Springer Monographs in Mathematics

Władysław Narkiewicz

Rational Number Theory in the 20th Century

From PNT to FLT

Springer

S*pringer* **M***onographs* in **M***athematics*

For further volumes:
www.springer.com/series/3733

Władysław Narkiewicz

Rational Number Theory in the 20th Century

From PNT to FLT

Springer

Władysław Narkiewicz
Institute of Mathematics
Wrocław University
Plac Grunwaldzki 2-4
50-384 Wrocław
Poland
narkiew@math.uni.wroc.pl

ISSN 1439-7382 Springer Monographs in Mathematics
ISBN 978-0-85729-531-6 e-ISBN 978-0-85729-532-3
DOI 10.1007/978-0-85729-532-3
Springer London Dordrecht Heidelberg New York

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library

Library of Congress Control Number: 2011937173

Mathematics Subject Classification: 11-00, 11-03, 01A60

Cover design: VTeX UAB, Lithuania

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

1. The beginning of a new century provides a good moment for looking back. Number theory has changed its appearance during the last hundred years. At the end of the 19th century it was regarded as a collection of dispersed results dealing with various old and newer problems, obtained by people who were mostly specializing in other subjects. After one hundred years number theory became a well-established part of mathematical sciences, having close relations to commutative algebra, homological algebra, algebraic geometry, function theory, real analysis, functional analysis, group theory and topology.

2. The aim of this book is to give a short survey of the development of the classical part of number theory between the proof of the Prime Number Theorem (PNT) and the proof of Fermat's Last Theorem (FLT), covering thus the twentieth century. Results obtained earlier or later will be also quoted, as far as they are connected with our main topics.

Actually it is now difficult to indicate the borders of number theory, as it tends to acquire grounds reserved earlier to analysis, algebra or geometry. It seems that A. Weil thought about limiting the possessions of number theory, when he wrote: "To the best of my understanding, analytic number theory is not number theory," [6630, p. 8] but nowadays it is fashionable to believe that number theory encompasses more and more of mathematical research.

The word "rational" in the title indicates that we shall concentrate on that part of number theory which deals with properties of integers and rational numbers, hence the theory of algebraic numbers will be excluded. This is motivated by the fact that its inclusion would enormously increase the size of the book, and, moreover, a large bibliography covering this part of number theory is available in my previous book [4543]. Nevertheless, some exceptions will be made, as we shall consider the class-number problems for quadratic and cyclotomic fields. The first of them coincides with the class-number problem for binary quadratic forms, and the second is intimately connected with the earlier approach to Fermat's Last Theorem. We shall also comment on the generalization of the Waring problem to algebraic number fields and describe the creation of class-field theory because of its influence on the reciprocity laws.

The history of the theory of modular forms which played a decisive role in the proof of Fermat's Last Theorem, and which underwent great progress in the last century, deserves a book of its own. Therefore we shall describe only those parts of its development which had a direct influence on number theory proper. This applies also to other branches of mathematics providing tools for arithmetical research. In particular we will not touch the more advanced topics in Diophantine geometry.

In consecutive chapters we shall present the main achievements of the relevant period, accompanied by comments about the development occurring in the next periods. An exception will be made for Fermat's Last Theorem, to which the last chapter is devoted. Our exposition will be concise, sometimes imitating the style of the celebrated Dickson's *History of the Theory of Numbers* [1545], although there is neither the possibility nor need to comment on all number-theoretical production. We have tried to list all the main achievements, quote many important papers, but restrain from including technical details in order to make the text available to non-specialists also. More attention will be paid to earlier work, in the hope that this will help to save it from falling into oblivion.

3. The first chapter contains a very short summary of the development of number theory in the 19th century, starting with Gauss's book *Disquisitiones Arithmeticae* [2208], and ending with the proof of the Prime Number Theorem by Hadamard and de la Vallée-Poussin and Hilbert's talk at the 1900 Congress of Mathematicians in Paris. The second chapter begins with a survey of some famous old problems (perfect numbers, Mersenne and Fermat primes, primality, ...), and then brings the story of our subject at the begin of the century (solution of the Waring problem, Brun's sieve, theorem of Thue, ...). In the next chapter the development up to 1930 will be covered (the inventing of the circle method by Hardy and Ramanujan, progress in the theory of Diophantine equations starting with Siegel's thesis, Mordell's finite basis theorem in the theory of elliptic curves). The most important events in the thirties, covered in Chap. 4, were Vinogradov's proof of the ternary Goldbach conjecture for large numbers, the solution of Hilbert's problem about transcendence of numbers α^β (with algebraic $\alpha \neq 0, 1$ and algebraic irrational β) obtained by Gelfond and Schneider, and the revival of the theory of modular forms by Hecke. The next two chapters report on later development, including the creation of the large sieve, and Chen's theorem on the binary Goldbach problem. The last chapter is devoted to Fermat's Last Theorem.

Information about results obtained after the period considered in each particular chapter is set in a smaller font.

Acknowledgements In writing this book I used the important collections of old books and journals available in the library of the Faculty of Mathematics and Computer Sciences of Wrocław University. I am very grateful to the librarians for their extraordinary patience. I have also used available reference journals, as well as various databases on the web, in particular those of Jahrbuch, Zentralblatt and MathSciNet.

I would like to express my sincere thanks to numerous friends and colleagues, who helped me in the search for information. In particular I would like to thank

Jerzy Browkin, Kalman Győry, Franz Lemmermeyer, Tauno Metsänkylä, Andrzej Schinzel and Michel Waldschmidt who read preliminary versions of my manuscript and suggested several improvements.

I am also very grateful to the Springer copyeditors for their remarkable job. Particular thanks go to Ms Karen Borthwick and Ms Lauren Stoney for their cooperation. I would like also to thank the Springer team of TeX experts for helpful suggestions which removed typesetting problems.

Wrocław, Poland
August 15, 2011

Władysław Narkiewicz

Contents

Notation

We will use the standard notation utilized in modern texts on number theory. In particular we shall denote by $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$ and $\mathbf{C}$ the ring of rational integers, the fields of rational, real and complex numbers, respectively. The field of p-adic numbers and its ring of integers will be denoted by $\mathbf{Q}_p$ and $\mathbf{Z}_p$, respectively.

The number of divisors, Euler's phi-function, the sum of divisors and the sum of kth powers of divisors of an integer n will be denoted by $d(n)$, $\varphi(n)$, $\sigma(n)$ and $\sigma_k(n)$, respectively. By $\omega(n)$ we shall denote the number of prime divisors of n, and by $\Omega(n)$ the number of prime factors of n, counted with their multiplicities. The symbol $\left(\frac{n}{p}\right)$ will denote the quadratic residue symbol of Legendre.

By $\mu(n)$ we shall denote the Möbius function, defined by

$$\mu(n) = \begin{cases} (-1)^{\omega(n)} & \text{if } n \text{ is square-free,} \\ 0 & \text{otherwise.} \end{cases}$$

The number of representations of n as a product of k factors > 1 will be denoted by $d_k(n)$. By ζ_n we shall denote the primitive nth root of unity $\exp(2\pi i/n)$.

The letter p in formulas will always denote a prime. By P_k we shall denote a number having at most k prime factors (i.e., $\mathit{\Omega}(P_k) \leq k$), and $\pi(x)$ will be the number of primes $p \leq x$.

By $\mathrm{li}(x)$ we shall denote the logarithmic integral defined by

$$\mathrm{li}(x) = \int_2^x \frac{dt}{\log t},$$

and $\Gamma(z)$ will be the usual Gamma-function.

We shall use Landau's o-notation, writing

$$f(x) = o(g(x))$$

when the ratio $\frac{|f(x)|}{g(x)}$ tends to 0, when x tends to infinity, and the O-notation

$$f(x) = O(g(x)),$$

introduced on p. 225 in [2520], to mean the existence of a constant C with

$$|f(x)| \leq Cg(x)$$

holding for large x. In particular $f(x) = o(1)$ means that $f(x)$ tends to 0, and $f(x) = O(1)$ implies that the function $f(x)$ is bounded. Instead of $f(x) = O(g(x))$ we shall also use Vinogradov's notation $f \ll g$ and $g \gg f$. If the implied constant depends on some parameters $a, b, \ldots$, then we shall write $O_{a,b,\ldots}$, $\ll_{a,b,\ldots}$, or $\gg_{a,b,\ldots}$, respectively.

The notation

$$f(x) = \Omega(g(x))$$

stands for the falsity of the relation $f(x) = o(g(x))$, and

$$f(x) = \Omega_{+}(g(x)), \qquad f(x) = \Omega_{-}(g(x))$$

means that for a sequence x_n tending to infinity one has

$$f(x_n) \geq Cg(x_n), \qquad f(x_n) < -Cg(x_n)$$

respectively, with a suitable positive constant C, assuming $g(x)$ to be positive.

The letter ε will usually be reserved for arbitrarily small positive numbers.

By $\Re z$, $\Im z$ we denote the real and imaginary part of the complex number z. The distance of a real number x from the nearest integers will be denoted by $\|x\|$, and by $\{x\}$ we shall denote the fractional part of x. The number of elements of a set A will be denoted by $\#A$.

For an algebraic integer a we shall denote by $\overline{|a|}$ the house of a, defined as the product of all conjugates of a, lying outside the unit circle.

Chapter 1
The Heritage

The 19th century brought essential progress in all branches of mathematics and number theory was no exception. The biggest steps in its development are connected with the names of three eminent mathematicians: C.F. Gauss[1], P.G.L. Dirichlet[2] and B. Riemann[3].

The book *Disquisitiones Arithmeticae* [2208] by the young Gauss, published in 1801, gave a solid basis for the subsequent development, presenting for the first time proofs of such fundamental results as the unique factorization property of positive integers and the quadratic reciprocity law. Its main subject was the theory of binary quadratic forms with integral coefficients. Gauss considered the action of the group $\Gamma = SL_2(\mathbf{Z})$ of unimodular 2×2 matrices with integral entries on the set of primitive binary forms $f(X, Y) = aX^2 + bXY + cY^2$ with even middle coefficient (this restriction turned out later to be unnecessary) and a fixed discriminant, defining the action of

$$M = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \in \Gamma$$

by

$$M \cdot f = f(\alpha X + \beta Y, \gamma X + \delta Y). \tag{1.1}$$

He introduced a composition in the set of resulting orbits inducing the structure of a finite Abelian group. He did not have yet the notion of a group which arose later, but several of his results in [2208] have a group-theoretical meaning. In particular his comments at the end of art. 306 indicate that he guessed the decomposition of the group formed by classes in the principal genus into a product of cyclic factors.

P.G.L. Dirichlet was the first who, in the thirties, applied analytical tools to arithmetical questions. This brilliant idea allowed him [1584, 1585] to prove the infini-

[1] Carl Friedrich Gauss (1777–1855), professor in Göttingen. See [1653, 3285].

[2] Peter Gustav Lejeune Dirichlet (1805–1859), professor in Breslau, Berlin and Göttingen. See [4327].

[3] Bernhard Riemann (1826–1866), professor in Göttingen. See [3722].

W. Narkiewicz, *Rational Number Theory in the 20th Century*,
Springer Monographs in Mathematics,
DOI 10.1007/978-0-85729-532-3_1, © Springer-Verlag London Limited 2012

tude of primes in arithmetical progressions $ax+b$ with co-prime integers a, b, and to give an analytical formula for the number of classes of binary quadratic forms [1586, 1587] studied by Gauss. For this aim Dirichlet introduced L-functions by the formula

$$L(s,\chi)=\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s},$$

where χ is a character of the group $G(k)=\{a \bmod k : (a,k)=1\}$ of reduced residue classes $\bmod k$, and s is a positive real number.

One should point out that Dirichlet followed Gauss in the style of presentation, giving very precise and flawless arguments, which was rather a rarity at that time.

Another revolutionary idea came from B. Riemann who in 1860 related in [5224] analytical properties of the series

$$\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s} \tag{1.2}$$

to the properties of prime numbers[4]. It had been known since L. Euler[5] that this series converges for $s>1$ and its sum is connected with prime numbers due to the formula

$$\zeta(s)=\prod_{p}\frac{1}{1-p^{-s}}, \tag{1.3}$$

but Riemann was the first to consider $\zeta(s)$ for complex arguments. He obtained its analytical continuation to a meromorphic function in the plane with a single simple pole at $s=1$ and showed that it satisfies the functional equation

$$\Gamma\left(\frac{s}{2}\right)\pi^{-s/2}\zeta(s)=\Gamma\left(\frac{1-s}{2}\right)\pi^{-(1-s)/2}\zeta(1-s) \tag{1.4}$$

for all complex $s\neq 0, 1$. He stated several properties of $\zeta(s)$ and the counting function of primes,

$$\pi(x)=\sum_{p\leq x}1,$$

for which complete proofs were later obtained, except for the assertion that every non-real zero of $\zeta(s)$ lies on the line $\Re s=1/2$. This is the famous *Riemann Hypothesis* (RH).

The only previous result about $\pi(x)$ was obtained by P.L. Čebyšev[6], who proved in 1850 [970] that for large x one has

$$0.92129\frac{x}{\log x}<\pi(x)<1.1055\frac{x}{\log x}\cdot \tag{1.5}$$

[4] For an analysis of Riemann's memoir see the book by H.M. Edwards [1691].

[5] Leonhard Euler (1752–1833), professor in St. Petersburg and Berlin. See [852, 1986].

[6] Pafnutiĭ Lvovič Čebyšev (1821–1894), professor in St. Petersburg. See [5015].

To the list of outstanding personalities of that time one should also add C.G.J. Jacobi[7], whose main achievement in number theory consisted of applying the theory of elliptic functions to various arithmetical questions. In that way he obtained several identities in the theory of partitions and gave explicit formulas for the determination of $r_k(n)$, the number of representations of an integer n as the sum of k squares for $k = 2, 4, 6$ and 8 [3075, 3077].

The theory of algebraic numbers, which started with Gauss's study [2211] of the complex integers $a + bi$ $(a, b \in \mathbf{Z})$, was further developed by P.G. Dirichlet (see [1593, 1594]) and E.E. Kummer[8] (see [3583]), who utilized it in his work on Fermat's Last Theorem, and reached adult status in the hands of R. Dedekind[9] (see [1423]).

The leading French mathematicians interested in number theory at that time were J. Liouville[10], who constructed the first transcendental numbers and produced several important results in the theory of Diophantine equations, and C. Hermite[11] who, among other deep results, established the transcendence of the number e, the basis of natural logarithms.

In the second half of the century two great personalities, J. Hadamard[12] and H. Poincaré[13], became interested in number theory. Hadamard [2426] confirmed a conjecture of Gauss's by proving in 1896 the Prime Number Theorem as a by-product of his theory of entire functions, and Poincaré, whose main interest was rather far away from number theory, published two papers in our subject. In the first [4935] he generalized Čebyšev's bound (1.5) to the case of primes congruent to unity mod 4, and in the second [4936] he considered rational points on elliptic curves defined by an equation of the form $y^2 = f(x)$, where f is a cubic polynomial without multiple roots.

One should also mention here E. Cahen[14], E. Maillet[15], H. Padé[16] and T. Pépin[17]. Maillet showed [4108] that for sufficiently large k, depending on the prime p, Fermat's equation

$$X^{p^k} + Y^{p^k} = Z^{p^k}$$

[7] Carl Gustav Jacob Jacobi (1804–1851), professor in Königsberg and Berlin. See [3438, 3439].

[8] Ernst Eduard Kummer (1810–1893), professor in Breslau and Berlin.

[9] Richard Dedekind (1831–1916), professor in Zürich and Braunschweig.

[10] Joseph Liouville (1809–1882), professor in Paris. See [4035].

[11] Charles Hermite (1822–1901), professor in Paris. See [4624, 4849].

[12] Jacques Salomon Hadamard (1865–1963), professor in Bordeaux and Paris. See [3868, 4221].

[13] Jules Henri Poincaré (1854–1912), professor in Paris. See [4850].

[14] Eugéne Cahen (1865–1941), teacher at Collège Rolin in Paris.

[15] Edmond Maillet (1865–1938), engineer, president of the Société Mathématique de France in 1918.

[16] Henri Padé (1863–1953), professor in Poitiers and Bordeaux.

[17] Jean François Théophile Pépin (1826–1904), catholic priest, Jesuit, teacher of mathematics.

has no solution in positive integers not divisible by p, and in [4107] studied representations of integers as sums of values of polynomials of small degree.

Cahen [878] made the first systematic study of general Dirichlet series and published in 1900 a textbook on number theory [879]. Padé introduced in [4714] a new kind of continued fractions which later played an important role in analysis and number theory, and Pépin [4775] studied various Diophantine equations, providing in particular a description of all integral solutions of $X^4 + 35Y^4 = Z^2$.

At the end of the 19th century several bright young mathematicians interested in number theory started their careers, Most of them came from Germany. One should list here first of all A. Hurwitz[18], a student of F. Klein[19]. He got his degree in 1881 in Leipzig, next year made his habilitation in Göttingen[20], became in 1884 extraordinary professor at the University of Königsberg[21], and stayed there until 1892 when he switched to ETH[22] in Zürich. In Königsberg he had two extremely bright students, D. Hilbert[23] and H. Minkowski[24]. Hilbert obtained his doctorate in 1886 at Königsberg, got an extraordinary professorship, and in 1893 became ordinarius there. In 1895 he left Königsberg for Göttingen which at that time was, in the hands of Klein, the center of mathematical life. Minkowski, a close friend of Hilbert, got his doctorate in 1885, in 1892 became professor in Bonn, returned in 1895 to Königsberg University, in 1896 went to ETH, and in 1902 settled in Göttingen. In 1899 E. Landau[25], a student of G. Frobenius[26], got his doctorate in Berlin, and after the early death of Minkowski became in 1909 his follower in Göttingen. To this list one should also add K. Hensel[27] who studied in Berlin and obtained his degree in 1884 under L. Kronecker[28]. Two years later he made his habilitation there, became professor in Berlin, and in 1901 switched to Marburg. He invented the p-adic numbers, which would play an important role in algebra and number theory in the coming century. Most of the work in number theory in Germany at the beginning of the 20th century was done by these men and their students.

[18] Adolf Hurwitz (1859–1919). See [2791, 6794].

[19] Christian Felix Klein (1849–1925), studied in Bonn under Plücker, passed his doctorate at the age of 19, professor in Erlangen, Munich, Leipzig and Göttingen. See [1259].

[20] He was unable to do this in Leipzig, since he pursued his secondary education at a Realgymnasium, considered unacceptable by Leipzig University [2791].

[21] Called now Kaliningrad, in honor of a Soviet official Mikhail Kalinin.

[22] Eidgenössische Technische Hochschule in Zürich.

[23] David Hilbert (1862–1943), professor in Königsberg and Göttingen. See [5149].

[24] Hermann Minkowski (1864–1909), professor in Bonn, Königsberg, Zürich and Göttingen. See [2790].

[25] Edmund Landau (1877–1938), professor in Göttingen. See [2518, 3418].

[26] Ferdinand Georg Frobenius (1849–1917), professor in Zürich and Berlin.

[27] Kurt Hensel (1861–1941), edited the *Journal für reine und angewandte Mathematik* from 1901 on. See [2603, 5533].

[28] Leopold Kronecker (1823–1891), professor in Berlin. See [3403].

The English mathematicians at the brink of the 20th century were not particularly keen on number theory. Among the few who produced papers on our subject one should point out H.J.S. Smith[29], who for the proof of his formula for $r_5(n)$ shared with Minkowski the prize of the Paris Academy in 1887, J.J. Sylvester[30], who after his return from America considered the problem of odd perfect numbers (see [2239]), J.W.L. Glaisher[31], who at that time was the editor of the journal *Messenger of Mathematics*, and A. Cunningham[32], whose interest encompassed the elementary theory of numbers, in particular factorization, and primality tests of large integers. Knowledge of foreign literature was not particularly high, so, for example, Glaisher devoted two papers to the series $\sum_{n=0}^{\infty}(-1)^n/(2n)^2$, not noticing its relation to $\zeta(2)$, and rediscovered [2245] Dirichlet's class-number formula in the case of discriminant equal to 7, writing "I do not know whether the following series for $\frac{\pi}{\sqrt{7}}$ has been remarked before." This was followed by a paper by N.M. Ferrers[33] [1996], who found Dirichlet's formula for discriminants 11 and 19, and only in [2246] Glaisher acknowledged Dirichlet's priority. Glaisher also wrote a series of papers [2242–2244, 2247] dealing with Bernoulli, Eulerian and related numbers, and later studied representations of integers by sums of squares (see Sect. 2.4.1).

The situation changed drastically when G.H. Hardy[34] became interested in arithmetical problems. In his first paper [2504] on this subject, published in 1906, he presented an analytical formula giving the maximal prime divisor $\theta(N)$ of a positive integer N:

$$\theta(N) = \lim_{r\to\infty}\lim_{m\to\infty}\lim_{n\to\infty}\sum_{j=0}^{m}\left(1-\cos\left(\frac{\pi(j!)^r}{N}\right)\right)^{2n}.$$

This was not a very serious result, but soon Hardy found out that the analytical tools at his possession could be used for the proof of important arithmetical applications, and this resulted in a series of path-breaking papers, co-authored in a later period by J.E. Littlewood[35] and S. Ramanujan[36].

In America there was increased interest in number theory at the time when Sylvester was professor at Johns Hopkins University from 1877 until 1883. During that time he published several papers in the *American Journal of Mathematics*,

[29] Henry John Stephen Smith (1826–1883), professor in Oxford. See [5659].

[30] James Joseph Sylvester (1814–1897), professor in Baltimore and Oxford. See [4748].

[31] James Whitbread Lee Glaisher (1848–1928), Fellow of Trinity College, Cambridge. See [2042].

[32] Allan Joseph Champneys Cunningham (1842–1928), military engineer, Fellow of King's College, London. In his obituary [6638] A.E. Western wrote: "It is probably true that no single person has ever before calculated and printed so large an amount of numerical work in this subject."

[33] Norman Macleod Ferrers (1829–1903), Fellow of Gonville and Caius College, Cambridge.

[34] Godfrey Harold Hardy (1877–1947), professor in Oxford and Cambridge. See [6181, 6370, 6663].

[35] John Edensor Littlewood (1885–1977), professor in Cambridge. See [865].

[36] Srinivasa Aiyangar Ramanujan (1887–1920), Fellow of Trinity College, Cambridge. See [84, 2512, 2516, 3237]. Cf. also [456, 457].

which he founded and edited until 1884. Among them was a paper [6008] in which he improved Čebyšev's bounds for the number of primes in the interval $[2, x]$. He published also an important treatise on partitions [6009]. Browsing through early issues of Sylvester's journal one also finds other papers written by J.C. Fields[37] [1998], A.S. Hathaway [2613], O.H. Mitchell[38] [4339] and others, in which various elementary and algebraic aspects of number theory were treated. After the return of Sylvester to Britain that interest weakened.

The list of prominent mathematicians doing number theory in other countries at the end of the 19th century is rather short. One should mention N.V. Bugaev[39], A.A. Markov[40], G.F. Voronoĭ[41], A.N. Korkin[42] and E.I. Zolotarev[43] in Russia[44], L. Gegenbauer[45] and F. Mertens[46] in Austria, and E. Césaro[47] and A. Genocchi[48] in Italy.

There were very few books on number theory at that time. After Gauss's [2208] came two editions of A.M. Legendre's[49] [3767] book (in 1808 and 1830), and in 1863 there appeared the first edition of Dirichlet's lectures [1592], edited and provided with several appendices by Dedekind. These lectures covered divisibility properties, congruences, the quadratic reciprocity law and the theory of binary quadratic forms. In Dedekind's appendices one finds i.a. the proof of Dirichlet's theorem on the infinitude of primes in progressions, the theory of Pell's equation, composition of binary quadratic forms and the principal results of the theory of algebraic numbers. Surprisingly this book aged quite well and can be read even today.

[37] John Charles Fields (1863–1932), professor in Toronto. Initiator of the Fields Medal. See [6015].

[38] Oscar Howard Mitchell (1851–1889), teacher of mathematics in Marietta College, Springfield, student of C.S. Peirce, worked mainly in mathematical logic. He introduced the English term *power residue*, writing in a footnote in [4338]: "Power residues is a term not used, I believe, but a needed translation of 'Potenz-Reste'." See [1580].

[39] Nikolaĭ Vasilievič Bugaev (1837–1903), professor in Moscow. See [5667].

[40] Andreĭ Andreevič Markov (1856–1922), professor in St. Petersburg. See [2349].

[41] Georgiĭ Fedoseevič Voronoĭ (1868–1908), professor in Warsaw. His name is sometimes spelt "Voronoï". See [5940].

[42] Aleksandr Nikolaevič Korkin (Korkine) (1837–1908), professor in St. Petersburg. See [4998].

[43] Egor Ivanovič Zolotarev (1847–1878), professor in St. Petersburg. See [3594].

[44] For a very detailed survey of the development of number theory in Russia before 1918 see the book by E.P. Ožigova [4711].

[45] Leopold Gegenbauer (1849–1903), professor in Czernowitz, Innsbruck and Vienna. See [5960].

[46] Franz Carl Josef Mertens (1840–1927), professor in Cracow, Graz and Vienna. See [1533].

[47] Ernesto Césaro (1859–1906), professor in Palermo and Naples. See [42].

[48] Angelo Genocchi (1817–1889), professor in Turin.

[49] Adrien-Marie Legendre (1752–1833), worked in Paris.

The exposition [198] of number theory written by P. Bachmann[50] also played an important role. In five volumes, appearing between 1892 and 1905, he treated elementary, analytical and algebraic number theory. Bachmann wrote also a survey of Gauss's achievements in number theory [200].

An introduction to the theory of algebraic numbers formed a part of the monumental treatise on algebra, published in 1894–1908 by H. Weber[51] [6602].

The list of other books dealing with our subject is rather short: one has to mention two books by V.A. Lebesgue[52] [3754, 3755], a textbook by P.L. Čebyšev [969], and the book [4030] by É. Lucas[53], published in 1891. In the last book one finds a simple primality test, which works fine for numbers which are not too large.

The end of the century brought certain important events, which may even suggest the idea that for number theory the 20th century actually began a few years earlier.

In 1891 Minkowski published his first paper [4321] in a subject which later acquired the name *Geometry of Numbers*. He showed there that geometrical considerations essentially simplify the study of reduction and extremal values of quadratic forms.

Two years later two independent proofs were given of the Prime Number Theorem, a statement conjectured already by Legendre [3767] and Gauss, asserting that for the number $\pi(x)$ of primes in the interval $[2, x]$ the asymptotic formula

$$\pi(x) = (1 + o(1))\frac{x}{\log x} \tag{1.6}$$

holds. These proofs were discovered in 1896 by Hadamard [2426] and C. de la Vallée-Poussin[54] [6263]. They both utilized the non-vanishing of Riemann's zeta-function $\zeta(s)$ on the line $\Re s = 1$. Hadamard established the inequality $\zeta(1+it) \neq 0$ by a short argument based on the behavior of the series

$$S(\sigma + it) = \sum_p \frac{\cos(t \log p)}{p^\sigma}$$

to the right of the presumed zero of the zeta-function. He then deduced the Prime Number Theorem by considering the integral

$$\frac{1}{2\pi i}\int_{a-i\infty}^{a+i\infty} \frac{\zeta'(s)}{\zeta(s)}\frac{x^s}{s^2}\,ds \tag{1.7}$$

[50] Paul Gustav Heinrich Bachmann (1837–1920), student of Kummer, professor in Breslau and Münster. See [2749].

[51] Heinrich Weber (1842–1913), professor in Heidelberg, Zürich, Königsberg, Charlottenburg, Marburg, Göttingen and Strassburg. See [6477].

[52] Victor Amédée Lebesgue (1791–1875), professor in Bordeaux.

[53] François Édouard Anatole Lucas (1842–1891), teacher in Moulins and Paris. See [1419].

[54] Charles de la Vallée-Poussin (1866–1962), professor in Louvain.

for $a > 1$, and applying the formula

$$\sum_{n \le x} a_n \log(x/n) = \frac{1}{2\pi i} \int_{a-i\infty}^{a+i\infty} \left(\sum_{n=1}^{\infty} \frac{a_n}{n^s} \right) \frac{x^s}{s^2}\, ds, \tag{1.8}$$

for non-integral x. To be valid, it suffices to have the absolute convergence[55] of the series

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

on the line $\Re s = a$. This resulted in the formula

$$\sum_{p \le x} \log p \cdot \log(x/p) = (1 + o(1))x,$$

from which an easy elementary argument led to

$$\theta(x) := \sum_{p \le x} \log p = (1 + o(1))x. \tag{1.9}$$

The usual form of the Prime Number Theorem, given by (1.6), is obtainable from (1.9) by a simple argument.

De la Vallée-Poussin, who at that time was interested in a class of real functions which later became known as almost periodic functions, based his proof on the uniqueness of the Fourier expansion of functions from this class. His arguments[56] as well as the deduction of (1.9) from the non-vanishing of $\zeta(1 + it)$ were rather cumbersome. At the end of his paper he gave a very simple proof of the last fact, whose modification, due to Mertens [4259], found its way into most textbooks.

The third big event was the publication in 1897 of Hilbert's report on the theory of algebraic numbers, the famous *Zahlbericht* [2783]. In it Hilbert recapitulated and partially simplified the results of previous research. The presented topics included the theory of quadratic and Abelian fields, and Kummer extensions, i.e., extensions of the form $k(\sqrt[p]{a})/k$, where p is an odd prime, k is the field generated by pth roots of unity, and $a \in k$ is not a pth power. Hilbert's work had a great influence on subsequent researchers, although in later times some aspects of his approach underwent severe criticism (see the highly interesting introduction to the English translation of [2783] written by F. Lemmermeyer and N. Schappacher). An exposition of Hilbert's results was presented a few years later in the book [5846] by J. Sommer.

Shortly afterwards Hilbert published an important paper [2786] containing his theory of quadratic extensions of arbitrary algebraic number fields. In it the Hilbert norm-residue symbol was introduced, which led to the quadratic reciprocity law in number fields, and later played an important role in several problems of algebraic number theory. A generalization of these results to Abelian extensions led to the

[55] Later O. Perron [4784] showed that this formula can also be used under much weaker assumptions.

[56] For details of the proofs of de la Vallée-Poussin and Hadamard see, e.g., [4542].

notion of the class-field (H. Weber [6603–6605], D. Hilbert [2785]; for a modern description of Weber's ideas see G. Frei [2072]). This notion led later, due to the work of T. Takagi[57], E. Artin[58], N.G. Čebotarev[59], P. Furtwängler[60] and H. Hasse[61] to class-number theory, which dominated algebraic number theory in the first half of the coming century.

The *Dedekind zeta-function*

$$\zeta_K(s) = \sum_I \frac{1}{N(I)^s} \tag{1.10}$$

(where I runs over all non-zero ideals of the ring of integers of a fixed algebraic number field K) was studied in 1900 by Dedekind [1422] in the case when $K = \mathbf{Q}(\sqrt[3]{D})$ is a pure cubic extension of the rationals. He showed that in this case one can write

$$\zeta_K(s) = \zeta(s)H(s),$$

where $\zeta(s)$ is the Riemann zeta-function, and $H(s)$ is a certain well-behaved Dirichlet series. A similar result in the case of an arbitrary algebraic number field was later established by E. Landau [3624].

The main mathematical event of the last year of the 19th century was certainly the International Congress of Mathematicians held in Paris. On that occasion Hilbert [2788] gave his famous talk on open mathematical problems. Among the 23 problems presented by him, six (7–12) were devoted entirely to number theory, and the 18th problem also contained a question related to the geometry of numbers (Kepler's conjecture).

The seventh problem dealt with transcendence proofs. Hilbert stated here his belief that in general a transcendental entire function should assume transcendent values at algebraic arguments, although he knew of examples of such functions assuming rational values at all algebraic arguments. In particular he asked for a proof of transcendence of values of the exponential function $e^{i\pi x}$ at irrational algebraic arguments x, and posed the question of transcendence, or at least irrationality, of numbers of the form α^β with algebraic[62] α, and algebraic irrational β, like $2^{\sqrt{2}}$ and $e^\pi = i^{-2i}$. Both problems were solved in the nineteen thirties (see Sect. 4.3.1).

The eighth problem dealt with prime numbers and contained a long list of questions commencing with the celebrated *Riemann Hypothesis* (RH), also called the *conjecture of Riemann*.

[57] Teiji Takagi (1875–1960), professor in Tokyo. See [2852, 4345].

[58] Emil Artin (1898–1962), student of Herglotz, professor in Hamburg, Princeton and at Notre Dame University and Indiana University. See [1051].

[59] Nikolai Grigorievič Čebotarev (Tschebotareff) (1894–1947), professor in Kazan.

[60] Philipp Furtwängler (1869–1940), professor in Bonn, Aachen and Vienna. See [2846, 2942].

[61] Helmut Hasse (1898–1979), studied in Göttingen and Marburg and got his doctorate in 1920 under K. Hensel. Professor in Halle (1925–1930), Marburg (1930–1934), Göttingen (1934–1939), Berlin (1949–1950) and Hamburg (1950–1966). See [2071].

[62] He did not state the obvious necessary condition $\alpha \neq 0, 1$.

The Riemann Hypothesis *Prove that all non-real zeros of the Riemann zeta-function lie on the line* $\Re s = 1/2$.

The next question asked for the evaluation of the difference $R(x)$ between the number $\pi(x)$ of primes $p \leq x$ and the integral logarithm $\mathrm{li}(x)$, defined by

$$\mathrm{li}(x) = \lim_{\varepsilon \to 0} \left(\int_0^{1-\varepsilon} \frac{dt}{\log t} + \int_{1+\varepsilon}^{x} \frac{dt}{\log t} \right). \tag{1.11}$$

In particular Hilbert asked whether this difference is not of higher order than $\sqrt{x}$. This can be interpreted either as $R(x) \ll \sqrt{x}$ or as $R(x) = O(x^{1/2+\varepsilon})$ for every positive ε. It is now known that the second bound is equivalent to the Riemann Hypothesis (H. von Koch[63] [3433]), and the fate of the first is still undecided.

Next came two old questions: the first was the binary *Goldbach conjecture*, which goes back to an exchange of letters in June 1742 between Euler and Goldbach[64] (see P.H. Fuss[65] [1909; 2168, I, letter 43]), and states that every even integer ≥ 6 is the sum of two primes. The second dealt with *twin primes*, asking whether there are infinitely many primes p, p' with $p - p' = 2$. Next came a generalization of the last question.

Show that if $(a, b, c) = 1$*, then the equation*[66] $ax + by + c = 0$ *is solvable with prime* x, y.

The last problem of this sequence asked for a generalization of results on the distribution of prime numbers to the case of prime ideals in algebraic number fields.

In his ninth problem Hilbert asked for reciprocity laws of power residues modulo prime powers in arbitrary algebraic number fields. He expressed the belief that its solution would follow from a generalization of the theory of cyclotomic fields (i.e., fields of the form $\mathbf{Q}(\zeta)$, where ζ is a root of unity) and quadratic extensions of arbitrary algebraic number fields developed earlier by him in [2783, 2786]. This problem later found a solution as a consequence of class-field theory.

The tenth problem dealt with the question of existence of a finite algorithm for checking the solvability of Diophantine equations in rational integers. A negative solution was found in the second half of the next century (see Sect. 6.6).

In the eleventh problem Hilbert asked for a theory of quadratic forms having coefficients in an arbitrary algebraic number field. In particular he proposed finding a method of solving quadratic Diophantine equation in several variables. This problem was solved later by H. Hasse and C.L. Siegel[67].

[63] Niels Fabian Helge von Koch (1870–1924), professor in Stockholm.

[64] Christian Goldbach (1690–1764), lived in St. Petersburg, where he served as an official responsible for code breaking.

[65] Paul Heinrich Fuss (1796–1855), great-grandson of Euler, worked in St. Petersburg.

[66] Hilbert omitted the necessary assumption $2|a + b + c$.

[67] Carl Ludwig Siegel (1896–1981), professor in Frankfurt, Göttingen and Princeton. See [2835, 5543].

The twelfth problem was the last concerning number theory. Here Hilbert asked for a description of finite Abelian extensions of arbitrary algebraic number fields. In the case of the field of rational numbers such a description is provided by the *Kronecker–Weber theorem* stating that every such extension is contained in a cyclotomic field. It was stated by Kronecker [3524] and the first proof (by an incomplete argument[68]) was presented by Weber [6599, 6600]. The first correct proof appeared in Hilbert's paper [2782] and in his report [2783]. Hilbert asked for a similar result in the case of an arbitrary algebraic number base field, and expressed the belief that a proof of Kronecker's conjecture asserting that Abelian extensions of an imaginary quadratic field are generated by certain values of elliptic functions could be obtained on the basis of the theory of complex multiplication[69], developed by Weber [6601]. He pointed out that the key to the solution may lie in the construction of reciprocity laws governing power residues in algebraic number fields.

In the eighteenth problem, devoted to geometry, Hilbert mentions the question of the maximally dense arrangement of spheres and tetrahedrons in three-dimensional space.

For surveys of Hilbert's problems and the following development see [46, 744, 3250]. For the seventh problem see N.I. Feldman[70] [1982], and for the twelfth see R.-P. Holzapfel [2849] and N. Schappacher [5422].

A survey of the main achievements of the 19th century in number theory has been presented by H. Opolka and W. Scharlau [4686]. It is noteworthy that in the two volumes of the classical work of Klein [3354, 3355] devoted to the history of mathematics in the 19th century one finds only a few mentions of arithmetical results.

A list of all papers dealing with the theory of numbers in that period, except those related to various reciprocity laws, can be found in L.E. Dickson's[71] *History of the Theory of Numbers* [1545] and the *Report on Algebraic Numbers* [1569]. An early survey was published in 1859–1865 by H.J.S. Smith [5831].

[68] See O. Neumann [4579].

[69] For the history of complex multiplication see the book [6450] of S.G. Vlăduţ.

[70] Naum Il'ič Feldman (1918–1994), professor in Moscow. See [3489].

[71] Leonard Eugene Dickson (1874–1954), professor in Chicago. See [43].

Chapter 2
The First Years

2.1 Elementary Problems

2.1.1 Perfect Numbers

1. One of the oldest mathematical problems concerns *perfect numbers*. A positive integer N is called *perfect*, if it equals the sum of its proper divisors, i.e., the equality $\sigma(N) = 2N$ holds[1]. It had been noted already by Euclid that if the numbers $2^p - 1$ and p are both prime, then $2^{p-1}(2^p - 1)$ is perfect. After 2000 years Euler [1907] proved that every even perfect number is of this form. Therefore the problem of the existence of infinitely many even perfect numbers is equivalent to the question of whether there are infinitely many *Mersenne primes*, i.e., primes of the form $M_p = 2^p - 1$. The first four such primes, corresponding to $p = 2, 3, 5$ and 7, were known already to the ancient Greeks, and the next three, M_{13}, M_{17} and M_{19}, were found, according to L.E. Dickson [1545], in the 15th and 16th centuries. To this list M. Mersenne[2] (see [1545, pp. 12–13]) added M_{31} and M_{127}, and asserted incorrectly the primality of M_{67} and M_{257}.

A factorization of M_{67} was given by F.N. Cole[3] in 1903 [1174], and the fact that M_{257} is composite was established in 1932 by D.H. Lehmer[4] [3774].

Mersenne also stated that for every other prime $p \le 257$ the number M_p is composite. Mersenne did not indicate any proofs of his assertions, and the first proofs of the primality of M_{31} and M_{127} were obtained by Euler [1902] and É. Lucas [4025, 4028], respectively. Lucas formulated two primality tests of M_p (the first working only for $p \equiv 3 \bmod 4$) but it seems that he never published complete proofs of them.

[1] As pointed out by F. Acerbi [11], the equality $6 = 1 + 2 + 3$ can be found in Plato's *Theaetetus*, which may be the first occurrence of a perfect number.

[2] Marin Mersenne (1588–1648), French monk, friend of Descartes.

[3] Frank Nelson Cole (1861–1926), professor at Columbia University. See [2009].

[4] Derrick Henry Lehmer (1905–1991), son of D.N. Lehmer, student of J. Tamarkin, professor at Berkeley. See [729].

W. Narkiewicz, *Rational Number Theory in the 20th Century*,
Springer Monographs in Mathematics,
DOI 10.1007/978-0-85729-532-3_2, © Springer-Verlag London Limited 2012

They were provided much later by D.H. Lehmer [3773, 3779] and A.E. Western[5] [6639]. The second test, which later has been widely used, runs as follows.

Define a sequence S_n by putting $S_1 = 4$ and $S_{k+1} = S_k^2 - 2$ for $k \geq 1$. If $p \neq 2$ is prime, then M_p is prime if and only if S_{p-1} is divisible by M_p.

A simple proof was later provided by M.I. Rosen [5288], and an extremely simple proof of the sufficiency part was given by J.W. Bruce [763]. For a description of the extension of Lucas' ideas see the book [6673] by H.C. Williams.

The number M_{61} was asserted to be prime by I.P. Pervušin[6] (see [4711, p. 277]), J. Hudelot (see [4029]) and P. Seelhoff[7] [5597]. Seelhoff's argument was later shown to be incomplete by F.N. Cole [1174] (cf. D.H. Lehmer [3771]). The primality of M_{89} and M_{107} was proved by R.E. Powers [5003, 5004] in 1911 and 1914, respectively.

The results of the first use of computers in the study of Mersenne primes were presented by R.M. Robinson[8] [5243] in 1954. With the advent of computers the Lucas–Lehmer test led to the discovery of several new Mersenne primes, and a special program, called GIMPS (*Great Internet Mersenne Prime Search*[9]), was created to find them. At the moment of writing, 47 Mersenne primes are known, the largest being M_p with $p = 43\,112\,609$ comprising almost 13 million digits, found in August 2008. This is actually the largest known prime number. In fact, after 1951 every largest known prime has been a Mersenne prime, the last other record being $189 \cdot M_{127}^2 + 1$ found by J.C.P. Miller[10] and D.J. Wheeler [4309] in 1951.

The problem of the existence of infinitely many even perfect numbers can be stated in group-theoretical terms. It was shown in 1997 by M.P.F. du Sautoy [5417] that there are only finitely many such numbers if and only if the sum of the series

$$\sum_{n=1}^{\infty} \frac{a(2^n)}{2^{ns}}$$

is a rational function, $a(m)$ denoting the number subgroups of the product $\prod_p PSL_2(\mathbf{F}_p)$ having index m.

2. It is still unknown whether an odd perfect number exists and there is a strong belief that this is not the case. It seems that R. Descartes[11] was unique in his belief in its existence when he wrote to B. Frénicle de Bessy[12] on December, 20th 1638: "... je[13] juge qu'on peut trouver des nombres impairs véritablement parfaits."

[5] Alfred Edward Western (1873–1961), worked as a solicitor. See [4308].

[6] Ivan Mikheevich Pervušin (1827–1900), orthodox priest. He spent forty years preparing a table of all primes below 10^7.

[7] Paul Peter Heinrich Seelhoff (1829–1896), teacher in Mannheim.

[8] Raphael Mitchell Robinson (1911–1995), professor at Berkeley. See [2728].

[9] Homepage: http://www.mersenne.org.

[10] Jeffrey Charles Percy Miller (1906–1981), worked at Cambridge University.

[11] René Descartes (1596–1650).

[12] Bernard Frénicle de Bessy (1605–1675).

[13] "I believe that one can find truly perfect odd numbers."

Certain necessary conditions for odd N to be perfect had already been given by Euler, and in 1832 B. Peirce[14] [4764] showed that an odd perfect number has at least four distinct prime divisors. J.J. Sylvester [6012] stated later that it must have at least five such divisors. The first correct proof of this assertion was provided in 1913 by L.E. Dickson [1543].

It was later shown that an odd perfect number N must have at least 6 (I.S. Gradštein [2297], U. Kühnel [3566]), 7 (C. Pomerance [4966]), 8 (E.Z. Chein [1009], P. Hagis, Jr. [2435]) and 9 (P. Nielsen [4613]) distinct prime divisors. If N is not divisible by 3, then it must have at least eleven prime divisors (M. Kishore [3343], P. Hagis, Jr. [2436]), and one of them must exceed 10^8 (T. Goto, Y. Ohno [2286]). Previous lower bounds for the largest prime divisor were 60 (H.-J. Kanold [3239]), 11 200 and 10^5 (P. Hagis, Jr., W.L. McDaniel [2439, 2440]), 10^6 (P. Hagis, Jr., G.L. Cohen [2438]) and 10^7 (P.M. Jenkins [3120]). Moreover N has to exceed 10^{300} (R.P. Brent, G.L. Cohen, H.J.J. te Riele [711]), and must satisfy $\Omega(N) \geq 75$ (K.G. Hare [2547]). Previous lower bounds were 29 (M. Sayers [5418]), 37 (D.E. Iannucci, M. Sorli [2999]) and 47 (K.G. Hare [2546]). The maximal prime-power divisor of N must exceed 10^{30} (G.L. Cohen [1135]). Several congruences which odd perfect numbers must satisfy were found by J.A. Ewell [1945], L.H. Gallardo [2186] and L.H. Gallardo, O. Rahavandrainy [2187].

Let $A(x)$ be the number of odd perfect numbers $\leq x$. In a letter to Mersenne in 1638 Descartes observed that an odd perfect number must have the form pa^2 with prime p, and this leads, with the use of Čebyšev's bound $\pi(x) = O(x/\log x)$, to

$$A(x) = O\left(\frac{x}{\log x}\right).$$

In 1955 B. Hornfeck[15] [2906] established $A(x) = O(\sqrt{x})$, and this bound was later reduced to $A(x) = o(\sqrt{x})$ and $O(x^{1/4}\log x/\log\log x)$ (H.-J. Kanold [3240, 3242]), and

$$A(x) = O\left(\exp\left(c\frac{\log x \log\log\log x}{\log\log x}\right)\right)$$

with certain $c > 0$ (B. Hornfeck, E. Wirsing [2908]). In 1959 E. Wirsing [6692] eliminated the triple logarithm in the last formula.

L.E. Dickson proved in [1543] that there can be at most finitely many odd perfect numbers with a given number of prime divisors, and in fact he established the same assertion for odd numbers N which satisfy the inequality $\sigma(N) \geq 2N$ and for every proper factor $M > 1$ of N one has $\sigma(M) < 2M$ (cf. [1544]).

Dickson's proof utilized algebraic tools and a simple elementary proof was much later found by H.N. Shapiro [5676]. In 1977 an effective proof was provided by C. Pomerance [4967], leading to the exorbitant bound

$$\log\log N \ll 2^{k^2}\log k$$

for odd perfect N with k prime divisors, improved later by D.R. Heath-Brown [2651] to $\log N < 4^k \log 4$ and by P. Nielsen [4612] to $\log N < 4^k \log 2$.

[14] Benjamin Peirce (1809–1880), professor at Harvard. See [1146].

[15] Bernhard Hornfeck (1929–2006), professor in Clausthal-Zellerfeld.

3. A number N is called *multi-perfect* if it divides its sum of divisors but is not perfect i.e., $\sigma(N) = kN$ holds with an integer $k \geq 3$. Several such numbers had already been found in the 17th century by Descartes, P. Fermat[16] and A. Jumeau (see [1545]), the first few being 120, 672, 30 240, 32 760, 523 776, 23 569 920, 33 550 336 and 45 532 800. In 1901 D.N. Lehmer[17] [3801] noted that also 2 178 540 is multi-perfect, and R.D. Carmichael[18] [910] showed that this list exhausts all such numbers below 10^9. He also extended an earlier result of J. Westlund [6641] by proving that 120 and 672 are the only multi-perfect numbers having three prime divisors [908], and later [911, 912] listed all those with four and five prime divisors (in the last case restricting himself to even numbers).

Now more than 5000 multi-perfect numbers are known, all even, and this leads to the conjecture that there are no odd multi-perfect numbers. It was proved by E.A. Bugulov [825] in 1966 that such a number must have at least 11 distinct prime divisors. Later G.L. Cohen and M.D. Hendy [1138] showed that if $k = \sigma(n)/n \geq 3$ and n is odd, then n has at least $(k^5 + 387)/70$ prime divisors, hence $\omega(n) \geq 20$ holds for $k \geq 4$ (for $k = 3$, H. Reidlinger [5153] proved $\omega(n) \geq 12$ for odd n).

In 1985 G.L. Cohen and P. Hagis, Jr. [1137] proved that an odd multi-perfect number has to exceed 10^{70} and to have a prime factor $> 10^5$. Dickson's result in [1543], quoted above, has been extended by H.-J. Kanold [3240] to multi-perfect numbers with fixed ratio $\sigma(n)/n$, which are not multiples of an even perfect number, and an effective proof has been provided by C. Pomerance [4967].

2.1.2 Pseudoprimes and Carmichael Numbers

1. Fermat's theorem states that if p is a prime and $p \nmid a$, then the number $a^{p-1} - 1$ is divisible by p. In particular p divides $2^{p-1} - 1$. This necessary condition for primality is not sufficient as there exist composite numbers n satisfying the congruence

$$2^{n-1} \equiv 1 \pmod{n}.$$

Such composites are called *pseudoprimes*. It seems that the first pseudoprime appeared in a paper by F. Sarrus[19] [5408] in 1819, who observed that $341 = 11 \cdot 31$ divides $2^{170} - 1$. This answered a question posed anonymously in [5022] asking if one can test an integer n for primality by checking whether the congruence

$$2^n \equiv \pm 1 \pmod{2n + 1}$$

[16] Pierre Fermat (1601–1665), lawyer in Toulouse and Bordeaux. See [3035, 4096].

[17] Derrick Norman Lehmer (1867–1938), student of E. Moore, father of D.H. Lehmer, professor at Berkeley.

[18] Robert Daniel Carmichael (1879–1967), professor at the University of Illinois. He wrote two textbooks on number theory: [917, 918].

[19] Pierre Frédéric Sarrus (1798–1861), professor in Strasbourg.

holds. In view of the fact that $2^{170} - 1 | 2^{340} - 1$ this was also a counterexample to the converse of Fermat's theorem, but this fact had not been noted by Sarrus.

It is not difficult to see that there are infinitely many pseudoprimes and, more generally, it was shown in 1904 by M. Cipolla[20] [1114] that for every $a \geq 2$ there exist infinitely many composite n with $a^{n-1} \equiv 1 \pmod{n}$.

Denoting by $P(x)$ the number of pseudoprimes below x, P. Erdős[21] [1802] showed first

$$P(x) \leq x \exp\left(-\frac{1}{3}\sqrt[4]{\log x}\right),$$

and then [1815]

$$P(x) \leq x \exp\left(-c\sqrt{\log x \log\log x}\right)$$

with some $c > 0$. This was later improved to

$$P(x) \leq x \exp\left(-\frac{1}{2}\log x \frac{\log\log\log x}{\log\log x}\right)$$

for large x by C. Pomerance [4974], who also obtained in [4975] the lower bound

$$P(x) \gg \exp\left(\log^{5/14} x\right).$$

This was improved in 1994 to $P(x) \gg x^{\alpha}$ with $\alpha = 2/7$ by W.R. Alford, A. Granville and C. Pomerance [53], and consecutive improvements were obtained by R.C. Baker and G. Harman [266] ($\alpha = 0.2932 > 2/7$) and G. Harman ($\alpha = 0.3322$ [2564], $\alpha = 1/3$ [2566]).

All pseudoprimes below 10^{13} have been computed (R.G.E. Pinch [4878]). Earlier this had been done up to $2.5 \cdot 10^{10}$ (C. Pomerance, J.L. Selfridge, S.S. Wagstaff, Jr. [4981]).

It was proved by A. Rotkiewicz [5317–5319] in 1963 that every progression $aX + b$ with co-prime a, b contains infinitely many pseudoprimes. A bound for the distance between consecutive pseudoprimes in a progression was given by H. Halberstam and A. Rotkiewicz [2458] in 1968. It is also known that every primitive binary quadratic form in the principal genus having a fundamental discriminant[22] and not negative definite represents infinitely many pseudoprimes (A. Rotkiewicz, A. Schinzel [5321]).

A survey of the theory of pseudoprimes was given in 1972 by A. Rotkiewicz [5320].

2. It was observed in 1899 by A. Korselt[23] [3491] that there exist composite integers n, e.g., $n = 561 = 3 \cdot 11 \cdot 17$, satisfying $a^{n-1} \equiv 1 \pmod{n}$ for all a prime to n. He showed also that this happens if and only if $n = p_1 p_2 \cdots p_r$ is square-free and $n - 1$ is divisible by the least common multiple of the numbers $p_1 - 1, \ldots, p_r - 1$. Numbers having this property were later studied by R.D. Carmichael [914, 915] and are now called *Carmichael numbers*.

[20] Michele Cipolla (1880–1947), professor in Catania and Palermo. See [4290].

[21] Paul Erdős (1913–1996), student of L. Fejér, professor in Budapest, published more than 1200 papers. See [188, 189, 2446, 5351].

[22] An integer d is called a *fundamental discriminant* if it is either square-free and congruent to unity mod 4, or is of the form $d = 4D$, where D is square-free and congruent to 2 or 3 mod 4.

[23] Alwin Reinhold Korselt (1864–1947), schoolteacher, got his Ph.D. in 1902 in Leipzig.

Denote by $C(x)$ the number of Carmichael numbers less than x. The first upper bound for $C(x)$ was given by W. Knödel in 1953, who first got [3411]

$$C(x) \ll x \exp\bigl(-\log 2\sqrt{\log x}\bigr),$$

and then [3412]

$$C(x) \ll x \exp\bigl(-c\sqrt{\log x \log\log x}\bigr)$$

for every $c < 1/\sqrt{2}$. This was improved three years later by P. Erdős [1815] who proved

$$C(x) \le x \exp\left(-c\frac{\log x \log\log\log x}{\log\log x}\right)$$

with some $c > 0$ and conjectured $C(x) \gg x^{1-\varepsilon}$ for every $\varepsilon > 0$. Some arguments against Erdős's conjecture were given by A. Granville and C. Pomerance [2321].

Much later, in 1994, W.R. Alford, A. Granville and C. Pomerance [53] proved that there are infinitely many Carmichael numbers; more precisely, one has

$$C(x) \gg cx^{2/7}$$

with a certain $c > 0$. The exponent $2/7 = 0.2857\ldots$ was replaced four years later by $0.2932\ldots$ (R.C. Baker, G. Harman [266]), and later G. Harman increased it first to 0.3322 [2564] and then to $1/3$ [2566]. It was conjectured by C. Pomerance [4980] that for $k \ge 3$ there are $x^{1/k+o(1)}$ Carmichael numbers $\le x$ having exactly k prime factors. In 1980 C. Pomerance, J.L. Selfridge[24] and S.S. Wagstaff, Jr. [4981] gave in the case $k = 3$ the bound $O(x^{c+\varepsilon})$ with $c = 2/3$ and any $\varepsilon > 0$. This was later improved to $c = 1/2$ (I.B. Damgård, P. Landrock, C. Pomerance [1319]), to $c = 5/14$ (R. Balasubramanian, S.V. Nagaraj [280]), and to $c = 7/20$ (D.R. Heath-Brown [2660]).

2.1.3 Primality

1. Testing of the primality of Fermat numbers $F_n = 2^{2^n} + 1$ goes back to Fermat, who in several letters (listed in Dickson's *History* [1545, p. 375]) asserted that all numbers F_n are prime. This is true for $1 \le n \le 4$ but fails already for $n = 5$ in view of the factorization $F_5 = 641 \cdot 6\,700\,417$ found by Euler [1897]. In 1877 T. Pépin [4772] stated the following test.

The number F_n $(n \ge 1)$ is prime if and only if it divides $a^{(F_n-1)/2} + 1$, where a is a quadratic non-residue of F_n.

In the last quarter of the 19th century, using this test and other elementary tools, it was possible to show that F_n is composite for $n = 6, 11, 12, 23, 32$, and 36. In the new century this list has been quickly enhanced due to the efforts of A. Cunningham, J.C. Morehead and A.E. Western who showed that also for $n = 7, 8, 9, 38$ and 73 one gets composite F_n [1298, 4418, 4419, 4421].

[24] John Selfridge (1927–2010), professor at Northern Illinois University.

The factorization of Fermat numbers forms a difficult task which for F_7 was done successfully only in 1971 by M.A. Morrison and J. Brillhart [4436, 4437]. Now one knows factorizations of F_n for $n \leq 11$ (R.P. Brent [709, 710], R.P. Brent, J.M. Pollard [712], A.K. Lenstra, H.W. Lenstra, Jr., M.S. Manasse, J.M. Pollard [3820]).

There is a polynomial in seven variables, whose positive values at non-negative integers coincide with Fermat primes, but its practical importance is minimal. The same applies also to Mersenne primes. This was established in 1979 by J.P. Jones [3154].

Now over 200 composite Fermat numbers are known and the smallest Fermat numbers of unknown status are F_{33}, F_{34} and F_{35}. A wealth of information about Fermat numbers is contained in a recent book by M. Křižek, F. Luca and L. Somer [3523]. The actual status is given on the web page http://www.prothsearch.net/fermat.htm.

2. Various elementary methods of primality testing were developed by A. Cunningham and H.J. Woodall (see, e.g., [1299]), who were able to find several large primes, the largest lying in some neighborhood of 3^{15}. They initiated the *Cunningham Project*[25] [1301], consisting of factoring numbers of the form $a^n \pm 1$. D.N. Lehmer also dealt with factorizations, and published lists of the smallest factors of integers up to 10^7 [3803, 3804].

These simple methods could not be used to test very large numbers for primality. The first real progress in this matter was made by D.H. Lehmer [3771, 3772] who in 1927 modified the Lucas test so that it could be applied to numbers like $(10^{24}+1)/(10^8+1)$ of 16 decimal digits (cf. J. Brillhart [730]). Later D.H. Lehmer [3773] formulated a test which used Lucas sequences, and which, in particular, leads to the modern form of the test for Mersenne primes.

In 1983 a new primality test, based on Gauss and Jacobi sums, was found by L.M. Adleman, C. Pomerance and R.S. Rumely [21]. It needed

$$O(\exp(c \log\log n \log\log\log n))$$

steps to test an integer n. This test has been simplified by H. Cohen and H.W. Lenstra, Jr. [1143], who also provided an implementation [1144].

A test based on the theory of elliptic curves was invented in 1993 by A.O.L. Atkin[26] and F. Morain [165].

The question of the existence of a polynomial time algorithm for primality testing obtained a positive answer due to the work of M. Agrawal, N. Kayal and N. Saxena [24]. The new algorithm uses the elementary fact that an integer n is a prime if and only if for some a not divisible by n the polynomial

$$(X-a)^n - X^n + a$$

has all its coefficients divisible by n. The original algorithm was later modified by H.W. Lenstra, Jr. and C. Pomerance [3825], and this modification uses $O(\log^6 n)$ operations

[25] See S.S. Wagstaff, Jr. [6490] for the current standing of this project.

[26] Arthur Oliver Lonsdale Atkin (1925–2008), professor at the University of Illinois in Chicago. See [6101].