klein four-group.

4.7.2 Solvable groups and solution by radicals

The notion of a solvable group in group theory allows one to determine whether a polynomial is solvable in radicals, depending on whether its Galois group has the property of solvability. In essence, each field extension L/K corresponds to a factor group in a composition series of the Galois group. If a factor group in the composition series is cyclic of order n, and if in the corresponding field extension L/K the field K already contains a primitive n-th root of unity, then it is a radical extension and the elements of L can then be expressed using the nth root of some element of K.

If all the factor groups in its composition series are cyclic, the Galois group is called *solvable*, and all of the elements of the corresponding field can be found by repeatedly taking roots, products, and sums of elements from the base field (usually Q).

One of the great triumphs of Galois Theory was the proof that for every $n > 4$, there exist polynomials of degree n which are not solvable by radicals—the Abel–Ruffini theorem. This is due to the fact that for $n > 4$ the symmetric group S_n contains a simple, non-cyclic, normal subgroup, namely A_n.

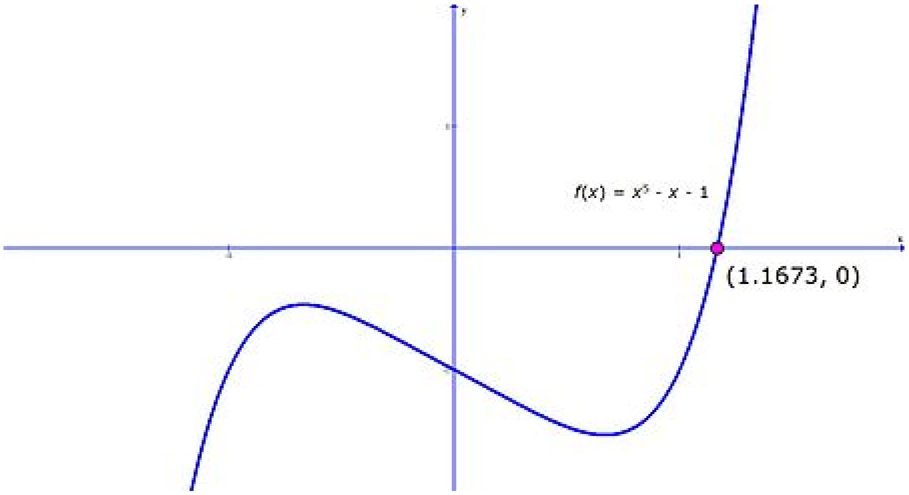


Fig 4.7.2

For the polynomial $f(x) = x^5 - x - 1$, the lone real root x=1.1673... is algebraic, but not expressible in terms of radicals. The other four roots are complex numbers.

4.7.3 A non-solvable quintic example

Van der Waerden cites the polynomial f(x)= $x^5 - x - 1$.By the rational root theorem this has no rational zeros. Neither does it have linear factors modulo 2 or 3.

The Galois group of f(x) modulo 2 is cyclic of order 6, because f(x) factors modulo 2 into $x^2 + x + 1$ and a cubic polynomial.f(x) has no linear or quadratic factor modulo 3, and hence is irreducible modulo 3. Thus its Galois group modulo 3 contains an element of order 5. It is known that a Galois group modulo a prime is isomorphic to a subgroup of the Galois group over the rationals. A permutation group on 5 objects with elements of orders 6 and 5 must be the symmetric group S_5, which is therefore the Galois group of f(x). This is one of the simplest examples of a non-solvable quintic polynomial. Serge Lang has said that Emil Artin found this example.

.*4.8* ***p*-adic number**

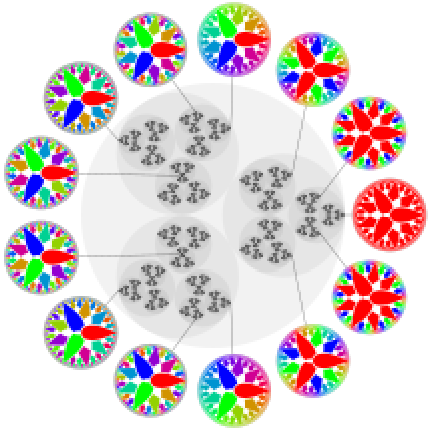


Fig 4.8

The 3-adic integers, with selected corresponding haracters on their Pontryagin dual group In mathematics the ***p*-adic number system** for any prime number *p* extends the ordinary arithmetic of the rational numbers in a way different from the extension of the rational number system to the real and complex number systems. The extension is achieved by an alternative interpretation of the concept of "closeness" or absolute value.

In particular, *p*-adic numbers have the interesting property that they are said to be close when their difference is divisible by a high power of *p* – the higher the power the closer they are. This property enables *p*-adic numbers to encode congruence information in a way that turns out to have powerful applications in number theory including, for example, in the famous proof of Fermat's Last Theorem by Andrew Wiles. *p*-adic numbers were first described by Kurt Hensel in 1897, though with hindsight some of Kummer's earlier work can be interpreted as implicitly using *p*-adic numbers. e *p*-adic numbers were motivated primarily by an attempt to bring the ideas and techniques of power series methods into number theory. Their influence now extends far beyond this. For example, the field of *p*-adic analysis essentially provides an alternative form of calculus.

More formally, for a given prime *p*, the field $\mathbf{Q}_p$ of *p*-adic numbers is a completion of the rational numbers. The field $\mathbf{Q}_p$ is also given a topology derived from a metric, which is itself derived from an alternative valuation on the rational numbers. This metric space is complete in the sense that every Cauchy sequence converges to a point in $\mathbf{Q}_p$. This is what allows the development of calculus on $\mathbf{Q}_p$, and it is the interaction of this analytic and algebraic structure which gives the *p*-adic number systems their power and utility.

The *p* in *p-adic* is a variable and may be replaced with a constant (yielding, for instance, "the 2-adic numbers") or another *placeholder variable* (for expressions such as "the ℓ-adic numbers").

p-adic expansions

4.8.1 P-adic expansions

When dealing with ordinary real numbers, if we take *p* to be a fixed prime number, then any positive integer can be written as a base *p* expansion in the form

$$\sum_{i=0}^{n} a_i p^i$$

where the a_i are integers in {0,…p-1}. For example, the binary expansion of 35 is $1\cdot 2^5 + 0\cdot 2^4 + 0\cdot 2^3 + 0\cdot 2^2 + 1\cdot 2^1 + 1\cdot 2^0$, often written in the shorthand notation 100011_2.

The familiar approach to extending this description to the larger domain of the rationals (and, ultimately, to the real's) is to use sums of the form:

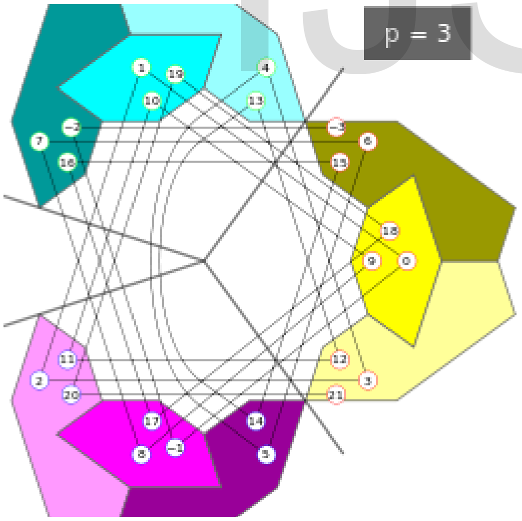
$$\pm \sum_{i=-\infty}^{n} a_i p^i .$$

A definite meaning is given to these sums based on Cauchy sequences, using the absolute value as metric. Thus, for example, 1/3 can be expressed in base 5 as the limit of the sequence $0.1313131313..._5$. In this formulation, the integers are precisely those numbers for which $a_i = 0$ for all $i < 0$.

With *p*-adic numbers, on the other hand, we choose to extend the base p expansions in a different way. Because in the *p*-adic world high positive powers of *p* are small and high negative powers are large, we consider infinite sums of the form:

$$\sum_{i=k}^{\infty} a_i p^i$$

where *k* is some (not necessarily positive) integer. With this approach we obtain the ***p*-adic expansions** of the *p*-adic numbers. Those *p*-adic numbers for which $a_i = 0$ for all $i < 0$ are also called the ***p*-adic integers**.



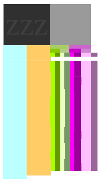


Fig 4.8.1

Similar picture for *p* = 3 shows 3 closed balls of radius 1/3, where each consists of 3 balls of 1/9

The real numbers can be defined as equivalence classes of Cauchy sequences of rational numbers; this allows us to, for example, write 1 as 1.000… = 0.999… . The definition of a Cauchy sequence relies on the metric chosen, though, so if we choose a different one, we can construct numbers other than the real numbers. The usual metric which yields the real numbers is called the Euclidean metric.

4.9 Ideal class group

In mathematics, the extent to which unique factorization fails in the ring of integers of an algebraic number field (or more generally any Dedekind domain) can be described by a certain group known as an ideal class group (or class group). If this group is finite (as it is in the case of the ring of integers of a number field), then the order of the group is called the class number. The multiplicative theory of a Dedekind domain is intimately tied to the structure of its class group. For example, the class group of a Dedekind domain is trivial if and only if the ring is a unique factorization domain.

5.Analyctic Number Theory

Analytic number theory is a branch of number theory that uses methods from mathematical analysis to solve problems about the integers .In Analytic number theory we study the analytic methods i.e,the mathematical analysis and the method of the theory of functions .First of all Euler used the analytic methods to study the number theory ,Dirichlet and Riemann developed this branch.

Analytic number theory can be split up into two major parts, divided more by the type of problems they attempt to solve than fundamental differences in technique. Multiplicative number theory deals with the distribution of the prime numbers, such as estimating the number of primes in an interval, and includes the prime number theorem and Dirichlet's theorem on primes in arithmetic progressions. Additive number theory is concerned with the additive structure of the integers, such as Goldbach's conjecture that every even number greater than 2 is the sum of two primes. One of the main results in additive number theory is the solution to Warning’s problem.

Developments within analytic number theory are often refinements of earlier techniques, which reduce the error terms and widen their applicability. For example, the *circle method* of Hardy and Little wood was conceived as applying to power series near the unit circle in the complex plane, it is now thought of in terms of finite exponential sums (that is, on the unit circle, but with the power series truncated.

5.1 Pro**blems and results in analytic number theory**

The great theorems and results within analytic number theory tend not to be exact structural results about the integers, for which algebraic and geometrical tools are more appropriate. Instead, they give approximate bounds and estimates for various number theoretical functions, as the following examples illustrate.

5.1 .1Multiplicative number theory

Euclid showed that there are an infinite number of primes but it is very difficult to find an efficient method for determining whether or not a number is prime, especially a large number. A related but easier problem is to determine the asymptotic distribution of the prime numbers; that is, a rough description of how many primes are smaller than a given number. Gauss, amongst others, after computing a large list of primes, conjectured that the number of primes less than or equal to a large number *N* is close to the value of the integral

$$\int_2^N \frac{1}{\log(t)}\,dt.$$

In 1859 Bernhard Riemann used complex analysis and a special meromorphic function now known as the Riemann zeta function to derive an analytic expression for the number of primes less than or equal to a real number *x*. Remarkably, the main term in Riemann's formula was exactly the above integral, lending substantial weight to Gauss's conjecture. Riemann found that the error terms in this expression, and hence the manner in which the primes are distributed, are closely related to the complex zeros of the zeta function. Using Riemann's ideas and by getting more information on the zeros of the zeta function, Jacques Hadamard and Charles Jean de la Vallée-Poussin managed to complete the proof of Gauss's conjecture. In particular, they proved that if

$$\pi(x) = (\text{number of primes } \le x),$$

then

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

This remarkable result is what is now known as the *Prime Number Theorem*. It is a central result in analytic number theory. More generally, the same question can be asked about the number of primes in any arithmetic progression *a* + *nq* for any integer *n*. In one of the first applications of analytic techniques to number theory, Dirichlet proved that any arithmetic progression with *a* and *q* co prime contains infinitely many primes.

5.1.2 Additive number theory:

One of the most important problems in additive number theory is Waring's problem, which asks whether it is possible, for any $k \geq 2$, to write any positive integer as the sum of a bounded number of k^{th} powers,

$$n = x_1^k + \cdots + x_\ell^k.$$

The case for squares, $k = 2$, was answered by Lagrange in 1770, who proved that every positive integer is the sum of at most four squares. The general case was proved by Hilbert in 1909, using algebraic techniques which gave no explicit bounds. An important breakthrough was the application of analytic tools to the problem by Hardy and Little wood. These techniques are known as the circle method, and give explicit upper bounds for the function $G(k)$, the smallest number of k^{th} powers needed, such as Vinogradov's bound G(k)≤k(3logk+11).

5.2 Methods of analytic number theory

5.2.1 Dirichlet series

One of the most useful tools in multiplicative number theory are Dirichlet series, which are functions of a complex variable defined by an infinite series

$$f(s) = \sum_{n=1}^{\infty} a_n n^{-s}.$$

Depending on the choice of coefficients a_n, this series may converge everywhere, nowhere, or on some half plane. In many cases, even where the series does not converge everywhere, the holomorphic function it defines may be analytically continued to a meromorphic function on the entire complex plane. The utility of functions like this in multiplicative problems can be seen in the formal identity

$$\left(\sum_{n=1}^{\infty} a_n n^{-s}\right)\left(\sum_{n=1}^{\infty} b_n n^{-s}\right) = \sum_{n=1}^{\infty}\left(\sum_{k\ell=n} a_k b_\ell\right) n^{-s};$$

hence the coefficients of the product of two Dirichlet series are the multiplicative convolutions of the original coefficients. Furthermore, techniques such as partial summation and Tauberian theorems can be used to get information about the coefficients from analytic information about the Dirichlet series. Thus a common method for estimating a multiplicative function is to express it as a Dirichlet series (or a product of simpler Dirichlet series using convolution identities), examine this series as a complex function and then convert this analytic information back into information about the original function.

5.2.2 Riemann Zeta function

Bernhard Riemann was born in 1826 and died in 1866,he was 39 years old.His theories contributed to Riemannian geometry,algebraic geometry, complex manifolds,and mathematical physics.He is best known for his work in analysis,for defining the Riemann integral using Riemann sums.In the field of number theory,Riemann only wrote one paper ,establishing the importance of the Riemann Zeta function and its relation to prime numbers.

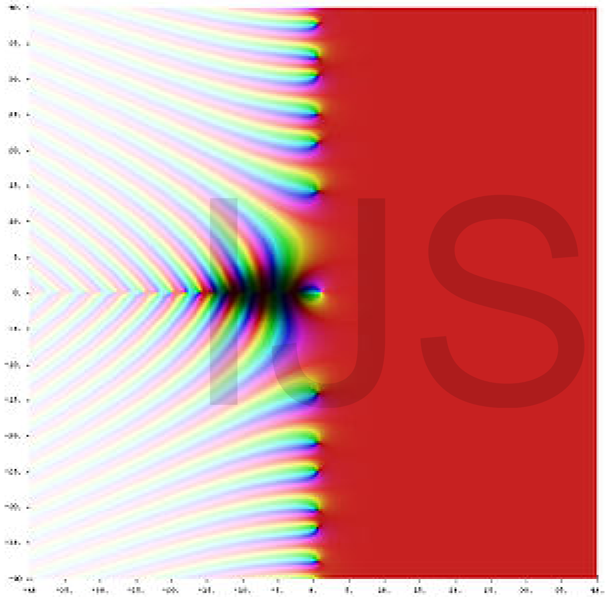


Fig 5.2.2

Riemann zeta function ζ(s) in the complex plane. The color of a point s encodes the value of ζ(s): colors close to black denote values close to zero, while hue encodes the value's argument. The white spot at s = 1 is the pole of the zeta function; the black spots on the negative real axis and on the critical line Re(s) = 1/2 are its zeros. Values with arguments close to zero including positive reals on the real half-line are presented in red.

The Riemann zeta function or Euler–Riemann zeta function, ζ(s), is a function of a complex variable s that analytically continues the sum of the infinite series $\sum_{n=1}^{\infty}\frac{1}{n^s},$ which converges when the real part of s is greater than 1. More general representations of ζ(s) for all s are given below. The Riemann zeta function plays a pivotal role in analytic number theory and has applications in physics, probability theory, and applied statistics.

This function, as a function of a real argument, was introduced and studied by Leonhard Euler in the first half of the eighteenth century without using complex analysis, which was not available at that time. Bernhard Riemann in his memoir "On the Number of Primes Less Than a Given Magnitude" published in 1859 extended the Euler definition to a complex variable, proved its meromorphic continuation and functional equation and established a relation between its zeros and the distribution of prime numbers.

The values of the Riemann zeta function at even positive integers were computed by Euler. The first of them, ζ(2), provides a solution to the Basel problem. In 1979 Apéry proved the irrationality of ζ(3). The values at negative integer points, also found by Euler, are rational numbers and play an important role in the theory of modular forms. Many generalizations of the Riemann zeta function, such as Dirichlet series, Dirichlet L-functions and L-functions, are known.

The Riemann zeta function ζ(s) is a function of a complex variable s = σ + it (here, s, σ and t are traditional notations associated with the study of the ζ-function). The following infinite series converges for all complex numbers s with real part greater than 1, and defines ζ(s) in this case:

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s} = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \cdots \qquad \sigma = \Re(s) > 1.$$

The Riemann zeta function is defined as the analytic continuation of the function defined for σ > 1 by the sum of the preceding series.

Leonhard Euler considered the above series in 1740 for positive integer values of s, and later Chebyshev extended the definition to real s > 1.

The above series is a prototypical Dirichlet series that converges absolutely to an analytic function for s such that σ > 1 and diverges for all other values of s. Riemann showed that the function defined by the series on the half-plane of convergence can be continued analytically to all complex values s ≠ 1. For s = 1 the series is the harmonic series which diverges to +∞, and

$$\lim_{s\to 1}(s-1)\zeta(s) = 1.$$

Thus the Riemann zeta function is a meromorphic function on the whole complex s-plane, which is holomorphic everywhere except for a simple pole at s = 1 with residue 1.

5.2.3 Specific values

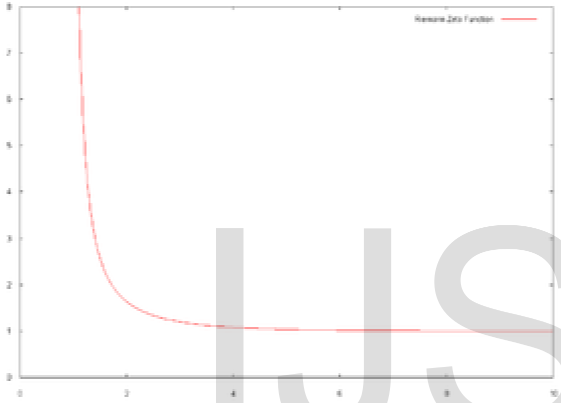


fig 5.2.3

Riemann zeta function for real s > 1

For any positive even number 2n,

$$\zeta(2n) = (-1)^{n+1}\frac{B_{2n}(2\pi)^{2n}}{2(2n)!}$$

where B_{2n} *is a Bernoulli number; for negative integers, one has*

$$\zeta(-n) = -\frac{B_{n+1}}{n+1}$$

for $n \geq 1$, *so in particular* ζ *vanishes at the negative even integers because* $B_m = 0$ *for all odd m other than 1. No such simple expression is known for odd positive integers.*

The values of the zeta function obtained from integral arguments are called zeta constants. The following are the most commonly used values of the Riemann zeta function.

$$\zeta(0) = -\frac{1}{2},$$

$\zeta(1/2) \approx -1.4603545$ *(sequence A059750 in OEIS)*

this is employed in calculating of kinetic boundary layer problems of linear kinetic equations.[3]

$$\zeta(1) = 1 + \frac{1}{2} + \frac{1}{3} + \cdots = \infty;$$

if we approach from numbers larger 1. Then this is the harmonic series. But its principal value

exists which is the Euler-Mascheroni constant $\gamma = 0.5772\ldots$.

$$\zeta(3/2) \approx 2.612;$$

this is employed in calculating the critical temperature for a Bose–Einstein condensate in a box with periodic boundary conditions, and for spin wave physics in magnetic systems.

$$\zeta(2) = 1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots = \frac{\pi^2}{6} \approx 1.645;$$

the demonstration of this equality is known as the Basel problem. The reciprocal of this sum answers the question: What is the probability that two numbers selected at random are relatively prime?[4]

$$\zeta(3) = 1 + \frac{1}{2^3} + \frac{1}{3^3} + \cdots \approx 1.202;$$

this is called Apéry's constant.

$$\zeta(4) = 1 + \frac{1}{2^4} + \frac{1}{3^4} + \cdots = \frac{\pi^4}{90} \approx 1.0823;$$

This appears when integrating Planck's law to derive the Stefan–Boltzmann law in physics.

5.2.4 Euler product formula

The connection between the zeta function and prime numbers was discovered by Euler, who proved the identity

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ prime}} \frac{1}{1-p^{-s}},$$

where, by definition, the left hand side is ζ(s) and the infinite product on the right hand side extends over all prime numbers p (such expressions are called Euler products):

$$\prod_{p \text{ prime}} \frac{1}{1-p^{-s}} = \frac{1}{1-2^{-s}} \cdot \frac{1}{1-3^{-s}} \cdot \frac{1}{1-5^{-s}} \cdot \frac{1}{1-7^{-s}} \cdot \frac{1}{1-11^{-s}} \cdots \frac{1}{1-p^{-s}} \cdots .$$

Both sides of the Euler product formula converge for Re(s) > 1. The proof of Euler's identity uses only the formula for the geometric series and the fundamental theorem of arithmetic. Since the harmonic series, obtained when s = 1, diverges, Euler's formula (which becomes $\prod_p p/(p-1)$) implies that there are infinitely many primes.[5]

The Euler product formula can be used to calculate the asymptotic probability that s randomly selected integers are set-wise co prime. Intuitively, the probability that any single number is divisible by a prime (or any integer), p is 1/p. Hence the probability that s numbers are all divisible by this prime is $1/p^s$, and the probability that at least one of them is not is $1 - 1/p^s$. Now, for distinct primes, these divisibility events are mutually independent because the candidate divisors are co prime (a number is divisible by co prime divisors n and m if and only if it is divisible by nm, an event which occurs with probability 1/(nm).) Thus the asymptotic probability that s numbers are co prime is given by a product over all primes,

$$\prod_p^{\infty}\left(1-\frac{1}{p^s}\right)=\left(\prod_p^{\infty}\frac{1}{1-p^{-s}}\right)^{-1}=\frac{1}{\zeta(s)}.$$

Apart from the trivial zeros, the Riemann zeta function doesn't have any zero on the right of σ=1 and on the left of σ=0 (neither can the zeros lie too close to those lines). Furthermore, the non-trivial zeros are symmetric about the real axis and the line σ = 1/2 and, according to the Riemann Hypothesis, they all lie on the line σ = ½

Mellin transform

The Mellin transform of a function ƒ(x) is defined as

$$\int_0^\infty f(x)x^{s-1}\,dx,$$

in the region where the integral is defined. There are various expressions for the zeta-function as a Mellin transform. If the real part of s is greater than one, we have

$$\Gamma(s)\zeta(s)=\int_0^\infty \frac{x^{s-1}}{e^x-1}\,dx,$$

where Γ denotes the Gamma function. By modifying the contour Riemann showed that

$$2\sin(\pi s)\Gamma(s)\zeta(s)=i\oint_C \frac{(-x)^{s-1}}{e^x-1}\,dx$$

for all s, where the contour C starts and ends at +∞ and circles the origin once.

We can also find expressions which relate to prime numbers and the prime number theorem. If π(x) is the prime-counting function, then

$$\log \zeta(s) = s \int_0^\infty \frac{\pi(x)}{x(x^s - 1)}\, dx,$$

for values with Re(s) > 1.

A similar Mellin transform involves the Riemann prime-counting function J(x), which counts prime powers p^n with a weight of 1/n, so that

$$J(x) = \sum \frac{\pi(x^{1/n})}{n}.$$

Now we have

$$\log \zeta(s) = s \int_0^\infty J(x) x^{-s-1}\, dx.$$

These expressions can be used to prove the prime number theorem by means of the inverse Mellin transform. Riemann's prime-counting function is easier to work with, and π(x) can be recovered from it by Möbius inversion.

Rising factorial

Another series development using the rising factorial valid for the entire complex plane is

$$\zeta(s) = \frac{s}{s-1} - \sum_{n=1}^{\infty} (\zeta(s+n) - 1) \frac{s(s+1)\cdots(s+n-1)}{(n+1)!}.$$

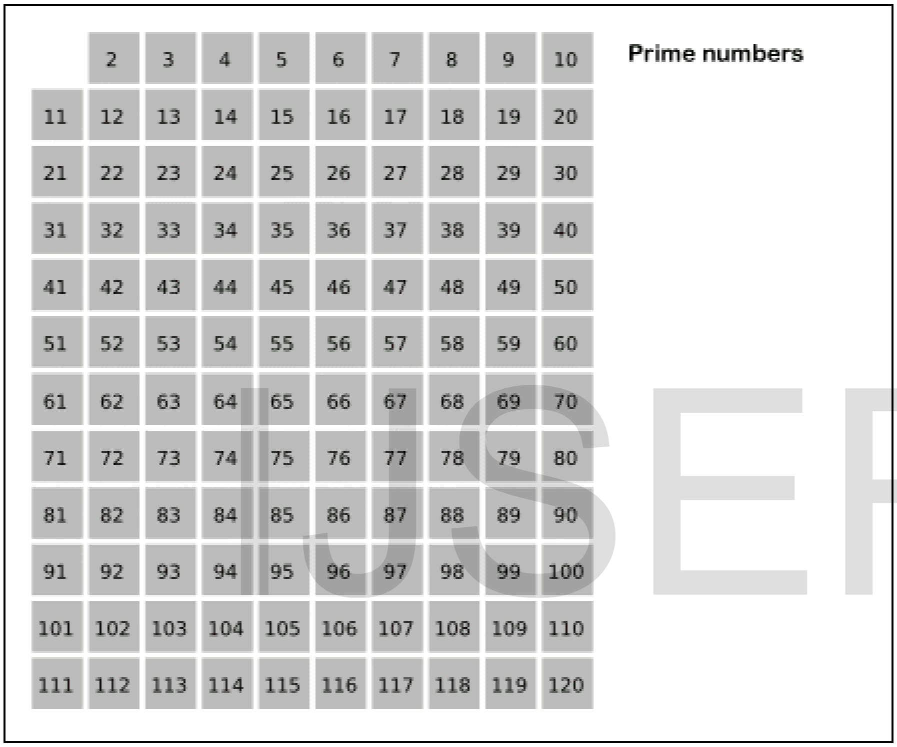
This can be used recursively to extend the Dirichlet series definition to all complex numbers.

The Riemann zeta function also appears in a form similar to the Mellin transform in an integral over the Gauss–Kuzmin–Wirsing operator acting on x^{s-1}; that context gives rise to a series expansion in terms of the falling factorial.

5.3 Proof of the Euler product formula for the Riemann zeta function

In number theory ,an Euler product is an expansion of a Dirichlet series into an infinite product indexed by prime numbers.The name arose from the case of the Riemann Zeta function , Where such a product representation was proved by Leonhard Euler.

The Euler Product formula



Prime numbers

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120

The Euler product formula for the Riemann zeta function reads

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ prime}} \frac{1}{1-p^{-s}}$$

where the left hand side equals the Riemann zeta function:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \ldots$$

and the product on the right hand side extends over all prime numbers *p*:

$$\prod_{p \text{ prime}} \frac{1}{1-p^{-s}} = \frac{1}{1-2^{-s}} \cdot \frac{1}{1-3^{-s}} \cdot \frac{1}{1-5^{-s}} \cdot \frac{1}{1-7^{-s}} \cdots \frac{1}{1-p^{-s}} \cdots$$

Proof of the Euler product formula

The method of Eratosthenes used to sieve out prime numbers is employed in this proof.

This sketch of a proof only makes use of simple algebra commonly taught in high school. This was originally the method by which Euler discovered the formula. There is a certain sieving property that we can use to our advantage:

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \ldots$$
$$\frac{1}{2^s}\zeta(s) = \frac{1}{2^s} + \frac{1}{4^s} + \frac{1}{6^s} + \frac{1}{8^s} + \frac{1}{10^s} + \ldots$$

Subtracting the second from the first we remove all elements that have a factor of 2:

$$\left(1 - \frac{1}{2^s}\right)\zeta(s) = 1 + \frac{1}{3^s} + \frac{1}{5^s} + \frac{1}{7^s} + \frac{1}{9^s} + \frac{1}{11^s} + \frac{1}{13^s} + \ldots$$

Repeating for the next term:

$$\frac{1}{3^s}\left(1 - \frac{1}{2^s}\right)\zeta(s) = \frac{1}{3^s} + \frac{1}{9^s} + \frac{1}{15^s} + \frac{1}{21^s} + \frac{1}{27^s} + \frac{1}{33^s} + \ldots$$

Subtracting again we get:

$$\left(1 - \frac{1}{3^s}\right)\left(1 - \frac{1}{2^s}\right)\zeta(s) = 1 + \frac{1}{5^s} + \frac{1}{7^s} + \frac{1}{11^s} + \frac{1}{13^s} + \frac{1}{17^s} + \ldots$$

where all elements having a factor of 3 or 2 (or both) are removed.

It can be seen that the right side is being sieved. Repeating infinitely we get:

$$\ldots\left(1 - \frac{1}{11^s}\right)\left(1 - \frac{1}{7^s}\right)\left(1 - \frac{1}{5^s}\right)\left(1 - \frac{1}{3^s}\right)\left(1 - \frac{1}{2^s}\right)\zeta(s) = 1$$

Dividing both sides by everything but the ζ(s) we obtain:

$$\zeta(s) = \frac{1}{\left(1-\frac{1}{2^s}\right)\left(1-\frac{1}{3^s}\right)\left(1-\frac{1}{5^s}\right)\left(1-\frac{1}{7^s}\right)\left(1-\frac{1}{11^s}\right)\ldots}$$

This can be written more concisely as an infinite product over all primes *p*:

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

To make this proof rigorous, we need only observe that when $\Re(s) > 1$, the sieved right-hand side approaches 1, which follows immediately from the convergence of the Dirichlet series for ζ(*z*).

The case $s = 1$

An interesting result can be found for ζ(1)

$$\ldots\left(1-\frac{1}{11}\right)\left(1-\frac{1}{7}\right)\left(1-\frac{1}{5}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{2}\right)\zeta(1) = 1$$

which can also be written as,

$$\ldots\left(\frac{10}{11}\right)\left(\frac{6}{7}\right)\left(\frac{4}{5}\right)\left(\frac{2}{3}\right)\left(\frac{1}{2}\right)\zeta(1) = 1$$

which is,

$$\left(\frac{\ldots\cdot 10\cdot 6\cdot 4\cdot 2\cdot 1}{\ldots\cdot 11\cdot 7\cdot 5\cdot 3\cdot 2}\right)\zeta(1) = 1$$

as, $\zeta(1) = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \ldots$

thus,

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \ldots = \frac{2\cdot 3\cdot 5\cdot 7\cdot 11\cdot\ldots}{1\cdot 2\cdot 4\cdot 6\cdot 10\cdot\ldots}$$

We know that the left-hand side of the equation diverges to infinity, therefore the numerator on the right-hand side (the primorial) must also be infinite for divergence. This proves that there are infinitely many prime numbers.

6. Computational Number Theory

"Computational number theory" studies the effectiveness of algorithms for computation of number-theoretic quantities. Considerable effort has been expended in primality-testing and integer factorization routines, for example -- procedures which are in principle trivial, but whose naive solution is untenable in large cases. This field also considers integer quantities (e.g the class number) whose usual definition is non constructive, and real quantities (e.g. the values of zeta functions) which must be computed with very high precision; thus this overlaps both computer algebra and numerical analysis.

computation has been a driving force in the development of mathematics. To help measure the sizes of their fields, the Egyptians invented geometry To help predict the positions of the planets, the Greeks invented trigonometry. Algebra was invented to deal with equations that arose when mathematics was used to model the world. The list goes on, and it is not just historical. If anything, computation is more important than ever. Much of modern technology rests on algorithms that compute quickly: examples range from the wavelets that allow CAT scans, to the numerical extrapolation of extremely complex systems in order to predict weather and global warming, and to the combinatorial algorithms that lie behind Internet search engines .

In pure mathematics we also compute, and many of our great theorems and conjectures are, at root, motivated by computational experience. It is said that Gauss , who was an excellent computationalist, needed only to work out a concrete example or two to discover, and then prove, the underlying theorem. While some branches of pure mathematics have perhaps lost contact with their computational origins, the advent of cheap computational power and convenient mathematical software has helped to reverse this trend.

One mathematical area where the new emphasis on computation can be clearly felt is number theory, and that is the main topic of this article. A prescient call to arms was issued by Gauss as long ago as 1801: The problem of distinguishing prime numbers from composite numbers, and of resolving the latter into their prime factors, is known to be one of the most important and useful in arithmetic.

It has engaged the industry and wisdom of ancient and modern geometers to such an extent that it would be superfluous to discuss the problem at length. Nevertheless we must confess that all methods that have been proposed thus far are either restricted to very special cases or are so laborious and difficult that even for numbers that do not exceed the limits of tables constructed by estimable men, they try the patience of even the practiced calculator. And these methods do not apply at all to larger numbers. . . Further, the dignity of the science itself seems to require that every possible means be explored for solution of a problem so elegant and so celebrated.

Factorization into primes is a very basic issue in number theory, but essentially all branches of number theory have a computational component. And in some areas there is such a robust computational literature that we discuss the algorithms involved as mathematically interesting objects in their own right.

6.1 Integer factorization

In number theory, integer factorization or prime factorization is the decomposition of a composite number into smaller non-trivial divisors, which when multiplied together equal the original integer.

When the numbers are very large, no efficient, non-quantum integer factorization algorithm is known; an effort concluded in 2009 by several researchers factored a 232-digit number (RSA-768), utilizing hundreds of machines over a span of 2 years The presumed difficulty of this problem is at the heart of widely used algorithms in cryptography such as RSA. Many areas of mathematics and computer science have been brought to bear on the problem, including elliptic curves, algebraic number theory, and quantum computing.

Not all numbers of a given length are equally hard to factor. The hardest instances of these problems (for currently known techniques) are semi primes, the product of two prime numbers. When they are both large, for instance more than 2000 bits long, randomly chosen, and about the same size (but not too close, e.g. to avoid efficient factorization by Fermat's factorization method), even the fastest prime factorization algorithms on the fastest computers can take enough time to make the search impractical; that is, as the number of digits of the primes being factored increases, the number of operations required to perform the factorization on any computer increases drastically.

- Many cryptographic protocols are based on the difficulty of factoring large composite integers or a related problem, the RSA problem. An algorithm that efficiently factors an arbitrary integer would render RSA-based public-key cryptography insecure.

6.1.1 Prime decomposition

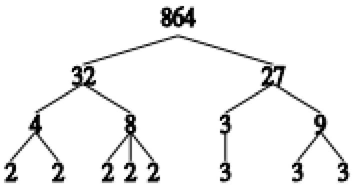


Fig 6.1.1

This image demonstrates the prime decomposition of 864. A shorthand way of writing the resulting prime factors is $2^5 \times 3^3$

By the fundamental theorem of arithmetic, every positive integer has a unique prime factorization. (A special case for 1 is not needed using an appropriate notion of the empty product.) However, the fundamental theorem of arithmetic gives no insight into how to obtain an integer's prime factorization; it only guarantees its existence.

Given a general algorithm for integer factorization, one can factor any integer down to its constituent prime factors by repeated application of this algorithm. However, this is not the case with a special-purpose factorization algorithm, since it may not apply to the smaller factors that occur during decomposition, or may execute very slowly on these values. For example, if N is the number $(2^{521} - 1) \times (2^{607} - 1)$, then trial division will quickly factor 10N as 2 × 5 × N, but will not quickly factor N into its factors.

Current state of the art

The most difficult integers to factor in practice using existing algorithms are those that are products of two large primes of similar size, and for this reason these are the integers used in cryptographic applications. The largest such semi prime yet factored was RSA-768, a 768-bit number with 232 decimal digits, on December 12, 2009 This factorization was a collaboration of several research institutions, spanning two years and taking the equivalent of almost 2000 years of computing on a single-core 2.2 GHz AMD Opt eron. Like all recent factorization records, this factorization was completed with a highly optimized implementation of the general number field sieve run on hundreds of machines.

Difficulty and complexity

If a large, *b*-bit number is the product of two primes that are roughly the same size, then no algorithm has been published that can factor in polynomial time, *i.e.*, that can factor it in time $O(b^k)$ for some constant *k*. There are published algorithms that are faster than $O((1+\varepsilon)^b)$ for all positive ε, *i.e.*, sub-exponential.

The best published asymptotic running time is for the general number field sieve (GNFS) algorithm, which, for a *b*-bit number n, is:

$$O\left(\exp\left(\left(\tfrac{64}{9}b\right)^{\frac{1}{3}}(\log b)^{\frac{2}{3}}\right)\right).$$

For an ordinary computer, GNFS is the best published algorithm for large *n* (more than about 100 digits). For a quantum computer, however, Peter Shor discovered an algorithm in 1994 that solves it in polynomial time. This will have significant implications for cryptography if a large quantum computer is ever built. Shor's algorithm takes only $O(b^3)$ time and $O(b)$ space on *b*-bit number inputs. In 2001, the first seven-qubit quantum computer became the first to run Shor's algorithm. It factored the number 15.

When discussing what complexity classes the integer factorization problem falls into, it's necessary to distinguish two slightly different versions of the problem:

- The function problem version: given an integer N, find an integer d with 1 < d < N that divides N (or conclude that N is prime). This problem is trivially in FNP and it's not known whether it lies in FP or not. This is the version solved by most practical implementations.
- The decision problem version: given an integer N and an integer M with 1 ≤ M ≤ N, does N have a factor d with 1 < d < M? This version is useful because most well-studied complexity classes are defined as classes of decision problems, not function problems. This is a natural decision version of the problem, analogous to those frequently used for optimization problems, because it can be combined with binary search to solve the function problem version in a logarithmic number of queries.

It is not known exactly which complexity classes contain the decision version of the integer factorization problem. It is known to be in both NP and co-NP. This is because both YES and NO answers can be verified in polynomial time given the prime factors (we can verify their primality using the AKS primality test, and that their product is N by multiplication).

The fundamental theorem of arithmetic guarantees that there is only one possible string that will be accepted (providing the factors are required to be listed in order), which shows that the problem is in both UP and co-UP. It is known to be in BQP because of Shor's algorithm. It is suspected to be outside of all three of the complexity classes P, NP-complete, and co-NP-complete. It is therefore a candidate for the NP-intermediate complexity class. If it could be proved that it is in either NP-Complete or co-NP-Complete, that would imply NP = co-NP. That would be a very surprising result, and therefore integer factorization is widely suspected to be outside both of those classes. Many people have tried to find classical polynomial-time algorithms for it and failed, and therefore it is widely suspected to be outside P.

In contrast, the decision problem "is N a composite number?" (or equivalently: "is N a prime number?") appears to be much easier than the problem of actually finding the factors of N. Specifically, the former can be solved in polynomial time (in the number n of digits of N) with the AKS primality test. In addition, there are a number of probabilistic algorithms that can test primality very quickly in practice if one is willing to accept the vanishingly small possibility of error. The ease of primality testing is a crucial part of the RSA algorithm, as it is necessary to find large prime numbers to start with.

7. Geometric Number Theory

"Geometric number theory" incorporates all forms of geometry. The classical Geometry of Numbers due to Minkowski begins with statements of Euclidean geometry on lattices (A convex body contains a lattice point if its volume is large enough); by extension this becomes the study of quadratic forms on lattices, and thus a method of investigating regular packings of spheres, say. But one may also investigate algebraic geometry with number theory, that is, one may study varieties such as algebraic curves and surfaces and ask if they have *rational* or *integral* solutions (points with rational or integral coordinates). This topic includes the highly successful theory of elliptic curves (where the rational points form a finitely generated group) and finiteness results (e.g. Siegel's, Thue's, or Faltings's) which apply to integral or higher-genus situations.

7.1 Geometry of numbers

In number theory, the geometry of numbers studies convex bodies and integer vectors in n-dimensional space. The geometry of numbers was initiated by Hermann Minkowski (1910).

- The geometry of numbers has a close relationship with other fields of mathematics, especially functional analysis and Diophantine approximation, the problem of finding rational numbers that approximate an irrational quantity.

7.1.1 Minkowski's results

Suppose that Γ is a lattice in *n*-dimensional Euclidean space R^n and *K* is a convex centrally symmetric body. Minkowski's theorem, sometimes called Minkowski's first theorem, states that if $vol(K) > 2^n vol(R^n/\Gamma)$then *K* contains a nonzero vector in Γ.

The successive minimum λ_k is defined to be the inf of the numbers λ such that λ*K* contains *k* linearly independent vectors of Γ. Minkowski's theorem on successive minima, sometimes called Minkowski's second theorem, is a strengthening of his first theorem and states that[]

$$\lambda_1 \lambda_2 \cdots \lambda_n vol(K) \le 2^n vol(R^n/\Gamma).$$

Later research in the geometry of numbers

In 1930-1960 research on the geometry of numbers was conducted by many number theorists (including Louis Mordell, Harold Davenport and Carl Ludwig Siegel). In recent years, Lenstra, Brion, and Barvinok have developed combinatorial theories that enumerate the lattice points in some convex bodies.

Influence on functional analysis

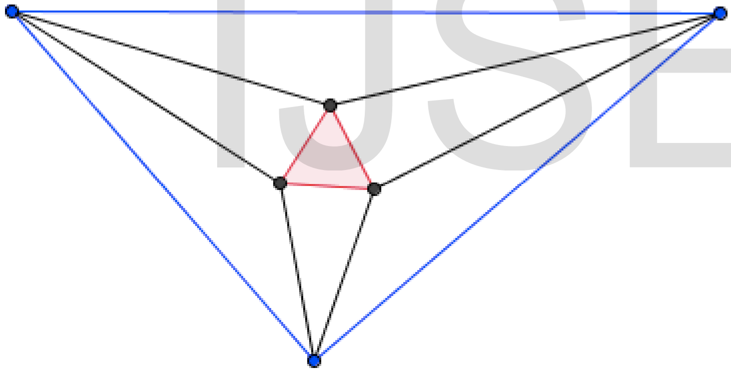
Minkowski's geometry of numbers had a profound influence on functional analysis. Minkowski proved that symmetric convex bodies induce norms in finite-dimensional vector spaces. Minkowski's theorem was generalized to topological vector spaces by Kolmogorov, whose theorem states that the symmetric convex sets that are closed and bounded generate the topology of a Banach space.Researchers continue to study generalizations to star-shaped sets and other non-convex sets.

7.2 Three geometric theorems

7.2.1 Morley's miracle

In 1899 Frank Morley, a professor at Haverford, discovered the following remarkable theorem.

The three points of intersection of the adjacent trisectors of the angles of any triangle form an equilateral triangle.



..

Fig 7.2.1

7.2.2 The Pascal line

When he was sixteen years old Blaise Pascal discovered the following theorem.

If any hexagon (convex or not) is inscribed in a conic section and opposite sides are extended until they meet, then the three points of intersection will be collinear.

The line is now called the Pascal line.

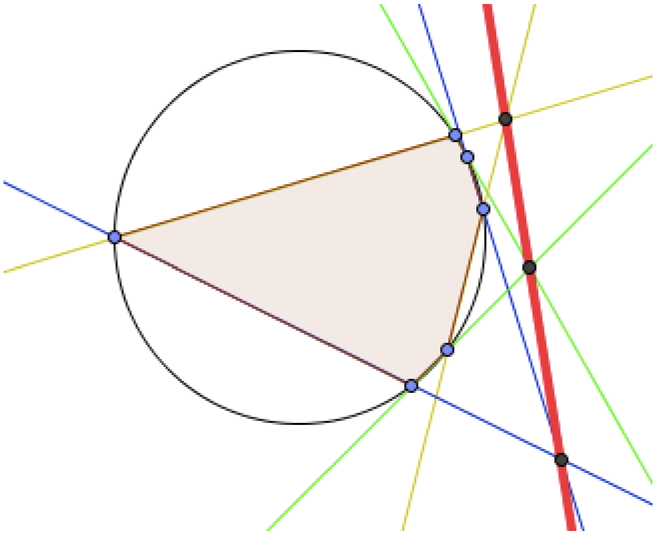


Fig 7.2.2

I've made a Geogebra applet illustrating the Pascal line in the case where the conic section is a circle. When you try the applet, do not forget to try the non convex configurations!

In fact, given a hexagon, we could keep the vertices fixed and permute their order to obtain other hexagons. A little combinatorics shows that there are 60 different hexagons for each collection of six points. Each configuration has its own Pascal line. There is a lot known about these Pascal lines and their intersections.

7.2.3 Steiner-Lehmus theorem

This last theorem is remarkable, not for what it says, but because of the difficulty of the proof. In 1840 C. L. Lehmus asked for a purely geometric proof of the following elementary-looking theorem.

***Any triangle with two angle bisectors of equal lengths is isosceles*.**

For example, suppose we have the triangle ABCshown below with angle bisectors $AD$and BE of the same length. Prove that $AC$and $BC$are the same length.

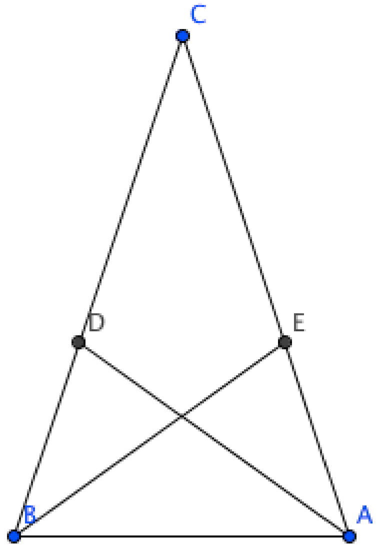


Fig 7.2.3

Steiner gave the first purely geometric proof. Now there are many geometric (and trigonometric) proofs, but they are all tricky and are all proofs by contradiction. In 1852 Sylvester asked whether there exists a direct proof of this theorem. It appears that this is still an open problem. (From what I understand, there have been direct proofs,

8. Applications

- ## 8.1 Chinese Remainder Theorem

- In the RSA algorithm calculations are made modulo *n*, where *n* is a product of two large prime numbers *p* and *q*. 1,024-, 2,048- or 4,096-bit integers *n* are commonly used, making calculations in $\mathbb{Z}/n\mathbb{Z}$very time-consuming. By the Chinese remainder theorem, however, these calculations can be done in the isomorphic ring $\mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/q\mathbb{Z}$instead. Since *p* and *q* are normally of about the same size, that is about $\sqrt{n}$, calculations in the latter representation are much faster. Note that RSA algorithm implementations using this isomorphism are more susceptible to fault injection attacks.

- The Chinese remainder theorem may also be used to construct an elegant Gödel numbering for sequences, which is needed to prove Gödel's incompleteness theorems.

- The following example shows a connection with the classic polynomial interpolation theory. Let *r* complex points ("interpolation nodes") $\lambda_1, \ldots, \lambda_r$be given, together with the complex data $a_{j,k}$, for all $1 \le j \le r$and $0 \le k < \nu_j$. The general Hermite interpolation problem asks for a polynomial $P(x) \in \mathbb{C}[x]$taking the prescribed derivatives in each node λ_j:

  $$P^{(k)}(\lambda_j) = a_{j,k} \quad \forall 1 \le j \le r, 0 \le k < \nu_j.$$

  Introducing the polynomials

  $$A_j(x) := \sum_{k=0}^{\nu_j - 1} \frac{a_{j,k}}{k!}(x - \lambda_j)^k$$

  the problem may be equivalently reformulated as a system of r simultaneous congruences:

  $$P(x) \equiv A_j(x) \pmod{(x - \lambda_j)^{\nu_j}}, \quad \forall 1 \le j \le r.$$

  By the Chinese remainder theorem in the principal ideal domain $\mathbb{C}[x]$, there is a unique such polynomial $P(x)$with degree $\deg(P) < n := \sum_j \nu_j$. A direct construction, in analogy with the above proof for the integer number case, can be performed as follows. Define the polynomials $Q := \prod_{i=1}^{r}(x - \lambda_i)^{\nu_i}$ and $Q_j := \frac{Q}{(x - \lambda_j)^{\nu_j}}$. The partial fraction decomposition of $\frac{1}{Q}$ gives *r* polynomials S_j with degrees $\deg(S_j) < \nu_j$such that

  $$\frac{1}{Q} = \sum_{i=1}^{r} \frac{S_i}{(x - \lambda_i)^{\nu_i}}$$

  so that $1 = \sum_{i=1}^{r} S_i Q_i$. Then a solution of the simultaneous congruence system is given by the polynomial

$$\sum_{i=1}^{r} A_iS_iQ_i = A_j + \sum_{i=1}^{r}(A_i - A_j)S_iQ_i \equiv A_j \pmod{(x-\lambda_j)^{\nu_j}} \quad \forall 1 \leq j \leq r$$

and the minimal degree solution is this one reduced modulo Q, that is the unique with degree less than *n*.

- The Chinese remainder theorem can also be used in secret sharing, which consists of distributing a set of shares among a group of people who, all together (but no one alone), can recover a certain secret from the given set of shares. Each of the shares is represented in a congruence, and the solution of the system of congruence's using the Chinese remainder theorem is the secret to be recovered. Secret Sharing using the Chinese Remainder Theorem uses, along with the Chinese remainder theorem, special sequences of integers that guarantee the impossibility of recovering the secret from a set of shares with less than a certain cardinality.

- The Good-Thomas fast Fourier transform algorithm exploits a re-indexing of the data based on the Chinese remainder theorem. The Prime-factor FFT algorithm contains an implementation.

- Dedekind's theorem on the linear independence of characters states (in one of its most general forms) that if *M* is a monoid and *k* is an integral domain, then any finite family $(f_i)_{i\in I}$of distinct monoid homomorphism's $f_i : M \to k$(where the monoid structure on *k* is given by multiplication) is linearly independent; i.e., every family $(\alpha_i)_{i\in I}$of elements $\alpha_i \in k$satisfying $\sum_{i\in I} \alpha_i f_i = 0$must be equal to the family $(0)_{i\in I}$.

  Proof using the Chinese Remainder Theorem: First, assume that *k* is a field (otherwise, replace the integral domain *k* by its quotient field, and nothing will change). We can linearly extend the monoid homeomorphisms $f_i : M \to k$to *k*-algebra homomorphism's $F_i : k[M] \to k$, where $k[M]$is the monoid ring of *M* over *k*. Then, the condition $\sum_{i\in I} \alpha_i f_i = 0$yields $\sum_{i\in I} \alpha_i F_i = 0$by linearity. Now, we notice that if $i \neq j$are two elements of the index set *I*, then the two *k*-linear maps $F_i : k[M] \to k$and $F_j : k[M] \to k$are not proportional to each other (because if they were, then $f_i$and $f_j$would also be proportional to each other, and thus equal to each other since $f_i(1) = 1 = f_j(1)$(since f_i and $f_j$are monoid homomorphism), contradicting the assumption that they be distinct). Hence, their kernels $\operatorname{Ker} F_i$and $\operatorname{Ker} F_j$are distinct. Now, $\operatorname{Ker} F_i$is a maximal ideal of $k[M]$ for every $i \in I$(since $k[M]/\operatorname{Ker} F_i \cong F_i(k[M]) = k$is a field), and the ideals $\operatorname{Ker} F_i$and $\operatorname{Ker} F_j$ are co prime whenever $i \neq j$ (since they are distinct and maximal). The Chinese Remainder Theorem (for general rings) thus yields that the map

  $$\phi : k[M]/K \to \prod_{i\in I} k[M]/\mathrm{Ker} F_i$$

  given by

  $$\phi(x+K) = (x + \mathrm{Ker} F_i)_{i\in I} \text{for all } x \in k[M]$$

  is an isomorphism, where $K = \prod_{i\in I} \operatorname{Ker} F_i = \bigcap_{i\in I} \operatorname{Ker} F_i$. Consequently, the map

  $$\Phi : k[M] \to \prod_{i\in I} k[M]/\mathrm{Ker} F_i$$

IJSER

given by
$\Phi\left(x\right)=\left(x+\operatorname{Ker}F_{i}\right)_{i\in I}$for all $x\in k\left[M\right]$
is surjective. Under the isomorphism $k[M]/\operatorname{Ker}F_i\to F_i(k[M])=k$, this map Φcorresponds to the map
$\psi:k\left[M\right]\to\prod_{i\in I}k$
given by
$x\mapsto\left[F_{i}\left(x\right)\right]_{i\in I}$for every $x\in k\left[M\right]$.
Now, $\sum_{i\in I}\alpha_iF_i=0$yields $\sum_{i\in I}\alpha_iu_i=0$for every vector $(u_i)_{i\in I}$in the image of the map ψ. Since $\psi$is surjective, this means that $\sum_{i\in I}\alpha_iu_i=0$for every vector $(u_i)_{i\in I}\in\prod_{i\in I}k$. Consequently, $(\alpha_i)_{i\in I}=(0)_{i\in I}$, QED.

8.2 Lagrange’s theorem

Theorem: For any prime all the coefficients of the polynomial

f(x)=(x-1)(x-2)….(x-p+1)-x^{p-1}+1 are divisible by p.

Proof: Let g(x) =(x-1)(x-2)….(x-p+1).the roots of g are the numbers

1, 2,…p-1,hence they satisfy the congruence .

g(x)≡ 0(modp)

By the Euler Fermat Theorem, these numbers also satisfy the congruence h(x)≡ $0(modp)$

h(x) =x^{p-1}-1

The difference f(x)=g(x)-h(x) has degree p-2 but the congruence f(x)≡ $0(modp)$ has p-1 solutions, 1,2,…..p-1.therefore,each coefficient of f(x) is divisible by p.

Wolstenholme’s Theorem

For any prime p≥ 5 we have $\sum_{k=1}^{p-1} \frac{(p-1)!}{k} \equiv 0(modp^2)$

Proof The sum in question is the sum of the products of the numbers 1,2,…p-1 taken p-2 at atime .This sum is also equal to the coefficient of –x in the polynomial g(x)=(x-1)(x-2)….(x-p+1).

In fact, g(x) can be written in the form g(x)=x^{p-1}-s_1x^{p-1}+s_2 x^{p-3}-….+s_{p-3x^2}-s_{p-2}x+(p-1)!.

Where the coefficient s_k is the kth elementary symmetric function of the roots, that is, the sum of the products of the numbers 1, 2….p-1, taken k at a time. Each of the numbers $s_{1,}s_2…s_{p-2}$ is divisible by p.we wish to show that s_{p-2} is divisible by p^2.

The product for g(x) shows that g(p)=(p-1)! So

(p-1)!=p^{p-1}-s_1p^{p-2}+….+s_{n-3p^2}-$s_{n-2}p$ +(p-1)!.

Canceling (p-1)! And reducing the equation mod p^3 we find, since p≥5,ps_{p-2} ≡0(mod p^3)

And hence s_{p-2} ≡0(modp^2),as required.

8.3 Reciprocity law

Determine whether 219 is a quadratic residue or nonresidue mod 383 solution .We evaluate the legender symbol(219/383) by using the multiplicative property,the reciprocity law, periodicity, and the special values(-1/p) and (2/p) calculated earlier

Since 219=3.73 the multiplicative property implies

(219/383)=(3/383)(73/383)

Using the reciprocity law and periodicity we have

$(3/383)=(383/3)(-1)^{\frac{(383-1)(3-1)}{4}}$

$=-(-1/3)=-(-1)^{\frac{(3-1)}{2}}=1$

$(73/383)=(383/73)(1)^{\frac{(383-1)(73-1)}{4}}$

$=(18/73)=(2/73)(9/73)$

$=(-1)^{\frac{((73)^2-1)}{8}}$

=1

Hence (219/383)=1 so 219 is a quadratic residue mod 383

8.4 Cryptography

Cryptography is derived from Greek word "cryptology" – "hidden secret" and graphein-writing. It is about constructing and analyzing protocols that overcome the influence of adversaries and which are related to various aspects in information security such as data integrity, authentication and non-repudiation.

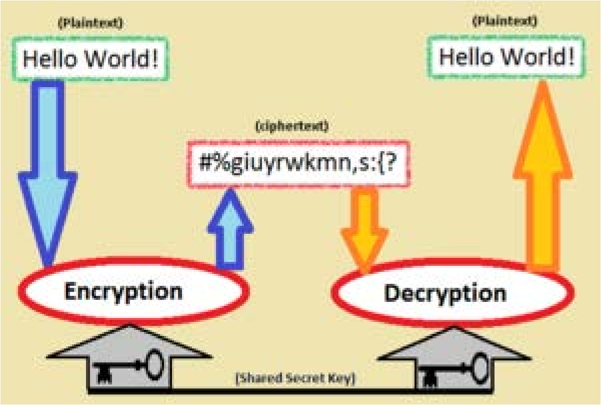


Fig 8.4

Symmetric-key cryptography, where the same key is used both for encryption and decryption

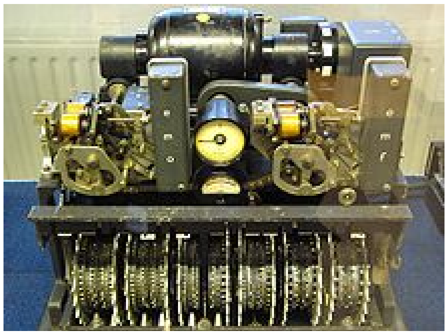


Fig 8.4.1

German Lorenz cipher machine, used in World War II to encrypt very-high-level general staff messages

Cryptography (or *cryptology*; from Greek κρυπτός, "hidden, secret"; and, *graphein*, "writing", "study", respectively) is the practice and study of techniques for secure communication in the presence of third parties (called adversaries). More generally, it is about constructing and analyzing protocols that overcome the influence of adversaries and which are related to various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation. Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce.

Modern cryptography is heavily based on mathematical theory and computer science practice; cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary. It is theoretically possible to break such a system but it is infeasible to do so by any known practical means. These schemes are therefore termed computationally secure; theoretical advances (e.g., improvements in integer factorization algorithms) and faster computing technology require these solutions to be continually adapted. There exist information-theoretically secure schemes that provably cannot be broken even with unlimited computing power—an example is the one-time pad—but these schemes are more difficult to implement than the best theoretically breakable but computationally secure mechanisms.

8.4.1 Cryptography and cryptanalysis

Before the modern era, cryptography was concerned solely with message confidentiality (i.e., encryption)—conversion of messages from a comprehensible form into an incomprehensible one and back again at the other end, rendering it unreadable by interceptors or eavesdroppers without secret knowledge (namely the key needed for decryption of that message). Encryption was used to (attempt to) ensure secrecy in communications, such as those of spies, military leaders, and diplomats. In recent decades, the field has expanded beyond confidentiality concerns to include techniques for message integrity checking, sender/receiver identity authentication, digital signatures, interactive proofs and secure computation, among others.

8.4.2 Classic cryptography

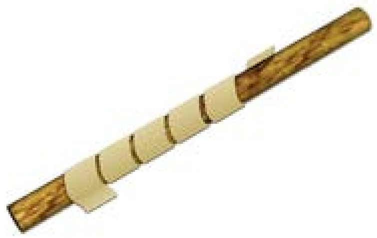


Fig 8.4.2
Reconstructed ancient Greek *scytale* (rhymes with "Italy"), an early cipher device

The earliest forms of secret writing required little more than local pen and paper analogs, as most people could not read. More literacy, or literate opponents, required actual cryptography. The main classical cipher types are transposition ciphers, which rearrange the order of letters in a message (e.g., 'hello world' becomes 'ehlol owrdl' in a trivially simple rearrangement scheme), and substitution ciphers, which systematically replace letters or groups of letters with other letters or groups of letters (e.g., 'fly at once' becomes 'gmz bu podf' by replacing each letter with the one following it in the Latin alphabet). Simple versions of either have never offered much confidentiality from enterprising opponents. An early substitution cipher was the Caesar cipher, in which each letter in the plaintext was replaced by a letter some fixed number of positions further down the alphabet. Suetonius reports that Julius Caesar used it with a shift of three to communicate with his generals. Atbash is an example of an early Hebrew cipher. The earliest known use of cryptography is some carved ciphertext on stone in Egypt (ca 1900 BCE), but this may have been done for the amusement of literate observers rather than as a way of concealing information. Cryptography is recommended in the Kama Sutra (ca 400 BCE) as a way for lovers to communicate without inconvenient discovery.

The Greeks of Classical times are said to have known of ciphers (e.g., the scytale transposition cipher claimed to have been used by the Spartan military). Steganography (i.e., hiding even the existence of a message so as to keep it confidential) was also first developed in ancient times. An early example, from Herodotus, concealed a message—a tattoo on a slave's shaved head—under the regrown hair Another Greek method was developed by Polybius (now called the "Polybius Square"). More modern examples of steganography include the use of invisible ink, microdots, and digital watermarks to conceal information.

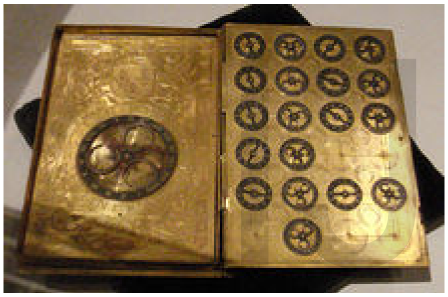


Fig 8.4.2 (a)

16th-century book-shaped French cipher machine, with arms of Henri II of France

Fig 8.4.2(b)

Enciphered letter from Gabriel de Luetz d'Aramon, French Ambassador to the Ottoman Empire, after 1546, with partial decipherment

Essentially all ciphers remained vulnerable to cryptanalysis using the frequency analysis technique until the development of the polyalphabetic cipher, most clearly by Leon Battista Alberti around the year 1467, though there is some indication that it was already known to Al-Kindi. Alberti's innovation was to use different ciphers (i.e., substitution alphabets) for various parts of a message (perhaps for each successive plaintext letter at the limit). He also invented what was probably the first automatic cipher device, a wheel which implemented a partial realization of his invention. In the polyalphabetic Vigenère cipher, encryption uses a *key word*, which controls letter substitution depending on which letter of the key word is used. In the mid-19th century Charles Babbage showed that the Vigenère cipher was vulnerable to Kasiski examination, but this was first published about ten years later by Friedrich Kasiski.

Although frequency analysis is a powerful and general technique against many ciphers, encryption has still often been effective in practice, as many a would-be cryptanalyst was unaware of the technique. Breaking a message without using frequency analysis essentially required knowledge of the cipher used and perhaps of the key involved, thus making espionage, bribery, burglary, defection, etc., more attractive approaches to the cryptanalytically uninformed.

8.4.3 Computer era

Just as the development of digital computers and electronics helped in cryptanalysis, it made possible much more complex ciphers. Furthermore, computers allowed for the encryption of any kind of data representable in any binary format, unlike classical ciphers which only encrypted written language texts; this was new and significant. Computer use has thus supplanted linguistic cryptography, both for cipher design and cryptanalysis. Many computer ciphers can be characterized by their operation on binary bit sequences (sometimes in groups or blocks), unlike classical and mechanical schemes, which generally manipulate traditional characters (i.e., letters and digits) directly. However, computers have also assisted cryptanalysis, which has compensated to some extent for increased cipher complexity. Nonetheless, good modern ciphers have stayed ahead of cryptanalysis; it is typically the case that use of a quality cipher is very efficient (i.e., fast and requiring few resources, such as memory or CPU capability), while breaking it requires an effort many orders of magnitude larger, and vastly larger than that required for any classical cipher, making cryptanalysis so inefficient and impractical as to be effectively impossible.

Fig 8.4.3

Credit card with smart-card capabilities. The 3-by-5-mm chip embedded in the card is shown, enlarged. Smart cards combine low cost and portability with the power to compute cryptographic algorithms.

cryptographic problems and quantum physics (see quantum cryptography and quantum computer).

8.5 Modern cryptography

8.5.1 Symmetric-key cryptography

Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key (or, less commonly, in which their keys are different, but related in an easily computable way). This was the only kind of encryption publicly known until June 1976.

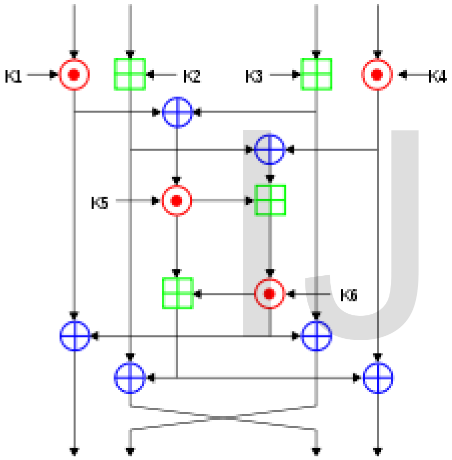


Fig 8.5.1
One round (out of 8.5) of the patented IDEA cipher, used in some versions of PGP for high-speed encryption of, for instance, e-mail

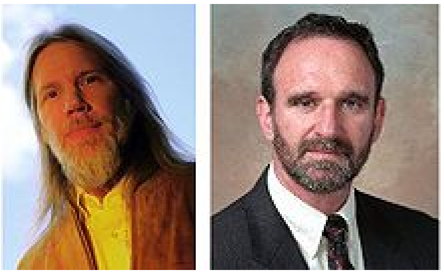
Symmetric key ciphers are implemented as either block ciphers or stream ciphers. A block cipher enciphers input in blocks of plaintext as opposed to individual characters, the input form used by a stream cipher.

The Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) are block cipher designs which have been designated cryptography standards by the US government (though DES's designation was finally withdrawn after the AES was adopted). Despite its deprecation as an official standard, DES (especially its still-approved and much more secure triple-DES variant) remains quite popular; it is used across a wide range of applications, from ATM encryptionto e-mail privacyand secure remote access. Many other block ciphers have been designed and released, with considerable variation in quality. Many have been thoroughly broken, such as FEAL.

Stream ciphers, in contrast to the 'block' type, create an arbitrarily long stream of key material, which is combined with the plaintext bit-by-bit or character-by-character, somewhat like the one-time pad. In a stream cipher, the output stream is created based on a hidden internal state which changes as the cipher operates. That internal state is initially set up using the secret key material. RC4 is a widely used stream cipher; see Category:Stream ciphers.[4] Block ciphers can be used as stream ciphers; see Block cipher modes of operation.

Message authentication codes (MACs) are much like cryptographic hash functions, except that a secret key can be used to authenticate the hash value upon receipt.

8.5.2 Public-key cryptography



Symmetric-key cryptosystems use the same key for encryption and decryption of a message, though a message or group of messages may have a different key than others. A significant disadvantage of symmetric ciphers is the key management necessary to use them securely. Each distinct pair of communicating parties must, ideally, share a different key, and perhaps each ciphertext exchanged as well. The number of keys required increases as the square of the number of network members, which very quickly requires complex key management schemes to keep them all straight and secret. The difficulty of securely establishing a secret key between two communicating parties, when a secure channel does not already exist between them, also presents a chicken-and-egg problem which is a considerable practical obstacle for cryptography users in the real worlWhitfield Diffie and Martin Hellman, authors of the first published paper on public-key cryptography.

*** THANK YOU ***