

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 $\sigma(N) = 2N$ holds¹. 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. Mersenne² (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. Cole³ in 1903 [1174], and the fact that M_{257} is composite was established in 1932 by D.H. Lehmer⁴ [3774].

Mersenne also stated that for every other prime $p \leq 257$ 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 $p \equiv 3 \pmod{4}$) but it seems that he never published complete proofs of them.

¹As 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.

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

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

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

They were provided much later by D.H. Lehmer [3773, 3779] and A.E. Western⁵ [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. Pervušin⁶ (see [4711, p. 277]), J. Hudelot (see [4029]) and P. Seelhoff⁷ [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. Robinson⁸ [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. Miller¹⁰ 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. Descartes¹¹ was unique in his belief in its existence when he wrote to B. Frénicle de Bessy¹² on December, 20th 1638: "... je¹³ juge qu'on peut trouver des nombres impairs véritablement parfaits."

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

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

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

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

⁹Homepage: <http://www.mersenne.org>.

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

¹¹René Descartes (1596–1650).

¹²Bernard 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. Peirce¹⁴ [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. Rahavandrany [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. Hornfeck¹⁵ [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 $\log N < 4^k \log 2$.

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

¹⁵Bernhard 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. Fermat¹⁶ and A. Jumeau (see [1545]), the first few being 120, 672, 30240, 32760, 523776, 23569920, 33550336 and 45532800. In 1901 D.N. Lehmer¹⁷ [3801] noted that also 2178540 is multi-perfect, and R.D. Carmichael¹⁸ [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. Sarrus¹⁹ [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

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

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

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

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

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

holds. In view of the fact that $2^{170} - 1 \nmid 2^{340} - 1$ 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. Cipolla²⁰ [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. Erdős²¹ [1802] showed first

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

and then [1815]

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

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

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

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 discriminant²² 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. Korselt²³ [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 $p_1 - 1, \dots, p_r - 1$. Numbers having this property were later studied by R.D. Carmichael [914, 915] and are now called *Carmichael numbers*.

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

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

²²An 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.

²³Alwin 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]

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

and then [3412]

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

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

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

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 $2/7 = 0.2857\dots$ was replaced four years later by $0.2932\dots$ (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 $k \geq 3$ there are $x^{1/k+o(1)}$ Carmichael numbers $\leq x$ having exactly k prime factors. In 1980 C. Pomerance, J.L. Selfridge²⁴ 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. Nagaraaj [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 $1 \leq n \leq 4$ but fails already for $n = 5$ in view of the factorization $F_5 = 641 \cdot 6700417$ found by Euler [1897]. In 1877 T. Pépin [4772] stated the following test.

The number F_n ($n \geq 1$) 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].

²⁴John 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. Křížek, 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. Atkin²⁶ 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

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

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

to test the primality of n . For expositions of this algorithm see A. Granville [2318] and F. Morain [4372].

3. The old method of Fermat based on the identity $a^2 - b^2 = (a - b)(a + b)$ remained for a long time the only non-trivial way to factorize large numbers. To find a factor of N one takes $m = \lfloor \sqrt{N} \rfloor$ and tries to find a square in the sequence $m^2 - N, (m+1)^2 - N, (m+2)^2 - N$, and if for some a one gets $(m+a)^2 - N = b^2$, then $N = (m+a-b)(m+a+b)$. This elementary method has been applied by A. Cunningham (see, e.g., [1294]), who also used various tricks to factorize several integers of specific form (for binomials $a^k + b$ see [1297]). In the *Jahrbuch* one finds a long list of papers by Cunningham and other authors in which large numbers were factorized at the beginning of the century.

Modern versions of Fermat's method were given by R.S. Lehman [3770] in 1974 and J. McKee [4234] in 1999.

A method based on the continued fraction expansion of \sqrt{N} , which works if the denominator of a complete quotient is a square, was used by D.N. Lehmer [3802, 3805].

Later this method was extended to the case when the product of two or more denominators of complete quotients is a square (D.H. Lehmer, R.E. Powers [3800]). It was further enhanced by M.A. Morrison and J. Brillhart in 1975 [4437], who applied it to a complete factorization of the seventh Fermat number.

A factorization algorithm, using $O(n^{1/4} \log^2 n)$ operations was proposed in 1974 by J.M. Pollard [4944], however its practical importance is minimal in view of the large implied constant. The following year he presented [4946] a more practical method (*Pollard's ρ method*) based on the iteration of a polynomial $f \bmod n$. If f_k denotes the k th iterate of f , then one looks at the greatest common divisor D of n and $f_r(a) - f_s(a)$ for $r \neq s$ and suitable a . If D happens to be distinct from n , then it is a proper divisor. A variant of this method was applied by R.P. Brent and J.M. Pollard [712] to factorize F_8 . J.M. Pollard also gave [4944] another algorithm (*Pollard's $p-1$ method*) in which one computes $\text{GCD}(n, 2^m - 1)$, where m runs over integers having many factors of the form $p-1$ with prime p .

At the beginning of the eighties C. Pomerance [4976, 4978] observed that the problem of finding a proper factor of N is equivalent to the question of finding a non-trivial square root of unity mod N , and that in certain cases the second task can be more feasible. This led to the *quadratic sieve factorization method*. Later development brought to life the *number field sieve*, in which elementary algebraic number theory is used to find a proper factor (see [3818]).

A test using elliptic curves (the *ECM algorithm*) was proposed in 1987 by H.W. Lenstra, Jr. [3822] (see Chap. 7 in the book [1277] by R. Crandall and C. Pomerance).

All these methods are heuristical, hence not quite rigorous, but in many cases lead to the desired result. There are also rigorous algorithms, but their practical value seems to be rather limited (see J.D. Dixon [1598], H.W. Lenstra, Jr., C. Pomerance [3824], C.-P. Schnorr [5545] and B. Vallée [6262]).

For surveys of primality tests and factorization methods see the books of H.C. Williams [6673] and R. Crandall, C. Pomerance [1277].

2.1.4 Other Questions

1. In 1907 R.D. Carmichael [909] asserted that there are no integers m such that the equation $\varphi(x) = m$ has only one solution, but later he recognized [920] that his proof was defective. It is still unknown whether his assertion, known as *Carmichael's conjecture*, is true.

Due to the much later work of V.L. Klee, Jr.²⁷ [3349] it is now known that any counterexample to Carmichael's conjecture must have many large prime divisors, and this has been used to infer that it should exceed $10^{10^{10}}$ (K. Ford [2028]). Previous bounds were 10^{10^4} (P. Masai, A. Valette [4165]) and 10^{10^7} (A. Schlaflly, S. Wagon [5456]). If Carmichael's conjecture is false, then the set of counterexamples has a positive lower density (K. Ford [2028]).

It was conjectured by W. Sierpiński²⁸ (see [5430]) that for every $m \geq 2$ there exists an integer k such that the equation $\varphi(x) = k$ has exactly m solutions, and A. Schinzel [5433] deduced this from a conjectured assertion about prime numbers (conjecture H , see Sect. 6.1.3). At the end of the century the conjecture of Sierpiński was settled for even m by K. Ford and S. Konyagin [2034], and K. Ford [2029] established it in the general case.

2. At the meeting²⁹ of the London Mathematical Society on 13 June 1901 A. Cunningham stated that there are no *idoneal numbers* between 1849 and 50000. These numbers were originally defined by Euler [1903–1905] as positive integers N with the property that any odd number which has a unique representation in the form $x^2 + Ny^2$ with $(x, Ny) = 1$ is necessarily either a prime or a square of a prime, or a double of a prime or, finally, a power of 2 (see [1545, p. 361]). This definition later obtained the following simpler form: a positive integer N is idoneal if any odd number which has a unique representation in the form $x^2 + Ny^2$, and in this representation the numbers x and Ny are co-prime, is necessarily a prime (see, e.g., the book [5784, 2nd ed., p. 229] by W. Sierpiński).

Euler gave a method of finding idoneal numbers (a precise version of it was presented by F. Grube [2369] in 1874), found 65 of them, the largest being 1848, and in [1905] checked that there are no others below 10000. It is an open question whether there are any larger ones. Later Gauss [2208, Sect. 303] interpreted idoneal numbers in the language of quadratic forms: it turned out that N is idoneal if and only if every genus of classes of positive definite quadratic forms of discriminant $-N$ contains only one class, hence the class-group is isomorphic to C_2^N for some N .

Much later it was proved by S. Chowla³⁰ [1074] that there are only finitely many idoneal numbers, and in 1954 Chowla and W.E. Briggs [1096] showed that under the *General Rie-*

²⁷Victor LaRue Klee (1925–2007), professor at the University of Washington. See [2348].

²⁸Wacław Sierpiński (1882–1969), student of Voronoï, professor in Lwów and Warsaw. See [5442].

²⁹See Proc. London Math. Soc., 34 (1902), p. 541.

³⁰Sarvadaman Chowla (1907–1995), student of J.E. Littlewood, professor in Benares, Waltair, Lahore, at the University of Kansas, University of Colorado in Boulder and Pennsylvania State University. See [185].

*mann Hypothesis*³¹ (GRH) Euler's list is complete, and in any case there can be only one idoneal number larger than 10^{60} . Earlier J.D. Swift [5999] showed that there are no new idoneal numbers below 10^7 . Cf. also E. Grosswald³² [2361].

The idoneal numbers are related to the Diophantine equation

$$n = xy + yz + zx,$$

with positive integers x, y, z , as pointed out by J. Borwein and K.K.S. Choi [649] (see also R. Crandall [1275] and M. Peters [4803]). The connection of this equation with class-groups of quadratic forms had already been noted in 1862 by J. Liouville [3935] (see also E.T. Bell³³ [396], L.J. Mordell³⁴ [4381] and W.G. Gage [2175]).

There is also a relation between idoneal numbers and sums of three squares (see E. Grosswald, A. and J. Calloway [2367], A. Schinzel [5432]).

2.2 Analytic Number Theory

2.2.1 Dirichlet Series

1. The first years of the 20th century were marked by a powerful entrance of methods of complex analysis into number theory. After the work of Dirichlet and Riemann it slowly became clear that the study of the analytical properties of suitable Dirichlet series may lead to essential progress in various arithmetical problems. The fundamental properties of the Riemann zeta-function, touched upon by Riemann in [5224], were developed further at the end of 19th century by H. von Mangoldt³⁵ [4125] and J. Hadamard [2424]. These results led to the proof of the Prime Number Theorem by J. Hadamard [2426] and C.J. de la Vallée-Poussin [6263, 6264] in 1896.

The corresponding studies of Dirichlet's L -functions were made by H. Kinkelin³⁶ [3338], A. Hurwitz [2955] and R. Lipschitz³⁷ [3937], and the first general treatment of functions defined by Dirichlet series

$$f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} \quad (2.1)$$

³¹This hypothesis, called sometimes the Great Riemann Hypothesis, states that the non-trivial zeros of a large class of functions, encompassing Dirichlet L -functions and Dedekind zeta-functions lie on the line $\Re s = 1/2$.

³²Emil Grosswald (1912–1989), professor at the University of Pennsylvania and Temple University. See [3419].

³³Eric Temple Bell (1883–1960), professor at the University of Washington and California Institute of Technology. See [5151].

³⁴Louis Joel Mordell (1888–1972), professor in Manchester and Cambridge. See [1375].

³⁵Hans von Mangoldt (1854–1925), professor in Hannover, Aachen and Danzig. See [3417].

³⁶Hermann Kinkelin (1832–1913), professor in Basel. See [5425].

³⁷Rudolf Lipschitz (1832–1903), professor in Breslau and Bonn. See [3493].

appeared in the thesis of E. Cahen [878]. It contained a wealth of results, but it was soon pointed out (e.g., in [6263] and [4784]) that some of Cahen's arguments are fallacious. Several years later E. Landau wrote in his book [3636, p. 724]: "...vierzehn³⁸ Jahre erforderlich waren, bis es möglich wurde bei jedem einzelnen der Cahenscher Resultate festzustellen, ob es richtig oder falsch ist."

2. Over the course of years several new kinds of functions defined by Dirichlet series were defined. So in his proof of the functional equation for Dirichlet's L -functions with real characters [2955] A. Hurwitz utilized the partial zeta-functions

$$\zeta_{k,l}(s) = \sum_{n \equiv l \pmod{k}} \frac{1}{n^s},$$

and proved that they are meromorphic, the only singularity being a simple pole with residue $1/k$ at $s = 1$. For rational $0 \leq u < 1$ (the case of arbitrary $u \in (0, 1)$ was treated later by H. Mellin³⁹ [4238]) he also considered the series

$$\zeta(s, u) = \sum_{n=0}^{\infty} \frac{1}{(n+u)^s}, \quad (2.2)$$

now called the *Hurwitz zeta-function*. The behavior of these functions for large $|s|$ was studied by G.N. Watson⁴⁰ [6589] in 1913.

A class of functions encompassing the Hurwitz zeta-functions was studied by C.J. Malmstén⁴¹ [4116], R. Lipschitz [3937] and M. Lerch⁴² [3834]. They are defined by

$$\mathfrak{K}_{u,x}(s) = \sum_{n=0}^{\infty} \frac{e^{2n\pi xi}}{(n+u)^s}, \quad (2.3)$$

and are usually called *Lerch zeta-functions*⁴³.

A modern exposition of the theory of these functions has been given recently by A. Laurinćikas and R. Garunkštis [3729].

³⁸"... it took fourteen years until it was possible to determine whether a particular Cahen's result is true or false."

³⁹Robert Hjalmar Mellin (1854–1933), professor in Helsinki. See [3894].

⁴⁰George Neville Watson (1886–1965), professor in Birmingham. See [5121].

⁴¹Carl Johan Malmstén (1814–1886), professor in Uppsala, later minister and governor of a province.

⁴²Matiaš Lerch (1860–1922), professor in Prague, Fribourg and Brno. See [1302, 4996].

⁴³Lerch himself called them *Lipschitz functions*.

In 1900 H. Mellin [4240] attached a class of zeta-functions (*Mellin zeta-functions*) to every non-constant polynomial $F(X)$ with non-negative coefficients, by putting

$$\zeta_F(s; a) = \sum_{n=1}^{\infty} \frac{1}{F(n+a)^s}$$

for positive a . This series converges in the half-plane $\Re s > 1/\deg F$. He showed also that if $P(x_1, \dots, x_n)$ is a complex polynomial whose coefficients have positive real parts, then the function

$$\sum_{k_1, \dots, k_n} \frac{1}{P(k_1, \dots, k_n)^s}$$

can be continued to a meromorphic function in the plane with all its poles on the real line (cf. E. Landau [3653], K. Mahler⁴⁴ [4060]).

These functions were later generalized (see T. Shintani⁴⁵ [5708], P. Cassou-Noguès [958]) and found important applications in the analytical theory of algebraic numbers.

3. In a huge paper [3619], published in 1903, E. Landau proved that the Dedekind zeta-function $\zeta_K(s)$ can be extended across the line $\Re s = 1$ to a regular function in the half-plane $\Re s > 1 - 1/n$ (n being the degree of the field K) with a simple pole at $s = 1$, and does not have zeros on that line as well as in a small region to the left of it. He noted also that in the case of quadratic or cyclotomic fields the zeta-function is meromorphic. Earlier only the existence of the limit

$$\lim_{s \rightarrow 1} (s-1)\zeta_K(s)$$

was known. Landau used these results to obtain lower and upper bounds for the number $\pi_K(x)$ of prime ideals in the ring of integers of the field K , both having the form $cx/\log x$ with certain $c > 0$, generalizing thus the classical result of Čebyšev [970] concerning $\pi(x)$. In the case of the Gaussian field $\mathbb{Q}(i)$ this result had been proved earlier by Poincaré [4935]

The next step was taken by E. Hecke⁴⁶ [2677], who in a series of papers published in 1917 and 1918 succeeded in continuing $\zeta_K(s)$ to a meromorphic function in the whole plane with a single pole at $s = 1$. Hecke proved also that $\zeta_K(s)$ obeys a functional equation similar to that of the Riemann zeta-function. Previously this was known only in the case of Abelian fields, when $\zeta_K(s)$ can be written as the product of suitable Dirichlet L -functions, and also for some other particular fields.

Hecke's proof was based on the theory of theta-functions and details were given only in the case of a real cubic field, having two imaginary conjugated fields.

⁴⁴Kurt Mahler (1903–1988), studied in Göttingen, lecturer in Manchester, professor in Canberra. See [947, 1129].

⁴⁵Takuro Shintani (1943–1980), professor in Tokyo. See [3007].

⁴⁶Erich Hecke (1887–1947), professor in Göttingen and Hamburg. See [4818, 5550].

A modern exposition of Hecke's method was presented in the book by J. Neukirch⁴⁷ [4576]. A proof based on ideas going back to Riemann was provided by C.L. Siegel in 1922 [5744, 5745], and another proof was furnished by Ch.H. Müntz⁴⁸ [4480] two years later. In 1950 K. Iwasawa (unpublished) and J. Tate [6057] found a proof based on integration in the group of ideles (see e.g., [3690, 4543]). This method was applied later to other kinds of zeta-functions (see e.g., G. Fujisaki [2135, 2136], S. Raghavan, S.S. Rangachari [5049], G. Shimura [5694], A. Weil⁴⁹ [6624]).

4. In his next paper [2678] E. Hecke proved the analytical continuation and functional equation for a class of Dirichlet series associated with characters of certain groups of ideal classes in algebraic number fields. Again theta-functions were used, but this time all details were given. At the end of his paper Hecke noted that analogous results can be proved⁵⁰ also for L -functions associated with partition of ideals in narrower classes, and his idea was later realized by E. Landau [3657]. This led to the generalization of Dirichlet's theorem on primes in progressions to arbitrary algebraic number fields. This generalization had been known to be true earlier in the case of the Gaussian field $\mathbf{Q}(i)$ (F. Mertens [4260], H. Weber [6606]). A broad exposition of Hecke's results in [2677] with numerous applications was given in Landau's book [3654] which appeared in 1918.

5. A new class of L -functions was brought to life by E. Hecke in [2679, 2680], who introduced a new family of ideal characters, called by him *Größencharaktere*, i.e., *characters of the magnitude*. Nowadays one defines these characters with the use of the idele group⁵¹ and calls them *Hecke characters*. With every Hecke character χ the function

$$L(s, \chi) = \sum_I \frac{\chi(I)}{N(I)^s}$$

was associated and E. Hecke showed that if $\chi \neq 1$, then this function can be extended to an entire function satisfying a functional equation.

Utilizing Kummer's ideal numbers Hecke used this result to study the distribution of ideal prime numbers in cones, which in the case of imaginary quadratic fields can be interpreted as the distribution of primes represented by a quadratic form $f(x, y)$ with the point (x, y) lying in an angle.

Hecke's result in the case of real quadratic fields was later improved by H. Rademacher⁵² [5033], who provided an error term for Hecke's formula (cf. [5034, 5035], where the distribution of primes of a real quadratic field in rectangles has been studied).

⁴⁷Jürgen Neukirch (1937–1997), professor in Regensburg.

⁴⁸Chaim Hermann Müntz (1884–1965), worked in Göttingen, Berlin and Leningrad. See [4700].

⁴⁹André Weil (1906–1998), professor in Chicago and Princeton. See the special issue of the *Notices AMS*, vol. 46/4, 1999.

⁵⁰He wrote: "Ich habe die Rechnung nicht durchgeführt." ["I did not perform the calculations."]

⁵¹See, e.g., [3690, 4543].

⁵²Hans Rademacher (1892–1969), professor in Breslau and at the University of Pennsylvania. See [89].

In the fifties Hecke's method was extended by J. Kubilius [3542, 3543, 3545] who proved in particular that there are infinitely many primes of the form $p = x^2 + y^2$ with $x \leq p^a$ for $a > 25/64 = 0.3906\dots$. Under the General Riemann Hypothesis this holds even with $x \leq C \log p$ with a suitable C (N.C. Ankeny⁵³ [100], J. Kubilius [3545]). Later this was shown to hold for $a > 1/3$ (K. Bulota [838]), $a > 1/4$ (F.B. Kovalčik [3501]), $a \geq 0.1631$ (M.D. Coleman [1178]) and $a \geq 0.119$ (G. Harman, P. Lewis [2568]).

6. A few years later the *Epstein zeta-functions* were introduced by P. Epstein⁵⁴ [1768, 1769]. They were associated with n -ary quadratic forms $Q(X_1, \dots, X_n)$ with complex coefficients whose values at real arguments lie in the half-plane $\Re s > 0$, and were defined by the formula

$$Z(s, Q) = \sum_{\substack{m_1, \dots, m_n = -\infty \\ (m_1, \dots, m_n) \neq (0, \dots, 0)}}^{\infty} \frac{1}{Q(m_1, \dots, m_n)^s}. \quad (2.4)$$

Epstein showed that in the case when the form Q is positive definite the function $Z(s, Q)$ can be continued to a meromorphic function in the plane having a single simple pole at $s = n/2$ and satisfying a functional equation (in the case of two variables a part of this assertion had been shown earlier by H. Mellin [4240]).

Later M. Deuring⁵⁵ [1498] gave fresh proofs in the case $n = 2$ and obtained for the zeros of $Z(s, Q)$ an asymptotical formula analogous to Mangoldt's formula (see (2.20)) concerning $\zeta(s)$ (cf. H.M. Stark [5898]). He found also [1502] a quickly convergent expansion of $Z(s, Q)$.

It turned out that the distribution of zeros of Epstein's zeta differs essentially from that of Riemann's zeta or Dirichlet's L -functions. Indeed, M. Deuring showed in [1498] that if the absolute value $D(Q)$ of the discriminant of $Q(X, Y)$ is sufficiently large, then $Z(s, Q)$ has a real zero between $1/2$ and 1 (cf. Chowla [1086], Chowla, A. Selberg⁵⁶ [1100, 5627], P.T. Bateman, E. Grosswald [356]), and one year later H. Davenport⁵⁷ and H. Heilbronn⁵⁸ [1386, 1387] proved the existence of zeros in the half-plane $\Re s > 1$. It was shown in 1935 by H.S.A. Potter and E.C. Titchmarsh⁵⁹ [5001] that $Z(s, Q)$ has infinitely many zeros on the line $\Re s = 1/2$.

The paper [1498] of M. Deuring contains the first example of the *Deuring–Heilbronn phenomenon* asserting that a real zero in $[1/2, 1)$ pushes away complex zeros ϱ with $1/2 < \Re \varrho < 1$. In the case of $Z(s, Q)$, M. Deuring showed that for large $D(Q)$ one must have $|\Im \varrho| > D^c$ for every such zero, with the exponent c being independent of the form Q .

⁵³Nesmith Cornett Ankeny (1927–1993), professor at MIT.

⁵⁴Paul Epstein (1871–1939), professor in Frankfurt.

⁵⁵Max Deuring (1907–1984), professor in Jena, Marburg, Hamburg and Göttingen. See [1704, 5277].

⁵⁶Atle Selberg (1917–2007), professor in Princeton, Fields Medal 1950. See [187].

⁵⁷Harold Davenport (1907–1969), professor in Bangor, London and Cambridge. See [4406, 4407, 5256].

⁵⁸Hans Arnold Heilbronn (1908–1975), student of Landau, professor in Bristol and Toronto. See [951].

⁵⁹Edward Charles Titchmarsh (1899–1963), professor in Liverpool and Oxford. See [924].

Zeta-functions for indefinite quadratic forms were treated by C.L. Siegel [5755] (over the rationals) and K. Ramanathan⁶⁰ [5071] (over algebraic number fields).

L -functions for quadratic forms were introduced in 1968 by H.M. Stark [5899, 5900, 5904–5906] in connection with the class-number problem for quadratic forms (see Sect. 6.5).

7. In 1899 H. Mellin [4238, 4240, 4241] introduced the *Mellin transform*, and applied it in the theory of differential equations [4239]. This transform became later, in hands of E. Hecke, a powerful tool in the theory of modular forms. It is defined by

$$g(s) = \int_0^\infty f(x)x^{s-1}dx, \quad (2.5)$$

and its inverse is given by

$$f(x) = \frac{1}{2\pi i} \int_{a-i\infty}^{a+i\infty} \frac{f(s)}{x^s} ds.$$

W.L. Ferrar⁶¹ [1993] in 1937 and N.S. Košliakov⁶² [3495] in 1941 used Mellin transform to prove various summation formulas.

An important step forward in the theory of Dirichlet series was made in 1908 by O. Perron⁶³ [4784], who put right several assertions of E. Cahen [878] and showed that if the function f is defined by the Dirichlet series (2.1) convergent for $\Re s > c$, then for positive $a > c$ and $x > 1$ one has the following formula (*Perron's formula*):

$$\sum_{n \leq x} a_n = \frac{1}{2\pi i} \int_{a-i\infty}^{a+i\infty} f(s) \frac{x^s}{s} ds.$$

(See also H. Mellin [4241] and W. Schnee [5534].)

An introduction to the theory of Dirichlet series was published in 1915 by G.H. Hardy and M. Riesz⁶⁴ [2543].

For a survey of early results in the theory of Dirichlet series see the article by H. Bohr⁶⁵ and H. Cramér⁶⁶ [580], published in 1923.

⁶⁰Kollagunta Gopalaiyer Ramanathan (1920–1992), professor at the Tata Institute. See [5048].

⁶¹William Leonard Ferrar (1893–1990), professor in Oxford. See [4580].

⁶²Nikolai Sergeevič Košliakov (1891–1958), professor in Leningrad.

⁶³Oskar Perron (1880–1975), professor in Tübingen, Heidelberg and Munich. See [2068, 2719].

⁶⁴Marcel Riesz (1886–1969), professor in Stockholm and Lund. See [2195, 2909, 2910].

⁶⁵Harald Bohr (1887–1951), professor in Copenhagen. He seems to be the only mathematician who won a medal at the Olympic Games. He did it in 1908, playing soccer for the Danish team. See [3127].

⁶⁶Carl Harald Cramér (1893–1935), student of Marcel Riesz, professor in Stockholm, worked in number theory and probability theory. See [2501].

2.2.2 Prime Number Distribution

1. Already Riemann had formulated a relation between zeros of the zeta-function $\zeta(s)$ and the distribution of primes. A simple-looking formula of this type (the *explicit formula for $\psi(x)$*) was proved by H. von Mangoldt [4125]. He considered the function

$$\psi(x) = \sum_{p^k \leq x} \log p$$

introduced in 1850 by Čebyšev [970] to be closely related to

$$\vartheta(x) = \sum_{p \leq x} \log p,$$

due to

$$\psi(x) = \vartheta(x) + \sum_{k=2}^{\lfloor \log x / \log 2 \rfloor} \sum_{p^k \leq x} \log p = \vartheta(x) + O(\sqrt{x} \log^2 x).$$

The function $\vartheta(x)$ is related to $\pi(x)$ by the inequalities

$$\vartheta(x) \leq \pi(x) \log x,$$

and

$$\begin{aligned} \vartheta(x) &\geq \sum_{x^{1-\varepsilon} \leq p \leq x} \log p \geq (1-\varepsilon)(\pi(x) - \pi(x^{1-\varepsilon})) \log x \\ &= (1-\varepsilon)\pi(x) + O(x^{1-\varepsilon}), \end{aligned}$$

valid for every positive ε . Therefore the Prime Number Theorem can be also stated in the form

$$\psi(x) = (1 + o(1))x$$

and

$$\vartheta(x) = (1 + o(1))x.$$

In 1895 H. von Mangoldt established the following relation between $\psi(x)$ and zeros of $\zeta(s)$.

If $x > 1$ is not a prime power, then

$$\psi(x) = x - \sum_{\varrho} \frac{x^{\varrho}}{\varrho} - \frac{1}{2} \log \left(1 - \frac{1}{x^2} \right) - \log(2\pi), \quad (2.6)$$

ϱ running over all non-real zeros of the zeta-function, arranged according to their absolute value.

A similar formula utilizing roots of $\zeta(s)$ from a bounded region was obtained in 1910 by H. von Koch [3435], who established

$$\psi(x) = x - \sum_{|\Im \varrho| < x^c} \frac{x^\varrho}{\varrho} \Gamma\left(1 - \frac{c\varrho \log x}{kx^c}\right) + O(x^{1-c} \log^2 x)$$

for any $0 < c < 1$ and arbitrary fixed $0 < k < \pi/2$. Two years later E. Landau [3646] deduced from (2.6) the equality

$$\psi(x) = x - \sum_{|\Im \varrho| \leq T} \frac{x^\varrho}{\varrho} + O\left(\frac{x}{T} \log^2 x + \frac{x \log T}{T} + \log x\right)$$

for $T \geq 3$.

Landau's result has been improved in 1982 by D.A. Goldston [2268, 2269] who replaced the error term by

$$O\left(\frac{x \log x \log \log x}{T} + \frac{x \log T}{T} + \log x\right),$$

and showed that under the Riemann Hypothesis the error term for large T does not exceed

$$\frac{x}{2T} + 2\sqrt{x} \log^2 T.$$

2. The first proofs of the Prime Number Theorem found by Hadamard and de la Vallée-Poussin did not lead to any evaluation of the error term. The first such evaluation appeared in a later paper of de la Vallée-Poussin [6264], who established

$$\pi(x) = \text{li}(x) + O(x \exp(-c \log^{1/2} x)), \quad (2.7)$$

with some positive c . He recognized the influence of the existence of a zero-free region of $\zeta(s)$ to the left of the line $\Re s = 1$ on the size of the error term, and based his proof of (2.7) on the observation that $\zeta(\sigma + it)$ does not vanish in the region

$$\sigma > \begin{cases} 1 - 0.0328214/\log(t - 3.806) & \text{if } |t| > 574, \\ 0.9872 & \text{if } |t| \leq 574. \end{cases}$$

To evaluate the error term in the Prime Number Theorem one usually does not deal directly with the Dirichlet series

$$P(s) = \sum_p \frac{1}{p^s},$$

whose sum of the first N coefficients coincides with $\pi(N)$, because $P(s)$ has a logarithmic singularity at $s = 1$. Therefore usually one considers the series

$$\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s} = -\frac{\zeta'(s)}{\zeta(s)}, \quad (2.8)$$

where $\Lambda(n)$ is the *von Mangoldt function*, defined by

$$\Lambda(n) = \begin{cases} \log p & \text{if } n \text{ is a power of a prime } p, \\ 0 & \text{otherwise.} \end{cases} \quad (2.9)$$

The series (2.8) converges absolutely in the half-plane $\Re s > 1$, and since the right-hand side can be extended over the line $\Re s = 1$ to a function having a simple pole at $s = 1$ it is easier to deal with it than with $P(s)$.

Because of the equality $\psi(x) = \sum_{n \leq x} \Lambda(n)$ the asymptotical behavior of $\psi(x)$ can be obtained by applying the formula (1.8) to (2.8), provided one is able to evaluate the integral occurring there. This can be done by shifting the integration path to the left, encompassing the point $s = 1$, where the integrand has a pole, but remaining in a region of non-vanishing of $\zeta(s)$. Since the residue of the integrand at $s = 1$ equals x , it remains to obtain a good bound for the part of the integral taken outside the line $\Re s = 1$.

A zero-free region for $\zeta(s)$ is usually obtained by using bounds for $\zeta'(s)/\zeta(s)$. These bounds are easily obtainable in the region to the right of the line $\Re s = 1$, as there $\zeta(s)$ and its derivative are represented by sums of absolutely convergent Dirichlet series. To obtain such bounds to the left of that line one uses the following formula, which is a consequence of Hadamard's theory of entire functions [2425]:

$$\frac{\zeta'(s)}{\zeta(s)} = \frac{1}{1-s} - \frac{1}{2} \frac{\Gamma'}{\Gamma} \left(1 + \frac{s}{2}\right) + \sum_{\varrho} \left(\frac{1}{s-\varrho} + \frac{1}{\varrho} \right) + C,$$

where ϱ runs over all non-real zeros of $\zeta(s)$, and C is a constant.

Later, when powerful methods of evaluation of exponential sums were invented, one could use the approximation of $\zeta(s)$ by the sums $\sum_{n \leq N} 1/n^s$, as it turned out that although the series $\sum_{n=1}^{\infty} 1/n^s$ diverges to the left of the line $\Re s = 1$, nevertheless its partial sums can be used to approximate $\zeta(s)$, due to the equality

$$\zeta(s) = \sum_{n \leq N} \frac{1}{n^s} + \frac{N^{1-s}}{s-1} + O(N^{-\Re s}), \quad (2.10)$$

valid for $\Re s \geq 1/2$, $1 \leq \Im s \leq N$. This reduces the problem of bounding $|\zeta(s)|$ to the evaluation of the exponential sum

$$\sum_{n \leq N} \exp(-s \log n).$$

An explicit form of the relation between zero-free regions and the error term in formula (2.7) was presented by A.E. Ingham⁶⁷ in 1932 in his book [3018]. The converse of Ingham's theorem was proved in an important particular case by P. Turán⁶⁸ [6219, 6223] and in the general case by J. Pintz [4894] (see also W. Staś [5911]). A similar result for the error term in the asymptotic formula for

$$\psi(x; k, l) = \sum_{\substack{n \leq x \\ n \equiv l \pmod{k}}} \Lambda(n)$$

gave K. Wiertelak [6664].

⁶⁷Albert Edward Ingham (1900–1967), worked in Leeds and Cambridge. See [864].

⁶⁸Paul Turán (1910–1976), professor in Budapest. See [1827, 2444].

3. C.J. de la Vallée-Poussin obtained in [6264] the evaluation

$$\psi(x) = x + O\left(x \exp(-c_1 \log^{1/2} x)\right), \quad (2.11)$$

(with a certain $c_1 > 0$), and then deduced (2.7) by a rather complicated argument. Later E. Landau [3617] observed that this can be obtained by elementary partial summation, utilizing the equality

$$\text{li}(x) = \sum_{n=2}^{\lfloor x \rfloor} \frac{1}{\log n} + O(1).$$

De la Vallée-Poussin used his approach also to obtain a quantitative form of Dirichlet's theorem on primes in progressions. He showed that if for co-prime k, l we denote by $\pi(x; k, l)$ the number of primes $p \leq x$ congruent to $l \pmod k$, then

$$\pi(x; k, l) = \left(\frac{1}{\varphi(k)} + o(1) \right) \text{li}(x). \quad (2.12)$$

4. The next step was taken by H. von Koch, who proved in 1901 [3433, 3434] that the equality

$$\pi(x) = \text{li}(x) + O(\sqrt{x} \log x) \quad (2.13)$$

is a consequence of the Riemann Hypothesis. On the other hand it was shown by E. Schmidt⁶⁹ [5474] that one cannot have

$$\pi(x) = \text{li}(x) + O\left(\frac{\sqrt{x}}{\log x}\right)$$

or

$$\psi(x) = x + o(\sqrt{x}).$$

A simpler proof of Schmidt's result can be found in J.E. Littlewood's paper [3944].

Much later P. Turán [6218] proved an effective result, showing that for large x one has

$$\max_{y \leq x} |\psi(y) - y| > \sqrt{x} \exp(-c \log x \log \log x / \log \log x)$$

with some explicit $c > 0$ (cf. W. Staś [5910]). These results were made more precise in 1980 by J. Pintz [4893, 4896] who showed that for a sequence x_n tending to infinity the difference $|\psi(x_n) - x_n|$ may be close to

$$\sup_{\rho} \left| \frac{x_n^{\Re \rho}}{\rho} \right|,$$

as suggested by formula (2.6). See also S.G. Révész [5169].

⁶⁹Erhard Schmidt (1876–1959), student of Hilbert, professor in Zürich, Erlangen, Breslau and Berlin. See [1579, 5264].

5. In 1903 E. Landau [3620] presented an important simplification of Hadamard's proof of the Prime Number Theorem eliminating the use of the theory of entire functions, and basing his arguments on simple analytical methods. His main tool was the inequality

$$\left| \frac{\zeta'(\sigma + it)}{\zeta(\sigma + it)} \right| \ll \log^c |t|,$$

with a certain c , valid in a region of the form

$$\sigma > 1 - \log^{-b} |t| \quad (|t| > \delta > 0)$$

which he used to evaluate the integral (1.7) in the case $a = 2$.

The error term obtained had the form $O(x \exp(-\log^{1/12} x))$, hence was worse than that given by (2.7), but later modifications [3630, 3634] permitted Landau to obtain the same order of the error term as in de la Vallée-Poussin's formula. He used the same approach [3623] to obtain an error term of the form $O(x \exp(-\log^c x))$ in (2.12), with $c > 0$ depending on k , and in [3631] he showed that c may be taken to be independent of k . A further simplification [3629] led to a proof which is now regarded as the standard proof of the Prime Number Theorem. In [3632] he obtained asymptotics for the number of zeros ϱ of L -functions, satisfying $0 < \Im \varrho < T$, and this led to the non-vanishing of these functions in the region

$$\left\{ s = \sigma + it : \sigma \geq 1 - \frac{1}{a \log t}, \quad t \geq 2 \right\},$$

for certain a , depending on k , and to the equality

$$\pi(x; k, l) = \frac{\text{li}(x)}{\varphi(k)} + O(x \exp(-b \log^{1/2} x)) \quad (2.14)$$

with positive b depending on k .

Landau's simplification [3620] of Hadamard's proof of the Prime Number Theorem enabled him to produce the first proof of the asymptotic equality (the *Prime Ideal Theorem*)

$$\pi_K(x) = \text{li}(x) + O(x \exp(-\log^{1/13} x)).$$

Later he was able to reduce the error term to $O(\exp(-c\sqrt{\log x}))$ [3654].

The best known evaluation of it, obtained in 1968 by T. Mitsui⁷⁰ [4344] and A.V. Sokolovskii [5844], is

$$O(\exp(-c \log^{3/5} x (\log \log x)^{-1/5})).$$

(See also J. Hinz [2816]).

The proof of the Prime Ideal Theorem came as a great surprise even for its author, who stated earlier in [3619] that a proof of the existence of the limit

$$\lim_{x \rightarrow \infty} \frac{\pi_K(x)}{x / \log x}$$

⁷⁰Takayoshi Mitsui (1929–1997), professor at Gakushuin University.

is not possible “at the contemporary state of the theory of ideals.” It turned out that no achievements in that theory were needed.

6. In 1905 E. Landau [3625] proved a very useful observation: if a Dirichlet series

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

with non-negative coefficients converges for $\Re s > a$ and diverges for $\Re s < a$, then $f(s)$ has a singularity at $s = a$. He utilized this result for a new proof of Čebyšev’s [972] assertion⁷¹ that the ratio

$$\frac{\pi(x; 4, 3) - \pi(x; 4, 1)}{\sqrt{x}/\log x}$$

can attain values arbitrarily close to unity. Čebyšev stated also that

$$\lim_{x \rightarrow +0} \sum_{p>2} (-1)^{(p-1)/2} e^{-px} = -\infty, \quad (2.15)$$

hence there are, in some sense, more primes congruent to 3 mod 4 than to 1 mod 4.

It was later proved by G.H. Hardy and J.E. Littlewood [2523] that (2.15) follows from the hypothetical non-vanishing of the series $L(s, \chi_4)$ (where χ_4 is the unique non-principal character mod 4) in the half-plane $\Re s > 1/2$. The same result was obtained independently by E. Landau [3655, 3656] who also established the converse implication.

7. J.E. Littlewood recalled in [3946] that his supervisor E.W. Barnes⁷² proposed, as a subject for his Ph.D. thesis, the proof of the Riemann Hypothesis. This turned his interests toward Riemann’s zeta-function and although no proof was found, nevertheless some results of primary rank emerged. One of them [2523, 3940] implied that the old conjecture based on numerical calculations for $x < 10^9$, stating that for all $x \geq 2$ the inequality $\pi(x) < \text{li}(x)$ holds, is incorrect. He obtained this by showing the existence of a positive constant c such that each of the inequalities

$$\pi(x) - \text{li}(x) < -c \frac{\log \log \log x}{\log x} x^{1/2}$$

and

$$\pi(x) - \text{li}(x) > c \frac{\log \log \log x}{\log x} x^{1/2}$$

occurs infinitely often, i.e.,

$$\pi(x) - \text{li}(x) = \Omega_{\pm} \left(\frac{\log \log \log x}{\log x} x^{1/2} \right),$$

⁷¹The first proof of this assertion was given by E. Phragmén [4840]. In his paper Landau lists several errors of earlier authors touching this subject.

⁷²Ernest William Barnes (1874–1953), Fellow of Trinity College in Cambridge, bishop of Birmingham (1924–1952). See [219].

hence the difference $\pi(x) - \text{li}(x)$ changes its sign infinitely often. Since this had already been deduced by E. Schmidt [5474] from the falsity of the Riemann Hypothesis, so Littlewood could assume its truth. Among his principal tools were the theorem of Phragmén-Lindelöf (proved in 1908 [4841]) and an old result of Kronecker from the theory of Diophantine approximations⁷³.

The use of the Phragmén-Lindelöf theorem in Littlewood's proof was later eliminated by A.E. Ingham [3020]. Much later, in 1975, H.G. Diamond [1523] also eliminated the use of the explicit formula for $\psi(x)$, used in previous proofs.

Littlewood's proof did not give any bound for the smallest integer N with $\pi(N) > \text{li}(N)$, and this question was pursued by S. Skewes⁷⁴ in 1933. In [5801] he showed that the Riemann Hypothesis implies $N < 10^{10^a}$ with $a = 10^{34}$, and in [5802], more than twenty years later, he got $N < \exp \exp \exp(7.703)$, if the Riemann Hypothesis is true, and $N < 10^{10^b}$ with $b = 10^{1000}$, if it is false. This was reduced in 1966 by R.S. Lehman [3768] to $N < 1.65 \cdot 10^{1165}$, by H.J.J. te Riele [6116] to $N < 6.69 \cdot 10^{370}$, by C. Bays and R.H. Hudson [368] to $N < 1.4 \cdot 10^{316}$, by K.F. Chao and R. Plymen [999] to $1.3984 \cdot 10^{316}$ and to $N < 1.3972 \cdot 10^{316}$ by Y. Saouter and P. Demichel [5394]. On the other hand the inequality $N > 10^{14}$ was established by T. Kotnik [3497].

Nevertheless the inequality $\pi(N) < \text{li}(N)$ is true on average, as the integral

$$\int_1^\infty (\pi(t) - \text{li}(t)) \exp(-\log^2 t/x) dt$$

is negative for all large x (Pintz [4903]).

Similar questions have also been posed for error terms in other asymptotical formulas. It seems that the first result of this type is due to E. Phragmén⁷⁵, who obtained in 1891 [4840] a sufficient condition for the infinitude of sign changes for a large class of functions, and applied this to the differences $\psi(x) - x$ and $\Pi(x) + \log 2 - \text{li}(x)$, where

$$\Pi(x) = \sum_{n \geq 1} \frac{\pi(x^{1/n})}{n} = \pi(x) + O(\sqrt{x}). \quad (2.16)$$

Littlewood's paper [3940] contains also the proof of

$$\psi(x) - x = \Omega_\pm(\sqrt{x} \log \log \log x).$$

Later E. Schmidt [5474] showed also that the difference $\Pi(x) - \text{li}(x)$ changes its sign infinitely often (cf. also E. Landau [3625]). See Sect. 4.1.2 for further development in the question of sign changes.

⁷³The importance of Kronecker's result in the theory of Dirichlet series had been demonstrated earlier by H. Bohr [576] who used it to show that $|\zeta(s)|$ attains arbitrarily small values in the half-plane $\Re s > 1$.

⁷⁴Stanley Skewes (1899–1988), professor in Capetown.

⁷⁵Lars Edvard Phragmén (1863–1937), professor in Stockholm (1892–1903), worked later in an insurance company. See [900].

8. In 1917 a new proof of the Prime Number Theorem was presented by G.H. Hardy and J.E. Littlewood [2523], who showed that it is an easy consequence of their Tauberian theorem, established earlier in [2522]. This theorem states, in its simplest form, that if λ_n is an increasing sequence tending to infinity and satisfying $\lambda_{n+1}/\lambda_n \rightarrow 1$, the series

$$f(y) = \sum_{n=1}^{\infty} a_n \exp(-\lambda_n y)$$

converges for positive y , the coefficients a_n satisfy

$$a_n > -c\lambda_n^{a-1}(\lambda_n - \lambda_{n-1})$$

with a certain positive c and $a \geq 0$, and

$$\lim_{y \rightarrow 0+0} f(y)y^{-a} = A,$$

then

$$\sum_{n \leq x} a_n = \left(\frac{A}{\Gamma(1+a)} + o(1) \right) \lambda_n^a.$$

There are various similar results available with arithmetical applications. The interested reader should consult the book [2517] by G.H. Hardy, published in 1949.

9. De la Vallée-Poussin considered in [6263] also the number $\pi(x; f)$ of primes $p \leq x$ represented by a primitive binary quadratic form⁷⁶ $f(X, Y) = aX^2 + bXY + cY^2$ of discriminant $D = b^2 - 4ac$. It had been known since Dirichlet (the *Dirichlet–Weber theorem* [1588, 6598]) that $\pi(x; f)$ tends to infinity with x , and C.J. de la Vallée-Poussin established the asymptotic equality

$$\pi(x; f) = \left(\frac{c(D)}{H(D)} + o(1) \right) \text{li}(x), \quad (2.17)$$

where $H(D)$ is the number of classes of forms of discriminant D , and $c(D)$ is equal either to 1 or to $1/2$, depending on algebraic properties of the class to which f belongs.

The first evaluation of the error term in this formula appeared in 1906 in a paper by E. Landau [3627], who showed that it is $O(x \exp(-\log^c x))$ for some unspecified $c > 0$, independent of the form in question. Later P. Bernays⁷⁷ in his thesis [443] used Landau's method to show that one can take $c = 1/8$. For positive definite forms this was later improved by E. Landau [3648] to $O(x \exp(-a\sqrt{\log x}))$, with a certain $a > 0$.

⁷⁶Actually he followed Gauss in considering only forms with even b , however there is no problem in applying his approach to the general case.

⁷⁷Paul Isaac Bernays (1888–1977), student of Landau, professor in Göttingen, Zürich and Princeton. His main work concerned logic and foundations of mathematics. See [4470].

It is now known that the error term in (2.17) is $O(x \exp(-c(\log x)^{3/5}(\log \log x)^{-1/5}))$. This follows from the bound for the error term in the asymptotical formula for the Prime Ideal Theorem for ideal classes in quadratic fields (see J. Hinz [2816]).

10. In 1911 a note by Gauss was discovered (see F. Klein [3353]) in which he stated that the number $\pi_k(x)$ of integers $n \leq x$ with $\omega(n) = k$ is asymptotically equal to

$$\frac{1}{(k-1)!} \frac{x(\log \log x)^{k-1}}{\log x}.$$

Although a proof of this assertion was at that time already known (occurring in Landau's book [3636]), nevertheless Landau, after hearing of this discovery, returned to the subject and proved in [3639] an asymptotic expansion of $\pi_k(x)$. Later a uniform upper bound for $\pi_k(x)$ was obtained by G.H. Hardy and S. Ramanujan [2540].

Asymptotics for $\pi_k(x)$ which is uniform for $k < c \log \log x$ (for all $c < e$) were obtained in 1953 by L.G. Sathe [5411–5414], and A. Selberg [5617] presented a simplification. The range for k was later extended by D. Hensley [2750], C. Pomerance [4977] and A. Hildebrand, G. Tenenbaum [2808].

11. An important conjecture concerning prime numbers was formulated in 1908 by L.E. Dickson, who wrote in [1537]:

“In order that m forms $a_i n + b_i$ shall give m prime numbers for at least one integer n , it is necessary for every prime $p \leq m$ and for every set of the a_i chosen from those not divisible by p , that at least two of the b_i/a_i shall be⁷⁸ congruent mod p . The sufficiency of these conditions is proposed as a problem worthy of an investigation . . .”

(Dickson omitted here the obviously necessary condition $(a_i, b_i) = 1$.) Nowadays one states this conjecture in a stronger form.

Dickson's conjecture *If*

$$f_i(X) = a_i X + b_i \in \mathbf{Z}[X] \quad (i = 1, 2, \dots, m; a_i > 0)$$

are given linear polynomials with the property that their product does not have a constant divisor > 1 , then for infinitely many positive integers n the values $f_1(n), \dots, f_m(n)$ are prime.

For $m = 1$ this is equivalent to Dirichlet's theorem on primes in progressions, but already in the case $m = 2$ its proof seems to be beyond reach. Indeed, the truth of this conjecture for the pair $X, X + 2$ would imply the infinitude of twin primes, which forms one of the greatest open problems in number theory.

⁷⁸The ratio here should be understood mod p .

Sieve methods provided a way to satisfy the assertion of Dickson's conjecture by almost primes, i.e., by numbers having a bounded number of prime factors. The first such results are presented in the book [2455] by H. Halberstam and H.-E. Richert⁷⁹, and subsequent improvements were made by D.R. Heath-Brown [2654] and K.-H. Ho, K.-M. Kwang [2838].

In 1973 D. Hensley and I. Richards [2755, 2756] showed that Dickson's conjecture contradicts the old conjecture asserting the inequality $\pi(x + y) \leq \pi(x) + \pi(y)$, but it is now commonly believed that this inequality may fail for some large x, y .

12. In 1909 E. Landau published his monumental treatise [3636]. In almost 1000 pages he presented a detailed survey of the actual knowledge of the distribution of prime numbers and included many of his own improvements. G.H. Hardy and H. Heilbronn wrote in [2518] about Landau's book:

"In it the analytic theory of numbers is presented for the first time, not as a collection of few beautiful scattered theorems, but as a systematic science. The book transformed the subject, hitherto the hunting ground of a few adventurous heroes, into one of the most fruitful fields of research . . ."

It was pointed out by T.H. Gronwall⁸⁰ in his long review of Landau's book [2351] that the exposition in it "is a model of clearness and rigor."

This was one of the first steps towards recognizing number theory as a serious research subject, as most mathematicians at the begin of the century regarded it as a kind of mathematical recreation. As late as in 1911 A. Châtelet⁸¹ wrote in his thesis: "Quoique les⁸² méthodes de la théorie des nombres paraissant encore bien vague et imprécises, on peut néanmoins signaler dans cette partie de la Science l'existence d'un petit nombre d'idées générales . . ." [1001, p. 105].

In August 1912 the International Congress of Mathematicians was held in Cambridge and E. Landau was invited to give a plenary talk. He chose to speak about solved and unsolved problems in the distribution of primes and the zeta-function [3641]. This fact can be regarded as the recognition of number theory as an important branch of mathematics (note that at the previous congresses in Heidelberg (1904) and Rome (1908) there were no plenary talks devoted to number theory). After sketching the main results concerning these topics, Landau stated four open problems. One of them was the Goldbach conjecture and the other three also dealt with primes.

(a) *Does the polynomial $X^2 + 1$ represent infinitely many primes at integral arguments?*

⁷⁹Hans-Egon Richert (1924–1993), professor in Marburg and Ulm.

⁸⁰Thomas Haakon Gronwall (Grönwall) (1877–1932), professor of physics at Columbia University. See [2251].

⁸¹Albert Châtelet (1883–1960), father of F. Châtelet, professor in Lille and Paris.

⁸²"... Although the methods of the theory of numbers appear rather vague and unprecise, one can point out the existence of a small number of general ideas in this part of science . . ."

This question is usually called *Landau's conjecture*, although it is a special case of a problem posed in 1857 by V. Bouniakowsky⁸³ [659], who conjectured that if $f(X)$ is an irreducible polynomial with integral coefficients and d is the maximal integer dividing all numbers $f(1), f(2), \dots$, then the polynomial $f(X)/d$ represents infinitely many primes at integral arguments.

Landau's conjecture (a) is equivalent to the following assertion.

For infinitely many primes one has

$$\{\sqrt{p}\} < \frac{1}{p^c} \quad (2.18)$$

with $c = 1/2$.

Now one knows that (2.18) holds for every $c < 0.262$, as shown by G. Harman and P. Lewis [2568]. Earlier I.M. Vinogradov⁸⁴ [6448] had this for $c < 0.1$, R.M. Kaufman [3284] proved this for $c < 0.1631\dots$, and A. Balog [297] and G. Harman [2553] got $c < 1/4$. Earlier N.C. Ankeny [100] and J. Kubilius [3545] deduced (2.18) for any $c < 1/2$ from the Riemann Hypothesis for Hecke L -functions, and R.M. Kaufman [3284] has shown that this follows already from the usual Riemann Hypothesis. There are similar results in the case when the primes p are restricted to an arithmetic progression (see A. Balog [298], D.I. Tolev [6187]).

The related question of bounding $\|\alpha p\|$ for irrational α for infinitely many prime p has been considered by I.M. Vinogradov [6436], who proved that the bound $p^{-\tau}$ with any $\tau < 1/5$ is possible, and this was later improved by R.C. Vaughan [6351] ($\tau < 1/4$), G. Harman [2554] ($\tau = 0.3$), C.H. Jia [3136, 3137] ($\tau = 4/13 = 0.3076\dots$), G. Harman ([2555]; $\tau = 7/22 = 0.3191\dots$), C.H. Jia ([3137]; $\tau = 9/28 = 0.3214\dots$), and D.R. Heath-Brown and C.H. Jia [2666] ($\tau < 16/49 = 0.3265\dots$). Recently K. Matomäki [4195] showed that one can take any $\tau < 1/3$ (earlier A. Balog [299] showed this to be a consequence of the General Riemann Hypothesis). On the other hand it was shown by G. Harman [2560] that there exist irrational numbers θ with

$$\|\theta p\| \geq \frac{0.002 \log p}{p \log \log p}$$

for all primes p .

The same question for simultaneous approximations was treated by A. Balog and J.B. Friedlander [302] and G. Harman [2558].

It was noted in 1972 by P. and S. Chowla [1066] that Landau's conjecture would follow if for every k there would exist prime numbers p such that the length of the period of the continued fraction of \sqrt{p} equals k , and in 1988 C. Friesen [2113] showed that there exist infinitely many square-free integers n with a given period length of \sqrt{n} (cf. F. Halter-Koch [2484]).

It should be pointed out that although no non-linear univariate polynomial is known to represent infinitely many primes, there exist polynomials representing many primes. The classical example is given by the polynomial $X^2 - X + 41$ which represents primes for $X = 0, 1, \dots, 40$. This was observed by Euler in 1772 and an explanation was given in 1913 by G. Rabinowitsch⁸⁵ [5023], who showed that

⁸³Victor Bouniakowsky (1804–1889), professor in St. Petersburg.

⁸⁴Ivan Matveevič Vinogradov (1891–1983), professor in Moscow. See [954].

⁸⁵Georg Rabinowitsch (Rainich) (1886–1968), professor at Johns Hopkins University and the University of Michigan.

the polynomial $X^2 - X + m$ represents primes for $X = 0, 1, \dots, m - 1$ if and only if the ring of integers of the quadratic field generated by $\sqrt{1 - 4m}$ has the unique factorization property.

Today we know that this holds only for $m = 2, 3, 5, 7, 11$ and 41 (theorem of Heegner–Stark, see Sect. 6.5). It was shown in 1992 by S. Louboutin, R.A. Mollin and H.C. Williams [4003] that Dickson’s conjecture implies that for every N there is a negative m such that the polynomial $X^2 - X + m$ represents primes for $X = 1, 2, \dots, N$.

It seems that the actual record for a polynomial representing the maximal number of distinct primes at consecutive integers is held by the polynomial

$$f(X) = 3X^5 + 7X^4 - 340X^3 - 122X^2 + 3876X + 997,$$

found in 2001 by F. Dress and B. Landreau (see [5181]), whose absolute value represents 49 distinct primes for $X \in [-24, 24]$. A heuristic approach was presented by F. Dress and M. Olivier [1624] in 1999.

On the other hand there are irreducible polynomials without a fixed divisor which do not attain prime values in long intervals (see K.S. McCurley [4227–4229]).

For a study of quadratic polynomials representing many primes see the book [4348] by R.A. Mollin.

(b) *Are there infinitely many primes p, p' satisfying $p - p' = 2$?*

Such prime pairs are called *twin primes*. It seems that this problem was first stated by A. de Polignac⁸⁶ [4940, 4941] in 1849. For bounds of the number of twin primes in an initial interval see the next section.

Several large twin primes have been found in the computer era, the largest having more than 100 000 digits⁸⁷.

(c) *Does every interval $[n^2, (n + 1)^2]$ contain a prime number?*

This conjecture was first stated in 1882 by L. Oppermann⁸⁸ [4697] and forms a part of the more general problem of the behavior of prime differences. See Sect. 3.1.3 for a survey of this question.

The contemporary status of Landau’s conjectures (b) and (c) has been described in a recent paper by J. Pintz [4908].

2.2.3 Riemann Zeta-Function and L-Functions

1. In his celebrated memoir [5224] Riemann asked whether all non-trivial⁸⁹ zeros of the zeta-function lie on the line $\Re s = 1/2$, usually called the *critical line*. The

⁸⁶Alphonse de Polignac (1817–1890).

⁸⁷For the largest twin primes see the Prime Page of C. Caldwell: <http://primes.utm.edu/top20>.

⁸⁸Ludvig Henrik Ferdinand Oppermann (1817–1883), professor in Copenhagen. See [2308].

⁸⁹The so-called trivial zeros are $s = -2, -4, -6, \dots$. They are poles of the function $\Gamma(s)$ and by the functional equation for Riemann’s zeta-function they are zeros of $\zeta(s)$.

first 15 such zeros were computed by J.P. Gram⁹⁰ [2309, 2310] and E. Lindelöf⁹¹ [3892]. Later R.J. Backlund⁹² [205] determined a further 64 zeros and it turned out that they all lie on the critical line. It is highly remarkable that the question of zeros of the zeta-function is so difficult in contrast to its non-zero values. It was shown in 1915 by H. Bohr [577] that for every complex $w \neq 0$ the equation $\zeta(z) = w$ has a solution in every strip $1/2 < \alpha < z < \beta < 1$ (this was established earlier under the Riemann Hypothesis by H. Bohr and E. Landau [585]). The density of the set of values of $\zeta(s)$ at every vertical line $\Re s = \theta$ for $\theta \in (1/2, 1]$ was evaluated by H. Bohr and R. Courant⁹³ [579] in 1914.

There are several assertions equivalent to the Riemann Hypothesis. One of the first results of this type was proved by J.E. Littlewood [3939] in 1912. He considered the Farey series⁹⁴ $0 < q_1 < \dots < q_M$ of order n , consisting of all rationals in $(0, 1)$ having denominators not exceeding n , and proved that the evaluation

$$\sum_{j=1}^M \cos(2\pi q_j) \ll n^{1/2+\varepsilon}$$

for every $\varepsilon > 0$ is equivalent to the Riemann Hypothesis.

An elementary statement equivalent to the Riemann Hypothesis, similar to Littlewood's criterion, was presented by J. Franel⁹⁵ [2067] in 1924, who showed that the Riemann Hypothesis is equivalent to the validity of the bound

$$\sum_{j=1}^M \left(q_j - \frac{j}{n} \right)^2 \leq \frac{B(\varepsilon)}{n^{1-\varepsilon}}$$

for every $\varepsilon > 0$ with a suitable $B(\varepsilon)$. For interesting early variants of Franel's result see the papers [3669, 3677] by E. Landau.

Much later several related equivalences involving Farey series were found by J. Kopřiva [3475, 3476], and a simpler proof given by A. Zulauf [6849] in 1977. Other relations between Farey series and the Riemann Hypothesis were studied by M. Mikolás, K.I. Sato, S. Kanemitsu and M. Yoshimoto [3233–3235, 4305–4307, 6790–6792].

⁹⁰Jorgen Pedersen Gram (1850–1916), worked in an insurance company.

⁹¹Ernst Leonard Lindelöf (1870–1946), professor in Helsinki. See [4499].

⁹²Ralf Josef Backlund (1888–1949), student of Lindelöf, worked in the insurance company Kaleva. One of the founders of the Actuarial Society of Finland.

⁹³Richard Courant (1888–1972), professor in Münster, Göttingen and at New York University. See [48, 5150].

⁹⁴The Farey series is named after John Farey (1766–1826), a geologist working in London, who in 1816 [1957] established certain simple properties of this series. It was pointed out by G.H. Hardy [2515] that actually Farey's results were anticipated by Haros [2569] in 1802 (his first name seems to be unknown, and the initial "C." appearing in Dickson's *History* stems from "citoyen" [= citizen], occurring in Haros's paper in the form "C^{en}"). See [115].

⁹⁵Jérôme Franel (1859–1939), professor in Zürich.

Another elementary condition equivalent to the Riemann Hypothesis was found in 1984 by G. Robin [5239], who showed that the Riemann Hypothesis is equivalent to the assertion that for every $n \geq 5041$ one has

$$\sigma(n) < e^\gamma n \log \log n, \quad (2.19)$$

where γ is Euler's constant. It was shown by Y.J. Choie, N. Lichiardopol, P. Moree and P. Solé [1058] that (2.19) holds for all square-free $n > 30$, and M. Wójtowicz [6710] established (2.19) for almost all n .

In 2002 J.C. Lagarias [3605] eliminated Euler's constant from this statement, showing that the Riemann Hypothesis is equivalent to the following assertion.

If we put $H_n = \sum_{j=1}^n 1/j$, then for all $n \geq 1$ one has

$$\sigma(n) \leq H_n + \exp(H_n) \log(H_n),$$

with equality occurring only for $n = 1$.

In 1922 H. Cramér [1268] showed the equivalence of the Riemann Hypothesis with the evaluation

$$\int_2^x \left(\frac{\psi(t) - t}{t} \right)^2 dt = O(\log x).$$

It was proved in 1948 by P. Turán [6217] that the Riemann Hypothesis would follow from the non-vanishing of partial sums $\sum_{n=1}^N n^{-s}$ of the series for $\zeta(s)$ in the half-plane $\Re s > 1$. However, it was shown by C.B. Haselgrove⁹⁶ [2574] that this assumption may fail, and R. Spira [5865, 5867] showed that this happens already for $N = 19$.

Another statement equivalent to the Riemann Hypothesis was formulated by B. Nyman [4646] and A. Beurling⁹⁷ [495] (cf. H. Bercovici, C. Foias [423], J.C. Carey [899]). It states that if we put $\varrho_a(t) = \{1/t\}$, then the Riemann Hypothesis will be equivalent to the density of the linear space spanned by the set $\{a\varrho_a(t) - \varrho_1(t) : a > 0\}$ in the L^2 space on the positive real half-line (the *Nyman–Beurling criterion*). For a refinement see L. Báez-Duarte [213].

The idea that zeros of $\zeta(s)$ may have an interpretation as eigenvalues of a linear operator in a suitable Hilbert space was used by A. Connes [1196, 1197] (see also P.B. Cohen [1150]) to prove the equivalence of the Riemann Hypothesis with the trace formula for a certain Hilbert space operator.

See J.B. Conrey [1203] for a survey.

In 1916 M. Riesz [5226] showed that the Riemann Hypothesis is equivalent to the bound

$$\left| \sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{\Gamma(k)\zeta(2k)} x^k \right| \ll x^{1/4+\varepsilon}$$

for every $\varepsilon > 0$ and large x .

Early unsuccessful attempts to prove the Riemann Hypothesis are described in Chap. 4 of [4542]. Later there were more such attempts, but without attaining the number of fruitless efforts to establish Fermat's Last Theorem.

⁹⁶Colin Brian Haselgrove (1926–1964), lecturer in Manchester.

⁹⁷Arne Karl August Beurling (1905–1986), professor in Uppsala and Princeton. See [26].

2. The fact that the strip $0 < \Re s < 1/2$ contains infinitely many zeros of the zeta-function follows from the formula for the number $N(T)$ of these zeros lying in the rectangle $0 < \Re s < 1/2$, $0 < \Im s < T$, conjectured by Riemann [5224] and established by H. von Mangoldt [4125] in 1895:

$$N(T) = \frac{1}{2\pi} T \log\left(\frac{T}{2\pi}\right) - \frac{T}{2\pi} + R(T), \quad (2.20)$$

with $R(T) = O(\log^2 T)$.

The error term in this formula was later reduced by von Mangoldt to $O(\log T)$ [4127], and a simpler proof was provided by R.J. Backlund [206, 208]. The same formula was obtained by H. Bohr, E. Landau and J.E. Littlewood [588] for the number of solutions of the equation $\zeta(s) = a$ in the strip $1 \leq \Im s \leq T$ for $a \neq 1$ (in the case $a = 1$ the term $\log(T/2\pi)$ must be replaced by $\log(T/4\pi)$). One conjectures that actually one has $R(T) = O(\log T / \log \log T)$, but it is only known that this is a consequence of the Riemann Hypothesis (J.E. Littlewood [3942], E.C. Titchmarsh [6165]). (Earlier H. Bohr [588] proved that the Riemann Hypothesis implies the bound $o(\log T)$.) On the other hand E. Landau [3637] proved that the Riemann Hypothesis implies the falsity of $R(T) = o(\log \log T)$, and later showed with H. Bohr [585] the existence of a positive c such that even $R(T) = o(\log^c T)$ is incompatible with the Riemann Hypothesis.

The integral

$$\int_0^T \frac{R(t)}{t} dt$$

was evaluated in 1924 by F. and R. Nevanlinna⁹⁸ [4581], who showed that it equals

$$\frac{7}{8} \log T + \kappa + O\left(\frac{\log T}{T}\right),$$

with a certain constant κ .

In 1946 A. Selberg [5610] obtained unconditionally

$$R(T) = \Omega_{\pm}\left(\frac{\log^{1/3} T}{(\log \log T)^{7/3}}\right).$$

The number of sign changes of $R(T)$ in $[0, T]$ was evaluated by A. Selberg [5609, 5610]. For a survey see A.A. Karatsuba, M.E. Korolev [3254].

The analogue of Mangoldt's formula (2.20) for zeros of Dirichlet's L -functions was proved by E. Landau [3632].

According to [580, p. 800] it was A. Piltz [4877] who first conjectured that all zeros of L -functions in the half-plane $\Re s > 0$ lie on the line $\Re s = 1/2$. In any case the first computations of small zeros of a sample of these functions performed by J. Großmann [2359] in 1913 showed that they seem to obey this law. This conjecture

⁹⁸Frithiof Nevanlinna (1894–1977) and Rolf Herman Nevanlinna (1895–1980), brothers, professors in Helsinki. See [2621].

of Piltz forms a part of the General Riemann Hypothesis. Of particular importance are the possible real zeros of L -functions.

It was checked by J.B. Rosser⁹⁹ [5300, 5301] in 1949 that L -functions associated with real characters modulo d do not have real zeros in the interval $(0, 1)$ for all $d \leq 227$. Rosser's result has been extended to $d \leq 593\,000$ (with one possible exception) by M. Low [4005], and to $d \leq 800\,000$ by G. Purdy [5017]. Low's approach to this question was much later used by M. Watkins [6576] to prove that for real odd (i.e., satisfying $\chi(-1) = -1$) Dirichlet characters $\chi \bmod k$ the corresponding L -function does not have zeros in $(1/2, 1)$ for $k \leq 3 \cdot 10^8$, and for even χ this has been shown for $k \leq 2 \cdot 10^5$ by K.S. Chua [1103]. At about the same time J.B. Conrey and K. Soundararajan [1220] established that for at least 20% of odd square-free integers k the L -function corresponding to the character

$$\chi(n) = \left(\frac{-8k}{n} \right)$$

does not have a real positive zero.

It was observed in 1912 by M. Fekete¹⁰⁰ (see [1970]) that if for a prime p and

$$\chi(n) = \left(\frac{n}{p} \right)$$

the polynomial

$$f_p(X) = \sum_{n=0}^{p-1} \chi(n) X^n$$

(*Fekete polynomial*) does not have zeros in $(0, 1)$, then the function $L(s, \chi)$ has no real positive zeros.

Although for most small primes $f_p(X)$ does not have zeros in $(0, 1)$, nevertheless it was shown much later by R.C. Baker and H.L. Montgomery [268] that for almost all primes p the interval $(0, 1)$ contains many zeros of $f_p(X)$, hence Fekete's criterion can be applied rather rarely. For a study of complex zeros of Fekete polynomials see J.B. Conrey, A. Granville, B. Poonen, K. Soundararajan [1217].

3. The question of the size of $|\zeta(s)|$ in the critical strip was considered by E. Lindelöf [3893] in 1908. He showed that the function $\mu(\sigma)$, defined as the greatest lower bound of numbers a for which one has

$$|\zeta(\sigma + it)| \ll t^a \tag{2.21}$$

for large t , is continuous and convex and conjectured (*Lindelöf's conjecture*) that one has

$$\mu(\sigma) = \begin{cases} 0 & \text{if } \sigma \geq 1/2 \\ 1/2 - \sigma & \text{if } \sigma < 1/2. \end{cases}$$

⁹⁹John Barkley Rosser (1907–1989), professor at Princeton, Harvard, Cornell and the University of Wisconsin. See [5361].

¹⁰⁰Michael Fekete (1886–1957), professor at the Hebrew University of Jerusalem. See [5262].

This is equivalent to the assertion

$$\zeta(1/2 + it) = O(t^\varepsilon)$$

for all $t > 0$ and $\varepsilon > 0$, as well as to the following two properties of the moments of $\zeta(s)$:

$$\int_1^T |\zeta(\sigma + it)|^{2k} dt = (T + o(T)) \sum_{n=1}^{\infty} \frac{d_k^2(n)}{n^{2\sigma}}, \quad \sigma > 1/2, \quad k = 1, 2, \dots, \quad (2.22)$$

where $d_k(n)$ is the number of decompositions of n into k factors, and

$$\int_1^T |\zeta(1/2 + it)|^{2k} dt \ll T^{1+\varepsilon}$$

for every $\varepsilon > 0$.

These equivalences were established by G.H. Hardy and J.E. Littlewood in [2533], where also other equivalent conditions are presented. Lindelöf's conjecture is also equivalent to the bound $o(\log T)$ for the number of zeros of the zeta-function in the region

$$\{\sigma + it : 1/2 + \delta \leq \sigma \leq 1, \quad T \leq t \leq T + 1\}$$

for every $\delta > 0$ (R.J. Backlund [207]), thus it is a consequence of the Riemann Hypothesis¹⁰¹ (cf. [3939]).

On the other hand Lindelöf's conjecture implies the still unproved *density conjecture*, which asserts that if $N(\alpha, T)$ denotes the number of zeros $\sigma + it$ of Riemann's zeta-function in the region $0 < t \leq T$, $\sigma \geq \alpha$, then the bound

$$N(\alpha, T) \ll T^{2(1-\alpha)(1+\varepsilon)} \quad (2.23)$$

holds for every $\varepsilon > 0$ and sufficiently large T , uniformly in $\alpha \in [1/2, 1]$. Let $\varrho(\alpha)$ be the largest lower bound of exponents ϱ such that one has $N(\alpha, T) \ll T^\varrho$. In 1914 H. Bohr and E. Landau proved for $\alpha > 1/2$ first that $\varrho(\alpha) \leq 1$ [586], and then $N(\alpha, T) = o(T)$ [587], showing thus that the majority of zeros of $\zeta(s)$ lie close to the line $\Re s = 1/2$. Six years later S. Wennberg [6636] established $N(\alpha, T) = O(T/\log^c T)$ with $c > 0$ depending on α , and in the same year F. Carlson¹⁰² [905] proved $\varrho(\alpha) \leq 4\alpha(1 - \alpha)$.

Later E.C. Titchmarsh [6168] established $\varrho(\alpha) \leq 4(1 - \alpha)/(3 - 2\alpha)$. In 1937 A.E. Ingham [3021] related $\varrho(\alpha)$ to $\mu(\alpha)$ by proving

$$\varrho(\alpha) \leq 2 + 4\mu(1/2),$$

which shows that (2.23) follows from the Lindelöf conjecture, and three years later he established that $\varrho(\alpha) \leq 3(1 - \alpha)/(2 - \alpha)$ [3023].

Note that G. Halász and P. Turán [2447] showed that for fixed $\Re s > 3/4$ the Lindelöf conjecture implies the stronger estimate

$$N(\sigma, T) \ll T^\varepsilon$$

for every $\varepsilon > 0$.

¹⁰¹The question of whether these two conjectures are equivalent is still open.

¹⁰²Fritz David Carlson (1888–1952), professor in Stockholm. See [2122].

The value of $\varrho(\alpha)$ was reduced to $\varrho(\alpha) \leq 2.5(1 - \alpha)$ by H.L. Montgomery [4355] in 1969, and to $\varrho(\alpha) \leq 2.4(1 - \alpha)$ by M.N. Huxley [2972] in 1972. This led to improvements in bounds for the difference of consecutive primes (see Sect. 3.1.3).

In a paper published in 1941 P. Turán [6215] deduced the density conjecture from a conjectured lower bound for sums of powers of complex numbers. Unfortunately this conjectured bound has recently been shown to be false by J. Andersson, who in his thesis [74, 75] provided a counterexample.

The book [6223] by P. Turán, published in 1953, presented his new method of studying sums of the form

$$1 + \sum_{j=1}^k z_j^t$$

with complex z_j and integral t , which led to several applications in number theory and function theory. It permitted to show that one can obtain a bound for the number of zeros of the zeta-function in a strip close to the line $\Re s = 1$ which does not differ much from that given by the density conjecture [6221]. The same approach gave certain necessary and sufficient conditions for the non-existence of roots of $\zeta(s)$ in some half-plane $\Re s > c$ with $c < 1$ (the *quasi-Riemannian hypothesis*) [6216]. The proof of the converse of Ingham's theorem concerning the relation between zero-free regions of $\zeta(s)$ and the error in the Prime Number Theorem was also achieved with this method [6219].

The density conjecture was shown to be true for σ close to 1 by P. Turán [6224], and this was made more precise in 1969 by H.L. Montgomery [4355] who established it for $\sigma \geq 0.9$. Later improvements were made by M.N. Huxley ($\sigma \geq 5/6 = 0.8333 \dots$ [2972], $\sigma \geq 189/230 = 0.8217 \dots$ [2976]), K. Ramachandra ($\sigma \geq 21/26 = 0.8076 \dots$ [5062]), M. Forti and C. Viola ($\sigma \geq 0.8059 \dots$ [2043]), M.N. Huxley ($\sigma \geq 0.8011 \dots$ and $\sigma \geq 0.8$ [2977, 2978]), M. Jutila ($\sigma \geq 43/54 = 0.7962 \dots$ and $\sigma \geq 11/14 = 0.7857 \dots$ [3170, 3171]), D.R. Heath-Brown ($\sigma \geq 15/19 = 0.7894 \dots$ [2627]) and J. Bourgain ($\sigma \geq 25/32 = 0.78125$ [661]).

It is now known that the equality (2.22) holds for all real $k > 0$ and $\sigma > \sigma_k$ with certain $\sigma_k < 1$. Early results are quoted in Landau's book [3636], and for later development see A.E. Ingham [3019], H. Bohr, B. Jessen¹⁰³ [581–583], H. Davenport [1345], R.T. Turpanaliev [6228] and the books of A. Ivić [3041, 3042].

4. In 1915 G.H. Hardy [2505] succeeded in obtaining a breakthrough in the search for zeros of Riemann's zeta-function. Earlier it had been known only that most of these zeros lie close to the critical line (Bohr, E. Landau [586, 587]) and Hardy showed that infinitely many zeros actually lie on that line. His main tool was a formula, due to H. Mellin [4242], expressing the theta-function

$$\Theta(y) = \sum_{n=-\infty}^{\infty} e^{-n^2 y} \quad (2.24)$$

by the zeta-function:

$$\Theta(y) = 1 + \sqrt{\pi/y} + \frac{1}{2\pi i} \int_{1/2-i\infty}^{1/2+i\infty} \Gamma(s/2) y^{-s/2} \zeta(s) ds,$$

valid for $\Re y > 0$.

¹⁰³Børge Jessen (1907–1993), professor in Copenhagen. See [431].

The theta-function, defined by (2.24), was considered first in 1823 by S.D. Poisson¹⁰⁴ [4937] and made its first application to number theory in hands of C.G.J. Jacobi [3075, 3077]. He used it to obtain formulas for the number of representations of a positive integer as the sum of 2, 3, 6 and 8 squares. Riemann [5224] utilized it in one of his proofs of the functional equation for $\zeta(s)$.

For modern expositions of the theory of theta-functions see the books of J. Fay [1963], J.-I. Igusa [3003] and D. Mumford [4477–4479].

Another proof of Hardy's theorem dealing with the existence of infinitely many zeros of $\zeta(s)$ on the critical line was given by H. Mellin in 1917 [4243].

E. Landau [3650] simplified Hardy's argument and proved that if $N_0(T)$ denotes the number of zeros $\varrho = 1/2 + it$ ($0 < t \leq T$) of the zeta-function lying on the critical line, then

$$N_0(T) \gg \log \log T. \quad (2.25)$$

Landau's method was modified in 1937 by E. Hecke [2699], who studied a class of Dirichlet series $f(s)$ extendable to the complex plane so that the product $(s - k)f(s)$ (with a certain $k > 0$) is entire, and which with certain $\lambda > 0$ and $\varepsilon = \pm 1$ satisfy the functional equation

$$R(k - s) = \varepsilon R(s),$$

where

$$R(s) = \left(\frac{2\pi}{\lambda} \right)^{-s} \Gamma(s) f(s).$$

He showed that $f(s)$ has infinitely many zeros on the line $\Re s = k/2$.

E. Landau also obtained the same assertion for Dirichlet L -functions. The role of the function Θ was played in this case by the series

$$\sum_{n=1}^{\infty} \chi(n) e^{-n^2 y},$$

χ being a Dirichlet character.

The inequality (2.25) has been consecutively improved to $N_0(T) \gg T^\alpha$, with $\alpha = 1/2$ (C.J. de la Vallée-Poussin [6265]), any $\alpha < 3/4$ (G.H. Hardy, J.E. Littlewood [2523]), and $\alpha = 1$ (G.H. Hardy, J.E. Littlewood [2527]).

A simple proof of the weaker bound

$$N_0(T) \gg \left(\frac{T}{\log T} \right)^{1/2}$$

was given in 1926 by M. Fekete [1969].

An explicit value for the constant c in the bound $N_0(T) \geq cT$ was found much later by C.L. Siegel [5749]. See Sect. 4.1.2, where also further results on $N_0(T)$ are quoted.

¹⁰⁴Siméon Denis Poisson (1781–1840), professor in Paris.

5. The first lower bound for the value at $s = 1$ of an L -function with a non-real character $\chi \bmod k$ was given by E. Landau [3640] who in 1911 showed

$$|L(1, \chi)| \gg \log^{-5} k.$$

This was improved two years later by T.H. Gronwall [2350] to

$$|L(1, \chi)| \gg \frac{1}{\log k (\log \log k)^{3/8}}.$$

and in 1926 by E. Landau [3673] to

$$|L(1, \chi)| \gg \frac{1}{\log k}.$$

Now for non-real characters modulo k bounds

$$|L(1, \chi)| \geq \frac{c}{\log k}$$

with explicit c are known. Such a result with $c = 1/58$ was obtained by T. Metsänkylä [4268] in 1970, and larger values of c were later given by S. Louboutin [3995] and P. Barrucand and S. Louboutin [338].

The elementary upper bound

$$|L(1, \chi)| \leq \log k + 2 \tag{2.26}$$

can be obtained by partial summation from the trivial bound

$$\left| \sum_{n \leq x} \chi(n) \right| < k.$$

For improvements see S. Louboutin [3994, 3996–4002], O. Ramaré [5091, 5092] and A. Granville and K. Soundararajan [2325, 2326]. The last authors obtained for non-real characters $\chi \bmod k$ the bound

$$|L(1, \chi)| \leq \lambda(34/35 + o(1)) \log k,$$

with

$$\lambda = \begin{cases} 1/4 & \text{if } k \text{ is 3-free,} \\ 1/3 & \text{otherwise.} \end{cases}$$

For corresponding bounds in the case of real characters see Sect. 4.1.2.

2.2.4 Character Sums

1. Sums involving a quadratic character $\chi \bmod p$, with prime $p \geq 3$, appear for the first time in the work of Gauss [2208, Sect. 356; 2209], who gave an explicit formula for the value of the sum

$$\tau_p(\chi) = \sum_{j=1}^{p-1} \chi(j) \zeta_p^j = \begin{cases} \sqrt{p} & \text{if } p \equiv 1 \pmod{4}, \\ i\sqrt{p} & \text{if } p \equiv 3 \pmod{4}. \end{cases} \tag{2.27}$$

There are several proofs known of this formula and a survey of them was given by B.C. Berndt and R. Evans [452]. See also the book [453] by B.C. Berndt, R. Evans and K.S. Williams.

Sums (2.27) with arbitrary characters χ , as well as the sums

$$\tau_N(\chi) = \sum_{j=1}^{N-1} \chi(j) \zeta_N^j$$

with arbitrary characters modulo N are now called *Gauss sums*. They appear in a natural way in many branches of number theory and for prime p they are related to sums of the form

$$G_k(p) = \sum_{n=0}^{p-1} \exp\left(\frac{2\pi i n^k}{p}\right).$$

(For quadratic characters χ one has $\tau_p(\chi) = G_2(p)$.)

For small k explicit formulas for $G_k(p)$ are known (see B.C. Berndt, R. Evans [451, 452] and the book [453]).

An old problem, proposed by E.E. Kummer in 1842 [3576, 3577], found its solution in 1979. Kummer considered for prime $p \equiv 1 \pmod{3}$ the cubic Gauss sums

$$\tau(p) = \sum_{n=1}^{p-1} \chi_p(n) \zeta_p^n,$$

χ_p being a cubic character mod p , and conjectured on the basis of calculations that the arguments of $\tau(p)$ are not uniformly distributed on the unit circle. This seemed not to be supported by numerical experiments performed by J. von Neumann¹⁰⁵ and H.H. Goldstine [4578] in 1953 and E. Lehmer [3806] three years later, and was finally disproved by D.R. Heath-Brown and S.J. Patterson [2671]. For an exposition of the proof see A.B. Venkov, A.B. Proskurin [6381]. It turned out later (S.J. Patterson [4759]) that Gaussian sums corresponding to characters of larger orders also have a similar behavior.

In the case of an odd prime power modulus p^k with $k \geq 2$ the Gaussian sums can be evaluated explicitly (R.W.K. Odoni [4658], J.-L. Mauclaire [4206, 4207]). Explicit formulas for cubic and quartic sums were given by C.R. Matthews [4199, 4200] in terms of Weierstrass \wp -functions and Jacobian elliptic functions, respectively, confirming earlier conjectures stated by J.W.S. Cassels [945], A.D. McGettrick [4231] and J.H. Loxton [4006, 4007].

A monograph on Gaussian sums has been written by B.C. Berndt, R. Evans and K.S. Williams [453].

2. The first non-trivial evaluation of the sum of character values in an interval was obtained for arbitrary primitive (i.e., not induced by a character belonging to a

¹⁰⁵John von Neumann (1903–1957), professor in Princeton. See [2249, 6251].

proper divisor of k) characters $\chi \bmod k$ by G. Pólya¹⁰⁶ [4957] and I.M. Vinogradov [6406] in 1918, who proved for

$$S(\chi) = \max_{x \geq 1} \left| \sum_{n \leq x} \chi(n) \right|,$$

the bound

$$S(\chi) \leq c\sqrt{k} \log k \quad (2.28)$$

with an absolute constant c . A simpler proof was provided by I. Schur¹⁰⁷ [5574]. Pólya's proof gave the value $1/\pi + o(1)$ for c , and this was replaced by $1/(\pi\sqrt{2})$ by E. Landau [3658], who also removed the assumption of primitivity.

For a generalization see E. Dobrowolski, K.S. Williams [1604].

In 1977 H.L. Montgomery and R.C. Vaughan [4366] deduced $S(\chi) \ll \sqrt{k} \log \log k$ from the General Riemann Hypothesis, and this bound cannot be improved, as it was shown by R.E.A.C. Paley¹⁰⁸ [4725] (cf. E. Landau [3678]) that there exists an infinite sequence $\chi_i \bmod k_i$ of quadratic characters satisfying

$$S(\chi_i) \geq \frac{1}{7} \sqrt{k_i} \log \log k_i.$$

In Paley's result the numbers k_i may be assumed to be prime, as shown by P.T. Bateman, S. Chowla and P. Erdős [354] in 1950.

The value of the constant c in (2.28) has been reduced several times, and the best known results are due to A. Hildebrand [2804] and A. Granville and K. Soundararajan [2326]. In the last paper the bound

$$S(\chi) \ll_k \sqrt{k} \log^{1-a(r)} k,$$

with $a(r) > 0$, r denoting the order of χ , was established.

A generalization of (2.28) to algebraic number fields was provided by J. Hinz [2817] (cf. P. Söhne [5842]).

3. Bounds for character sums turned out to be useful in the study of the distribution of primitive roots. The first result of this type was obtained in 1918 by I.M. Vinogradov [6406], who showed that $g(p)$, the least primitive root mod p , does not exceed

$$4^{\omega(p-1)} \sqrt{p} \log p,$$

$\omega(n)$ being the number of distinct primes dividing n .

A small modification in Vinogradov's argument allows replacement of the factor $4^{\omega(p-1)}$ in this inequality by $2^{\omega(p-1)}$, but it took 12 years before I.M. Vinogradov [6415] could improve his result to

$$g(p) \leq 2^{\omega(p-1)} \sqrt{p} \log \log p.$$

¹⁰⁶George Pólya (1887–1985), professor at ETH in Zürich, Brown University and Stanford. See [52].

¹⁰⁷Issai Schur (1875–1941), professor in Bonn and Berlin. See [3162].

¹⁰⁸Raymond Edward Allan Christopher Paley (1907–1933), worked in Cambridge and at MIT. See [6662].

The tables of $g(p)$ for $p < 25410$ prepared by A. Cunningham, H.J. Woodall and T.G. Creak [1300] indicated that this bound is much larger than it should be and after the next 12 years Vinogradov's bound was improved to

$$g(p) < 2^{1+\omega(p-1)} \sqrt{p}$$

by L.K. Hua¹⁰⁹ [2929]. In 1945 P. Erdős [1794] established for large p the bound

$$g(p) < \sqrt{p} \log^{17} p,$$

and in 1950 P. Erdős and H.N. Shapiro [1859] showed

$$g(p) \ll \omega(p-1)^c \sqrt{p}$$

with a certain constant c . The bounds for character sums obtained in 1962 by D.A. Burgess led to the evaluation

$$g(p) \ll p^{1/4+\varepsilon}$$

for every $\varepsilon > 0$ (D.A. Burgess [855], Y. Wang [6553]), which still holds the record. This bound seems to be rather far from optimal, as it was proved by E. Bach [190] in 1990 that the General Riemann Hypothesis implies

$$g(p) < 3 \log^2 p.$$

Explicit bounds were provided by E. Grosswald [2364], who showed that for $p > \exp \exp(24)$ one has $g(p) < p^{0.449}$.

In 1969 P.D.T.A. Elliott showed [1728] that infinitely often one has $g(p) < 475 \log^{8/5} p$, and this was superseded in 1984 by R. Gupta and M.R. Murty [2393] who obtained the bound $g(p) < 2250$ for infinitely many p . Two years later this bound was reduced to $g(p) \leq 7$ for infinitely many p by D.R. Heath-Brown [2640].

On the other hand it was shown by S.S. Pillai¹¹⁰ [4871] in 1944 that $g(p) \gg \log \log p$ holds infinitely often, and now it is known that infinitely often $g(p)$ can exceed $c \log p \log \log \log p$ for a certain $c > 0$ (S.W. Graham, C.J. Ringrose [2307]). It follows from the General Riemann Hypothesis that the bound $g(p) > c \log p \log \log p$ holds for infinitely many primes p (H.L. Montgomery, in [4357, Theorem 13.5]).

The mean value of $g(p)$ was considered by D.A. Burgess [861], who established

$$\sum_{p \leq x} g(p) \ll x \log^A x$$

with some unspecified A , and this was made more precise by him and P.D.T.A. Elliott [863] to

$$\sum_{p \leq x} g(p) \ll x \log x (\log \log x)^4.$$

In 1991 L. Murata [4482] showed that the General Riemann Hypothesis implies

$$\sum_{p \leq x} g(p) \ll x (\log \log x)^7,$$

¹⁰⁹Loo Keng Hua (1910–1985), professor in Beijing and at the University of Illinois. See [2451, 6558].

¹¹⁰S. Sivasankaranarayana Pillai (1901–1950), worked in Annamulai, Travancore and Calcutta. See [991].

and the exponent 7 has been replaced by any number > 4 by P.D.T.A. Elliott and L. Murata [1750]. For a numerical study see A. Paszkiewicz, A. Schinzel [4758].

Let $h(p)$ be the least primitive root mod p^2 . For small primes p one usually has $g(p) = h(p)$, and in fact one knows only two primes for which this equality fails: $p = 40487$ (E.L. Litver, G.E. Yudina [3949]) and $p = 6692367337$ (A. Paszkiewicz [4757]). For the mean value of $h(p)$ S.D. Cohen, R.W.K. Odoni¹¹¹ and W.W. Stothers [1153] obtained

$$\sum_{p \leq x} h(p) \leq x \log x (\log \log x)^4,$$

improving by the factor $\log^3 x (\log \log x)^2$ an earlier bound of D.A. Burgess [862]. They also proved $h(p) \ll p^c$ for every $c > 1/4$.

Denote by $g^*(p)$ the least prime primitive root mod p . In 1969 P.D.T.A. Elliott [1728] showed that for almost all primes p one has

$$g^*(p) \ll \exp(c \log \log p \log \log \log p)$$

for certain $c > 0$, and this was improved by A. Nongkynrih [4625] in 1995 and G. Martin [4160] two years later. Under the Riemann Hypothesis, L. Murata [4482] obtained $g^*(p) = O(p^\varepsilon)$ for all $\varepsilon > 0$ and almost all primes p .

4. G. Pólya used (2.28) to show that if $0 \leq \alpha < \beta < 1$ are given, then for large primes p the interval $[\alpha p, \beta p]$ contains approximately the same number of quadratic residues and non-residues.

Another application of the Pólya–Vinogradov inequality was given by I.M. Vinogradov [6407, 6409–6411], who evaluated $n_2(p)$, the smallest quadratic non-residue mod p . He showed that for large p one has

$$n_2(p) < p^c \log^2 p$$

with $c = e^{-1/2}/2 = 0.303\dots$, and also obtained a similar bound for the smallest k th non-residue mod p .

The exponent of the logarithm in the last inequality was reduced by H. Davenport and P. Erdős [1381]. Elementary methods allow $n_2(p) = O(p^{2/5})$ to be obtained, as shown by A. Brauer¹¹² [676].

It took 30 years to halve the exponent in Vinogradov's bound, which was done by D.A. Burgess [854] in 1957. One expects that actually the bound $n_2(p) = O(\log^2 p)$ is true, which is known to be a consequence of the General Riemann Hypothesis (N.C. Ankeny [99], K.A. Rodoskiĭ¹¹³ [5245]). On the other hand it was shown by S.W. Graham and C.J. Ringrose [2307] that the inequality

$$n_2(p) \geq c \log p \log \log \log p$$

(with a certain positive c) holds for infinitely many primes p . This is an improvement upon the earlier lower bound

$$n_2(p) \geq c \log p$$

¹¹¹Robert Winston Keith Odoni (1947–2002), professor in Exeter and Glasgow. See [1152].

¹¹²Alfred Brauer (1894–1985), elder brother of Richard Brauer. Student of Schur, worked at Berlin University until 1935. Professor at the University of North Carolina. See [5266].

¹¹³Kirill Andreeviĭ Rodoskiĭ (1913–2004), professor in Moscow. See [126].

for infinitely many p , obtained independently by V.R. Fridlender [2094], H. Salié [5380] and P. Turán [6220]. For most primes one has $n_2(p) \leq C(\varepsilon)p^\varepsilon$ for every $\varepsilon > 0$, as shown in 1942 by Yu.V. Linnik¹¹⁴ [3903], and the inequality $n_2(p) \leq 7$ for infinitely many p follows from the result of D.R. Heath-Brown quoted above.

I.M. Vinogradov considered in [6407] also the question of the size of $n'(p)$, the smallest prime quadratic residue mod p , and was able to show that for large p one has

$$n'(p) \leq p^{1/2} \exp(-\log p / \log \log p).$$

He conjectured also that for every $\varepsilon > 0$ one has $n'(p) = o(p^\varepsilon)$.

This conjecture is still open, but in 1967 P.D.T.A. Elliott [1727] showed it to be a consequence of the General Riemann Hypothesis. The best known unconditional result is due to Yu.V. Linnik and A.I. Vinogradov¹¹⁵ [3932], who in 1966 obtained $n'(p) = O(p^a)$ for every $a > 1/4$, using Burgess's method.

2.2.5 Möbius Function and Mertens Conjecture

1. The leading person promoting the use of analytical methods in number theory at the beginning of the century was E. Landau, who considered in his thesis [3615] the Möbius function $\mu(n)$ and presented a simple proof of the equality¹¹⁶

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n} = 0,$$

proved first by H. von Mangoldt [4126]. Later [3618] he established the bound

$$\sum_{n=1}^N \frac{\mu(n)}{n} = o\left(\frac{1}{\log N}\right).$$

Another property of the Möbius function, equivalent to the Prime Number Theorem, is given by

$$M(x) = \sum_{n \leq x} \mu(n) = o(x).$$

¹¹⁴Juri Vladimirovič Linnik (1915–1972), professor in Leningrad. See [3000, 4123].

¹¹⁵Askold Ivanovič Vinogradov (1929–2005), professor at the Steklov Institute.

¹¹⁶Later E. Landau [3638] proved that this equality is equivalent to the Prime Number Theorem, i.e., each of these results implies the other in a simple way.

It was asserted in 1885 by T.J. Stieltjes¹¹⁷ [5952] that with a certain constant B one has $|M(x)| \leq B\sqrt{x}$. Since this bound implies the convergence of the series

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

in the half-plane $\Re s > 1/2$, Stieltjes' assertion, if true, would imply the non-vanishing of $\zeta(s)$ in that half-plane and hence the truth of the Riemann Hypothesis.

2. The stronger inequality

$$|M(x)| \leq \sqrt{x}$$

is usually called the *Mertens conjecture*, since F. Mertens stated it in 1897 [4258] and checked it for $x < 10\,000$. Later R.D. von Sterneck¹¹⁸ [5935, 5936, 5938] pursued the checking up to 500 000 and noted that apart from some numbers in the vicinity of 200 one even has

$$|M(x)| \leq \frac{1}{2}\sqrt{x}. \quad (2.29)$$

In 1912 J.E. Littlewood [3939] showed that the evaluation

$$M(x) = \sum_{n \leq x} \mu(n) = O(x^{1/2+\varepsilon}) \quad (2.30)$$

is equivalent to the Riemann Hypothesis.

It was shown later that the Riemann Hypothesis allows replacement of the right-hand side of (2.30) by

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

(E. Landau [3670]) and by

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

(E.C. Titchmarsh [6165]). Recently H. Maier and H.L. Montgomery [4100] reduced this bound to

$$O(\sqrt{x} \exp(c \log^{39/61} x)),$$

K. Soundararajan [5857] obtained

$$O(\sqrt{x} \exp(c \log^{1/2} x (\log \log x)^{14})),$$

and M. Balazard and A. de Roton [288] showed that the exponent 14 can be replaced by any number exceeding $5/2$. It was conjectured by S.M. Gonek (see N. Ng [4590]) that, still under the Riemann Hypothesis, one has

$$M(x) = O(\sqrt{x} (\log \log \log x)^{5/4})$$

and this bound is best possible.

¹¹⁷Thomas Jan Stieltjes (1856–1894), professor in Toulouse. See [6335].

¹¹⁸Robert Daublebsky von Sterneck (1871–1928), professor in Czernowitz, Graz and Vienna.

The first proved result concerning the Mertens conjecture is due to A.E. Ingham who showed in 1942 [3024] that if the Riemann Hypothesis is true and there are only finitely many non-trivial vanishing linear relations between imaginary parts of complex zeros of the zeta-functions, then Mertens conjecture is false, as in that case one has

$$\liminf_{x \rightarrow \infty} \frac{M(x)}{\sqrt{x}} = -\infty,$$

and

$$\limsup_{x \rightarrow \infty} \frac{M(x)}{\sqrt{x}} = \infty.$$

He established also the same result for the related sum

$$L(x) = \sum_{n \leq x} \lambda(n),$$

where $\lambda(n) = (-1)^{\Omega(n)}$ is the *Liouville function*. This showed that the conjecture of G. Pólya, who in 1919 [4959] predicted the truth of the inequality

$$L(x) \leq 0$$

for all $x \geq 2$, contradicts the assumed properties of $\zeta(s)$. Pólya's conjecture was checked by H. Gupta¹¹⁹ [2387] up to 20000, but it was disproved in 1958 by C.B. Haselgrove [2574]. Pólya observed also that the equality $L(n) = 0$ is related to discriminants of binary quadratic forms with class-number one.

The oscillations of $M(x)$ were studied by S. Knapowski¹²⁰ [3379, 3380], who showed under the Riemann Hypothesis that $M(x)$ assumes both positive and negative values satisfying

$$|M(x)| > x^{1/2} \exp\left(\frac{-15 \log x \log \log \log x}{\log \log x}\right).$$

This was improved by I. Kátai [3268]. See also J. Pintz [4898].

The fact that Sterneck's inequality (2.29) does not persist indefinitely had been noticed in 1963 by G. Neubauer [4574] who showed that for a certain $x \leq 8 \cdot 10^9$ one has $M(x) > 0.53\sqrt{x}$, and W.B. Jurkat [3165] obtained

$$\liminf_{x \rightarrow \infty} \frac{M(x)}{\sqrt{x}} < -0.505.$$

In 1981 R.J. Anderson and H.M. Stark [73] established

$$\limsup_{x \rightarrow \infty} \frac{M(x)}{\sqrt{x}} > 0.557$$

(cf. J. Pintz [4897, 4899]), and a few years later Mertens conjecture was disproved by A.M. Odlyzko and H.J.J. te Riele [4657], who showed that infinitely often the ratio $M(x)/\sqrt{x}$ attains positive and negative values lying outside the interval $[-1, 1]$ (cf. H.J.J. te Riele [6115]). Two years later J. Pintz [4902] managed to show that this happens for some $x \leq \exp(3.21 \cdot 10^{64})$ and in 2006 T. Kotnik and H.J.J. te Riele [3498] replaced this bound by the still exorbitant $x \leq \exp(1.59 \cdot 10^{40})$.

¹¹⁹Hansraj Gupta (1902–1988), professor at Panjab University. See [1059, 1651].

¹²⁰Stanisław Knapowski (1931–1967), docent in Poznań and professor in Miami. See [6226].

3. The Möbius function plays a decisive role in the distribution of square-free integers, because the number $M_2(x)$ of square-free integers below x equals $\sum_{n \leq x} \mu^2(n)$.

In the 19th century it had already been shown (see, e.g., L. Gegenbauer [2218]) that one has

$$M_2(x) = \frac{6}{\pi^2}x + R(x)$$

with $R(x) = O(\sqrt{x})$. In 1905 E. Landau [3626] improved this to

$$R(x) = O(\sqrt{x}/\log \log x),$$

and the results of A. Axer¹²¹ [181] show that the Riemann Hypothesis implies $R(x) = O(x^\lambda)$ for every $\lambda > \lambda_0 = 2/5$.

More generally, if $M_k(x)$ denotes the number of k -free integers below x , then

$$M_k(x) = \frac{x}{\zeta(k)} + O(x^{1/k}) \quad (2.31)$$

as was known already to L. Gegenbauer [2219], and it was shown in 1929 by C.J.A. Evelyn and E.H. Linfoot [1914–1918, I] that the error term in (2.31) can be improved to

$$O(x^{1/k} \exp(-c\sqrt{\log x \log \log x}))$$

with certain $c > 0$. They proved also [1914–1918, IV] that for any $a < 1/2k$ the error term here is $\Omega(x^a)$.

Much later A. Walfisz¹²² [6535] reduced the error term in (2.31) to

$$O(x^{1/k} \exp(-a_k \log^{3/5} x (\log \log x)^{-1/5}))$$

with certain $a_k > 0$.

Assuming the Riemann Hypothesis, the number λ_0 in Axer's result has been consecutively reduced to $9/28 = 0.3214 \dots$ (H.L. Montgomery, R.C. Vaughan [4367]), $8/25 = 0.32$ (S.W. Graham [2302]), $7/22 = 0.3181 \dots$ (R.C. Baker, J. Pintz [269], S.W. Graham [2303], C.H. Jia [3130]) and $17/54 = 0.3148 \dots$ (C.H. Jia [3134]). For larger k the best known bounds under the Riemann Hypothesis were obtained by S.W. Graham and J. Pintz [2306]: for sufficiently large k one has $O(x^{d_k})$ with $d_k = 1/(k + bk^{1/3})$ with constant b .

On the other hand the error term in (2.31) is $\Omega_\pm(x^{1/2k})$ (H.M. Stark [5896]), hence in particular $R(x) = \Omega(x^{1/4})$. See also R. Balasubramanian, K. Ramachandra [283, 284], B. Saf-fari [5368].

Sign changes of $R(x)$ have been studied by R. Balasubramanian and K. Ramachandra [284] and A. Sankaranarayanan [5391].

2.2.6 Ramanujan

1. S. Ramanujan was a self-educated person with an extraordinary talent. After discovering several amazing identities involving integrals, continued fractions and

¹²¹Alexander Axer (1880–1948), teacher in Zürich.

¹²²Arnold Walfisz (1892–1962), worked first in an insurance company in Warsaw, becoming later professor in Tbilisi. Co-founder of *Acta Arithmetica*. See [3986].

arithmetical functions, he wrote in 1913 to G.H. Hardy asking him for advice. Ramanujan's formulas clearly impressed Hardy who invited the young man to Cambridge, initiating in this way a fruitful collaboration which ended abruptly when Ramanujan's health deteriorated and he died in 1920 shortly after returning to India.

2. In a letter, sent in February 1913 to G.H. Hardy (see [5088]) S. Ramanujan formulated certain formulas, which are particular cases of the identities

$$1 + \sum_{n=1}^{\infty} \frac{x^{n^2}}{\prod_{j=1}^n (1 - x^j)} = \prod_{n=0}^{\infty} \frac{1}{(1 - x^{5n+1})(1 - x^{5n+4})},$$

and

$$1 + \sum_{n=1}^{\infty} \frac{x^{n(n+1)}}{\prod_{j=1}^n (1 - x^j)} = \prod_{n=0}^{\infty} \frac{1}{(1 - x^{5n+2})(1 - x^{5n+3})}.$$

His proof appeared in [5082].

Actually these identities were found earlier by L.J. Rogers [5259, 5260] and therefore they are now called the *Rogers–Ramanujan identities*.

Later I. Schur [5573] noted that these identities conceal information on partitions. If we define the *difference of the partition* $n = a_1 + \dots + a_s$ as the minimum of $a_i - a_j$ for $i \neq j$, then the Rogers–Ramanujan identities show that the number of partitions of n with difference ≥ 2 is equal to the number of partitions of n into parts congruent to 1 or 4 mod 5, and the number of partitions of n with difference equal to 2 is equal to the number of partitions of n into parts congruent to 2 or 3 mod 5.

A combinatorial construction of the bijections leading to a proof of Schur's result was given by A.M. Garsia and S.C. Milne [2198, 2199] in 1981. Their method turned out to be applicable also to other similar problems. A survey was given in 1986 by P. Paule [4760]. For later results see, e.g., K. Alladi, B. Gordon [54], C. Boule, I. Pak [657], D. Stockhofe [5954], J.A. Sellers, A.V. Sills, G.L. Mullin [5631].

For other proofs of the Rogers–Ramanujan identities see, e.g., G.E. Andrews [83], G.E. Andrews, R.J. Baxter [85], D.M. Bressoud [714], D.M. Bressoud, D. Zeilberger [715], F.J. Dyson [1674], A. Selberg [5605].

In 1961 B. Gordon [2282] obtained an extension of the Rogers–Ramanujan identities extending Schur's interpretation to other moduli. Several other generalizations of these identities were obtained much later by H.L. Alder [44], G.E. Andrews (see [78, 79]), W.N. Bailey [218], W. Connor [1198], B. Gordon [2283] and L.J. Slater [5819, 5820]. A survey was presented in 1969 by H.L. Alder [45] (see also Chap. 7 in Andrews' book [80]). In 2006 a survey of bijections between various classes of partitions was given by I. Pak [4723].

A problem related to the Rogers–Ramanujan identities was proposed in 1979 by G.E. Andrews [81], who asked for the determination of all pairs of sequences $\{a_n\}, \{b_n\}$ of positive integers satisfying the equality

$$\prod_{i=1}^{\infty} (1 - x^{a_i})^{-1} = 1 + \sum_{n=1}^{\infty} \frac{x^{b_n}}{\prod_{j=1}^n (1 - x^j)}$$

(the *Ramanujan pairs*). Several such pairs were found later (see D. Acreman, J.H. Loxton [12], M.D. Hirschhorn [2824], R. Blecksmith, J. Brillhart, I. Gerst [553]).

3. The first important paper by S. Ramanujan appeared¹²³ in 1915 [5076]. He considered there the sequence of *highly composite numbers*, defined as positive integers having more divisors than all smaller integers, and established the lower bound

$$Q(x) \gg \frac{\log x (\log \log x)^{1/2}}{(\log \log \log x)^{3/2}}$$

for the number $Q(x)$ of such numbers $\leq x$.

Much later P. Erdős [1793] established

$$\log^a x \ll Q(x) \ll \exp(b(\log \log x)^2)$$

with certain $b > 0$ and $a > 1$. J.-L. Nicolas proved $1.136 \leq a \leq 1.71$ [4594, 4595] and presented a survey [4596] in 1988.

In 1943 S.S. Pillai [4870] introduced the analogue of highly composite numbers, called *highly abundant numbers*, replacing $d(n)$ by $\sigma(n)$ in their definition. This notion was studied in 1944 by L. Alaoglu¹²⁴ and P. Erdős [41]. A variant, in which $\sigma(n)$ is replaced by $\sigma(n)/n$ leads to *superabundant numbers* (see [41], P. Erdős, J.-L. Nicolas [1845], J.-L. Nicolas [4593]).

4. In Ramanujan's paper [5078], devoted to the study of the sum

$$\Sigma_{r,s}(n) = \sum_{j=0}^n \sigma_r(j) \sigma_s(n-j)$$

(with $\sigma_k(0) = -\zeta(-k)/2$), the function $\tau(n)$ appeared, which is defined by

$$\Delta(q) = q \prod_{n=1}^{\infty} (1 - q^n)^{24} = \sum_{n=1}^{\infty} \tau(n) q^n, \quad (2.32)$$

$\Delta(\exp(2\pi iz))$ being the classical discriminant function in the theory of elliptic functions. The function $\tau(n)$ is called the *Ramanujan function*, although it had been considered already by Jacobi, and the formula (2.32) is called *Jacobi's formula*. There are several proofs of (2.32), see, e.g., the books [3427, 5641, 5698]. The function $\tau(n)$ appears in [5078] in the formula for the number of representations of an integer as the sum of 24 squares. S. Ramanujan computed its values up to $n = 30$, and stated several conjectures. He asserted that $\tau(n)$ is multiplicative and for prime p and $n = 2, 3, \dots$ one has

$$\tau(p^n) = \tau(p) \tau(p^{n-1}) - p^{11} \tau(p^{n-2}),$$

thus

$$\Phi_{\tau}(s) = \sum_{n=1}^{\infty} \frac{\tau(n)}{n^s} = \prod_p \frac{1}{1 - \tau(p)p^{-s} + p^{11-2s}} \quad (2.33)$$

holds for sufficiently large $\Re s$.

¹²³For some reason only a part of Ramanujan's manuscript was printed, and the missing sections appeared in print as late as 1997 [5087].

¹²⁴Leonidas Alaoglu (1914–1981), worked at the Lockheed Corporation.

Both of these assertions were proved¹²⁵ by L.J. Mordell [4376] in 1917.

Moreover S. Ramanujan established the bound $\tau(n) = O(n^7)$, showed $\tau(n) = \Omega(n^5)$, stated the inequality

$$|\tau(p)| \leq 2p^{11/2} \quad (2.34)$$

for prime p and asserted that for infinitely many n the inequality

$$|\tau(n)| \geq n^{11/2} \quad (2.35)$$

holds.

In 1929 J.R. Wilton¹²⁶ [6681] established a functional equation for the function $\Phi_\tau(s)$ and showed that it has infinitely many zeros on the line $\Re s = 6$. The last result was later generalized by E. Hecke [2699] to Dirichlet series associated with a class of modular forms. Over 12 000 smallest zeros $\Phi_\tau(s)$ have been shown to be simple and to lie on the line $\Re s = 6$ by J.B. Keiper [3294].

In 1927 G.H. Hardy [2514] showed $\tau(n) = O(n^6)$ and this bound was reduced in the same year to $O(n^{47/8})$ by H.D. Kloosterman [3371]. In 1933 Kloosterman's bound was improved to $O(n^{35/6})$ by H. Davenport [1343] and H. Salié [5379], and in 1939 R.A. Rankin [5111] replaced it by $O(n^{29/5})$. The bounds for exponential sums established by A. Weil in [6617] imply $O(n^c)$ for every $c > 23/4$ (R.A. Rankin [5114]). In 1967 Y. Ihara [3006] (cf. Y. Morita [4431]) deduced (2.34) from Weil conjectures, concerning relations between modular forms and representations of the Galois group of $\overline{\mathbf{Q}}/\mathbf{Q}$, which were established in 1974 by P. Deligne [1447, 1448]. Deligne's result implied, more generally, the bound

$$|a_p| \leq 2p^{(k-1)/2}$$

for the coefficients of the Fourier expansion

$$f(q) = q + \sum_{n=1}^{\infty} a_n q^n \quad (q = e^{2\pi iz})$$

of any normalized primitive cusp form f of weight ≥ 2 and any level, and this led to

$$|a_n| \leq d(n)n^{(k-1)/2}.$$

For an exposition see J.-P. Serre [5649]. A table of values of $\tau(n)$ for prime $n < 300$ was prepared by D.H. Lehmer [3783] in 1943, H. Gupta [2390] gave values of $\tau(n)$ for $n < 400$, and G.N. Watson [6592] extended it up to 1000.

On the other hand G.H. Hardy [2514] established

$$x^{12} \ll \sum_{n \leq x} \tau^2(n) \ll x^{12}, \quad (2.36)$$

and this implies that for infinitely many n one has

$$\tau(n) \geq cn^{11/2} \quad (2.37)$$

with a certain $c > 0$ which is close to (2.35).

¹²⁵R. Fueter wrote in his review of Mordell's paper in the *Jahrbuch* that the multiplicativity of τ was also established by J.W.L. Glaisher. I was unable to confirm this.

¹²⁶John Raymond Wilton (1884–1944), professor in Adelaide. See [923].

In 1939 R.A. Rankin [5111] proved asymptotics for the sum in (2.36), and several years later improved the bound (2.37) by showing that the ratio $|\tau(n)|/n^{11/2}$ is unbounded [5123]. It was conjectured that

$$\tau(n) = \Omega\left(n^{11/2} \exp\left(\frac{c_1 \log n}{\log \log n}\right)\right) \quad (2.38)$$

holds with certain positive c_1 . H. Joris [3161] obtained in 1975

$$\tau(n) = \Omega\left(n^{11/2} \exp(c_2 \log^a n)\right)$$

for every $a < 1/22$, and ten years later R. Balasubramanian and M.R. Murty [278] showed this for every $a < 2/3$ (cf. M.R. Murty [4483]). Finally (2.38) was established in 1983 by M.R. Murty [4484], who also obtained its analogue for the coefficients of cusp forms of weight k , with the exponent $11/2$ being replaced by $(k-1)/2$.

In 1972 H. Joris [3160] established

$$A(x) = \sum_{n \leq x} \tau(n) = \Omega_{\pm}(x^{23/4} \log \log \log x),$$

and this was improved to

$$A(x) = \Omega_{\pm}(x^{23/4} \exp(c \log^{1/4} x \log \log \log^{-3/4} x))$$

by J.L. Hafner and A. Ivić [2433] in 1989 as a particular case of their bound for the sum of coefficients for a class of cusp forms.

It was conjectured by A.O.L. Atkin and J.-P. Serre (see [5650]) that for prime p one has

$$|\tau(p)| \gg p^{\alpha}$$

for every $\alpha < 9/2$, with the implied constant depending on α . In this direction M.R. Murty, V.K. Murty and T.N. Shorey showed in 1987 [4491] that if $\tau(n)$ is odd (which happens if and only if n is an odd square, as shown in 1943 by H. Gupta [2389]), then

$$|\tau(n)| \geq \log^c n,$$

holds with an absolute constant $c > 0$.

The Atkin–Serre conjecture implies the non-vanishing of $\tau(p)$. This was earlier conjectured by D.H. Lehmer [3783], who showed in 1947 [3785] that $\tau(n)$ is non-zero for $n \leq 3\,316\,798$ and later extended this to $n \leq 21\,492\,639\,999$ (unpublished, see Lehmer's review of [2391] in Math. Reviews, 10, p. 514). Much later this was extended to $n \leq 10^{15}$ (see J.-P. Serre [5654]) and $n \leq 2 \cdot 10^{19}$ (J. Bosman [655]).

It is also not known whether there exist infinitely many primes p with $p|\tau(p)$. Only six such primes are known: 2, 3, 5, 7, 2411 and 7758337633, the last found in 2010 by N. Lygeros and O. Rozier [4036].

Hardy's conjecture [2516]

$$\sum_{p \leq x} \tau(p) \log p = O(x^{13/2})$$

was established by R.A. Rankin [5110–5112] in 1939 in the stronger form

$$\sum_{p \leq x} \tau(p) \log p = o(x^{13/2}),$$

and in 1972 C.J. Moreno [4423] improved this to

$$\sum_{p \leq x} \tau(p) \log p = O(x^{13/2} \exp(-A\sqrt{\log x}))$$

for some $A > 0$.

It is not known whether $\tau(n)$ assumes infinitely many prime values. The smallest n with prime $\tau(n)$ is $n = 63\,001$, as shown by D.H. Lehmer [3790] in 1965.

It was conjectured by J.-P. Serre in [5639] that if one writes

$$\tau(p) = 2p^{11/2} \cos(\theta_p)$$

with $0 \leq \theta_p \leq \pi$, then the sequence $\{\theta_p\}$ is uniformly distributed with respect to the measure

$$\frac{2}{\pi} \sin^2 t \, dt.$$

This conjecture, which resembles the *Sato–Tate conjecture* for elliptic curves, formulated by J. Tate [6060, 6061] in 1965 (see Sect. 6.7), is still open (cf. P. Solé [5845]).

A survey covering, more generally, evaluations of coefficients of arbitrary modular forms was given by R.A. Rankin [5128] in 1986. Another survey of problems around Ramanujan's τ -function was prepared by M.R. Murty [4487].

At the end of the short note [5083], S. Ramanujan asserted the following divisibility properties of $\tau(n)$: $5|\tau(5n)$, $7|\tau(n)$ if $\left(\frac{n}{7}\right) \neq 1$, and $23|\tau(n)$ if $\left(\frac{n}{23}\right) = -1$. Several other congruences satisfied by the values of $\tau(n)$ modulo certain powers of the primes 2, 3, 5, 7, 23 and 691 appear in Ramanujan's manuscript, published in 1999 by B.C. Berndt and K. Ono [455] (cf. R.A. Rankin [5124]). One of them,

$$\tau(n) \equiv \sigma_{11}(n) \pmod{691},$$

appears there with a proof (the first published proof of this congruence is due to Wilton [6682]).

The conjectured congruences for $\tau(n)$ were later proved by M.H. Ashworth [152], R.P. Bambah [307], O. Kolberg¹²⁷ [3449, 3450], D.B. Lahiri [3612] and J.R. Wilton [6683], and a uniform proof was given by J.-P. Serre and H.P.F. Swinnerton-Dyer [6002, 6003]. (See also [5638, 5644].)

Since

$$\sum_{n=1}^{\infty} \tau(n) e^{2\pi i n z}$$

is the Fourier expansion of the unique normalized cusp form of weight 12, the question could be asked whether similar congruences hold also for Fourier coefficients of other cusp forms. In the case, when the space of cusp forms of a fixed weight k is of dimension one, which happens for $k = 12, 16, 18, 20, 22$ and 26. S. Ramanujan stated certain congruences in an unpublished manuscript, whose contents were described by R.A. Rankin in [5124].

In these cases all congruences mod p for prime p have been listed by J.-P. Serre and H.P.F. Swinnerton-Dyer [6002], with one possible exception, which concerned the unique normalized cusp form of weight 16 in the case $p = 59$. This case was settled later by K. Haberland [2418–2420] in 1983. Congruences modulo odd prime powers were considered in [6003] (see also B. Gordon [2284], E. Papier [4739]). The more general question,

¹²⁷The congruence for $\tau(n)$ mod 49 proved in [3450] is attributed in [6002, 6003] to some unpublished notes of D.H. Lehmer.

regarding congruences modulo prime powers between coefficients of modular forms was answered by N.M. Katz [3278] (see also F. Diamond [1517], K.A. Ribet [5187]).

An explicit formula for $\tau(n)$ was found in 1984 by J.A. Ewell [1943]:

$$\tau(n) = \sum_{k=1}^n (-1)^{n-k} r_{16}(n-k) 2^{3e(k)} \sigma_3(o(k)),$$

where $o(k)$ denotes the maximal odd factor of k , $e(k) = k/o(k)$ and $r_{16}(k)$ is the number of representations of k as the sum of 16 squares.

5. The paper [5079] by S. Ramanujan settled the problem when a diagonal quaternary quadratic form

$$\sum_{j=1}^4 a_j X_j^2 \tag{2.39}$$

with positive integral coefficients represents all positive integers. Particular cases of this question were considered earlier by J. Liouville, H.J.S. Smith and T. Pepin (for an account of these results see [1545, Chap. 10]). Ramanujan asserted that there are exactly 55 such forms, and listed all of them, but made an error¹²⁸, stating that the form $x^2 + 2y^2 + 5(z^2 + t^2)$ has the desired property, although it does not represent the number 15. He was particularly interested in the form $x^2 + y^2 + 10z^2$, noted that odd numbers which are not represented by it “do not seem to obey any simple law,” and listed sixteen such numbers, the largest being 391.

Later two more such numbers (679 and 2719) were discovered (B.W. Jones, G. Pall [3152], H. Gupta [2388]), and it was shown in 1997 by K. Ono and K. Soundararajan [4685] under the General Riemann Hypothesis that 2719 is the largest number having this property.

For later results on representations of integers by quadratic forms see Sect. 3.2.2.

6. S. Ramanujan stated a wealth of formulas, most of which were later proved. He published some of them, but the majority was hidden in his notebooks [5085, 5086], analyzed later by G.E. Andrews and B.C. Berndt [86–88, 447, 449] (see also the proceedings of a conference devoted to the work of S. Ramanujan [84]).

Several formulas, related to the number $d(n)$ of divisors of n were presented in [5077]. Among them one finds the following asymptotic formula, which in the case $k = 1$, $l = 0$ was established by G.F. Voronoï [6469] (see Sect. 2.6.2):

$$\sum_{n \leq x} d(kn + l) = a(k, l)x(\log x + 2\gamma - 1) + b(k, l)x + O(x^{1/3} \log x), \tag{2.40}$$

where k, l are fixed positive integers, and $a(k, l), b(k, l)$ are appropriate coefficients of the Dirichlet series of certain explicitly given functions.

This formula with a weaker error term of order $O(\sqrt{x})$ later got an elementary proof by T. Estermann¹²⁹ [1877], and in 1932 A. Page [4716] established (2.40).

¹²⁸This error was pointed out by L.E. Dickson [1546], who also gave a fresh proof of Ramanujan's result.

¹²⁹Theodor Estermann (1902–1991), professor at University College, London. See [5315].

The paper [5077] also contains asymptotic expressions for the sums

$$\sum_{n \leq x} d^a(n), \quad \sum_{n \leq x} 1/d(n), \quad \sum_{n \leq x} \sigma^2(n),$$

as well as closed formulas for various Dirichlet series, like

$$\sum_{n=1}^{\infty} \frac{\sigma_a(n)\sigma_b(n)}{n^s} = \frac{\zeta(s)\zeta(s-a)\zeta(s-b)\zeta(s-a-b)}{\zeta(2s-a-b)}.$$

These assertions were later proved by B.M. Wilson¹³⁰ [6677] and similar sums involving the divisor function were treated by A.E. Ingham [3016] in 1927, who obtained asymptotics for the sums

$$\sum_{m \leq n} d(m)d(m+k) \quad (k \neq 0), \quad \sum_{m < n} d(m)d(n-m).$$

The error terms were later improved by T. Estermann [1880–1882], R.A. Smith [5835], J.-M. Deshouillers, H. Iwaniec [1489, 1490], M. Ishibashi, S. Kanemitsu [3029], S. Kanemitsu [3232], Y. Motohashi [4460] and Y.-F.S. Pétermann, J. Wu [4801].

Not every assertion made by Ramanujan turned out to be true. Considering the number $B(x)$ of integers $\leq x$ which are sums of two squares, he stated in an unpublished manuscript the formula

$$B(x) = c \int_1^x \frac{dt}{\log^{1/2} t} + O\left(\frac{x}{\log x}\right)^{1/2},$$

with a certain positive c and an arbitrary N . At that time only the evaluation

$$B(x) = (c + o(1)) \frac{x}{\sqrt{\log x}}$$

with

$$c = \frac{1}{\sqrt{2}} \prod_{p \equiv 3 \pmod{4}} \frac{1}{\sqrt{1-p^{-2}}}$$

was known (E. Landau [3633]).

In 1928 a paper by G.K. Stanley¹³¹ [5888] appeared in which she claimed that Landau's evaluation cannot be improved, hence Ramanujan's formula fails for $N > 3/2$. She was right, but there were errors in her calculation, pointed out by D. Shanks [5674], who established

$$B(x) = \frac{cx}{\log^{1/2} x} + \frac{c_1 x}{\log^{3/2} x} + O\left(\frac{x}{\log^{5/2} x}\right),$$

with positive c_1 , showing definitely the falsity of Ramanujan's statement.

A quick way of computing $B(x)$ was proposed by P. Shiu [5715] who adapted an old method of counting primes in large intervals developed by E. Meissel¹³² in 1870 [4236], modified in 1959 by D.H. Lehmer [3789].

¹³⁰Bertram Martin Wilson (1896–1935), professor in Dundee. See [2576].

¹³¹Gertrude Katherine Stanley (1898–1974), professor at Westfield College, London. See [5126].

¹³²Daniel Friedrich Ernst Meissel (1826–1895), teacher in Kiel. See [4763].

For a discussion of other assertions by S. Ramanujan which turned out to be incorrect see P. Moree [4415].

The corresponding question for numbers which are sums of three squares was considered in 1908 by E. Landau [3633]. He showed that the number of such integers $\leq x$ equals

$$\frac{5}{6}x + \Delta(x),$$

with $\Delta(x) = O(\log x)$.

Much later, in 1988, the mean value of $\Delta(x)$ was determined by P. Shiue [5716]:

$$\sum_{n \leq x} \Delta(n) = \left(\frac{3}{16 \log 2} + o(1) \right) x \log x.$$

7. The paper [2540] by G.H. Hardy and S. Ramanujan gave birth to probabilistic number theory. Roughly, its main result states that with probability one every natural number n has $\log \log n$ distinct prime divisors. More precisely, evaluating the number of $n \leq x$ with a given $\omega(n)$, they established the following assertion.

If $f(x)$ is a function tending to infinity, then for the number $N_f(x)$ of $n \leq x$ satisfying

$$\frac{|\omega(n) - \log \log n|}{\sqrt{\log \log n}} < f(n)$$

one has $N_f(x) = o(x)$.

Later a much simpler proof based on the inequality

$$\sum_{n \leq x} (\omega(n) - \log \log n)^2 = O(x \log \log x)$$

was found by P. Turán [6212]. See Sect. 5.5 for further results.

8. In 1916 G.H. Hardy and S. Ramanujan [2539] proved a Tauberian theorem¹³³, which in the case of the usual Dirichlet series takes the following form

If the series $f(s) = \sum_{n=1}^{\infty} a_n n^{-s}$ has positive coefficients, converges for $s > 0$ and for $s \rightarrow 0$ satisfies

$$\log f(s) = (A + o(1))s^{-\alpha} \left(\log \frac{1}{s} \right)^{-\beta},$$

then for x tending to infinity one has

$$\log \sum_{n \leq x} a_n = (B + o(1)) \log^{\alpha/(1+\alpha)} x (\log \log x)^{-\beta/(1+\alpha)},$$

with B depending explicitly on A, α, β .

¹³³ A monograph devoted to Tauberian theorems has been written by H.R. Pitt [4918]. For their history see the recent book by J. Korevaar [3477].

They used it to obtain an asymptotical formula for the number of integers $n \leq x$ having the form

$$n = 2^{\alpha_2} 3^{\alpha_3} \dots p^{\alpha_p}$$

with $\alpha_2 \geq \alpha_3 \geq \dots \geq \alpha_p$, considered earlier by S. Ramanujan in [5076], and applied it also to a study of the *partition function* $p(n)$, counting all representations of a positive integer n as sums of positive integers. This function had been considered already by Euler [1899], who proved the identity

$$1 + \sum_{n=1}^{\infty} p(n)x^n = \prod_{k=1}^{\infty} (1 - x^k)^{-1} \quad (|x| < 1). \quad (2.41)$$

At Hardy's request all values of $p(n)$ for $n \leq 200$ were calculated by P.A. MacMahon¹³⁴ (see [2541, pp. 114–115]). This function grows rapidly, its value at $n = 200$ being 3 972 999 029 388.

Later H. Gupta [2385, 2386] extended MacMahon's table up to $n = 600$.

The Tauberian theorem of G.H. Hardy and S. Ramanujan led to the equality

$$\log p(n) = (c + o(1))\sqrt{n}$$

with $c = \pi\sqrt{2/3}$, and in the next year they observed [2541] that a more precise result can be obtained with the use of Cauchy's integral theorem.

It soon turned out that the same approach can be used to solve various additive problems, and so the *circle method* was born. They considered the sum $f(z)$ of the power series occurring in (2.41), and noted that if Γ is a path lying inside the unit circle, and encompassing the origin, then one has

$$p(n) = \frac{1}{2\pi i} \oint_{\Gamma} \frac{f(z)}{z^{n+1}} dz.$$

One reads in their paper:

“The idea which dominates this paper is that of obtaining asymptotic formulae for $p(n)$ by a detailed study of the integral . . . This idea is an extremely obvious one; it is the idea which has dominated nine-tenths of modern research in the analytic theory of numbers: and it may seem very strange that it should never have been applied to this particular problem before.”

They explained this situation by “the extreme complexity of the behavior of the generating function $f(x)$ near a point of the unit circle.” In fact, they noted that every point of the unit circle is an essential singularity for f .

Taking for Γ the circle $z = Re^{2\pi i\theta}$ ($0 \leq \theta < 1$, $0 < R < 1$) they dissected Γ into arcs $\gamma_{p,q}$, corresponding to θ lying in a small interval centered at the rational number $p/q \in [0, 1)$ with co-prime p, q , belonging to the *Farey series* of order N , which consists of all rational numbers from the unit interval, having denominator $\leq N$, and

¹³⁴Percy Alexander MacMahon (1854–1929), worked at military schools. He wrote a large monograph on combinatorics [4055]. See [246].

arranged according to their value. They also introduced an auxiliary function $F_t(z)$, defined for positive t by

$$F_t(z) = \sum_{n=1}^{\infty} \psi_t(n) z^n,$$

where

$$\psi_t(x) = \frac{d}{dx} \frac{\cosh(t\sqrt{x-1/24}) - 1}{\sqrt{x-1/24}}.$$

Putting

$$\Psi(z) = \frac{1}{\pi\sqrt{2}} \sum_{q \leq a\sqrt{n}} \sqrt{q} \sum_{\substack{p < q \\ (p,q)=1}} \omega_{p,q} F_{C/q} \left(z \exp\left(\frac{-2p\pi i}{q}\right) \right) \quad (2.42)$$

(where a is a suitable positive constant, $C = \pi\sqrt{2/3}$, and the numbers $\omega_{p,q}$ are certain 24th roots of unity), and

$$\Phi(z) = f(z) - \Psi(z)$$

they succeeded in showing that on the one hand all integrals

$$\frac{1}{2\pi i} \int_{\gamma_{p,q}} \frac{\Phi(z)}{z^{n+1}} dz$$

are small, and on the other hand the integral

$$\frac{1}{2\pi i} \int_{\gamma_{p,q}} \frac{\Psi(z)}{z^{n+1}} dz$$

can be swiftly evaluated. This led to an explicit expression of $p(n)$ as a finite sum of \sqrt{n} terms with an error of the order $O(n^{-1/4})$, implying in particular the equality

$$p(n) = \left(\frac{1}{4\sqrt{3}} + o(1) \right) \frac{\exp(\pi\sqrt{2n/3})}{n}.$$

A simpler proof of the last result was given in 1920 by J.V. Uspensky¹³⁵ [6254]. It is reproduced in the book [184] by R. Ayoub.

An elementary proof of this formula (but without identifying the leading constant) was provided by P. Erdős [1792] in 1942.

In 1937 H. Rademacher [5036, 5037] observed that a modification of the Hardy–Ramanujan approach leads to an infinite series converging rapidly to $p(n)$, whose tail may be effectively estimated. The first 18 terms evaluated at $n = 599$ approximate $p(599)$ with an error smaller than $1/2$, leading to

$$p(599) = 435\,350\,207\,840\,317\,348\,270\,000,$$

justifying a conjecture by D.H. Lehmer [3780]. An analogue of his result for the number of partitions into unequal parts was obtained in 1942 by L.K. Hua [2930].

¹³⁵Jacob Victorovič Uspensky (1883–1947), professor in St. Petersburg and Stanford.

For the theory of partitions see the books [80, 82] by G.E. Andrews.

The roots of unity $\omega_{p,q}$ occurring in (2.42) are made explicit by the formula

$$\omega_{p,q} = \exp(s(p, q)),$$

where

$$s(p, q) = \pi i \sum_{j=1}^q \frac{j}{q} \left(\left\{ \frac{pj}{q} \right\} - \frac{1}{2} \right) \quad (2.43)$$

(see H. Rademacher [5032]). The sums $s(p, q)$ were introduced by R. Dedekind in his comments to Riemann [1420], and are called *Dedekind sums*. They were later studied by H. Rademacher [5031] and H. Rademacher and A. Whiteman [5042].

Later several arithmetical applications of Dedekind sums were given, and there were even applications outside number theory (see the book [2830] by F. Hirzebruch and D. Zagier). A book on Dedekind sums was written by H. Rademacher and E. Grosswald [5041] in 1972, and generalizations were given by T.M. Apostol [111], L.J. Goldstein [2267], G.J. Rieger [5221], K.H. Rosen, W.M. Snyder [5287], and D. Zagier [6808].

The method applied by G.H. Hardy and S. Ramanujan [2541] to study the partition function $p(n)$ was applied to related problems by E.M. Wright¹³⁶ in three papers [6739–6741]. In particular, he obtained asymptotics for the number of partitions of an integer into k th powers, improving upon an earlier result by G.H. Hardy and S. Ramanujan [2541].

9. The Ramanujan sums, defined by

$$c_r(n) = \sum_{\substack{1 \leq a < r \\ (a,r)=1}} \exp\left(\frac{2\pi i a n}{r}\right),$$

were used by Ramanujan¹³⁷ in [5080] to expand arithmetical functions f in a series of the form

$$f(n) = \sum_{r=1}^{\infty} a_r c_r(n).$$

He proved several interesting examples of these expansions, such as

$$\frac{\sigma(n)}{n} = \frac{\pi^2}{6} \sum_{r=1}^{\infty} \frac{c_r(n)}{r^2},$$

and

$$d(n) = - \sum_{r=1}^{\infty} \frac{\log r}{r} c_r(n),$$

and obtained similar formulas for the number of representations of an integer n as the sum of an even number of squares studied earlier by him in [5078] (for an exposition see [2516, Chap. 9]).

¹³⁶Edward Maitland Wright (1906–2005), professor in Aberdeen. See [4761].

¹³⁷It has been pointed out in [2545] that these sums already appear in Landau's book [3636].

Simpler proofs of Ramanujan's results were given in 1921 by G.H. Hardy [2513].

It was shown by R.D. Carmichael [922] in 1932 that Ramanujan sums satisfy

$$\lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n \leq N} c_r(n) c_s(n) = \begin{cases} \varphi(r) & \text{if } r = s, \\ 0 & \text{otherwise,} \end{cases}$$

and hence can be regarded in some sense as an orthogonal system. The theory of Ramanujan expansions was later systematically developed by several authors (see, e.g., A. Hildebrand [2796], W. Schwarz [5581], L.G. Lucht [4031]). For connections with the theory of almost periodic functions see M. Kac¹³⁸, E.R. van Kampen, A. Wintner¹³⁹ [3178]¹⁴⁰. A survey with ample bibliography was given in 1988 by W. Schwarz [5582].

10. A few years later S. Ramanujan [5081, 5084¹⁴¹], considered again the partition function, and proved that for $(a, b) \in \{(5, 4), (7, 5), (11, 6)\}$ it satisfies the congruence

$$p(an + b) \equiv 0 \pmod{a}. \quad (2.44)$$

He conjectured also that there exist similar congruences with the modulus being a power of 5, 7 or 11. More precisely, he asserted that if q is one of these three primes then for $n \geq 1$ the congruence $24m \equiv 1 \pmod{q^n}$ implies the divisibility of $p(m)$ by q^n . In an unpublished manuscript (see [5124]) he considered also the residues of $p(n)$ modulo powers of 13.

Ramanujan's assertion was not quite accurate. This was noted by S. Chowla [1072] who pointed out (using a table of values of $p(n)$ prepared by H. Gupta [2385, 2386]) that it fails for the modulus 7^3 . It turned out, however, that a modified form of this assertion is true. This was shown for $q = 5, 7$ by G.N. Watson in 1938 [6591] (for some special cases see H.B.C. Darling [1328, 1329], V. Krečmar [3521]) and for $q = 11, 13$ by J. Lehner [3808] and A.O.L. Atkin [161]. For related results see A.O.L. Atkin [163], F.G. Garvan [2200], B. Gordon [2284], K. Hughes [2946].

Some of Ramanujan's congruences have a combinatorial interpretation discovered by F.J. Dyson [1675] and proved by A.O.L. Atkin and H.P.F. Swinnerton-Dyer [167]. For further developments see F.G. Garvan [2201, 2202], G.E. Andrews, F.G. Garvan [91], F.G. Garvan, D. Kim, D. Stanton [2203].

In 1992 I. Kiming and J.B. Olsøn [3336] showed that if (2.44) holds for a prime a , then $24b \equiv 1 \pmod{a}$, and in 2003 S. Ahlgren and M. Boylan [28] showed that in this case the only congruences of the form (2.44) are those found by Ramanujan.

Other congruences for $p(an + b)$ were found later by M. Newman¹⁴², S. Ahlgren, G.E. Andrews, A.O.L. Atkin, J.N. O'Brien, D. Eichhorn, K. Mahlburg, K. Ono and R.L. Weaver [27, 30, 92, 166, 1698, 4059, 4585, 4683, 6596].

¹³⁸Mark Kac (1914–1984), professor at Cornell University and Rockefeller University. See [3310].

¹³⁹Aurel Friedrich Wintner (1903–1958), professor in Baltimore. See [2573].

¹⁴⁰Essentially the same paper, with a different proof of one of the lemmas and an author (P. Erdős) added, appeared in 1940 [1836].

¹⁴¹This paper was published posthumously by G.H. Hardy.

¹⁴²Morris Newman (1924–2007), worked until 1977 at the National Bureau of Standards, later became professor at the University of California in Santa Barbara. See [2256].

It was conjectured by P. Erdős that for every prime p there is an integer n such that p divides $p(n)$, and in 1989 A. Schinzel and E. Wirsing [5454] showed that the number of primes dividing at least one of the numbers $p(n)$ with $n \leq x$ is $\gg \log x$. K. Ono [4683] established Erdős's conjecture for primes $p \geq 5$, and showed that in this case the set of such numbers n has a positive lower density. It is still unknown whether $p(n)$ is divisible by 3 for infinitely many n .

Still open is a stronger conjecture, posed in 1960 by M. Newman [4587], asserting that every arithmetic progression contains values of the partition function. A sufficient condition for its validity was given by K. Ono [4683], implying its correctness for all primes moduli $3 < p < 1000$ (for certain small values of p this was shown earlier by A.O.L. Atkin [162], T. Kløve [3375, 3376], O. Kolberg [3448] and M. Newman [4587]). This was extended to $3 < p < 2 \cdot 10^5$ by J.H. Bruinier and K. Ono [794], and in 2005 S. Ahlgren and M. Boylan [29] established Newman's conjecture for prime powers moduli $\neq 3^n$.

These results were obtained with the use of the theory of modular forms, which is not surprising, as already S. Ramanujan in his *Lost Notebook* [5086] gave congruences relating the generating functions of partitions to modular forms, e.g.,

$$\sum_{n=0}^{\infty} p(13n+6)q^n \equiv p(6) \prod_{n=1}^{\infty} (1-q^n)^{11} \pmod{13}.$$

Similar congruences modulo arbitrary prime powers were later given by S. Ahlgren and M. Boylan [28].

In 1966 M.V. Subbarao¹⁴³ [5983] conjectured that every arithmetical progression $Ax + B$ contains infinitely many integers n with $p(n)$ even and this was established in 1996 by K. Ono [4681]. M.V. Subbarao conjectured that the same holds also for odd values of $p(n)$. See also K. Ono [4682].

In 2000 J. Getz, a high school student, proved the truth of Subbarao's conjecture for infinitely many progressions [2236]. Both conjectures were established earlier for several small values of A (F.G. Garvan, D. Stanton [2204], M.D. Hirschhorn [2826], M.D. Hirschhorn, M.V. Subbarao [2828]).

11. The paper [5084] by Ramanujan contained only part of the results which were described in the manuscript of 43 pages found in his papers. In 1928 the collection of Ramanujan's notebooks was given by G.H. Hardy to G.N. Watson, who in 1935 presented in [6590] complete proofs of three theorems contained in that manuscript. The first deals with positive integers n having the property that for primes lying in a fixed residue class mod k and dividing n their maximal power dividing n is a square. If $B(x)$ denotes the number of such $n \leq x$, then one has

$$B(x) = (c(k) + o(1)) \frac{x}{\log^{1-1/\varphi(k)} x}$$

with some positive $c(k)$. The second asserts that for every odd k , every d and almost all n , the number $\sigma_k(n)$ is divisible by d , more precisely,

$$A_{k,d} = \#\{n \leq x : d \nmid \sigma_k(n)\} \ll \frac{x}{\log^{1/\varphi(k)} x}.$$

¹⁴³Matukumalli Venkata Subbarao (1921–2006), professor at the University of Alberta. See [3273].

Much later this was made more precise by R.A. Rankin [5118] and E.J. Scourfield [5591] (cf. [4535]).

The third assertion states that $\tau(n)$ is divisible by 691 for almost all n .

Similar results were established later for larger moduli (R.P. Bambah and S. Chowla [309, 1088]), and it was shown by J.-P. Serre [5646, 5647, 5654] that for every integer k and almost all integers n one has $k|\tau(n)$, and the same applies to coefficients of modular forms of integral weight.

12. In [5075] S. Ramanujan formulated the following question: “ $2^n - 7$ is a perfect square for the values 3, 4, 5, 7, 15 of n . Find other values.” It turned out much later that there are no other solutions¹⁴⁴. This was proved by T. Nagell¹⁴⁵ in 1948 in a Norwegian paper, and an English translation appeared in 1961 [4517].

The same result was proved independently in 1956 by J. Browkin and A. Schinzel [749] and in 1959 by T. Skolem, S. Chowla and D.J. Lewis [5810]. The more general equation

$$x^2 + A = p^y, \quad (2.45)$$

where p is a fixed prime and A is a fixed integer not divisible by p , has been considered by R. Apéry¹⁴⁶ [109], who showed that for $p > 2$ and positive A there are at most two solutions, and the same holds for $p = 2$ and $15 \leq A \equiv 7 \pmod{8}$. For $p = 2$ and $A \not\equiv 0, 4, 7 \pmod{8}$ there is at most one solution (J. Browkin, A. Schinzel [750]). Much later F. Beukers [485] confirmed the conjecture posed in [750] that for $p = 2$ and positive A the equation (2.45) has at most one solution, except when $A = 7, 23$ or $2^k - 1$ with a certain $k \geq 4$. M.H. Le [3746] showed that if p is odd and $\max\{D, p\}$ is sufficiently large, then two solutions exist only if for some a one has $p = 4a^2 + 1$ and $D = 3a^2 + 1$. For the case $A = 7$ see J.-L. Lesage [3838], S. Siksek, J.E. Cremona [5788]. In the case of A negative, F. Beukers [485] showed that for $p = 2$ one has at most 4 solutions, and in [486] he extended this to the case of odd p . Later M.H. Le [3742] showed that for large $|A|$ there are at most three solutions and determined in [3743, 3745] all cases for $p = 2$ with four solutions. Now it is known that for $p \neq 2$ this equation has at most three solutions (M.L. Bauer, M.A. Bennett [361]).

In paper [823] by Y. Bugeaud, M. Mignotte and S. Siksek all solutions of the equation $x^2 + D = y^n$ (with $n \geq 3$) were found for all $1 \leq D \leq 100$ for which this had not been done earlier, in particular for $D = 7$.

The equation

$$x^2 + y^m = 2^n$$

(with $(x, y) = 1$, $y \geq 2$, $n \geq 3$) was considered in 1995 by Y.-D. Guo and M.H. Le [2384], who showed that it has finitely many solutions and in all solutions one has $m \leq 10^9$. Later Y. Bugeaud [808] reduced this bound to $m \leq 7.3 \cdot 10^5$, and M.H. Le showed [3748] that for large y it does not have solutions with $m \geq 2$. Later M.A. Bennett and C.M. Skinner [419] showed that the only solutions with $m \geq 2$ are $(x, m, n, y) = (\pm 13, 3, 9, 7)$, and for odd negative $y \neq -1$ with $m \geq 3$, $n \geq 1$ one has $(x, m, n, y) = (\pm 71, 3, 7, 17)$.

¹⁴⁴On p. 327 of [5088] it is noted that this question was answered by K.J. Sanjana and T.P. Trivedi in 1913, but actually they noticed only that there are no other small solutions.

¹⁴⁵Trygve Nagell (1895–1988), docent in Oslo and professor in Uppsala. See [946].

¹⁴⁶Roger Apéry (1916–1994), professor in Caen. See [108].

For the equation

$$x^2 \pm y^m = p^n$$

with odd prime p see Y. Bugeaud [809], A. Bérczes, I. Pink [427].

It was shown by M.A. Bennett, M. Filaseta and O. Trifonov [418] that if with positive m, n one has

$$x^2 + 7 = 2^n m,$$

then either $x < m^2$ or $m \in \{1, 3, 5, 11, 181\}$.

For a survey of the developments up to 1992 see J.H.E. Cohn [1164].

2.2.7 Modular Forms

1. The theory of modular forms in one variable forms a part of the theory of automorphic functions, defined as functions on a complex space, which behave in a special way under the action of a discrete group of transformations. This subject developed quickly in the second half of the 19th century, mainly in hands of C. Hermite, F. Klein, H. Poincaré and their students. (The main results being contained in the papers of F. Klein [3351, 3352], H. Poincaré [4930–4934], A. Hurwitz [2954] and in the lectures of F. Klein [3356, 3357], published in 1890. See also the early survey by R. Fricke¹⁴⁷ [2092].) It is interesting to observe how Klein, who often used various transformation groups in his research, avoided the use of properties of abstract groups. This can be clearly seen in his lectures, where in several places he meticulously defines factor groups in each individual case although the general notion was at that time already known. His attitude towards abstract groups never did change, as can be seen from the following sentence in his book [3354, p. 338] published in 1926:

“Die¹⁴⁸ Lehre von den Vertauschungsgruppen hat sich ... zu einer selbständigen Disziplin entwickelt. Wir begegnen da Namen wie Cayley, Sylow, Dyck, Hölder, Frobenius, Burnside und in neuerer Zeit vielfach auch Amerikanern. Für viele Gemüter ist es ein besonderer Reiz, daß man auch hier wieder arbeiten kann, ohne von sonstiger Mathematik viel zu wissen ...”

2. We recall quickly some properties of modular forms. Let $\Gamma = SL_2(\mathbf{Z})$ be the group of invertible 2×2 matrices with integral entries and unit discriminant. It acts on the upper complex half-plane \mathfrak{H} by

$$A \cdot z = \frac{az + b}{cz + d},$$

¹⁴⁷Robert Fricke (1861–1930), professor in Braunschweig.

¹⁴⁸“The theory of permutation groups developed itself ... to an independent discipline. We meet there the names of Cayley, Sylow, Dyck, Hölder, Frobenius, Burnside, and in recent time also many Americans. For many minds it is a particular attraction that one can work here without knowing much of the rest of mathematics ...”

where

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma. \quad (2.46)$$

A complex-valued function defined and regular on \mathfrak{H} is called a *modular form* of weight k , if for $A \in \Gamma$ one has

$$f(A \cdot z) = (cz + d)^k f(z). \quad (2.47)$$

Since the last equality implies $f(z + 1) = f(z)$, one can expand f in a series of the form

$$f(z) = c_0 + \sum_{n=1}^{\infty} c_n \exp(2\pi i n z), \quad (2.48)$$

with complex coefficients c_n . If $c_0 = 0$, then f is called a *cuspidal form*.

Now let $N \geq 1$ be an integer. Denote by $\Gamma(N) \subset \Gamma$ the group of matrices (2.46) with $a \equiv d \equiv 1 \pmod{N}$ and $b \equiv c \equiv 0 \pmod{N}$. If f is regular on \mathfrak{H} , satisfies (2.47) for $A \in \Gamma(N)$, and for every $A \in \Gamma$ one has

$$f(A \cdot z)(cz + d)^{-k} = c_0(A) + \sum_{n=1}^{\infty} c_n(A) \exp\left(\frac{2\pi i n z}{N}\right),$$

then f is called a *modular form of weight k and level N* (note that in older literature these forms were said to be of weight $-k$). If for all $A \in \Gamma$ one has $c_0(A) = 0$, then f is called a *cuspidal form*. Modular forms of weight zero are called *modular functions*.

In the same way one defines modular forms associated to the subgroups $\Gamma_0(N)$ and $\Gamma_1(N)$ of Γ , which contain $\Gamma(N)$ and are defined by

$$\Gamma_0(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : N|c \right\},$$

and

$$\Gamma_1(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a \equiv d \equiv 1 \pmod{N}, N|c \right\}.$$

Every subgroup of Γ containing $\Gamma(N)$ for some N is called a *congruence subgroup* and is of finite index in Γ . There exist subgroups of finite index in Γ which are not congruence subgroups, and the first such example was given in 1880 by F. Klein [3351] without a proof. First proofs were provided six years later by R. Fricke [2091] and G. Pick¹⁴⁹ [4854].

The groups $\Gamma(N)$, $\Gamma_0(N)$ and $\Gamma_1(N)$ are finitely generated. In the case of prime N a set of generators and their relations for $\Gamma_0(N)$ was given in 1929 by H. Rademacher [5030], and for $\Gamma(N)$ by H. Frisch [2069] in 1933. For the group

$$\Gamma_0^0(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : N|(b, c) \right\}$$

this was done in 1950 by E. Grosswald [2360].

¹⁴⁹Georg Alexander Pick (1859–1942), professor in Prague.

Now it is known that Γ contains infinitely many subgroups of finite index which are not congruence subgroups (see, e.g., I. Reiner¹⁵⁰ [5154], K.K. Wohlfahrt [6706, 6708], M. Newman [4588]). Remarkably, this phenomenon happens only in dimension $n = 2$, as it was shown in 1962 by H. Bass, M. Lazard and J.-P. Serre [348] and J.L. Mennicke [4252] that for $n \geq 3$ any subgroup of finite index in $SL_n(\mathbf{Z})$ contains a group of matrices, congruent to the unit matrix modulo a certain integer. This was extended in 1967 to $SL_n(R)$, where R is a ring of integers in a not totally complex field by H. Bass, J. Milnor, J.-P. Serre [349]. The case $n = 2$ for arbitrary global fields was worked out by J.-P. Serre [5640]. In 1969 H. Matsumoto [4197] generalized these results to a large class of algebraic groups. For surveys of the theory of congruence subgroups of algebraic groups see A.S. Rapinchuk [5129] and M.S. Raghunathan [5050].

One considers also, more generally, modular forms with characters¹⁵¹, i.e., functions f satisfying for $A \in \Gamma_0(N)$, instead of (2.47), the equality

$$f(A \cdot z) = \chi(d)(cz + d)^k f(z), \quad (2.49)$$

where χ is a character mod N . The simplest examples are provided by theta-functions

$$\theta(z, F) = \sum_{n_1, \dots, n_k \in \mathbf{Z}} \exp(2\pi i z F(n_1, \dots, n_k)),$$

where F is a positive-definite quadratic form in an even number of variables (see, e.g., E. Hecke [2700, 2701]).

The set of all modular forms of fixed weight k , level N and character χ forms a finite-dimensional linear space $\mathfrak{M}_k(N, \chi)$ over the complex field, and the cusp forms form a subspace $\mathfrak{C}_k(N, \chi)$ of $\mathfrak{M}_k(N, \chi)$. Similarly one defines modular forms and cusp forms associated with other congruence subgroups.

3. At the end of the 19th century Hilbert considered a generalization of the theory of modular forms to several variables. He did not publish his results and gave his notes to O. Blumenthal¹⁵² who used them in his habilitation thesis [565].

Hilbert modular forms are associated with the *Hilbert modular group*

$$\Gamma(K) = GL_2(\mathbf{Z}_K)/\{\pm E\},$$

where K is a totally real algebraic number field of degree $n \geq 2$, \mathbf{Z}_K is its ring of integers and E denotes the unit matrix. This group acts on the product \mathfrak{H}_n of n upper complex half-planes by

$$A(z_1, \dots, z_n) = \left(\frac{a^{(1)}z + b^{(1)}}{c^{(1)}z + d^{(1)}}, \dots, \frac{a^{(n)}z + b^{(n)}}{c^{(n)}z + d^{(n)}} \right)$$

¹⁵⁰Irving Reiner (1924–1986), professor at the University of Illinois. See [3104].

¹⁵¹Sometimes called, after E. Hecke, modular forms of *Nebentypus*.

¹⁵²Otto Blumenthal (1876–1944), professor in Aachen (1905–1933), executive editor of *Mathematische Annalen* (1906–1938). See [385].

for

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad (2.50)$$

$x^{(j)}$ denoting the j th conjugate of $x \in K$.

A regular function $f : \mathfrak{H}_n \rightarrow \mathbf{C}$ is called a *Hilbert modular form* of weight k if for A as in (2.50) one has

$$f(A\bar{z}) = N(cz + d)^k f(z), \quad (2.51)$$

$N(\cdot)$ denoting the norm $K \rightarrow \mathbf{Q}$.

Originally an extra regularity condition appeared in the definition, but it was shown in 1954 by M. Koecher [3436, 3437] that it is redundant. In the special case $K = \mathbf{Q}(\sqrt{5})$ this was shown earlier (in 1928) by F. Götzky [2289].

In 1903 O. Blumenthal [565] presented a construction of the fundamental domain for $\Gamma(K)$, applying a method of E. Picard¹⁵³ [4846–4848], who used it to construct functions of two variables satisfying (2.51) with $k \geq 4$.

Blumenthal's construction of the fundamental domain was not quite correct. This was pointed out in 1940 by H. Maass¹⁵⁴ [4037], who gave an explicit construction of the fundamental domain for a class of groups generalizing $\Gamma(K)$ (cf. O. Herrmann [2768], T. Tamagawa [6041] and Chap. 3 in Siegel's lectures [5776]).

In 1928 H.D. Kloosterman¹⁵⁵ [3372] introduced modular forms associated to congruence subgroups of the Hilbert group. Later [3373] he constructed a family of modular forms, generalizing the classical θ -series.

The theory of Hilbert modular forms was presented in the books by E. Freitag [2085], G. Shimura [5697] and C.L. Siegel [5776].

2.3 The First Sieves

1. The first arithmetical sieve appeared in the second edition of Legendre's book [3767]. Legendre formalized the ancient method of Eratosthenes for counting prime numbers in an interval, which can be described as follows.

If an integer N is given, and $2 = p_1 < p_2 < \dots < p_k$ are all primes smaller than \sqrt{N} , then deleting from the set of all integers in $I_N = [\sqrt{N}, N]$ all numbers divisible by at least one of the p_j 's we obtain a list of primes in I_N . To count these primes one first forms a list of all integers in the interval $[\sqrt{N}, N]$ and deletes from it all multiples of the primes p_1, p_2, \dots, p_k . This gives $\sum_{i=1}^k [N/p_i]$ deletions. Numbers divisible by two primes p_i were deleted twice, hence one has to subtract their number, equal to $\sum_{p_i \neq p_j} [N/p_i p_j]$. One realizes now that numbers divisible by three primes are left undeleted, so one has to

¹⁵³Charles Émile Picard (1856–1941), professor in Toulouse and Paris. See [2427].

¹⁵⁴Hans Maass (1911–1992), professor in Heidelberg. See [867].

¹⁵⁵Hendrik Douwe Kloosterman (1900–1968), professor in Leiden. See [5880].

delete them, and proceeding in this way one is led to the following formula for the number $\pi(N)$ of primes not exceeding N .

$$\pi(N) = \pi(\sqrt{N}) + \sum_{i=1}^k (-1)^i \sum_{p_{j_1} < \dots < p_{j_i} < \sqrt{N}} \left[\frac{N}{p_{j_1} \cdots p_{j_i}} \right] = \sum_{d|D} \mu(d) \left[\frac{N}{d} \right],$$

where D denotes the product of all primes $< \sqrt{N}$ and $\mu(d)$ is the Möbius function.

This formula does not lead to a non-trivial evaluation of $\pi(N)$, since the error obtained by the replacement of $[N/p_i]$ by $N/p_i + O(1)$ is larger than the main term, due to the $2^{\pi(\sqrt{N})}$ terms in the considered sum.

The include-exclude procedure described above is applicable also in a more general setting. Let Ω be a given finite set, let $X_1, \dots, X_k \subset \Omega$, $Y = \Omega \setminus \bigcup_{i=1}^k X_i$, and let f be a function on Ω having non-negative values. If, for $X \subset \Omega$, one puts

$$\Phi(X) = \sum_{x \in X} f(x),$$

and

$$A_r(f) = \Phi(\Omega) + \sum_{m=1}^r (-1)^m \sum_{1 \leq i_1 < i_2 < \dots < i_m \leq k} \Phi(X_{i_1} \cap \dots \cap X_{i_m})$$

for $r = 1, 2, \dots, k$, then this procedure leads to the formula

$$\Phi(Y) = A_k(f). \quad (2.52)$$

2. There are rather few results which can be achieved with the use of this simple sieve. A variant of it, dealing with arithmetic progressions, was utilized in 1909 by J.C. Morehead [4420] in his search for Fermat primes.

An attempt to modify the Eratosthenian sieve method appeared in the paper [4256] by J. Merlin, edited posthumously by J. Hadamard; however the arguments appearing there are unconvincing. This paper gave an impulse to V. Brun¹⁵⁶ [798, 800–802], who presented the first non-trivial applications of the sieve. His approach was based on the observation that to obtain a reasonably small error term one should at some point stop the procedure leading to (2.52). In fact, a short calculation utilizing the simple fact that the sum

$$\sum_{j=0}^r (-1)^j \binom{k}{j}$$

is non-negative for even r , and non-positive for odd r , leads to

$$A_r(f) \leq \Phi(Y) \leq A_s(f), \quad (2.53)$$

for odd r and even s , satisfying $1 \leq r, s \leq k$.

¹⁵⁶Viggo Brun (1885–1978), professor in Oslo. See [5594].

Although this idea is simple, its application involves cumbersome combinatorial arguments. Nevertheless V. Brun succeeded in proving the following important results.

(a) *The number $\pi_2(x)$ of twin primes below x does not exceed $100x/\log^2 x$ for large x , hence the series of their inverses converges.*

The coefficient 100 was later reduced to 19.43 by A.A. Buhštab¹⁵⁷ [833]. One expects that for large x one has

$$\pi_2(x) \leq (c + \varepsilon)B \frac{x}{\log^2 x}, \quad (2.54)$$

with $c = 1$ and

$$B = 2 \prod_{p>2} \left(1 - \frac{1}{(p-1)^2}\right).$$

In 1947 A. Selberg [5611] proved this with $c = 10.6$, and in [5614] stated that one can have $c = 8$. Later this was improved to $c = 6$ (C.D. Pan¹⁵⁸ [4734]), $c = 4$ (E. Bombieri, H. Davenport [608]), $c = 3.9171$ (J.R. Chen¹⁵⁹ [1026]), $c = 34/9 = 3.77\dots$ (É. Fouvry, H. Iwaniec [2056]), $c = 64/17 = 3.76\dots$ (É. Fouvry [2047, 2048]), $c = 3.5$ (E. Bombieri, J.B. Friedlander, H. Iwaniec [611–613]), $c = 3.454$ (É. Fouvry, F. Grupp [2053]), $c = 3.418$ (J. Wu [6755]), $c = 3.406$ (Y. Cai, M.G. Lu [886]) and $c = 3.3996$ (J. Wu [6759, 6760]), which is the current record.

Brun's method is also applicable to prime pairs with any fixed even difference. See B.I. Segal [5598].

(b) *Every large even integer is the sum of two positive integers, each of which has at most 9 prime divisors.*

For later progress, culminating in the replacement of 9 by 2, see Sect. 5.2.

(c) *In every interval of the form $[x, x + \sqrt{x}]$ there exists an integer, having at most 11 prime divisors.*

Later the number 11 was replaced by 9 (W.E. Mientka [4288]), by 4 (S. Uchiyama [6249]) and by 2 (J.R. Chen [1023, 1024]).

It took some time to recognize the importance of the new sieve, although V. Brun gave a short and readable exposition of his idea in [803]. It seems that the first who used the new method was T. Nagell [4504], who proved in 1922 that if f is a polynomial with integral coefficients, and $P(x)$ denotes the number of primes represented by $f(n)$ with $n \leq x$, then $P(x) = o(x)$ (for $P(x) = x^2 + 1$ this had been shown already by Brun in [799]). This re-

¹⁵⁷Aleksandr Adol'fovič Buhštab (1905–1990), professor in Baku and Moscow. See [3541].

¹⁵⁸Pan Cheng Dong (1934–1997), professor in Shandong.

¹⁵⁹Chen Jing Run (1933–1996), professor at the Academia Sinica in Beijing. See [4736].

sult was strengthened in 1931 by H. Heilbronn [2706] to $P(x) = O(x/\log x)$ using Brun's sieve. In his result H. Heilbronn allowed f to be an integer-valued polynomial with rational coefficients. It was shown by G. Pólya [4953] that every such polynomial is of the form

$$\sum_{j=0}^n a_j \binom{x}{j}$$

with $a_j \in \mathbf{Z}$. The analogue of the last result for polynomials in algebraic number fields was obtained in 1919 by A. Ostrowski¹⁶⁰ [4707] and Pólya [4958] (for the theory of integer-valued polynomials see the book by P.-J. Cahen and J.-L. Chabert [880]; see also [4541]).

3. Let $F(X)$ be a polynomial with integral coefficients. We have already mentioned Bouniakowsky's old question of whether an irreducible polynomial $F \in \mathbf{Z}[X]$ without constant factors represents infinitely many numbers $\pm p$ with p prime. Since this seems to be out of reach, one tried to show that such a polynomial represents at least infinitely many numbers with a bounded number of prime divisors. The result by V. Brun [802] implied that the polynomial $x(x+2)$ represents infinitely many integers having at most 18 prime factors, and in 1923 H. Rademacher [5024] gave a simplified exposition of Brun's sieve utilizing it to show that an irreducible polynomial of degree d having integral coefficients and without fixed divisors represents infinitely many integers having at most $4d - 1$ prime divisors.

This bound was later reduced by G. Ricci¹⁶¹ [5194, 5195, 5199, 5200] first to $[cd]$ with $c = 3.0243$, and then to $3d - 1$. It took some time before this bound was reduced to 3 for $d = 2$ and $d + c \log d$ with a certain constant c for $d \geq 3$ by P. Kuhn [3563, 3564], and to $d + 1$ by A.A. Buhštab [837] and H.-E. Richert [5209] (for $3 \leq d \leq 5$ and $d = 6, 7$ this had been shown earlier by Y. Wang [6552] and B.V. Levin [3856], respectively). For $d = 2$ this bound was reduced in 1978 to 2 by H. Iwaniec [3055].

A.A. Buhštab's result was generalized to the case of polynomials in algebraic number fields by H. Sarges [5397] (cf. J. Hinz [2823]).

For analogues of these results for binary forms $F \in \mathbf{Z}[X, Y]$ see G. Greaves¹⁶² [2331, 2332].

In another paper [5025] H. Rademacher extended Brun's method to algebraic number fields, and this enabled him to settle certain additive questions in this domain. An exposition of the early version of Brun's method (V. Brun [801]) was given in the first volume of Landau's textbook [3674].

Various classes of sieve, including the sieve of Brun, are described in the book by H. Halberstam and H.-E. Richert [2455].

¹⁶⁰Alexander Ostrowski (1893–1986), professor in Basel. See [1705, 3119].

¹⁶¹Giovanni Ricci (1904–1973), professor in Pisa and Milano. See [1292].

¹⁶²George Richard Herbert Greaves (1941–2008), professor in Cardiff.

2.4 Additive Problems

2.4.1 Sums of Squares

1. It was asserted by Fermat and proved by Euler that any prime congruent to unity mod 4 can be represented as the sum of two squares. An explicit formula (using character sums) for the summands occurring in such a representation was given in 1907 by E. Jacobsthal¹⁶³ [3084], and a similar result for the representation of primes $p \equiv 1 \pmod{6}$ by the form $x^2 + 3y^2$ was obtained by L. Schrutka von Rechtenstamm¹⁶⁴ [5569] in 1911. Earlier results giving explicit solutions of $x^2 + dy^2 = p$ for various values of d and primes p are described in [1545, Chap. 2].

Later similar results for other quadratic forms were obtained by S. Chowla ($x^2 + 27y^2 = 4p$ [1085]), A.L. Whiteman ($x^2 + 2y^2 = p$, $x^2 + 7y^2 = 4p$ [6651, 6652]) and B.W. Brewer ($x^2 + 5y^2 = p$ [723, 724]). The last author used the sums

$$\Lambda_n(p) = \sum_{x=0}^{p-1} \left(\frac{V_n(x)}{p} \right),$$

where the polynomials V_n are defined by

$$V_1(X) = X, \quad V_2(X) = X^2 - 2, \quad V_{n+2}(X) = xV_{n+1}(X) - V_n(X),$$

and are special cases of Dickson's polynomials of the first kind, defined by L.E. Dickson in his thesis [1535]. For the properties and applications of Dickson's polynomials see the monograph by R. Lidl, G.F. Mullen and G. Turnwald [3887].

The sum $\Lambda_n(p)$ is called the *Brewer sum* and was later investigated by several authors (see, e.g., A.L. Whiteman [6653, 6654], R.E. Giudici, J.B. Muskat, S.F. Robinson [2241], B.C. Berndt, R. Evans [450] and the book by B.C. Berndt, R. Evans and K.S. Williams [453]).

2. In the 19th century much work was done to find explicit formulas for $r_k(n)$, the number of representations of an integer n as the sum of k squares. Such formulas were provided for various small k by C.F. Gauss [2208, Sect. 291], C.G.J. Jacobi [3075, 3077, 3078], P.G. Dirichlet [1587], G. Eisenstein¹⁶⁵ [1709, 1710], L. Kronecker [3526, 3529], J. Liouville [3936], H. Minkowski [4318] and H.J.S. Smith [5833].

Elementary proofs of Jacobi's formulas were given much later by M.D. Hirschhorn [2827] for $k = 2$, and by J.A. Ewell [1942], M.D. Hirschhorn [2825], G.E. Andrews, S.B. Ekhad, D. Zeilberger [90] for $k = 4$.

This classical question was revived in the first decades of the 20th century. E.T. Bell [394] wrote that this was possibly due "to its connection with X-ray analyses of crystal structure," but this is a rather doubtful assertion. In 1907

¹⁶³Ernst Jacobsthal (1882–1965), professor in Berlin and Trondheim. See [5628].

¹⁶⁴Lothar Wolfgang Schrutka von Rechtenstamm (1881–1945), professor in Brno and Vienna.

¹⁶⁵Gotthold Eisenstein (1823–1852), worked in Berlin.

J.W.L. Glaisher [2248] presented his results concerning explicit formulas for $r_k(n)$ ($k = 2, 4, \dots, 18$) obtained with the use of modular forms¹⁶⁶, the details appearing in a series of papers in the *Quarterly Journal of Mathematics*. Similar formulas in the cases of $k = 3, 5, 7, 9$ and 11 were found in 1920 by E.T. Bell [394, 395]. Formulas for the number of representations of even numbers as sums of ten and twelve squares, stated by Liouville, were proved in 1907 by G. Humbert¹⁶⁷ [2947] and K. Petr¹⁶⁸ [4828] with the use of theta-functions. In the same year A. Hurwitz [2962] expressed $r_3(n^2)$ in terms of divisor functions, the case of $r_5(n^2)$ having been treated by him already in 1884 [2956]. In 1914 B. Boulyguine¹⁶⁹ [658, 839] gave formulas for $r_{2k}(n)$. A few years later L.J. Mordell [4375, 4377] applied modular forms to a study of $r_k(n)$ in the case when k is either a power of 2 or odd.

Modular forms were also later used to obtain explicit formulas for $r_k(n)$ (see, e.g., R.A. Rankin¹⁷⁰ [5119]). In 1965 R.A. Rankin [5120] proved that for $k \geq 9$, $r_k(n)$ cannot be expressed by divisor functions. The analogue of this result for representations of integers by an arbitrary quadratic form was obtained by G.P. Gogišvili [2254, 2255].

An elementary proof of Hurwitz's formula for $r_3(n^2)$ was given much later by J. Lagrange [3609]. Similar formulas for $r_k(n^2)$ for $k = 7, 9, 11$ and 13 were established by H.F. Sandham [5387, 5388]. In 1950 P.T. Bateman [351] proved that the function $r_k(n)/2k$ is multiplicative only for $k = 1, 2, 4$ and J. Lagrange [3609] showed in 1972 that $r_k(n^2)/2k$ is multiplicative if and only if $1 \leq k \leq 8$.

Exact formulas for an infinite sequence of k ($k = 4m^2$ and $k = 4m(m + 1)$) were given much later by S.C. Milne [4314, 4315] (cf. D. Zagier [6812], K. Ono [4684]).

2.4.2 The Waring Problem

1. The first great old problem in number theory which was settled in the 20th century was the celebrated *Waring problem*, which got its name from an English mathematician of the 18th century, E. Waring¹⁷¹. In 1770 he published a book *Meditationes Algebraicae* [6565] in which, among other questions, he considered the possibility of representing positive integers as sums of powers. He did not prove anything in this respect, but formulated an assertion which later became known as the Waring Problem. He wrote¹⁷²:

¹⁶⁶Later elementary proofs of these formulas have been found. See J.A. Ewell [1944], J.G. Huard, K.S. Williams [2941] and the book [4548] by M.B. Nathanson.

¹⁶⁷Marie Georges Humbert (1859–1921), professor in Paris, father of P. Humbert.

¹⁶⁸Karel Petr (1868–1950), professor in Prague.

¹⁶⁹Vasilii Vasilevič Bulygin [Boulyguine] (1888–1918).

¹⁷⁰Robert Alexander Rankin (1915–2001), professor in Birmingham and Glasgow. See [454].

¹⁷¹Edward Waring (1734–1798), professor in Cambridge.

¹⁷²We use the English translation by D. Weela [6565, Theorem 47, part 9].

“Every integer is a sum of two, three, . . . , nine cubes; every integer is also the square of a square, or the sum of up to nineteen such; and so forth. Similar laws may be affirmed for the correspondingly defined numbers or quantities of any degree.”

2. One denotes by $g(k)$ the smallest number of terms which are sufficient to represent any positive integer as the sum of k th powers of non-negative integers. Thus Waring’s assertion states that $g(3) = 9$, $g(4) = 19$ and usually one extrapolates his statement to the following form:

The number $g(k)$ is finite for every $k \geq 2$.

In the case $k = 2$ this question had been considered already by C. Bachet¹⁷³ and Fermat [1989, p. 307], and the corresponding theorem ($g(2) = 4$) had been established by J.L. Lagrange¹⁷⁴ [3610] in 1770. A similar problem was considered by Descartes, who in two letters to Mersenne [1477, 1478] stated that the only numbers which are not sums of four positive squares are $a \cdot 4^n$ for $a = 2, 6, 14, n = 0, 1, 2, \dots$ as well as 1, 3, 5, 9, 11, 17, 29 and 41. This was shown to be true as late as in 1911 by E. Dubouis [1633] and rediscovered by G. Pall [4727] in 1933 (Pall’s proof is reproduced in the book [5784] by W. Sierpiński). Dubouis also described positive integers which are not sums of a given number of positive squares.

Waring [6565] himself checked that every number up to 3 000 is the sum of nine cubes, and C.G.J. Jacobi arranged the checking at first up to 3 000 [6835], and then to 12 000 [3080]. This led him to conjecture that all large integers are sums of at most five positive cubes and every integer larger than 8 042 is the sum of at most six positive cubes. These conjectures are still open.

During the 19th century the values of $g(3)$, $g(4)$ and $g(5)$ were shown to be finite, and explicit bounds $g(3) \leq 21$, $g(4) \leq 41$ and $g(5) \leq 192$ were found by E. Maillet [4106], É. Lucas [4027] and E. Maillet [4107], respectively. They proved this by establishing various polynomial identities. For example, to prove the finiteness of $g(4)$ the following easily verified identity can be used:

$$6(x_1^2 + x_2^2 + x_3^2 + x_4^2)^2 = \sum_{1 \leq i < j \leq 4} (x_i + x_j)^4 + \sum_{1 \leq i < j \leq 4} (x_i - x_j)^4. \quad (2.55)$$

As, according to Lagrange, every positive integer is the sum of at most 4 squares, this identity shows that every number of the form $6n^2$ is the sum of at most 12 fourth powers, and, again using Lagrange’s result, one obtains that every multiple of 6 is the sum of at most 48 fourth powers. This implies the bound $g(4) \leq 53$. This argument is due to J. Liouville (see [3754]). Using essentially the same approach S. Realis¹⁷⁵ [5136] and É. Lucas [4026, 4027] reduced Liouville’s upper bound to

¹⁷³Claude Gaspar Bachet de Méziriac (1581–1638), lived in Bourg-en-Bresse.

¹⁷⁴Joseph Louis Lagrange (1736–1813), worked in Turin, Berlin and Paris.

¹⁷⁵Savino Realis (1818–1886), engineer in Turin. See [962].

47 and 41, respectively. In 1906 A. Fleck¹⁷⁶ [2012] modified this method and obtained $g(4) \leq 39$, and one year later E. Landau [3628] combined formula (2.55) with a careful investigation of 48 cases to get $g(4) \leq 38$. This was slightly improved by A. Wieferich¹⁷⁷ [6658] to $g(4) \leq 37$. In the same year he also considered [6659] the fifth and seventh powers, and established the bounds $g(5) \leq 59$ and $g(7) \leq 3\,806$. Later $g(5) \leq 58$ was proved by W.S. Baer [211].

For the next step one had to wait several years, when in 1933 L.E. Dickson [1556] proved $g(4) \leq 35$, earlier giving [1546] a new proof of Wieferich's bound.

Going in the opposite direction, A.J. Kempner¹⁷⁸ showed in his thesis [3298], that infinitely many integers require at least 16 biquadrates.

3. In the cubic case R.D. von Sterneck [5939] in 1903 extended Jacobi's check up to 40 000, and pointed out that every number in the interval (8 042, 40 000) can be written as the sum of six cubes. In 1906 A. Fleck [2012] reduced Maillet's bound to 13, and three years later A. Wieferich [6656] was able to confirm Waring's assertion in the cubic case, proving the equality $g(3) = 9$. His proof followed the ideas developed in the previous century, as it was based on the identity

$$\sum_{i=1}^3 ((y + x_i)^3 + (y - x_i)^3) = 6y(y^2 + x_1^2 + x_2^2 + x_3^2). \quad (2.56)$$

Actually Wieferich's proof was incomplete, as it omitted a rather long interval. This was pointed out by P. Bachmann [199] and repaired by A.J. Kempner [3298].

See [4538] for an exposition of Wieferich's argument modified by B. Scholz [5559]. Simpler proofs eliminating the use of numerical computations were later given by L.E. Dickson [1551] and E. Herzog [2772].

In [2013] A. Fleck gave the first proof of the finiteness of $g(6)$, establishing $g(6) \leq 2\,451$, and this was reduced to 970 by A.J. Kempner in 1912 [3298], and to 488 by W.S. Baer in 1913 [211]. The inequality $g(8) < \infty$ was established in 1908 by E. Maillet [4110], and the first explicit bound for this number ($g(8) \leq 36\,119$) was obtained by A. Hurwitz [2963] in the same year.

The next improvement came in 1927 when L.E. Dickson [1548] got $g(6) \leq 190$ and $g(8) \leq 2\,690$.

4. The year 1909 turned out to be rather good for the Waring problem as in that year E. Landau [3635] proved that all large integers can be represented as the sum

¹⁷⁶Albert Fleck (1861–1943), medical doctor, known for finding errors in purported proofs of Fermat's Last Theorem. See [5980].

¹⁷⁷Arthur Josef Alwin Wieferich (1884–1954), student of M. Dehn in Münster, schoolteacher.

¹⁷⁸Aubrey Kempner (1880–1973), professor at the University of Colorado in Boulder. Student of Minkowski, obtained his Ph.D. in Göttingen in 1909.

of 8 non-negative cubes¹⁷⁹ (another proof was later found by L.K. Hua [2915]), and D. Hilbert [2789] succeeded in establishing the essential part of Waring's assertion, proving the finiteness of $g(k)$ for every k .

Hilbert's proof was the culmination of previously applied methods being based on a rather complicated identity, found earlier by F. Hausdorff¹⁸⁰ [2614], involving an integral in 25-dimensional real space. Later work by F. Hausdorff [2615], E. Schmidt [5475], E. Stridsberg¹⁸¹ [5969], G. Frobenius [2117] and R. Remak¹⁸² [5157] simplified Hilbert's reasoning.

Hilbert's approach to the Waring problem is now only of historic interest since newer methods are much simpler and lead to better bounds for the number of summands. It was later shown by G.J. Rieger [5216] that Hilbert's proof gives the bound

$$g(k) \leq (2k+1)^{260^{A(k)}}$$

with

$$A(k) = (k+3)^{3k+8},$$

whereas it is now known that for large k one has

$$g(k) = \left\lceil (3/2)^k \right\rceil + 2^k - 2,$$

which is of much smaller order (K. Mahler [4088]). For expositions of Hilbert's approach see [1754] and [4538].

5. The minimal number of non-negative k th powers needed to represent every sufficiently large integer is denoted by $G(k)$. Already in 1908 A. Hurwitz [2963] and E. Maillet [4110] had proved the lower bound $G(k) \geq 1+k$ which has not been improved since, except for certain classes of k (see Sect. 3.2.1). As no number congruent to 7 mod 8 is the sum of three squares, the theorem of Lagrange implies $G(2) = 4$, and Landau's result in [3635] gives $G(3) \leq 8$. On the other hand one has $G(3) \geq 4$, as no number congruent to ± 4 mod 9 is the sum of three cubes.

Landau's bound has not been improved for several years. In 1943 Yu.V. Linnik ([3906], cf. [3931]) established $G(3) \leq 7$, which still holds the record. The proof was based on his previous results on representations of integers by ternary quadratic forms [3901]. It was pointed out by G. Pall [4729] that the argument in [3901] is incomplete, but can be corrected. A simpler proof, using the Siegel–Walfisz theorem on primes in progressions, was presented by G.L. Watson¹⁸³ [6578]. Another proof, due to R.C. Vaughan, can be found in [6360, 6361]. Later, effective proofs were found by R.J. Cook [1242], K.S. McCurley [4223], H. Kadirı [3210] and O. Ramaré [5093, 5094]. In the last paper it is shown that every integer $n > \exp(524)$ is the sum of at most 7 cubes. One expects that this happens already for

¹⁷⁹Actually 23 and 239 are the only positive integers which are not of that form (L.E. Dickson [1567]).

¹⁸⁰Felix Hausdorff (1869–1942), professor in Leipzig and Bonn. See [727].

¹⁸¹Eric Stridsberg (1871–1950), worked in an insurance company.

¹⁸²Robert Remak (1888–1942), student of Frobenius, worked in Berlin. See [4262].

¹⁸³George Leo Watson (1909–1988), professor at University College, London.

$n > 455$. It was proved by J. Brüdern [773] that the summands could be taken to have at most 69 prime divisors, and later 69 was replaced by 4 by K. Kawada [3286].

Vaughan's paper [6360, 6361] also contains an asymptotic formula for the number of representations of an integer N as the sum of 8 positive cubes, its main term being $cN^{5/3}$, and also a lower bound of order $N^{4/3}$ in the case of 7 cubes.

In 1926 A.E. Western [6637] after doing some numerical experiments conjectured that all integers $\geq 10^{14}$ are sums of at most 4 cubes, thus $G(3) = 4$, and his conjecture was made more precise by J.-M. Deshouillers, F. Hennecart and B. Landreau [1493], who believe that there are exactly 113 936 676 integers which are not sums of four cubes, the largest being 7 373 170 279 850.

It was shown in 1939 by H. Davenport [1356] that the number of $n \leq x$ which are not sums of 4 cubes is $O(x^c)$ for every $c > 29/30$. Denote by α the largest lower bound for the value of c in this result. In 1986 R.C. Vaughan [6360, 6361] proved $\alpha \leq 103/115 = 0.895\dots$, then J. Brüdern [769, 772] improved this first to $\alpha \leq 131/147 = 0.891\dots$, and then to $\alpha \leq 37/42 = 0.8809\dots$, and T.D. Wooley [6728] got $\alpha \leq 0.8808$.

R.C. Vaughan [6365, 6366] proved in 1989 that the number of integers $n \leq x$ which are sums of four positive cubes is $\gg x^\beta$ for every $\beta < 11/12 = 0.9167$, and this was later improved by T.D. Wooley [6728, 6735] to any $\beta < 0.91681$ and $\beta < 0.91686$.

It has been conjectured that the number $N_k(x)$ of integers $\leq x$ which are sums of three positive k th powers is of order $x^{3/k}$ for $k \geq 3$. The best known lower bound,

$$N_k(x) \gg x^{3/k - \exp(-k/17)}$$

is due to T.D. Wooley [6728], who improved earlier results by R.C. Vaughan [6365, 6366].

In the case of biquadrates, the inequality $G(4) \geq 16$ obtained by A.J. Kempner [3298] was turned into equality by H. Davenport [1354] in 1939. In 2000 J.-M. Deshouillers, F. Hennecart and B. Landreau [1488] showed that every integer between 13 793 and 10^{245} is the sum of at most 16 fourth powers. Five years later J.-M. Deshouillers, K. Kawada and T.D. Wooley [1494] proved that the maximal integer which is not a sum of 16 fourth powers equals 13 792.

2.5 Diophantine Approximations

2.5.1 Approximation by Rationals, Theorem of Thue

1. The first result dealing with approximations of real numbers by rationals goes back to Dirichlet who proved in 1842, in a paper concerning continued fractions [1589], that for every real α and $N = 1, 2, \dots$ one can find a rational p/q with $q \leq N$ and

$$\left| \alpha - \frac{p}{q} \right| \leq \frac{1}{qN}.$$

He showed, more generally, that for any given reals $\alpha_1, \dots, \alpha_n$ and $N \geq 1$, one can find integers q_1, \dots, q_n satisfying

$$1 \leq \max\{|q_1|, \dots, |q_n|\} \leq N,$$

and

$$\left\| \sum_{j=1}^n \alpha_j q_j \right\| < \frac{1}{N^n}.$$

In 1850 C. Hermite [2761] showed the existence of a constant c depending only on n such that if $\alpha_1, \dots, \alpha_n$ are distinct real numbers, then for infinitely many positive integers q there exist $b_1, \dots, b_n \in \mathbf{Z}$ such that

$$\left| \alpha_j - \frac{b_j}{q} \right| \leq \frac{c}{q^{1+1/n}}. \quad (2.57)$$

This was also proved by L. Kronecker [3530] in 1884, and in 1903 É. Borel¹⁸⁴ [636] showed that the exponent $1 + 1/n$ is best possible. Borel's paper contains the first explicit use of the notion of the height of a rational number.

An effective version of the last result was given by A.K. Lenstra, H.W. Lenstra, Jr. and L. Lovász [3819] in 1982, as a corollary to their polynomial-time algorithm to find a nearly orthogonal basis of a lattice in \mathbf{R}^n . For other applications of this algorithm to Diophantine approximations see R. Tijdeman [6161].

2. Let $c(n)$ denote the greatest lower bound of possible values of c in (2.57). H. Minkowski proved in his book [4324] that $c(n) \leq n/(n+1)$ and this was slightly strengthened by H.F. Blichfeldt¹⁸⁵ [557]. The equality $c(1) = \sqrt{5}$ had been established already in 1891 by A. Hurwitz [2958], but for $n \geq 2$ the exact value of $c(n)$ is not known. Minkowski in [4325] established the bound $c(2) \leq \sqrt{8/19} = 0.6488 \dots$

Later the inequality $c(2) \geq 1/\sqrt[4]{23} = 0.4566 \dots$ was proved by P. Furtwängler¹⁸⁶ [2165, 2166], who confirmed an earlier assertion by H.F. Blichfeldt [558]. It is conjectured that $c(2) = \sqrt{2/7} = 0.5345 \dots$. For numerical investigation in the case $n = 3$ see G. Szekeres¹⁸⁷ [6020].

In 1921 O. Perron [4787] obtained the first lower bound for $c(n)$ of the order $1/(n2^n)$. Later P. Furtwängler [2165, 2166] strengthened Perron's bound and his result was improved in 1985 by S. Krass [3513].

3. The result proved in 1851 by J. Liouville in [3934] went in another direction. He proved the following assertion, which allowed him to construct several transcendental numbers.

If α is a real algebraic number of degree $n \geq 2$, then for every rational p/q one has

$$\left| \alpha - \frac{p}{q} \right| > \frac{C}{q^n}, \quad (2.58)$$

where C is a positive constant, depending only on α .

The proof is a simple consequence of the mean value theorem. The analogue of Liouville's result for approximations of algebraic numbers by algebraic numbers of lower degree was given in 1910 by É. Borel in his book [638].

¹⁸⁴Émile Borel (1871–1956), professor in Paris. See [1183, 2070].

¹⁸⁵Hans Frederick Blichfeldt (1873–1945), professor at Stanford. See [1568].

¹⁸⁶Philipp Furtwängler (1869–1940), professor in Bonn, Aachen and Vienna. See [2846, 2942].

¹⁸⁷György Szekeres (1911–2005), worked in chemical industry in Budapest and Shanghai, professor at Macquarie University. See [2238].

Liouville's theorem has subsequently been improved. The first such result is due to A. Thue¹⁸⁸ [6142], who proved¹⁸⁹ that if α is algebraic of degree $n \geq 2$, then for all rational integers $q > 0$, p one has

$$\left| \alpha - \frac{p}{q} \right| \geq \frac{c(\alpha, \varepsilon)}{q^t} \quad (2.59)$$

for $t = n/2 + \varepsilon$ with arbitrary $\varepsilon > 0$ and positive $c(\alpha, \varepsilon)$. In the special case when α is an n th root of a rational number, Thue had established this result earlier [6141].

4. Thue's result had important applications to the theory of Diophantine equations and to multiplicative properties of polynomials. It implied in particular that the maximal prime divisor of $(ax + b)(cx + d)$ (where $a, b, c, d \in \mathbf{Z}$, $ad \neq bc$ and $ac \neq 0$) tends to infinity with x . Later G. Pólya [4954] showed that the same holds for all irreducible quadratic polynomials. This was a rather far generalization of an old result of C. Størmer¹⁹⁰ [5961], who established this in 1898 for the polynomials $x^2 + x$, $x^2 + 2x$ and $x^2 + 1$. For later developments see Sect. 3.1.4.

In his thesis [5738], C.L. Siegel gave a strengthening of Thue's result, replacing in (2.59) the exponent $t = d/2 + \varepsilon$ by $2\sqrt{d}$. He used this to prove Pólya's assertion for every polynomial over \mathbf{Z} with at least two distinct zeros, and also gave an extension to algebraic number fields. Siegel [5741] also discovered another consequence of Thue's theorem by proving that if u_n is a recurring sequence of rationals of order 3, defined by

$$u_{n+3} = Pu_{n+2} - Qu_{n+1} + u_n,$$

with integral P, Q , then apart from six explicitly given cases the equation

$$u_n = 0 \quad (2.60)$$

can have at most a finite number of solutions. A similar result was proved by M. Ward¹⁹¹ [6561] for linear recurrences of order 4. Much later it was shown by S.J. Scott [5588] that if the polynomial $X^3 - PX^2 + QX - 1$ has a negative discriminant and non-zero roots, then there are at most three solutions (under stronger assumptions this was proved earlier by M. Ward [6564] and M.F. Smiley [5830]).

In 1934 T. Skolem¹⁹² [5806] showed that if u_n is a linear recurrence in \mathbf{Q} , then the set of integers n satisfying (2.60) forms a union of finitely many (possibly zero) arithmetical progressions and a finite set. This was generalized in 1935 to algebraic number fields by K. Mahler [4078] and to arbitrary fields of zero characteristic by C. Lech [3756] in 1953 (the *Skolem–Mahler–Lech theorem*). This result fails for fields of positive characteristics (C. Lech [3756]), but an analogue of it was established in this case in 2007 by H. Derksen [1475].

¹⁸⁸Axel Thue (1863–1922), professor in Oslo.

¹⁸⁹For comments on Thue's work on Diophantine approximations and Diophantine equations see [5773].

¹⁹⁰Frederik Carl Størmer (1874–1957), professor in Oslo. See [804].

¹⁹¹Morgan Ward (1901–1963), professor at Caltech. See [3792].

¹⁹²Thoralf Albert Skolem (1887–1963), professor in Oslo and Bergen. See [4518].

In the same paper [4078] K. Mahler proved that if

$$u_{n+k} = \sum_{j=0}^{k-1} A_j u_{n+j}$$

is a linear recurrence with coefficients in an algebraic number field K , which is non-degenerate, i.e., the roots and ratios of roots of its companion polynomial

$$P(X) = X^k - \sum_{j=0}^{k-1} A_j X^j \quad (2.61)$$

are not roots of unity, then $|u_n|$ tends to infinity, hence the equation

$$u_n = c \quad (2.62)$$

can have only finitely many solutions.

In the case $k = 2$, M. Ward conjectured that for a non-degenerate linear recurrence with integral terms equation (2.62) can have at most five solutions. In 1973 R. Alter and K.K. Kubota [61] proved the conjecture in the case when $(M, N) = 1$, and four years later K.K. Kubota [3553–3555] established it in all cases. Later F. Beukers [483] showed that apart from finitely many cases, which can be explicitly listed, the equation $u_N = \pm c$ can have at most 3 solutions. Kubota [3555] also obtained an upper bound depending only on the degree N of the field K , containing all elements u_n . This was made more precise by F. Beukers and R. Tijdeman [493], who showed that in this case there are at most $100 \max\{300, N\}$ solutions (for the rational field they got the bound 29).

In 1984 J.-H. Evertse [1923] showed that if u_n is a non-degenerated linear recurrence of any order with algebraic terms and not of the form $u_n = a\zeta^n$ with a root of unity ζ , then there can be only finitely many pairs m, n with $u_m = u_n$. For sequences lying in an algebraic number field, explicit bounds for the number of solutions of (2.62) were given by A.J. van der Poorten¹⁹³ and H.-P. Schlickewei [6305] (for $c = 0$) and Schlickewei [5468] (any c).

It was conjectured that for a non-degenerate recurrent complex sequence of order k the number of solutions of (2.62) with $c = 0$ is bounded by a value depending only on k . For rational sequences this was established in 1996 by H.P. Schlickewei [5469], who in the case $k = 3$ proved this also for complex sequences [5470]. In this case the bound does not exceed 61 (F. Beukers, H.P. Schlickewei [492]). In the case when the companion polynomial has only simple zeros the conjecture was established by J.-H. Evertse, H.P. Schlickewei and W.M. Schmidt [1940] with the explicit bound $\exp((6k)^{3k})$. They also obtained an effective version of the Skolem–Mahler–Lech theorem in this case. In the general case the conjecture was proved in 1999 by W.M. Schmidt [5526] with the bound $\exp \exp \exp(3k \log k)$. This bound has subsequently been reduced to somewhat smaller numbers $\exp \exp \exp(20k)$ (W.M. Schmidt [5527]) and $\exp \exp(k^{\sqrt{11k}})$ (P.B. Allen [55]). See also H.P. Schlickewei [5468–5470] and A.J. van der Poorten, H.P. Schlickewei [6305].

5. It was shown by Čebyšev [971] in 1868 that if α is irrational and β is not an integer, then for infinitely many integers q one has

$$\|\alpha q - \beta\| < \frac{c}{|q|}$$

¹⁹³ Alfred Jacobus van der Poorten (1942–2010), professor at Macquarie University.

with $c = 1/2$. Hermite [2765] in 1879 proved this with $c = \sqrt{2/27} = 0.272\dots$, and in 1896 Minkowski [4323] showed that one can take $c = 1/4$. It was later proved by J.H. Grace¹⁹⁴ [2296] that this is best possible.

In 1946 A.J. Khintchine¹⁹⁵ [3326] considered the function $M(\alpha)$, defined as the least upper bound (taken over $\beta \in \mathbf{R}$, not of the form $\beta = m\alpha + n$ with integral m, n) of

$$\liminf_{q \rightarrow \infty} q \|q\alpha + \beta\|.$$

He proved the bound

$$M(\alpha) \leq \frac{1}{4} (1 - 2\lambda(\alpha)^2)^{1/2},$$

where

$$\lambda(\alpha) = \liminf_{q \rightarrow \infty} q \|q\alpha\|.$$

6. For irrational $\alpha > 0$ let p_n/q_n be the n th convergent of the continued fraction of α , and define the sequence λ_n by

$$\left| \alpha - \frac{p_n}{q_n} \right| = \frac{1}{\lambda_n q_n^2}. \quad (2.63)$$

It was proved by A. Hurwitz [2958] in 1891 that the inequality $\lambda_n > \sqrt{5}$ holds for infinitely many n . This result was made more precise by É. Borel [635, 636], who in 1903 showed that the inequality

$$\max\{\lambda_{n-2}, \lambda_{n-1}, \lambda_n\} > \sqrt{5} \quad (2.64)$$

holds for every n . The inequality

$$\max\{\lambda_{n-1}, \lambda_n\} > 2$$

had been known earlier (T. Vahlen [6257]).

Borel's result was generalized in 1950 by N. Obreškov¹⁹⁶ [4652], who showed that if $[a_0; a_1, a_2, \dots]$ is the continued fraction of α , then the left-hand side of (2.64) exceeds $\sqrt{a_n^2 + 4}$ (cf. F. Bagemihl and R.C. McLaughlin [216]). For $s = 2$ this had been proved earlier by M. Fujiwara¹⁹⁷ [2139, 2140] and G. Humbert [2948]. A very simple proof of Borel's theorem was provided in 1963 by H.G. Forder [2040], and one year later A.L. Schmidt [5473] gave simple proofs for the theorems of Borel and Fujiwara–Humbert. The mean value $M_N(\alpha) = \frac{1}{N} \sum_{j=1}^N \lambda_j$ was studied in 1949 by A. Brauer and N. Macon [683, 684], who established $M_N(\alpha) \geq \sqrt{5}$.

¹⁹⁴John Hilton Grace (1873–1922), worked in Cambridge. See [6182].

¹⁹⁵Aleksandr Jakovlevič Khintchine [Hinčin] (1894–1959), professor in Moscow. See [2252].

¹⁹⁶Nikola Obreškov (1896–1963), professor in Sofia. See [6195].

¹⁹⁷Matsusaburo Fujiwara (1881–1946), professor at Tōhoku University. See [3556].

For real α put $M(\alpha) = \limsup \lambda_n$, with λ_n defined in (2.63). It was shown in 1921 by P.J. Heawood¹⁹⁸ [2673] that the inequality $M(\alpha) < 3$ holds only for certain quadratic irrationalities, whereas there exist uncountably many α 's with $M(\alpha) = 3$. In the same year O. Perron [4788] showed that the distinct values of $M(\alpha) < 3$ form a sequence and determined the first 11 of its elements¹⁹⁹: $\sqrt{5}$, $\sqrt{8}$, $\sqrt{211}/5$, $\sqrt{1517}/13$, \dots . This has been also established independently by K. Shibata [5688]. This sequence arises also in A.A. Markov's [4153, 4154] theory of indefinite quadratic forms (see the monograph [1310] by T.W. Cusick and M.E. Flahive).

7. In a paper by Jacobi [3081] (published posthumously by E. Heine²⁰⁰ in 1868) a generalization of the continued fraction algorithm was proposed. This algorithm was later studied by P. Bachmann [197], and in 1907 O. Perron [4783] published a large paper in which he essentially generalized Jacobi's approach. The algorithm consists of iterations of the mapping T defined in the following way: if $u = (x_1, \dots, x_n)$ is an n -tuple of positive real numbers, and x_s is the smallest of them, then for $i = 1, 2, \dots, n$ write $x_i = A_i x_s + y_i$ with integral A_i and $0 \leq y_i < x_s$, and put $T : u \mapsto (y_1, \dots, y_n)$. This algorithm can be used to determine the greatest common divisor of n given positive integers and to find units in algebraic number fields (see L. Bernstein, H. Hasse [468] and the book by L. Bernstein [467]).

A broad exposition of the theory of continued fractions was published in 1913 by O. Perron [4785].

The history of continued fractions up to 1939 has been written by C. Brezinski [725], who also prepared a complete bibliography [726] on that subject. The theory of numbers with bounded partial quotients (with a bibliography of over 300 items) was surveyed in 1992 by J. Shallit [5670].

8. The first results dealing with the approximation of complex numbers by ratios of integers from a fixed imaginary quadratic field appear in the papers of C. Hermite [2762] and A. Hurwitz [2957] as well as in Minkowski's book [4324, Sect. 39]. In particular, Hermite showed that for every complex z there are infinitely many distinct pairs of co-prime integers a, b of the field $\mathbf{Q}(i)$ with

$$\left| z - \frac{a}{b} \right| < \frac{1}{c|b|^2}$$

with $c = \sqrt{2}$, and Hurwitz proved the analogous result for the field $\mathbf{Q}(\sqrt{-3})$. Minkowski showed that in the case of the field $\mathbf{Q}(i)$ one can replace here $\sqrt{2}$ by $\pi/\sqrt{6}$, but left open the question of whether this constant is optimal. In 1925 L.R. Ford²⁰¹ [2039] showed that this is not the case, the optimal value being $\sqrt{3}$ (cf. [2038]). Ford's result was rediscovered a few years later in 1930 by O. Perron [4789, 4790].

¹⁹⁸Percy John Heawood (1861–1955), professor in Durham. See [1581].

¹⁹⁹The first two terms were known already to Hurwitz [2958].

²⁰⁰Heinrich Eduard Heine (1821–1881), professor in Bonn and Halle.

²⁰¹Lester Randolph Ford (1886–1967), professor at the Illinois Institute of Technology.

Most of these results were obtained with the use of various kinds of continued fractions for complex numbers.

Later Perron [4792] extended Hurwitz's result to all imaginary quadratic fields $\mathbf{Q}(\sqrt{-D})$. The least upper bound of possible values of the corresponding constant c , say $c(D)$, is called the *Hurwitz constant* of the field K , thus Ford's result gives $c(1) = \sqrt{3}$. The value of $c(D)$ is known only in the following cases: $c(2) = \sqrt{2}$ (O. Perron [4792]), $c(3) = \sqrt[4]{13}$ (O. Perron [4791]), $c(5) = c(6) = 1$ (L.J. Vulakh [6485]), $c(7) = \sqrt[4]{8}$ (N. Hofreiter²⁰² [2844]), $c(11) = \sqrt{5}/2$ (R. Descombes, G. Poitou²⁰³ [1479]), $c(15) = \sqrt{2}$ (L.J. Vulakh [6486]), $c(19) = 1$ (G. Poitou [4939]). This constant is related to the geometry of fundamental domains of Fuchsian groups (see, e.g., R.A. Rankin [5116], L.J. Vulakh [6484, 6485]).

2.5.2 Uniform Distribution

1. At the International Congress of Mathematicians held in Cambridge in 1912, G.H. Hardy and J.E. Littlewood [2519] announced a far reaching generalization of the following result, due essentially to Kronecker, concerning the distribution of fractional parts of sequences of the form $u_n = n\alpha$ for irrational α .

If the real numbers $1, \alpha_1, \dots, \alpha_N$ are linearly independent over the rationals, and β_1, \dots, β_N are arbitrary reals, then for every $\varepsilon > 0$ the system of inequalities

$$|y\alpha_j + \beta_j - x_j| < \varepsilon \quad (j = 1, 2, \dots, N)$$

is solvable with integral y, x_1, \dots, x_N .

They applied the results of A. Pringsheim²⁰⁴ [5011] and F. London [3987], dealing with limits of double sequences, to prove that if $\theta_1, \dots, \theta_n$ are irrational real numbers, linearly independent over the rationals, then for any given numbers $0 \leq \alpha_{ij} < 1$ ($i, j = 1, 2, \dots, n$) one can find a sequence n_1, n_2, \dots of integers such that

$$\lim_{r \rightarrow \infty} \{n_r^i \theta_j\} = \alpha_{ij}$$

holds for $i, j = 1, 2, \dots, n$.

The proof appeared in [2520]. There is also a proof there of the assertion that if λ_n is any sequence tending to infinity, then for almost all real θ the set $\{\{\theta\lambda_n\} : n = 1, 2, \dots\}$ is dense in the interval $(0, 1)$. This may fail for some irrational θ . Indeed, Hardy and Littlewood showed in [2519] that there exist irrational numbers θ such that the sequence $\{2^n\theta\}$ is not dense in the unit interval. This led to the question of existence of numbers α for which the sequence $\{q^n\alpha\}$ (with a certain integral $q > 1$) tends to zero. The answer was given by Hardy, who proved in [2510] that if

²⁰²Nikolaus Hofreiter (1904–1990), professor in Vienna. See [2836].

²⁰³Georges Poitou (1926–1989), professor in Paris. See [3215].

²⁰⁴Alfred Pringsheim (1850–1941), professor in Munich. See [4795].

$\alpha > 1$ is an algebraic integer then it has this property if and only if all its remaining conjugates lie in the interior of the unit circle. Such numbers have several peculiar properties, and are known under the name of *Pisot–Vijayaraghavan numbers*²⁰⁵, or *PV-numbers*, since Hardy's result was later rediscovered by C. Pisot²⁰⁶ [4916, 4917] and T. Vijayaraghavan²⁰⁷ [6391–6394]. Actually this characterization of *PV*-numbers was proved for the first time in 1912 by A. Thue [6143] in a paper unknown to Hardy, Pisot and Vijayaraghavan.

C. Pisot [4916] and T. Vijayaraghavan [6391–6394] independently obtained certain characterizations of *PV*-numbers. One of them states that $a > 1$ is a *PV*-number if and only if for some real $\lambda \neq 0$ the series

$$\sum_{n=1}^{\infty} \|\lambda a^n\|^2$$

is convergent. R. Salem²⁰⁸ [5373] proved that the set S of all *PV*-numbers is closed and nowhere dense, as conjectured in [6392]. In the same paper he studied algebraic integers $a > 1$ all of whose remaining conjugates lie in the closed unit circle and which are not *PV*-numbers. They are now called *Salem numbers*. It turned out later that *PV*- and Salem numbers play an important role in harmonic analysis (see R. Salem [5371, 5372] and the book by Y. Meyer [4282]).

The two smallest *PV*-numbers were found by C.L. Siegel [5765] (they are the positive roots of $X^3 - X - 1$ and $X^4 - X^3 - 1$). He conjectured that $\theta = (1 + \sqrt{5})/2$ is the smallest limit point of the set of *PV*-numbers, and this was later established by J. Dufresnoy and C. Pisot [1635], who in [1636–1638] found all *PV*-numbers smaller than θ .

The book by M.J. Bertin, A. Decomps-Guilloux, M. Grandet-Hugot, M. Pathiaux-Delefosse and J.-P. Schreiber [470] gives a broad account of the theory of *PV*-numbers and Salem numbers.

2. In 1914 H. Weyl²⁰⁹ [6646, 6647] introduced the notion of uniform distribution mod 1 of real sequences.

A sequence x_1, x_2, \dots of elements in the interval $[0, 1)$ is called *uniformly distributed*²¹⁰ mod 1, provided for every $0 \leq a < b \leq 1$ one has

$$\lim_{N \rightarrow \infty} \frac{\#\{n \leq N : a \leq x_n < b\}}{N} = b - a. \quad (2.65)$$

²⁰⁵This name was introduced by R. Salem [5371, 5372].

²⁰⁶Charles Pisot (1910–1984), professor in Bordeaux and Paris. See [66].

²⁰⁷Tirukkannapuram Vijayaraghavan (1902–1955), professor at Andhra University and Director of the Ramanujan Institute in Madras. See [1369].

²⁰⁸Raphael Salem (1898–1963), professor at MIT and in Paris.

²⁰⁹Hermann Weyl (1885–1955), professor at ETH in Zürich, Göttingen and Princeton. See [1053, 4540, 4589].

²¹⁰In [6646] Weyl did not use the term *uniform distribution*, calling this property *gleichmäßig dicht*, i.e., *uniformly dense*.

Weyl proved that a sequence (x_n) has this property if and only if for every non-zero integer m one has

$$\sum_{n=1}^N \exp(2\pi i m x_n) = o(N). \quad (2.66)$$

This is the original *Weyl criterion*. This name is nowadays usually attached to uniform distribution in compact Abelian groups G , where it takes the form

$$\sum_{n=1}^N \chi(x_n) = o(N)$$

for every character $\chi \neq 1$ of G .

In 1948 P. Erdős and P. Turán [1866, 1867] obtained a bound (the *Erdős–Turán inequality*) for the difference

$$\frac{\#\{n \leq N : a \leq x_n < b\}}{N} - (b - a)$$

in the case of a finite sequence x_n (cf. J.D. Vaaler [6256]). This result was later generalized to sequences in \mathbf{R}^n (see J.F. Koksma²¹¹ [3446], T. Cochrane [1131], P.J. Grabner, R.F. Tichy [2295]).

Weyl's criterion implies in particular that for every irrational real number α the sequence $\{n\alpha\}$ is uniformly distributed mod 1, a fact earlier proved independently by P. Bohl²¹² [575], H. Weyl [6645] and W. Sierpiński [5782]. This strengthened an old result by Kronecker [3530] which implied that for irrational α the sequence $\{n\alpha\}$ is dense in $[0, 1]$.

A simple heuristical argument shows that for irrational α the sum $\sum_{k \leq N} \{k\alpha\}$ should be close to $N/2$. The difference

$$C_\alpha(N) = \sum_{k \leq N} \{k\alpha\} - \frac{N}{2} \quad (2.67)$$

was considered by C. Størmer [5962] and M. Lerch [3836] in 1904, who showed that if α is irrational and has bounded partial quotients, then $C_\alpha(N) = O(\log N)$ (cf. A. Ostrowski [4708]).

G.H. Hardy and J.E. Littlewood [2528, 2529] showed later that for any irrational α one has $|C_\alpha(t)| \geq c \log t$ infinitely often, and A. Ostrowski [4708] obtained this with $c = 1/720$. In 1995 T.C. Brown and P.J.-S. Shiue [755] showed that one can take $c = 1/256$. In 1957 V.T. Sós [5848] showed that $C_\alpha(t)$ may be bounded from one side. For the use of Dirichlet series in this question see E. Hecke [2682].

²¹¹Jurjen Ferdinand Koksma (1904–1964), professor in Amsterdam. See [3570].

²¹²Piers Bohl (1865–1921), professor in Riga. See [3404].

3. To apply his criterion to polynomial sequences H. Weyl needed evaluations of exponential sums of the form

$$S_f(N) = \sum_{n=1}^N \exp(2\pi i f(n)), \quad (2.68)$$

where $f(X) = a_M X^M + \cdots + a_0$ is a polynomial with real coefficients, of which at least one, distinct from a_0 , is irrational. Such sums are now called *Weyl sums*.

Assuming that the leading coefficient a_M of f is irrational, writing

$$|S_f(N)|^2 = \sum_{m=1}^N \sum_{n=1}^N \exp(2\pi i (f(m) - f(n))),$$

and putting $m = n + r$, Weyl got

$$f(m) - f(n) = r M a_M r^{M-1} + \cdots = r g(r, n),$$

where g is a polynomial in r with integral coefficients of degree $M - 1$, and this allowed him to reduce the problem to the case of linear polynomials, which can be settled elementarily. This led to

$$|S_f(N)| \ll N^{1+\varepsilon} \left(N^{-t} + q^{-t} + \left(\frac{N^M}{q} \right)^{-t} \right),$$

where $t = 1/2^{M-1}$ and q is the denominator of a rational approximation r to the leading coefficient a_M of f , satisfying the condition

$$|a_M - r| \leq 1/q^2.$$

This bound implies the asserted uniform distribution mod 1 of the sequence of consecutive polynomial values. Independently the same result was obtained by G.H. Hardy and J.E. Littlewood [2520, 2521].

In 1928 I. Schoenberg²¹³ [5546] gave a generalization considering arbitrary continuous distributions of sequences of real numbers in the unit interval. He obtained an analogue of Weyl's criterion, applied it to prove the existence of the limit

$$F(t) = \lim_{x \rightarrow \infty} \frac{1}{x} \# \left\{ n \leq x : \frac{\varphi(n)}{n} \leq t \right\}$$

(φ being Euler's function), and this implied the existence of a distribution function for the additive function $\log(\varphi(n)/n)$.

H. Weyl proved also in [6647] that for every sequence $0 < \lambda_1 < \lambda_2 < \cdots$ of integers the sequence $\lambda_n x$ is uniformly distributed mod 1 for almost all x .

²¹³Isaac Jacob Schoenberg (1903–1990), professor at the Universities of Pennsylvania and Wisconsin. See [153].

It is not always easy to find a number x having this property. The first effective example in the case $a_n = n!$ was given in 1950 by N.M. Korobov²¹⁴ [3485]:

$$x = x_c = \sum_{k=1}^{\infty} \frac{[k^c]}{k!}$$

for every $c \in (1, 2)$.

If λ_n is a lacunary sequence of positive reals (i.e., $\lambda_{n+1}/\lambda_n \geq c > 1$), then there are irrationals θ such that the sequence $\{\lambda_n \theta\}$ is not dense in $(0, 1)$, hence not uniformly distributed (we have noted already that this has been observed for $\lambda_n = 2^n$ by G.H. Hardy and J.E. Littlewood [2519]). This was shown in 1979 by A.D. Pollington [4947], who answered a question from P. Erdős [1824] (for sequences with $c \geq 5^{1/3}$ this had been proved earlier by E. Strzelecki [5978]). B. de Mathan [4186] proved later that the set of such θ 's has Hausdorff dimension one. The *Hausdorff dimension* of a set A of reals was introduced by Hausdorff in [2617] in the following way.

For $r > 0$ let $\mu^r(A)$ be the largest lower bound of the sums

$$\sum_n |I_n|^r,$$

where I_n is a sequence of intervals whose union contains A . The number ρ with the property

$$\mu^r(A) = \begin{cases} 0 & \text{if } r > \rho, \\ \infty & \text{if } r < \rho \end{cases}$$

is called the Hausdorff dimension of A . Cf. A.S. Besicovitch²¹⁵ [475] and the book [5255] by C.A. Rogers²¹⁶.

Weyl's sums turned out to be of importance in several arithmetical problems. In particular they were applied to evaluations of the zeta-function, the distribution of primes, the Waring problem and Diophantine approximations.

Stronger bounds for Weyl sums were later obtained by I.M. Vinogradov [6422, 6428, 6436, 6447] and Yu.V. Linnik [3908]. See L.K. Hua [2938] and G.I. Arkhipov, A.A. Karatsuba²¹⁷, V.N. Čubarikov [123, 124] for surveys. For later improvements see E. Bombieri, H. Iwaniec [615, 616], E. Bombieri [604], L.D. Pustynnikov [5018], M.N. Huxley, G. Kolesnik [2991], M.N. Huxley [2984].

4. H. Weyl considered also sums of the form

$$S_f(p) = \sum_{j=0}^{p-1} \exp\left(\frac{2\pi i f(x)}{p}\right)$$

²¹⁴Nikolai Mikhailovič Korobov (1917–2004), professor in Moscow. See [4616].

²¹⁵Abram Samoilovič Besicovitch (1891–1970), professor in Perm, Petrograd (Leningrad) and Cambridge. See [6090].

²¹⁶Claude Ambrose Rogers (1920–2005), professor in Birmingham and at University College London.

²¹⁷Anatolij Alekseevič Karatsuba (1937–2008), professor in Moscow. See [120].

with prime p , where $f \in \mathbf{Z}[X]$ is of degree n and not all of its coefficients are divisible by p . He obtained the bound

$$|S_f(p)| = O(p^c), \quad (2.69)$$

for any $c > 1 - 1/2^{n-1}$. In the case $n = 2$ one has $|S_f(p)| = \sqrt{p}$, by reduction to quadratic Gauss's sums. This bound was later improved by L.J. Mordell [4382] (for further development see Sect. 4.1.1).

5. A real number a is called *simply normal* with respect to an integer $q \geq 2$ if in the q -expansion of a every digit occurs with the same frequency. A number which is normal with respect to every q is called *absolutely simply normal*. Note that in earlier literature these numbers were called *normal* and *absolutely normal*, respectively. Now a number θ is said to be normal with respect to q if every combination of k digits in the q -expansion of θ occurs with frequency q^{-k} .

One of the first applications of probability theory to arithmetical questions occurred in a paper by É. Borel, who asserted in 1909 [637] that almost all real numbers are simply normal with respect to any $q \geq 2$. His arguments were rather heuristical but soon other proofs of this assertion were given by G. Faber²¹⁸ [1948] and F. Hausdorff [2616]. Borel also stated in [637] that almost every number is absolutely simply normal (cf. [640]), and an elementary proof of this result was provided in 1917 by W. Sierpiński [5783] who also gave the first effective example.

Later A.M. Turing²¹⁹ gave an effective way of constructing such numbers (see V. Becher, S. Figueira, R. Picchi [371]).

Borel's result implies in particular that if for real $x \in (0, 1)$ one denotes by $S_n(x)$ the number of occurrences of 1 in the first n binary digits of x , and $\mu_n(x) = |S_n(x) - n/2|$, then for almost all x one has

$$\mu_n(x) = o(n).$$

Hausdorff's argument in [2616] improved this result to

$$\mu_n(x) = O(n^\alpha)$$

for every $\alpha > 1/2$, and G.H. Hardy and J.E. Littlewood [2520, 2521] in 1914 established

$$\mu_n(x) = O(\sqrt{n \log n}),$$

and showed that the bound

$$\mu_n(x) = O(\sqrt{n})$$

fails for a set of x of positive measure.

²¹⁸Georg Faber (1877–1966), professor in Tübingen, Stuttgart, Königsberg, Strasbourg and Munich.

²¹⁹Alan Mathison Turing (1912–1954), worked in Cambridge and Manchester. During Second World War, a member of the Bletchley Park code-breaking team. Forerunner of computer science. See [2839, 6230].

Almost ten years later A.J. Khintchine [3317] showed that for almost all $x \in (0, 1)$ one has

$$\limsup_{n \rightarrow \infty} \frac{|\mu_n(x)|}{\sqrt{n \log \log n}} \leq 1.$$

The Hausdorff dimension of the set

$$\left\{ x \in (0, 1) : \limsup_{n \rightarrow \infty} \frac{S_n(x)}{n} \leq t \right\}$$

was determined for $t < 1/2$ by A.S. Besicovitch [478] and V. Knichal²²⁰ [3408, 3409].

The more general case of q -ary expansions was considered by I.J. Good²²¹ in [2280]. He conjectured a formula for the Hausdorff dimension of sets of real numbers whose digits appear with a prescribed frequency, and it was later established by H.G. Eggleston [1692] (*theorem of Besicovitch–Eggleston*) (cf. L. Barreira, B. Saussol, J. Schmeling [335], J. Cigler [1111], L. Olsen [4676], F. Schweiger [5586], B. Volkmann [6457–6462]).

A characterization of normal numbers in terms of Rademacher functions was given later by M. Mendès France [4245].

In 1932 D.G. Champernowne²²² [989] proved that the number $0.123456789101112\dots$ is normal, and conjectured that the same happens for the number whose decimal digits are formed by the juxtaposition of the sequence of primes. This was established in 1946 by A.H. Copeland and P. Erdős [1246], who showed that the same happens if the primes are replaced by any quickly increasing sequence of integers. Later H. Davenport and P. Erdős [1382] extended Champernowne's result to all numbers with decimal expansion $0.f(1)f(2)f(3)\dots$, where $f(x)$ is an integer-valued polynomial attaining positive values for $x = 1, 2, \dots$. As shown later by K. Mahler [4081] all these numbers are transcendental. For further variants and generalizations see P. Bundschuh [844], P. Bundschuh, P.J.-S. Shiue, X. Yu [849], M.G. Madritsch, J. Thuswaldner, R.F. Tichy [4057], K. Mahler [4094], H. Niederreiter [4600], J.W. Sander [5386], Z. Shan, E.T.H. Wan [5672], I. Shiokawa [5710], Y. Nakai, I. Shiokawa [4528–4530], P. Szűsz²²³, B. Volkmann [6032].

Denote by $B(q)$ the set of all numbers normal with respect to an integer $q \geq 2$. It was shown in 1960 by W.M. Schmidt [5484] that the equality $B(r) = B(s)$ holds if and only if the ratio $\log r / \log s$ is rational. For other results on relations between sets $B(q)$ for various q see J.W.S. Cassels [941], W.M. Schmidt [5485], C.M. Colebrook, J.H.B. Kemperman [1175], A.D. Pollington [4948, 4949]. For rational r one has $B(q) + \{r\} = B(q)$. Examples of irrational r with this property were given by N. Spears and J.E. Maxfield [5860], and a description of the set of such r 's was provided by G. Rauzy [5135].

The notion of normality was generalized to the case of non-integral bases. One says that a real number a is normal with respect to $\theta > 1$ if the sequence $\{a\theta^n\}$ is uniformly distributed mod 1. Let $B(\theta)$ be the set of all real a satisfying this condition. M. Mendès France [4249] asked whether the above result by W.M. Schmidt [5484] holds also for non-integral bases, and this got a negative answer in 1993, when G. Brown, W. Moran and A.D. Pollington established $B(10) \neq B(\sqrt{10})$ [751] (cf. [752] and W. Moran, A.D. Pollington [4373]).

²²⁰Vladimír Knichal (1908–1974), professor in Brno. See [3587].

²²¹Irving John Good (1917–2009), professor at Virginia Tech. During Second World War, a member of the Bletchley Park code-breaking team.

²²²David Gawen Champernowne (1912–2000), professor of economics in Oxford and Cambridge.

²²³Peter Szűsz (1924–2008), professor at SUNY.

For a historical survey of the theory of normal numbers see G. Harman [2563].

M. Mendès France defined (in a footnote in [4246]) a set B of reals to be *normal* if there exists a sequence λ_n of reals such that the sequence $\lambda_n x$ is uniformly distributed modulo 1 if and only if x lies in B . Various examples, including real number fields of finite degree or the set of all real transcendental numbers, were given by M. Mendès France [4247] and Y. Meyer [4281, 4282]. Characterizations of normal sets were given by F. Dress and M. Mendès France [1623] and G. Rauzy [5134]. See also F. Dress [1621], J. Lesca, M. Mendès France [3839], M. Mendès France [4248].

G. Rauzy's question of whether a finite union of normal sets is normal was answered in the positive by T.C. Watson [6593] (this had been shown earlier for subsets of $\mathbf{Z} \setminus \{0\}$ by F. Dress and M. Mendès France [1623]). Watson's paper characterizes normal sets B as $F_{\sigma\delta}$ -sets satisfying $0 \notin B$ and $-B = B$.

Normal sets associated with sequences which are recognizable by automata have been studied by C. Mauduit [4210].

2.6 Geometry of Numbers

2.6.1 Lattice Points

1. Although geometrical arguments in arithmetical questions may also be found in earlier papers, one usually associates the name *Geometry of Numbers* with the research started by H. Minkowski in 1891, who in his first paper on this subject [4322] applied geometrical methods to the study of minima of positive-definite quadratic forms with real coefficients. He later published two books [4324, 4328] in which he showed that the utilization of geometrical methods can provide insight in various arithmetical problems.

Recall that a subgroup Λ of the real n -space \mathbf{R}^n is called an *n -dimensional lattice*, if it is isomorphic to \mathbf{Z}^n . Every such lattice can be written in the form

$$\Lambda = \left\{ \sum_{j=1}^n x_j \omega_j : x_1, \dots, x_n \in \mathbf{Z} \right\},$$

where $\omega_1, \dots, \omega_n$ are suitably chosen elements of Λ , linearly independent over the rationals. The volume $d(\Lambda)$ of the set

$$\left\{ \sum_{j=1}^n r_j \omega_j : 0 \leq r_j < 1 \right\}$$

is called the *discriminant* of Λ . Lattices in small dimensions had already been considered by C.F. Gauss [2212] and A. Bravais²²⁴ [693].

Minkowski used lattices very efficiently in various problems. The central result of the book [4324] is the *convex body theorem* (a *convex body* is defined as a compact

²²⁴Auguste Bravais (1811–1863), professor of physics and mineralogy in Paris.

convex subset of \mathbf{R}^n , symmetrical about the origin, and containing the origin in its interior).

Let X be a convex body in \mathbf{R}^n , and let $\Lambda \in \mathbf{R}^n$ be a lattice of discriminant $d(\Lambda)$. If $V(X)$ exceeds $2^n d(\Lambda)$, then X contains at least one non-zero point of Λ . If X is compact, then the same assertion holds under the weaker assumption $V(X) \leq 2^n d(\Lambda)$.

For simple proofs of this theorem see H.F. Blichfeldt [557], L.J. Mordell [4384], R. Remak [5161].

2. The convex body theorem has several important applications, most of them already appearing in [4324]. One of them is the theorem on linear forms (*Linearformensatz*), which in its simplest form runs as follows.

Let for $i = 1, 2, \dots, n$

$$L_i(X_1, \dots, X_n) = \sum_{j=1}^n a_{ij} X_j$$

be real linear forms in n variables with non-zero discriminant $D = \det[a_{ij}]$. If t_1, \dots, t_n are positive numbers satisfying $t_1 t_2 \cdots t_n > |D|$, then the system of inequalities

$$|L_j(x_1, \dots, x_n)| \leq t_j \quad (j = 1, 2, \dots, n) \quad (2.70)$$

has a non-zero integral solution.

The proof is based on the observation that the volume of the set defined by the inequalities (2.70) equals $\det[a_{ij}]$. There also exist proofs avoiding the use of geometry. Several of them are listed in the book by J.F. Koksma [3444].

From several other applications of the convex body theorem we mention here only two simple proofs of the old result stating that an integer is the sum of three squares if and only if it is not of the form $4^a(8b+7)$, given by N.C. Ankeny [102] and L.J. Mordell [4398].

3. In his book [4324] Minkowski established the following assertion in the case $n = 2$.

Let

$$L_i(X_1, \dots, X_n) = \sum_{j=1}^n a_{ij} X_j \quad (i = 1, 2, \dots, n)$$

be linear forms with real coefficients and non-vanishing determinant $D = \det[a_{ij}]$. Then for every real y_1, \dots, y_n there exist rational integers x_1, \dots, x_n satisfying

$$\prod_{i=1}^n |L_i(x_1, \dots, x_n) - y_i| \leq \frac{D}{2^n}. \quad (2.71)$$

The assertion (2.71) in the general case is usually quoted as a conjecture of Minkowski, although, as noted by F.J. Dyson [1678], there is no evidence that Minkowski considered the case $n > 2$.

The inequality (2.71) was established for $n = 3$ by R. Remak [5159] in 1923, and other proofs were provided later by H. Davenport [1353] and B.J. Birch and H.P.F. Swinnerton-Dyer [536]. The case $n = 4$ was handled successfully in 1948 by F.J. Dyson [1678], and in the case $n = 5$ a sketch of the proof was given in 1973 by B.F. Skubenko²²⁵ [5816]. A complete proof on lines indicated by Skubenko was given by R.P. Bambah and A.C. Woods [311]. A proof for $n = 6$ was found by C.T. McMullen [4235] in 2005, and recently the conjecture was established for $n = 7$ (R.J. Hans-Gill, R. Madhu, S. Ranjeet [2499]).

It was shown by N.G. Čebotarev [968] that on the right-hand side of (2.71) one can put $D/2^{n/2}$ (for a small improvement see L.J. Mordell [4389]), and later this was replaced by $c_n D/2^{n/2}$ with $c_n = 1/(2e - 1 + o(1))$ (H. Davenport [1361]), and $c_n = 1/(3(2e - 1) + o(1))$ (E. Bombieri [594]). This was later improved to $c_n \ll (\log n/n)^{1/3}$ (B.F. Skubenko [5817]), $c_n \ll n^{-3/7} \log^{4/7} n$ (Kh.N. Narzullaev, Skubenko [4545]), $c_n \ll \log n/\sqrt{n}$ (A.K. Andriyasyan, I.V. Ilin, A.V. Malyšev²²⁶ [97]), and $c_n \ll \sqrt{\log n/n}$ (A.V. Malyšev [4124]).

4. In [4324] one also finds the first occurrence of an abstractly defined metric in the set of all n -term sequences of reals, defined as a function $f(p, q)$ satisfying the triangle inequality and the condition: $f(p, q) = 0$ is equivalent to $p = q$. Note that Minkowski explicitly avoided the symmetry condition.

An important result established by Minkowski in [4324] is the *Brunn–Minkowski theorem*, which gives a lower bound for the volume of the set

$$A + B = \{a + b : a \in A, b \in B\},$$

where A, B are convex sets in \mathbf{R}^n , in terms of volumes of A and B :

$$V(A + B)^{1/n} \geq V(A)^{1/n} + V(B)^{1/n}. \quad (2.72)$$

It was shown by L.A. Lusternik²²⁷ [4033] in 1935 that (2.72) also holds for arbitrary non-empty compact sets A, B , the volume being replaced by the Lebesgue measure. For further developments see R.J. Gardner [2196].

Minkowski's book also contains applications of his methods to the theory of algebraic numbers. In particular, there he proved a lower bound for the absolute value of the discriminant of an algebraic number field, which implied the non-existence of a non-trivial extension of the rationals with discriminant equal to 1, and led to a simple proof of Hermite's [2763] assertion that there can be only finitely many algebraic number fields having a fixed discriminant. One also finds in [4324] a new proof of Dirichlet's theorem on the structure of units in algebraic number fields as well as a geometrical interpretation of the theory of continued fractions.

²²⁵Boris Faddeevič Skubenko (1929–1993). See [96].

²²⁶Aleksandr Vasilevič Malyšev (1928–1993), professor in Leningrad. See [643].

²²⁷Lazar Aronovič Lusternik (1899–1981), professor in Moscow. See [47].

5. In [4324, Sect. 40] Minkowski considered systems $S = \{L_1, \dots, L_n\}$ of n real linear forms in n variables of unit discriminant, and defined

$$M_n = \sup_S \min_{P \neq 0} |L_1(P) \cdots L_n(P)|, \quad (2.73)$$

$P = (x_1, \dots, x_n) \in \mathbf{Z}^n$. He proved the inequality $M_n \leq n!/n^n$ implying

$$M = \limsup_{n \rightarrow \infty} \sqrt[n]{M_n} \leq \frac{1}{e} = 0.367 \dots$$

The value of M_n is related to $D(n)$, the minimal absolute value of discriminants of algebraic number fields of degree n , because of the inequality

$$M_n \geq \frac{1}{\sqrt{D(n)}}$$

(N. Hofreiter [2845]).

Minkowski's bound was improved in 1936 by H.F. Blichfeldt [563], who obtained $M \leq \sqrt{2/3\pi e} = 0.279 \dots$, and, as noted by C.A. Rogers in [5251], the inequality $M \leq 0.188 \dots$ is hidden in Blichfeldt's paper [564]. In [5251] Rogers obtained $M \leq \pi/4 \exp(1.5) = 0.175 \dots$

The equality $M_3 = 1/7$ was established in 1938 by H. Davenport [1350]. Simpler proofs were later provided by H. Davenport [1359] and L.J. Mordell [4391]. In [1352] Davenport determined forms with

$$\min_{P \neq 0} |L_1(P)L_2(P)L_3(P)| \geq \frac{1}{9.1}$$

(cf. H.P.F. Swinnerton-Dyer [6001]). The corresponding constant in the case of three forms, one real and the other two complex conjugate, equals $1/\sqrt{23}$ (H. Davenport [1351]).

If the forms L_i in (2.73) have complex coefficients and are pairwise conjugated, then the corresponding value of M does not exceed $2/\sqrt{\pi e^3} = 0.2517 \dots$ (H.P. Mulholland [4469]).

6. The second book by Minkowski [4328] is, contrary to its title, devoted mostly to a new development of the theory of algebraic numbers, in which the main role is played by lattices in real n -spaces. Nevertheless it contains some important results concerning lattice points in convex bodies such as, for example, the following *theorem on successive minima*, which extends the convex body theorem.

Let X be a convex body of unit volume, put for $\lambda > 0$

$$\lambda X = \{\lambda x : x \in X\},$$

and for $j = 1, 2, \dots, n$ let λ_j be the minimal value of λ with the property that λX contains j linearly independent points of the integral lattice. Then

$$\frac{2^n}{n!} \leq \prod_{j=1}^n \lambda_j \leq 2^n.$$

For simpler proofs of this result see H. Davenport [1357], T. Estermann [1892] and R.P. Bambah, A.C. Woods, H. Zassenhaus²²⁸ [312].

²²⁸Hans Zassenhaus (1912–1991), professor in Hamburg and at McGill University, Notre Dame University and Ohio State University. See [4923, 4928].

In the same book a conjecture is stated concerning the minimal area $\Delta(p)$ of a parallelogram having one of its vertices at the origin and the remaining three lying on the line $|x|^p + |y|^p = 1$, with $p \geq 1$ being fixed. Minkowski conjectured that for $1 < p < 2$ one has

$$\Delta(p) = (1 - 2^{-p})^{1/p},$$

and that for $p > 2$ the value of $\Delta(p)$ is a root of the polynomial

$$(4^{1/p}x + 1)^p + (4^{1/p}x - 1)^p - 2^{p+1}.$$

It turned out later that this conjecture is correct for large p (H. Cohn [1154]), as well as for certain small p (L.J. Mordell [4390], V.G. Kuharev [3560]), but incorrect for several other small values of p (C.S. Davis²²⁹ [1411], H. Cohn [1154], G.L. Watson [6580, 6581]).

7. A subset X of \mathbf{R}^n is called a *star body* if it contains the origin and every radius vector from the origin meets the boundary of X in one point. The following assertion was stated without proof by Minkowski in [4321].

If $X \subset \mathbf{R}^n$ is a bounded star body of volume $V < \zeta(n)$, then there exists a lattice of unit determinant, not containing a non-zero point of X . If X is, in addition, symmetrical about the origin, then this holds under the assumption $V < 2\zeta(n)$.

The first proof of his assertion was given by E. Hlawka²³⁰ in 1943 [2832], and therefore it is usually called the *Minkowski–Hlawka theorem*. Other proofs were later found by C.A. Rogers [5250] and C.L. Siegel [5767].

A stronger result for symmetric convex bodies was shown by K. Mahler [4084]. Let K be such a body in \mathbf{R}^n of volume $V(K)$, let $\Delta(K)$ be the largest lower bound for the discriminant of a lattice having only the origin in common with K , and put

$$Q(K) = \frac{V(K)}{\Delta(K)}$$

and

$$c_n = \inf_{K \subset \mathbf{R}^n} Q(K).$$

Mahler's result gives $c_2 \geq \sqrt{12} = 3.4641 \dots$, and

$$c_n \geq 2\zeta(n) + \frac{1}{6}$$

for every $n \geq 2$. Later H. Davenport and C.A. Rogers [1400] improved upon this and obtained

$$\liminf_{n \rightarrow \infty} c_n \geq 4.921 \dots$$

Cf. C.G. Lekkerkerker [3813], C.A. Rogers [5252], W.M. Schmidt [5483].

In 1961 V. Ennola [1766] proved $c_2 \geq 3.5252 \dots$, and in 1970 P.P. Tammela [6042] got $c_2 \geq 3.5706 \dots$, which is not very far from the upper bound $c_2 \leq 3.6096 \dots$, established by K. Reinhardt [5155] and K. Mahler [4085], conjectured to be optimal.

²²⁹Clive Selwyn Davis (1916–2009), professor at the University of Queensland.

²³⁰Edmund Hlawka (1916–2009), professor in Vienna. See [5529, 6153].

8. Denote by $m(f)$ the minimal value attained by a positive definite real quadratic form f at a non-zero point of the lattice \mathbf{Z}^n , and define the *Hermite constant* γ_n by

$$\gamma_n = \max \frac{m(f)}{D^{1/n}(f)}, \quad (2.74)$$

the maximum being taken over all forms f in n variables, $D(f)$ being the discriminant of f .

A.N. Korkin and E.I. Zolotarev introduced and studied the important notion of *extreme forms* [3478–3480], presented an algorithm to check whether a form is extreme and described all such forms in dimensions ≤ 5 . Extreme forms are positive definite quadratic forms f having the property that for every form g of the same discriminant, whose coefficients are sufficiently close to the corresponding coefficients of f one has $m(g) < m(f)$.

H. Minkowski proved the bound

$$\gamma_n \leq \frac{4}{\pi} \Gamma\left(1 + \frac{n}{2}\right)^{2/n},$$

improving for $n \geq 9$ the inequality

$$\gamma_n \leq \left(\frac{4}{3}\right)^{(n-1)/2},$$

due to C. Hermite [2761]. For large n a better evaluation was provided in 1914 by H.F. Blichfeldt [557], who established

$$\gamma_n < \frac{2}{\pi} \Gamma\left(2 + \frac{n}{2}\right)^{2/n} \quad (2.75)$$

(cf. R. Remak [5161]).

An important step forward was made by G.F. Voronoï [6471–6473] who in 1908 presented an algorithm for γ_n , which is however extremely cumbersome in higher dimensions. This algorithm also gives a way of constructing all *perfect quadratic forms*, defined in the following way: let $f(\bar{x}) = f(X_1, \dots, X_n)$ be a positive definite quadratic form, put

$$M(f) = \min_{\bar{x} \neq \bar{0}} f(\bar{x}),$$

and let this minimum be attained at points $\bar{u}_1, \dots, \bar{u}_s \in \mathbf{R}^n$. The form f is said to be perfect if the conditions $f(\bar{u}_i) = M(f)$ ($i = 1, 2, \dots, s$) determine f uniquely. Every *extreme form* is perfect.

Voronoï's algorithm allowed a complete list of perfect forms for $n = 6$ to be obtained later (see H.S.M. Coxeter²³¹ [1261], E.S. Barnes²³² [330]). There are seven such forms. A simpler method of producing perfect and extreme forms was presented by Barnes in 1958 [331, 332]. Much later, Voronoï's method allowed the determination of all 33 perfect forms for $n = 7$

²³¹Harold Scott MacDonald Coxeter (1907–2003), professor in Toronto, See [5237].

²³²Eric Stephen Barnes (1924–2000), professor in Adelaide.

(K. Stacey [5883], D.-O. Jacquet-Chiffelle [3091]). Other criteria for an extreme form appear in E.S. Barnes [333]. In the book [4164] by J. Martinet 1096 perfect forms of dimension 8 are described, and it was proved later by M.D. Skirič, A. Schürmann and F. Vallentin [5786] that this list is complete.

The lattices associated with perfect forms are called *perfect lattices*, and a monograph dealing with them has been written by J. Martinet [4164].

The analogue of γ_n for forms over number fields was introduced in 1997 by M.I. Icaza [3001] and it was determined for binary forms in certain particular fields by R. Baeza, R. Coulangeon, M.I. Icaza, M. O’Ryan [212], R. Coulangeon, M.I. Icaza, M. O’Ryan [1258] and M. Pohst, M. Wagner [4929].

9. The evaluation of γ_n is closely related to the problem of arranging disjoint spheres of the same radius in an n -dimensional space (the *sphere packing problem*), with centers located in grids of a lattice (the so-called *regular arrangement*).

It had been observed already by Gauss [2212] that the density ϱ_n of the closest such arrangement (i.e., the limit of the ratio of the volume occupied by the spheres to the volume of the smallest cube containing them) is related to γ_n by the formula

$$\varrho_n = \frac{1}{\Gamma(1 + n/2)} \left(\frac{\pi \gamma_n}{4} \right)^{n/2}. \quad (2.76)$$

Thus the old result $\gamma_2 = 2/\sqrt{3}$ of Lagrange [3611] implies $\varrho_2 = \pi/\sqrt{12}$, and the equalities $\gamma_3 = \sqrt[3]{2}$ and $\varrho_3 = \pi/\sqrt{18}$ follow from Gauss’s comments [2212] on the book by L.A. Seeber²³³ [5596]. The cases $n = 4, 5$ were treated by A.N. Korkin and E.I. Zolotarev [3478–3480], who obtained $\gamma_4 = \sqrt{2}$, and $\gamma_5 = \sqrt[5]{8}$, implying $\varrho_4 = \pi^2/16$ and $\varrho_5 = \pi^2/\sqrt{450}$.

In 1905 the lower bound

$$\varrho_n \geq \frac{\zeta(n)}{2^{n-1}} \quad (2.77)$$

was obtained by H. Minkowski in his paper [4326], where he constructed a reduction theory for positive definite quadratic forms in several variables. An approach to the reduction theory based on a study of form matrices was proposed in 1911 by A. Châtelet [1001].

A simpler presentation of Minkowski’s reduction theory was given in 1928 by L. Bieberbach²³⁴ and I. Schur [503]. A generalization to quadratic forms over arbitrary fields was made much later by P. Humbert²³⁵ [2949, 2950].

In the twenties H.F. Blichfeldt [559, 560] obtained $\varrho_6 = \pi^3/48\sqrt{3}$ and $\varrho_7 = \pi^3/105$. The result in dimension 6 has been independently obtained by N. Hofreiter [2843]. Blichfeldt published his proofs only in 1935 [562], when he also established the equality $\varrho_8 = \pi^4/384$. These results imply

$$\gamma_6 = 2/\sqrt[6]{3}, \quad \gamma_7 = \sqrt[7]{64}, \quad \gamma_8 = 2$$

for the constants γ_n defined by (2.74).

²³³Ludwig August Seeber (1793–1855), professor of physics in Freiburg.

²³⁴Ludwig Bieberbach (1886–1982), professor in Basel, Frankfurt and Berlin. See [2375].

²³⁵Pierre Humbert (1891–1953), professor in Montpellier, son of G. Humbert.

For $9 \leq n \leq 12$ and $n = 15$ lower bounds for ϱ_n were obtained later by T.W. Chaundy [1006], E.S. Barnes [331, 332], E.S. Barnes and G.E. Wall [334] and H.S.M. Coxeter and J.A. Todd²³⁶ [1264] by explicit constructions. They are listed in the book by C.A. Rogers [5254], where also the opinion is expressed that these bounds are optimal. A construction of packings for $n = 2^k$ ($k \geq 4$) as well as for $n \leq 24$ was given in 1964 by J. Leech [3760, 3761] (cf. J.H. Conway [1223]). The lattice Λ found by Leech in the case $n = 24$ (the *Leech lattice*) plays an important role in coding theory (see I.F. Blake [545], W. Ebeling [1681]). It turned out later that the factor group of the group of rotations of Λ by its center is a new sporadic simple group of more than $8 \cdot 10^{15}$ elements, containing two other new sporadic groups (J.H. Conway [1222]). Various constructions of the Leech lattice were given later (J.H. Conway, N.J.A. Sloane [1226, 1227], N.D. Elkies [1719], N.D. Elkies, B.H. Gross [1725], J. Lepowsky, A. Meurman [3832], M. Craig [1265]).

The Leech lattice is an example of a *unimodular lattice*, i.e., having discriminant 1. All such lattices in \mathbf{R}^N for $N \leq 23$ were listed by J.H. Conway and N.J.A. Sloane [1228, 1229], for $N = 24$ this has been done by H.-V. Niemeier [4615], and for $N = 25$ by R.E. Borcherds [627]. For partial results in larger dimensions see, e.g., R. Bacher, B.B. Venkov [192], C. Bachoc, G. Nebe, B.B. Venkov [203], P. Gaborit [2172], H. Koch, G. Nebe [3430], H. Koch, B.B. Venkov [3431, 3432], M. Kervaire²³⁷ [3306]. See also the book by J.H. Conway and N.J.A. Sloane [1230].

The case of higher dimensions is still open, and only some bounds are known. Upper bounds result from (2.75) as well as from the inequality

$$\gamma_n \leq \gamma_{n-1}^{(n-1)(n-2)}$$

proved by L.J. Mordell [4392] (cf. A. Oppenheim²³⁸ [4694]). The lower bound

$$\gamma_n \geq (1 + o(1)) \frac{8}{\pi^2 e} \frac{n \zeta(n)}{2^{n-1}}$$

follows from Minkowski's bound (2.77) for ϱ_n . It was improved much later by C.A. Rogers [5250], H. Davenport and C.A. Rogers [1400], and K. Ball [291]. The upper bound was made smaller (also in the non-regular case) by H.F. Blichfeldt [561], R.A. Rankin [5113], C.A. Rogers [5253], V.M. Sidelnikov [5733], G.A. Kabatiansky and V.I. Levenšteín [3176] (for $n \geq 43$), V.I. Levenšteín [3846] and K. Bezdek [496] (for $n \geq 8$). See the books by C.A. Rogers [5254], J.H. Conway and N.J.A. Sloane [1230] and K. Böröczky [646], as well as a survey by G. Fejes Tóth [1964]. The best known upper bounds for $4 \leq n \leq 36$ were given by H. Cohn and N.D. Elkies [1159].

In the three-dimensional non-regular case upper bounds were given by J.H. Lindsey [3899] and D.J. Muder [4464, 4465], and the final step was taken by T. Hales in a series of papers, one with S.P. Ferguson, published between 1997 and 2006 ([2460–2465, 2467], cf. S.P. Ferguson [1988]) who confirmed an old conjecture²³⁹ of Kepler stating that the maximal density equals $\pi/\sqrt{18}$ (for corrections see [2468]). This concluded the realization of the program put forward by Hales in 1992 [2459]. For the history of Kepler's conjecture see T. Hales [2466].

²³⁶John Arthur Todd (1908–1994), reader in Cambridge. See [160].

²³⁷Michel Kervaire (1927–2007), professor at the Courant Institute and in Geneva. See [1712].

²³⁸Alexander Oppenheim (1903–1997), professor in Singapore, Reading and at the Universities of Ghana and Benin.

²³⁹It formed a part of Hilbert's eighteenth problem.

A related conjecture was proposed in 1943 by L. Fejes Tóth [1966] (cf. his books [1967, 1968]). Let A be the set of centers of spheres realizing a packing of spheres in \mathbf{R}^3 , and for any $P \in A$ define its *Voronoi cell* as the set of all points of \mathbf{R}^3 which are closer to P than to any other point in A . The conjecture asserts that the volume of every Voronoi cell is at least equal to the volume of a regular dodecahedron of unit inradius. It has been known for some time that it implies Kepler's conjecture. Recently the dodecahedron conjecture has been established by T. Hales and S. McLaughlin [2469].

10. Dense regular arrangements of disjoint congruent convex bodies other than spheres have also been considered, and it seems that this question in \mathbf{R}^3 has been first considered by H. Minkowski [4325] in 1904. In the case of congruent tetrahedrons the problem is equivalent to the question of minimal positive value attained by $|x| + |y| + |z|$ at points of a lattice of given determinant D . Minkowski showed that this minimum is $\leq cD$, with $c = (108/19)^{1/3}$, and deduced the possibility of the approximation of two real numbers a_1, a_2 by rationals $r_1 = p_1/q, r_2 = p_2/q$ with the same denominator, so that both differences $|r_i - a_i|$ are $\leq \sqrt{8/19}/q^{3/2}$.

The methods used by H.F. Blichfeldt in [562] were later adapted by G. Fejes Tóth and W. Kuperberg [1965] to obtain upper bounds for the packing density for a large class of convex bodies.

A problem which is in some sense dual to the packing problem deals with a covering of \mathbf{R}^n by overlapping equal spheres whose centers form a lattice. The main question is to find the sparsest such covering, but the answer is known only for $n = 2$ (R. Kershner [3304]), $n = 3$ (R.P. Bambah [308]), $n = 4$ (B.N. Delone²⁴⁰, S.S. Ryškov [1456]) and $n = 5$ (S.S. Ryškov, E.P. Baranovskii [5359, 5360]). In higher dimensions only bounds are known (see H. Davenport [1366], R.P. Bambah, H. Davenport [310], P. Erdős, C.A. Rogers [1852], C.A. Rogers [5253], H.S.M. Coxeter, L. Few, C.A. Rogers [1263], M.N. Bleicher [554], P. Erdős, L. Few, C.A. Rogers [1828], S.S. Ryškov [5358]).

11. The problem of minimas attained by indefinite binary quadratic forms at integral points had already been considered by A.A. Markov in two papers [4153, 4154] published in 1879 and 1884. If $f(x, y) = ax^2 + bxy + cy^2$ is such a form with real coefficients, $D(f) = b^2 - 4ac$ is its discriminant, and $m(f)$ is the minimal absolute value of $f(x, y)$ attained at points $(x, y) \neq (0, 0)$ with integral coordinates, then Markov showed that the maximal value of the ratio

$$\delta(f) = \frac{m(f)}{\sqrt{D(f)}}$$

equals $2/\sqrt{5}$, and there are only denumerably many non-equivalent forms f with $\delta(f) > 2/3$. His cumbersome proof used continued fractions. He found a connection between this problem and the Diophantine equation

$$x^2 + y^2 + z^2 = 3xyz, \quad (2.78)$$

and showed that solutions of it could be arranged in a binary tree (the numbers x occurring in this equation are called *Markov numbers*).

²⁴⁰Boris Nikolaevič Delone [Delaunay] (1890–1980), professor in Leningrad and Moscow. See [1950].

Similar results for solutions of the equation $x^2 + y^2 + z^2 = nxyz$ were obtained in 1907 by A. Hurwitz [2961].

Solutions of the more general equation

$$x_1^2 + x_2^2 + \cdots + x_n^2 = ax_1x_2 \cdots x_n$$

were investigated in a series of papers of A. Baragar [316, 317, 319].

Simpler proofs of Markov's results were given by G. Frobenius [2118] in 1913 (see also R. Remak [5160] and J.W.S. Cassels [927]).

It was noted by H. Cohn [1155, 1156] that Markov numbers are of importance in the theory of geodesics on Riemann surfaces (cf. A. Haas [2417]). In another paper [1157] Cohn showed that they are also related to primitive words of the free group with two generators.

In 1982 D. Zagier [6811] showed that the number $M(x)$ of Markov numbers below x satisfies

$$M(x) = c \log^2 x + O(\log x (\log \log x)^2)$$

with some explicitly given $c > 0$. He also noted that the existence of

$$\lim_{x \rightarrow \infty} \frac{M(x)}{\log^2 x}$$

was earlier established in C. Gurwood's Ph.D. thesis [2396].

The problem of whether there are two solutions of (2.78) with the same value of z was stated by G. Frobenius [2118] in 1913 and is still open. Only some partial results are known (see A. Baragar [318], P. Schmutz [5531], J.O. Button [870], Y. Zhang [6829], A. Srinivasan [5881]).

A large part of the book [1310] by T.W. Cusick and M.E. Flahive is devoted to Markov numbers.

In [4156] A.A. Markov treated the analogous problem for indefinite ternary quadratic forms f , and gave a proof for the inequality

$$\frac{M(f)^3}{|D(f)|} \geq \frac{2}{3}$$

(the discriminant $D(f)$ being defined as the determinant of the matrix of f), which, as he wrote in a footnote, had been communicated to him by A.N. Korkin around 1880. He also determined the next two possible values of the ratio $M(f)^3/|D(f)|$, namely $2/5$ and $1/3$.

In the case of indefinite quaternary quadratic forms of signature zero the first seven possible values of $M(f)^4/|D(f)|$ were listed later by A. Oppenheim [4692, 4693], who noted also that the largest value, equal to $4/9$ had been found much earlier by A.A. Markov. The next four values were found in 1945 by B.A. Venkov²⁴¹ [6384].

12. Packing and coverings were treated in the books by K. Bórczky, Jr. [646], J.H. Conway and N.J.A. Sloane [1230] and C.A. Rogers [5254].

²⁴¹Boris Alekseevič Venkov (1900–1962), professor in Leningrad. See [6386].

An introduction to the geometry of numbers can be found in the books by J.W.S. Cassels [934], C.G. Lekkerkerker [3814] and C.L. Siegel [5777]. For a survey see [2371] and the recent monograph by P.M. Gruber on convex geometry [2370] contains also much information on that subject.

2.6.2 Integral Points in Regions

1. For a bounded region $\Omega \subset \mathbf{R}^2$ denote by $N(\Omega)$ the number of points with integral coordinates lying in Ω . Already C.F. Gauss [2213] had shown that if Ω is a plane convex body of area $V(\Omega)$ and for positive x ,

$$x\Omega = \{xP : P \in \Omega\}$$

denotes its dilatation, then

$$N(x\Omega) = x^2 V(\Omega) + R(x) \quad (2.79)$$

with $R(x) = O(x)$.

The next general result in this topic was obtained in 1917 by I.M. Vinogradov [6403] who showed that if $\Omega \subset \mathbf{R}^2$ is a region bounded by a closed curve Γ , the curvature $\kappa(P)$ exists at each point $P \in \Gamma$ and satisfies $0 < r \leq \kappa(P) \leq R$, then

$$N(\Omega) = V(\Omega) + O\left(\frac{R^2 \log^{2/3} r}{r^{4/3}}\right).$$

An exposition of Vinogradov's proof, leading to a better error term (R^2 being replaced by $R^{4/3}$) can be found in the book by A.O. Gelfond²⁴² and Yu.V. Linnik [2234, Chap. 8].

The next results were obtained by J.G. van der Corput²⁴³, who in his thesis [6274, 6275] developed a method to evaluate the number $N(\Omega)$ in the case when the boundary of Ω consists of convex arcs, satisfying certain regularity conditions. This allowed him, in a joint paper with E. Landau [3682], to improve Vinogradov's result to

$$N(\Omega) = V(\Omega) + O(R^{2/3}). \quad (2.80)$$

The exponent $2/3$ in (2.80) was later reduced by M.N. Huxley [2981–2983] to $0.636\dots$, $0.630\dots$ and $0.629\dots$.

The error term $R(x)$ in (2.79) was shown by V. Jarník [3106] in 1924 to be $\Omega(\sqrt{x})$ and in 1985 W.G. Nowak [4635] proved

$$R(x) = \Omega(\sqrt{x} \log^4 x)$$

for regions with boundary of class C^∞ and finite non-zero curvature. He also obtained [4638–4640] a corresponding result in higher dimensions. A broad survey of these questions in

²⁴² Aleksandr Osipovič Gelfond (1906–1968), professor in Moscow. See [3858].

²⁴³ Johannes Gualtherus van der Corput (1890–1973), student of J.C. Kluyver, professor in Groningen, Amsterdam and Berkeley. See [787].

arbitrary dimension was given in 2006 by A. Ivić, E. Krätzel, M. Kühleitner and W.G. Nowak [3043].

In his next papers [6276, 6278–6281] J.G. van der Corput produced bounds for exponential sums

$$\sum_{a \leq n \leq b} \exp(\pi i f(n)),$$

depending on bounds for the derivatives of f , which can be used in certain important cases to obtain good bounds for the difference between $N(\Omega)$ and the volume of Ω . In particular he improved the bounds of the error terms in the classical circle and divisor problems (see below).

It was observed by V. Jarník²⁴⁴ (see H. Steinhaus²⁴⁵ [5920]) that this method implies that if Γ is a closed rectifiable Jordan curve of length $L > 1$ in the plane, encompassing a region of area V , then for the number N of points with integral coordinates lying in that region one has $|N - V| < L$. For convex regions M. Nosal [4627] obtained the inequalities

$$-1 - L/2 < V - N < L/2,$$

and showed that the left inequality is best possible. An analogous result in 3-space was obtained by W.M. Schmidt [5504] and J. Bokowski and J.M. Wills [591], and in \mathbf{R}^n by J. Bokowski, H. Hadwiger and J.M. Wills [590]. For a survey see J.M. Wills [6676].

In 1972 H. Chaix [981] proved that one can take 16 400 for the implied constant in (2.80).

See also B. Randol [5102], Y. Colin de Verdière [1182], W.G. Nowak [4632, 4633], A. Iosevich [3027] and the book by M.N. Huxley [2986].

The books by F. Fricker [2093] and by E. Krätzel [3517] published in 1982 and 1988, respectively, give a good presentation of problems concerning the number of lattice points in various regions. A survey of later development was given by W.G. Nowak [4637].

2.6.2.1 The Circle Problem

1. In the *circle problem* one asks for the number $F(x)$ of points with integral coordinates lying in the circle of radius \sqrt{x} , centered at the origin. Clearly

$$F(x) = \sum_{n \leq x} r_2(n) = \sum_{a^2 + b^2 \leq x} 1 = 1 + 4 \sum_{0 \leq n < \sqrt{x}} [\sqrt{x - n^2}],$$

$r_2(n)$ being the number of representations of n as the sum of two squares of integers.

Gauss's result (2.79) implies

$$F(x) = \pi x + O(\sqrt{x}),$$

and the first improvement was obtained in 1906 by W. Sierpiński [5780]. He used the method applied a few years earlier by his teacher G.F. Voronoï [6469] to the divisor problem to obtain

$$F(x) = \pi x + A(x) \tag{2.81}$$

²⁴⁴Vojtěch Jarník (1897–1970), student of Landau, professor in Prague. See [4628].

²⁴⁵Hugo Steinhaus (1887–1972), professor in Lwów and Wrocław. See [3177].

with $A(x) \ll x^{1/3}$. A simpler, but nevertheless rather involved, proof was later provided by E. Landau [3645].

A really simple proof was found much later by W.G. Nowak [4629]. See also the book [3064, Sect. 4.4] by H. Iwaniec and E. Kowalski.

Denote by a the greatest lower bound for numbers c , for which one has $A(x) \ll x^c$. There were several improvements of Sierpiński's result $a \leq 1/3$. The first was obtained by J.G. van der Corput [6277], who got $a < 0.33$. (It was pointed out by A. Walfisz [6526] that his argument in fact gives $a \leq 163/494 = 0.3299\dots$) Independently, a slightly weaker result ($a \leq 37/112 = 0.3303\dots$) was obtained by J.E. Littlewood and A. Walfisz [3948].

Here is the list of subsequent improvements:

- $a \leq 27/82 = 0.3292\dots$ (L.W. Nieland [4611], using the method of evaluations of exponential sums, introduced by J.G. van der Corput in [6282]; cf. E.C. Titchmarsh [6171]),
- $a \leq 15/46 = 0.32608\dots$ (E.C. Titchmarsh [6175]),
- $a \leq 13/40 = 0.325$ (L.H. Hua [2928]),
- $a \leq 12/37 = 0.3243\dots$ (W.L. Yin [6780], J.R. Chen [1015]),
- $a \leq 35/108 = 0.32407\dots$ (W.G. Nowak [4631]),
- $a \leq 139/429 = 0.32400\dots$ (K. Kolesnik [3457], W.G. Nowak [4641]),
- $a \leq 7/22 = 0.3181\dots$ (H. Iwaniec, C.J. Mozzochi [3067]; cf. W. Müller, W.G. Nowak [4475]),
- $a \leq 23/73 = 0.31506\dots$ (M.N. Huxley [2982]).

The best known result is due to M.N. Huxley [2983] who in 2003 obtained

$$A(x) = O\left(x^{131/416} \log^{18637/8320} x\right).$$

(Note that $131/146 = 0.3149\dots$)

For a long time it has been conjectured that $a = 1/4$, and G.H. Hardy [2509] showed that this holds in the mean, by proving

$$\frac{1}{x} \int_1^x |A(t)| dt \ll x^{1/4+\varepsilon}$$

for every $\varepsilon > 0$. On the other hand the inequality $a \geq 1/4$ was established by G.H. Hardy [2506] and E. Landau [3652], and in [2508] Hardy proved that $A(x) = \Omega((x \log x)^{1/4})$.

This was improved in 1940 by A.E. Ingham [3022], who showed that one cannot have $A(x) = O((x \log x)^{1/4})$. Much later J.L. Hafner [2430] established

$$A(x) = \Omega_-\left((x \log x \sqrt{\log \log x})^{1/4}\right),$$

and the current record holder is K. Soundararajan [5852], who in 2003 got

$$A(x) = \Omega\left((x \log x)^{1/4} (\log \log x)^a (\log \log \log x)^{-5/8}\right)$$

with $a = 3(\sqrt[3]{2} - 1)/4 = 0.1949\dots$

The integral $I_2(x) = \int_0^x A^2(t) dt$ was considered in 1922 by H. Cramér [1269], who obtained

$$I_2(x) = cx^{3/2} + O(x^{5/4+\varepsilon})$$

for every $\varepsilon > 0$ with a certain $c > 0$. Later E. Landau [3665] and A. Walfisz [6526] replaced the error term by $O(x^{1+\varepsilon})$ and $O(x \log^3 x)$, respectively.

After forty years I. Kátai [3268] proved the error term here to be $O(x \log^2 x)$, and in 2004 W.G. Nowak [4644] replaced this by $O(x \log^{3/2} x \log \log x)$.

Asymptotics of higher moments $\int_0^x A^n(x) dx$ for small n were found by K.M. Tsang ($n = 3, 4$) [6202] and D.R. Heath-Brown ($n \leq 9$) [2648].

The related problem of evaluating the sum $S_2(x) = \sum_{n \leq x} r_2^2(n)$ was considered by W. Sierpiński who, in his dissertation [5781, Sect. 6], obtained

$$S_2(x) = 4x \log x + ax + R_2(x) \quad (2.82)$$

with a certain constant a and $R_2(x) = O(x^{3/4} \log x)$.

S. Ramanujan stated that the error in (2.82) is $O(x^c)$ for every $c > 3/5$, and B.M. Wilson [6677] conjectured that this holds for every $c > 1/2$. This was accomplished in 1989 by W. Recknagel [5137], who showed

$$R_2(x) = O(\sqrt{x} \log^6 x).$$

Now the bound $R_2(x) = O(x^{1/2} \log^{11/3} x (\log \log x)^{1/3})$ is known (M. Kühleitner [3561]). On the other hand A. Schinzel [5447] obtained $R_2(x) = \Omega(x^{3/8})$.

2. The corresponding problem in the 3-space concerns the evaluation of

$$F_3(x) = \sum_{a^2+b^2+c^2 \leq x} 1,$$

the number of lattice points in the sphere of radius \sqrt{x} , centered at the origin.

It is not difficult to show by an argument similar to that used by Gauss that one has

$$F_3(x) = \frac{4\pi}{3} x^{3/2} + r(x),$$

with $r(x) = O(x)$, and in 1914 D. Cauer [967] obtained $r(x) = O(x^{3/4})$.

In 1926 A. Walfisz [6525] showed that if c denotes the greatest lower bound for numbers a with $r(x) = O(x^a)$, then $c \leq 43/58 = 0.7413\dots$, and for the next step one had to wait until 1949, when I.M. Vinogradov [6438] obtained $c \leq 113/162 = 0.6975\dots$, six years later [6439] improved this to $c \leq 11/16 = 0.6875$, and stated in 1960 [6444] that he could show $c \leq 19/28 = 0.6785\dots$. Later J.R. Chen [1014] got $c \leq 35/52 = 0.6730\dots$, and I.M. Vinogradov [6445] and J.R. Chen [1016, 1017] showed $c \leq 2/3$. This was made more precise by I.M. Vinogradov [6446] (see also his book [6448]), who proved

$$r(x) \ll x^{2/3} \log^6 x.$$

The next improvement came from F. Chamizo and H. Iwaniec [987], who in 1995 got $c \leq 29/44 = 0.6590$. The best known evaluation of the error term is due to D.R. Heath-Brown [2655], who four years later proved $c \leq 21/32 = 0.65625$.

On the other hand it is known that one has $r(x) = \Omega_-((x \log x)^{1/2})$, as shown by G. Szegő²⁴⁶ [6017] in 1926, and in 2000 K.M. Tsang [6204] obtained $r(x) = \Omega_+((x \log x)^{1/2})$, improving upon a previous result by W.G. Nowak [4636].

²⁴⁶Gábor Szegő (1895–1985), professor in Königsberg, St. Louis and at Stanford. See [154].

This problem is closely related to a question in the theory of equivalence classes of binary quadratic forms. This notion goes back to Lagrange, who in a long paper [3611] considered binary quadratic forms

$$f(x, y) = ax^2 + bxy + cy^2 \quad (2.83)$$

with rational integral coefficients a, b, c and fixed discriminant $d(f) = b^2 - 4ac$. A form is called *primitive* if $(a, b, c) = 1$. In the case of a negative discriminant only positive definite forms (i.e., with $a > 0$) were considered. Lagrange defined two forms f, g to be equivalent if one could transform f into g by a linear substitution

$$x' = ax + by, \quad y' = cx + dy,$$

assuming that the matrix

$$\mathfrak{M} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

lies in the group $GL_2(\mathbf{Z})$, i.e., $a, b, c, d \in \mathbf{Z}$ and $\det(\mathfrak{M}) = \pm 1$. The *class-number*, i.e., the cardinality of the set of equivalence classes, turned out to be finite. Later Gauss [2208] built an extensive theory of quadratic forms, however he distinguished between *proper* and *improper equivalence*, depending on the sign of the determinant (proper equivalence of two forms meaning their equivalence under the action of $SL_2(\mathbf{Z})$). Moreover he considered only forms with even middle coefficient in which case the discriminant is a multiple of 4. The number of equivalence classes of primitive forms of discriminant d is usually denoted by $h(d)$, and in the older literature the number of classes of Gaussian forms $aX^2 + 2bXY + cY^2$ with the determinant $D = b^2 - ac$ was denoted by $H(D)$, thus $H(D) = h(4D)$.

Much later it was shown by B.J. Birch and J.R. Merriman [535] that if one defines, in the same way, the equivalence of two binary forms with integral coefficients in a fixed algebraic number field, having the same degree and discriminant, then the number of resulting classes is finite. An effective proof of this result was given by K. Győry [2400] for forms over \mathbf{Z} and by J.-H. Evertse and K. Győry [1934] in the general case (cf. A.Bérczes, J.-H. Evertse, K. Győry [425], J.-H. Evertse [1925]). This has been generalized to the case of decomposable forms in several variables by J.-H. Evertse and K. Győry [1935].

It was shown by Gauss ([2208, Sect. 291], cf. also [3526]) that if $r_3(n)$ is the number of representations of the number n as the sum of three squares, then r_3 and H are related by the formula

$$r_3(n) = \begin{cases} 12H(n) & \text{if } n \equiv 1 \pmod{4} \text{ and } n \text{ is not a square,} \\ 8H(n) & \text{if } n \equiv 3 \pmod{8}, \\ 12H(n) & \text{if } n \equiv 2 \pmod{4}, \\ 12H(n) - 6 & \text{if } n \text{ is an odd square.} \end{cases}$$

Since $r_3(n) = r_3(n/4)$ in the case $4|n$, and

$$H(4n) = \begin{cases} 2H(n) - 1 & \text{if } n \text{ is an odd square,} \\ 2H(n) & \text{otherwise,} \end{cases}$$

then, as shown by E. Landau [3642–3644], the asymptotics of

$$\mathcal{H}(x) = \sum_{d \leq x} H(-d),$$

can be deduced from evaluations of the sum $\sum_{a^2+b^2+c^2 \leq x} 1$, in which a, b, c are restricted to fixed residue classes mod 2.

The study of $\mathcal{H}(x)$ has its origin in Gauss's book [2208], where it is stated in Sect. 302 that $\mathcal{H}(x)$ is asymptotically equal to

$$\frac{4\pi}{21\zeta(3)}x^{3/2} - \frac{2}{\pi^2}x + o(x). \quad (2.84)$$

Although Gauss asserted that he found that formula “through theoretical investigations,” his book does not contain the proof of this assertion. If one also admits forms with b odd, then Gauss's formula has to be modified to the form,

$$\mathcal{H}'(x) = \sum_{d \leq x} h(-d) = \frac{\pi}{18\zeta(3)}x^{3/2} - \frac{3}{2\pi^2}x. \quad (2.85)$$

The first proof of a result about $\mathcal{H}(x)$ is due to F. Mertens [4257], who established that in fact $\mathcal{H}(x)$ is asymptotic to $(4\pi/21\zeta(3))x^{3/2}$. Later E. Landau considered this question, and in 1912 proved [3644] Gauss's assertion (2.84) with the error term $R(x) = O(x^{5/6} \log x)$. The first improvement of this error term was achieved by I.M. Vinogradov who in [6403] slightly reduced the exponent of the logarithm and in [6404] obtained $R(x) = O(x^{3/4} \log^2 x)$.

Subsequent improvements in the bound for the error term in the problem of lattice points in three-dimensional spheres, quoted above, led to corresponding improvements for $\mathcal{H}(x)$ and $\mathcal{H}'(x)$ (see F. Chamizo, H. Iwaniec [988]).

Asymptotic formulas for the sums $\sum_{d \leq x} h^k(-d)$ for integers $k \geq 2$, with $-d$ running over fundamental discriminants, were given by M.B. Barban²⁴⁷ [321] (cf. M.B. Barban, G. Gordover [326] and A.F. Lavrik [3736]). The error terms in these formulas were improved by D. Wolke [6711].

In [6405] I.M. Vinogradov also considered the analogue of formula (2.84) for the case of indefinite binary quadratic forms. Its origin goes back to Gauss, who in [2208, Sect. 304] asserted that the sum

$$\mathcal{H}^+(x) = \sum_{0 < d \leq x} H(d) \log \varepsilon_{4d}$$

(with $\varepsilon_m = x + y\sqrt{m}$, where x, y are the smallest positive integers satisfying $x^2 - my^2 = 4$) is asymptotic to $cx^{3/2}$ with a certain constant c . The value of this constant given in [2208] is not correct, however the true value, $c = \pi^2/18\zeta(3)$ can be found in Gauss's manuscripts.

The equality

$$\mathcal{H}^+(x) = cx^{3/2} + O(x \log x)$$

²⁴⁷Mark Borisovič Barban (1935–1968), professor in Taškent. See [6402].

has been established as late as in 1944 by C.L. Siegel [5764]. Later, in 1975, T. Shintani [5706] proved the equality

$$\mathcal{H}^+(x) = cx^{3/2} + c_1x \log x + c_2x + O(x^a),$$

with explicitly given constants c_1, c_2 and any $a > 3/4$. In 2006 F. Chamizo and A. Ubis [986] obtained a similar asymptotic formula for the sum

$$\sum_{0 < d \leq x} H(d) \log \varepsilon_d.$$

The case when the summation runs only over fundamental discriminants (in which case the corresponding sums give mean values for the class-number of imaginary quadratic fields and the product of the class-number by the regulator of real quadratic fields) was treated in 1985 by D. Goldfeld and J. Hoffstein [2260]. This was later extended by B. Datskovsky [1338], who considered similar sums with conditions on ramification of given finitely many primes. Cf. P. Sarnak [5405, 5406] and N. Raulf [5132].

The asymptotic behavior of the related sum $\mathcal{H}_0(x) = \sum_{0 < d \leq x} H(d)$ is still unknown. In 1984 C. Hooley [2898] conjectured the equality

$$\mathcal{H}_0(x) = \left(\frac{25}{12\pi^2} + o(1) \right) x \log^2 x,$$

which remains unproved.

Surprisingly, a similar question for class-numbers of irreducible binary cubic forms of given discriminant found its answer in 1951 (H. Davenport [1364, 1365]). In the case of higher degree, only partial results are known (J. Nakagawa [4526]).

3. Similar questions have also been considered in higher dimensions. Denote by $P_k(x)$ the number of points with integral coordinates in a sphere of radius \sqrt{x} in k -dimensional real space, i.e.,

$$P_k(x) = \sum_{a_1^2 + \dots + a_k^2 \leq x} 1,$$

and let $V_k(x) = c_k x^{k/2}$ with

$$c_k = \frac{\pi^{k/2}}{\Gamma(1 + k/2)}$$

be the volume of that sphere. The problem consists of the evaluation of the difference

$$D_k(x) = |P_k(x) - V_k(x)|,$$

and the first result in the case $k \geq 3$ seems to be due to H. Minkowski [4326], who proved in 1905 the evaluation

$$D_k(x) = O(x^{(k-1)/2}). \quad (2.86)$$

In the case $k = 4$ the bound (2.86) was improved by E. Landau [3642, 3643] to $D_4(x) \ll x^{1+\varepsilon}$ for every positive ε , but his proof, as noted in [3667, 3668], actually gives the stronger bound $D_4(x) = O(x \log x)$.

The next improvement for $k = 4$ was obtained in 1927 by A. Walfisz [6526], who deduced $D_4(x) \ll x \log x / \log \log x$ from his formula²⁴⁸

$$\sum_{n \leq x} \frac{\sigma(n)}{n} = \frac{\pi^2}{6}x - \frac{1}{2} \log x + O\left(\frac{\log x}{\log \log x}\right).$$

In [6527], published in 1931, he considered the second moment of $D_4(x)$ and showed

$$\int_1^x D_4^2(t) dt = \frac{2\pi^2}{3}x^3 + O(x^{5/2} \log x),$$

improving upon a result of V. Jarník [3112–3114], who had the bound $O(x^3)$. Much later L.K. Hua [2932] proved $D_4(x) \ll x \log^{3/4} x (\log \log x)^{1/2}$, and the best known result is due to A. Walfisz, who in the Russian edition of his book [6532] gave the bound

$$D_4(x) \ll x \log^{2/3} x.$$

On the other hand, in 1927 A. Walfisz [6526] proved $D_4(x) = \Omega(x \log \log x)$, and the more precise results $D_4(x) = \Omega_+(x \log \log x)$ and $D_4(x) = \Omega_-(x \log \log x)$ were obtained in the nineties by S.D. Adhikari, R. Balasubramanian and A. Sankaranarayanan [16] and S.D. Adhikari and Y.-F.S. Pétermann [17], respectively.

The case $k \geq 5$ turned out to be the simplest. In this case it was observed by V. Jarník (see [3668]) that the bound

$$D_k(x) \ll x^{k/2-1},$$

proved in 1924 in the thesis of A. Walfisz [6516], cannot be improved.

In 1927, for $P_k(n)$ ($k \geq 5$, n integral) H. Petersson²⁴⁹ [4804] obtained the expansion

$$P_k(n) = \sum_{j=0}^{[(n-1)/4]} \alpha_{k,j}(n) (n+1/2)^{k/2-j} + O(n^{k/4} \log n),$$

with bounded $\alpha_{k,j}(n)$, using the theory of theta-functions and complex integration. For $5 \leq k \leq 8$ he got a better error term, namely $O(n)$ for $k = 5, 7$ and $O(n \log n)$ for $k = 6, 8$. A very detailed exposition of these results for $k \geq 4$ is contained in the book by A. Walfisz [6532].

4. A natural generalization of the circle problem concerns the number of integral points in an ellipse, or, more generally, in a k -dimensional ellipsoid $Ell(x)$, defined by the equation

$$F(x_1, \dots, x_k) \leq x,$$

where F is a positive definite quadratic form with real coefficients. Let $D = D(F)$ be the discriminant of F . There is a difference of behavior between forms which are constant multiples of forms with rational coefficients (such forms are called *rational*), and all other forms, called *irrational*.

²⁴⁸Much later he showed the error term to be $O(x \log^{4/5} x \log \log x)$ [6521].

²⁴⁹Hans Petersson (1902–1984), student of Hecke, professor in Hamburg and Münster. See [6709].

E. Landau showed in [3642, 3643] that if $N(x)$ is the number of integral points in $Ell(x)$, and

$$V = \frac{\pi^{k/2}}{\Gamma(1 + \frac{k}{2})\sqrt{D}}$$

is the volume of $Ell(1)$, then

$$P(x) = N(x) - Vx^{k/2} = O(x^{\lambda+\varepsilon}),$$

holds for every $\varepsilon > 0$ with $\lambda = k(k-1)/2(k+1)$ (later [3651] he was able to remove ε from this formula).

In the case of rational f and $k=4$, E. Landau [3667, 3668] proved $P(x) \ll x \log^2 x$, and this was improved in the case of diagonal forms to $O(x \log x)$ by H.D. Kloosterman [3370]. In 1932 A. Walfisz [6519] utilized the connection between lattice points in ellipsoids and modular functions discovered by E. Hecke [2687] to get the bound $P(x) = O(x \log x / \log \log x)$. Later [6521] he got $P(x) = O(x \log^{4/5} x \log \log x)$, and in 1960 reduced the bound to $P(x) \ll x \log^{2/3} x$ [6534]. The second moment of $P(x)$ was considered in 1935 by A. Walfisz [6519], who used modular forms to achieve

$$\int_0^x P^2(t) dt = cx^3 + O(x^{5/2} \log^2 x)$$

with $c > 0$. Later [6520] he found a simpler proof.

For $5 \leq k \leq 7$ the bound

$$P(x) \ll x^{k/2-1}$$

was established in 1924 by E. Landau [3667] and A. Walfisz [6516] proved the same evaluation for all $k \geq 8$. A. Walfisz also showed [6517] that for $k \geq 5$ this bound is best possible.

The case of irrational f turned out to be much harder. For diagonal forms with exactly one irrational coefficient, say α , A. Walfisz [6518] proved in 1927 the bound

$$P(x) = o(x^{k/2-1})$$

for $k \geq 10$, showed that this evaluation cannot be improved and obtained a slightly stronger result holding for almost all α . This last result was superseded in the following year by V. Jarník who in [3108] proved that for almost all diagonal forms in $k \geq 4$ variables one has

$$P(x) \ll x^{k/4+\varepsilon}$$

for every $\varepsilon > 0$ (cf. [3115]). He also obtained, for such forms, the evaluation

$$P(x) \ll \begin{cases} x^{k/2-1} \log x & \text{if } k \geq 5, \\ x \log^2 x & \text{if } k = 4. \end{cases}$$

In [3109] he proved that for every irrational diagonal form in at least six variables one has

$$P(x) = o(x^{k/2-1})$$

and

$$P(x) = \Omega(x^{(k-1)/4}).$$

For $k=5$, V. Jarník and A. Walfisz [3117] showed later that $P(x) = o(x^{3/2})$ and in the case $k=4$ obtained $P(x) = \Omega(x \log \log x)$.

Optimal lower and upper bounds for the first and second moment of $P(x)$ in the case of rational diagonal forms were given by V. Jarník in the last two parts of [3112–3114].

Analogous questions for shifted ellipsoids, defined by

$$\sum_{i,j=1}^n a_{ij}(X_i - b_i)(X_j - b_j) \leq x$$

with rational a_{ij} , b_i were studied by E. Landau [3668] and Ch.H. Müntz [4481].

5. In 1914 D. Cauer [967] considered in his thesis the number $A_\lambda(t)$ of lattice points in the region bounded by the curve defined by

$$|x|^\lambda + |y|^\lambda = t,$$

and showed that for every real $\lambda \geq 2$ the equality

$$A_\lambda(t) = \frac{2\Gamma^2(1/\lambda)}{\lambda\Gamma(2/\lambda)} t^{2/\lambda} + O(t^c)$$

with $c = c(\lambda) = 1/\lambda - 1/(2\lambda^2 - \lambda)$.

The value of c was improved for $\lambda > 3$ to $c \leq 1/\lambda - 1/\lambda^2$ in the thesis of J.G. van der Corput [6274]. For $\lambda = 3$ this was done by E. Krätzel [3514], W.G. Nowak [4630] did this for $\lambda > 41/14 = 2.928\dots$, and W. Müller and W.G. Nowak [4474] extended it to $\lambda > 38/13 = 2.923\dots$. The bound obtained is best possible. See also B. Randol [5102] and S.B. Abialimov [6].

2.6.2.2 Dirichlet's Divisor Problem

1. In 1849 Dirichlet [1590] considered the mean value of the number $d(n)$ (earlier denoted mostly by $\tau(n)$) of positive divisors of an integer n and proved the following asymptotic formula:

$$D(x) = \sum_{n \leq x} d(n) = x \log x + (2\gamma - 1)x + \Delta(x), \quad (2.87)$$

where $\Delta(x) = O(x^{1/2})$ and $\gamma = 0.577215\dots$ is Euler's constant²⁵⁰, defined by

$$\gamma = \lim_{n \rightarrow \infty} \left(\sum_{k=1}^n \frac{1}{k} - \log n \right).$$

Since

$$\sum_{n \leq x} d(n) = \sum_{n \leq x} \sum_{d|n} 1 = \sum_{d \leq x} \sum_{\substack{n \leq x \\ d|n}} 1 = \sum_{d \leq x} \left[\frac{x}{d} \right],$$

²⁵⁰Whether γ is irrational is an old unsolved problem.

the function $D(x)$ counts lattice points (a, b) with $1 \leq a \leq x$, $b \geq 1$, lying under the hyperbola $y(t) = x/t$. Dirichlet's idea consisted of separately considering points (a, b) with $a \leq \sqrt{x}$ and $b \leq \sqrt{x}$, which leads to

$$D(x) = 2 \sum_{a \leq \sqrt{x}} \sum_{b \leq x/a} 1 - \sum_{a, b \leq \sqrt{x}} 1 = 2x \sum_{a \leq \sqrt{x}} \frac{1}{a} - x + O(\sqrt{x}),$$

and so his result is a consequence of the formula

$$\sum_{n \leq t} \frac{1}{n} = \log t + \gamma + O\left(\frac{1}{t}\right).$$

In a letter to Kronecker [1591], Dirichlet asserted that he can reduce the exponent in the error term in (2.87) but gave no details and the first published improvement of Dirichlet's evaluation was obtained by G.F. Voronoï [6469] in 1903. He used a special partition of the region $\{(x, y) : x, y \geq 1, xy \leq t\}$ in the plane to deduce that the error term in (2.87) is of the order $O(x^{1/3} \log x)$. In the next year [6470] he proved a Bessel function expansion of the sum

$$\sum_{n=a}^b d(n) f(n),$$

where f is a continuous function, having only finitely many maxima and minima in the interval (a, b) . This gave, in particular, an expansion of $D(x)$ (cf. G.H. Hardy [2508], H. Cramér [1270], W.W. Rogosinski²⁵¹ [5261], A. Walfisz [6515]).

Simpler proofs were later provided by N.S. Košliakov [3494, 3495], A.L. Dixon²⁵² and W.L. Ferrar [1596], J.R. Wilton [6684], T. Meurman [4275].

Similar expansions for sums $\sum_{n \leq x} F(n)$ were later obtained for various arithmetic functions F . For $F = \sigma_k$ this was done in 1927 by A. Oppenheim [4689] (cf. J.R. Wilton [6685]), and for $F = r_2$ by J.R. Wilton [6680] in 1928.

Voronoï's formula formed a special case of a more general conjectured expansion (*Voronoï's summation formula*), generalizing the classical Poisson formula. In the simplest case it has the following form.

For every arithmetic function $A(n)$ there exist analytic functions $\alpha(x)$ and $\delta(x)$ such that for every function f continuous in $[a, b]$ and having there finitely many maxima and minima, one has

$$\begin{aligned} & \frac{A(a)f(a) + A(b)f(b)}{2} + \sum_{n=a+1}^{b-1} A(n)f(n) \\ &= \int_a^b f(t)\delta(t) dt + \sum_{n=1}^{\infty} A(n) \int_a^b f(t)\alpha(nt) dt. \end{aligned}$$

²⁵¹Werner Wolfgang Rogosinski (1894–1946), professor in Königsberg and at the University of Durham.

²⁵²Arthur Lee Dixon (1867–1955), professor in Oxford. See [1994].

For certain classes of arithmetical functions this conjecture has been established by A. Walfisz [6523, 6524] in 1925, N.S. Košliakov [3494] in 1928, W.L. Ferrar [1992, 1993] in 1935, A.P. Guinand [2379] in 1937, and B.C. Berndt [444–446] in 1969–1972.

E. Landau [3644, 3649] gave fresh proofs of Voronoï's bound for $\Delta(x)$, and in [3642, 3643] proved a very general theorem concerning the sum of coefficients $A(x) = \sum_{n \leq x} a_n$ of a Dirichlet series $\sum_{n=1}^{\infty} a_n n^{-s}$. This theorem asserted that if the series converges in a half-plane $\Re s > \alpha$, its coefficients satisfy, for every positive ε , the inequality $|a_n| \ll n^{\alpha+\varepsilon}$, the function $f(s)$ defined by this series satisfies a kind of functional equation and does not grow too quickly when $|\Im s|$ tends to infinity, then the sum $A(x)$ is well approximated by the sum of residues of $x^s f(s)/s$ in a certain well-defined perpendicular strip. This allowed him to make important progress in the problem of evaluation of the number of points with integral coordinates in various regions. In particular, this led to a new proof of Voronoï's result.

2. It is not difficult to show (see, e.g., [3661]) that the error term in the divisor problem equals

$$\Delta(x) = -2 \sum_{n \leq \sqrt{x}} \left(\left\{ \frac{x}{n} \right\} - \frac{1}{2} \right) + O(1),$$

so all further work was aimed at the evaluation of the sum occurring here. Since the Fourier series of the function $\alpha(t) = \{t\} - 1/2$ has the form

$$\alpha(t) = -\frac{1}{\pi} \sum_{n=1}^{\infty} \frac{\sin(2\pi nt)}{n} = \frac{i}{2\pi} \sum_{\substack{n \in \mathbb{Z} \\ n \neq 0}} \frac{\exp(2\pi n x t i)}{n},$$

one can approximate $\alpha(t)$ by a convenient partial sum of this series, and the whole question is reduced to a good evaluation of the resulting exponential sum. This type of argument is applicable to a wealth of number-theoretical problems, and this explains why evaluations of exponential sums became a very important tool.

A lower bound for $\Delta(x)$ was furnished by G.H. Hardy [2507, 2508], who obtained

$$\limsup_{x \rightarrow \infty} \frac{\Delta(x)}{(x \log x)^{1/4} \log \log x} > 0,$$

and

$$\liminf_{x \rightarrow \infty} \frac{\Delta(x)}{x^{1/4}} < 0.$$

Much later A.E. Ingham [3022] showed

$$\liminf_{x \rightarrow \infty} \frac{\Delta(x)}{x^{1/4}} = -\infty.$$

It is conjectured that $\Delta(x)$ is of the order $O(x^{1/4+\varepsilon})$ for every $\varepsilon > 0$, and this is supported by a result by G.H. Hardy [2509], who proved

$$\frac{1}{x} \int_1^x |\Delta(t)| dt \ll x^{1/4+\varepsilon}$$

for every positive ε .

The best known lower bound for $\Delta(x)$ is due to K. Soundararajan [5852], who obtained

$$\Delta(x) = \Omega\left((x \log x)^{1/4} (\log \log x)^a (\log \log \log x)^{-5/8}\right)$$

with $a = 1.139 \dots$. The previous record belonged to J.L. Hafner [2429], who in 1981 got

$$\Delta(x) = \Omega_+\left((x \log x)^{1/4} (\log \log x)^{(3+\log 4)/4} \exp(-c(\log \log \log x)^{1/2})\right),$$

with a certain $c > 0$, improving upon previous results of K.S. Gangadharan [2190] and K. Corrádi, I. Kátai [1250].

The first improvement of Voronoï's upper bound was obtained by J.G. van der Corput [6277] who in 1922 obtained

$$\Delta(x) \ll x^a$$

with $a \leq 163/494 = 0.32995 \dots$. He applied his method of dealing with exponential sums developed in [6276], as well as Weyl's evaluations of such sums [6647]. In 1923 he presented a survey of various methods of dealing with the divisor and circle problems and their generalizations in a talk in Geneva [6280], and five years later [6282] improved the bound to

$$\Delta(x) \ll x^a \log^b x$$

with $a = 27/82 = 0.3292 \dots$ and $b = 11/41$, using evaluations of sums of the form

$$\sum_{n=a}^b \exp(4\pi i \sqrt{un}),$$

with a suitable parameter u , which are special cases of the main result of [6279].

Later the following evaluations of the form $\Delta(x) \ll x^{a+\varepsilon}$ for every positive ε were obtained:

- $a = 15/46 = 0.3260 \dots$ (T. Chih [1054], H.-E. Richert [5204]),
- $a = 13/40 = 0.325$ (W.L. Yin [6778]),
- $a = 12/37 = 0.3243 \dots$ (G. Kolesnik [3453]),
- $a = 346/1067 = 0.3242 \dots$ (G. Kolesnik [3454]),
- $a = 35/108 = 0.3240 \dots$ (G. Kolesnik [3456]),
- $a = 7/22 = 0.3181 \dots$ (H. Iwaniec, C.J. Mozzochi [3067]; cf. W.Müller, W.G. Nowak [4475]),
- $a = 23/73 = 0.315 \dots$ (M.N. Huxley [2982]).

Now the record is held by M.N. Huxley [2983], who in 2003 got $a = 131/416 = 0.31498 \dots$.

The behavior of higher moments

$$M_k(x) = \int_1^x |\Delta^k(t)| dt$$

and

$$M_k^*(x) = \int_1^x \Delta^k(t) dt \quad (2 \nmid k)$$

of the error term in the divisor problem is, for large k , still unknown. The evaluation

$$M_1^*(x) = o(x^{5/4})$$

follows from results by G.F. Voronoï [6470], and H. Cramér [1269] established

$$M_2(x) = cx^{3/2} + \Delta_2(x)$$

with $\Delta_2(x) \ll x^{5/4+\varepsilon}$ for every $\varepsilon > 0$ (earlier G.H. Hardy [2509] proved $M_2(x) \ll x^{3/2+\varepsilon}$ for all $\varepsilon > 0$). Cramér's result supports the conjecture about the true order of $\Delta(x)$.

In 1956 K.C. Tong [6191, 6192] reduced the last bound to $O(x \log^5 x)$, and in 1988 E. Preissmann [5010] diminished it to $O(x \log^4 x)$. This seems to be fairly close to the optimal bound, as this error term is certainly not $o(x \log^2 x)$ (Y.K. Lau, K.M. Tsang [3733]). It was conjectured by Tsang [6203] that

$$\Delta_2(x) = -\frac{1}{4\pi^2} x \log^2 x + cx \log x + O(x)$$

holds with a certain constant c .

One conjectures also that $M_k(x)$ equals $(c_k + o(1))x^{1+k/4}$ with a certain $c_k > 0$, but this has been established only for $k \leq 9$ by D.R. Heath-Brown [2648], who showed also the existence of the limits

$$\lim_{x \rightarrow \infty} M_k^*(x) x^{-1-k/4}$$

for these k . For the values of c_k and bounds of the corresponding error terms see K.M. Tsang [6202], A. Ivić, P. Sargos [3047] for $k = 3, 4$, and W. Zhai [6821–6823] for $4 \leq k \leq 9$.

In 1952 P. Erdős [1807] proved that if $f \in \mathbf{Z}[X]$ is irreducible, then the ratio

$$\frac{1}{x \log x} \sum_{n \leq x} d(f(n))$$

lies between two positive constants depending on f (for a correction see F. Delmer [1453]). For reducible polynomials a corresponding result was obtained in 1968 by V. Ennola [1767].

If f is linear the problem reduces to the evaluation of the sum

$$D(x; q, a) = \sum_{\substack{n \leq x \\ n \equiv a \pmod{q}}} d(n).$$

Such sums were considered in 1957 by A.I. Vinogradov and Yu.V. Linnik [6401], who showed that for $c < 1$, $q \leq x^c$ and $(a, q) = 1$ one has

$$|D(x, q, a)| \ll_c \frac{x}{q} \prod_{p|q} \left(1 - \frac{1}{p}\right) \quad (2.88)$$

(see M.G. Qi [5020] for a correction). Also in 1957 C. Hooley [2855], applied Weil's evaluations of Kloosterman sums to show that for $q < x^{2/3}$ one has, with suitable $A > 0$,

$$D(x; q, a) = \left(1 + O\left(\frac{1}{\log^c x}\right)\right) \sum_{\substack{n \leq x \\ (a, q)=1}} d(n),$$

uniformly in $q \leq x^a$. H.G. Kopetzky [3474] gave explicit formulas for the coefficients α, β in the equality

$$D(x; q, a) = \alpha(q, a)x \log x + \beta(q, a)x + O(\sqrt{x}),$$

valid for fixed q . The error term was later diminished to $O(x^c)$ for every $c > 35/108 = 0.3240\dots$ by W.G. Nowak [4634].

For further progress see É. Fouvry [2049] and É. Fouvry, H. Iwaniec [2057].

In the quadratic case there is an asymptotical equality

$$\sum_{n \leq x} d(an^2 + \beta n + \gamma) = (A + o(1))x \log x,$$

proved (according to P. Erdős [1807]) by R. Bellman and H.N. Shapiro. More precise results were later obtained by C. Hooley [2859], N. Gafurov [2174] and J. McKee [4232, 4233]. See also E.J. Scourfield [5590].

3. The question of the asymptotic behavior of the sum

$$S_\alpha(x) = \sum_{n \leq x} \sigma_\alpha(n)$$

can be regarded as a generalization of the divisor problem, to which it reduces in the case $\alpha = 0$. Already Dirichlet [1590] had considered the sum $S_1(x)$ and proved that it equals $cx^2 + O(x \log x)$ with $c = \pi^2/12$. In 1914 S. Wigert²⁵³ [6666] established

$$S_{-1}(x) = \frac{\pi^2}{6}x + O(\log x),$$

and elementary methods lead, for $0 < |\alpha| < 1$, to

$$S_\alpha(x) = \zeta(1 - \alpha)x + \frac{\zeta(1 + \alpha)}{1 + \alpha}x^{1+\alpha} + T_\alpha(x),$$

with $T_\alpha(x) = o(x^{1-\alpha})$.

The maximal order of σ_a was determined in 1913 by T.H. Gronwall [2350]:

$$\limsup_{n \rightarrow \infty} \frac{\sigma_a(n)}{n^a} = \zeta(a) \quad (a > 1),$$

$$\limsup_{n \rightarrow \infty} \frac{\sigma(n)}{n \log \log n} = e^\gamma,$$

γ being Euler's constant, and

$$\limsup_{n \rightarrow \infty} \frac{\log(\sigma_a(n)/n^a) \log \log n}{\log^{1-a} n} = \frac{1}{1-a}, \quad 0 < a < 1.$$

The equality

$$\limsup_{n \rightarrow \infty} \frac{\log d(n) \log \log n}{\log n} = \log 2$$

had earlier been proved by S. Wigert [6665].

In 1927 A. Walfisz [6526] established

$$S_{-1}(x) = \frac{\pi^2}{6}x - \frac{\log x}{2} + O\left(\frac{\log x}{\log \log x}\right)$$

²⁵³Severin Wigert (1871–1941), worked in Stockholm.

and

$$S_1(x) = \frac{\pi^2}{12}x + O\left(\frac{x \log x}{\log \log x}\right),$$

and now it is known that

$$S_1(x) = \frac{\pi^2}{12}x + O(x \log^{2/3+\varepsilon} x)$$

holds for every $\varepsilon > 0$ (N.M. Korobov [3487]). On the other hand, it has been shown by Y.-F.S. Pétermann [4799] that the error term is $\Omega(x \log \log x)$ (for the case $25/38 < |a| < 1$ see [4800]).

In [6527], which appeared in 1931, A. Walfisz obtained evaluations of the second moment of the error terms T_α in the case $\alpha = \pm 1$, showing

$$\int_1^x T_\alpha^2(t) dt = \begin{cases} c_{-1}x + O(x^{1/2} \log x) & \text{if } \alpha = -1, \\ c_1x^3 + O(x^{5/2} \log x) & \text{if } \alpha = 1. \end{cases}$$

Similar results for $\alpha \in (-1, 1)$, $|\alpha| \neq 1/2$ were later obtained by H. Cramér [1269, 1271] and S. Chowla [1071]. The case $|\alpha| = 1/2$ was treated in Walfisz's paper [6528]. For integral α see R.A. MacLeod [4053, 4054].

4. There is another generalization of the divisor problem, going back to the dissertation of A. Piltz [4876] who considered the summatory function $D_k(x)$ of coefficients of the Dirichlet series for $\zeta^k(s)$. These coefficients have a simple arithmetic interpretation as it can easily be seen that for $\Re s > 1$ we have

$$\zeta^k(s) = \sum_{n=1}^{\infty} \frac{d_k(n)}{n^s}, \quad (2.89)$$

where $d_k(n)$ denotes the number of representations of n as a product of k factors. In particular $d_2(n)$ coincides with the number of divisors of n . Piltz proved the asymptotic formula

$$D_k(x) = x A_k(\log x) + \Delta_k(x), \quad (2.90)$$

where $A_k(x)$ is a polynomial of degree $k - 1$, and

$$\Delta_k(x) = O(x^{1-1/k} \log^{k-2} x) \quad (k \geq 2).$$

A simpler proof was given by E. Landau [3647] in 1912.

If we denote by α_k the lower bound of the numbers α for which the bound $\Delta_k(x) = O(x^\alpha)$ holds, then Piltz's result gives $\alpha_k \leq 1 - 1/k$. The first improvements of this bound were given by E. Landau [3642, 3643], who used his general theorem about sums of coefficients of Dirichlet series to obtain $\alpha_k \leq (k-1)/(k+1)$ for $k \geq 3$, and in [3649] proved

$$\Delta_k(x) \ll x^{(k-1)/(k+1)} \log^{k-1} x.$$

At the same time he observed [3642, 3643] that the Riemann Hypothesis implies $\alpha_k \leq 1/2$. On the other hand one has $\alpha_k \geq 1/2 - 1/2k$ (G.H. Hardy [2508]).

The next improvement was obtained by G.H. Hardy and J.E. Littlewood [2530], who proved $\alpha_k \leq 1 - 2/k$ for $k \geq 4$ and in [2527] obtained²⁵⁴ $\alpha_k \leq 1 - 3/(k+2)$. Moreover they showed in [2533] that the evaluation $\alpha_k \leq 1/2$, as well as

$$\int_1^x \Delta_k^2(t) dt \ll x^{1-1/k+\varepsilon}$$

for every $\varepsilon > 0$ and $k = 1, 2, \dots$, are both equivalent to the Lindelöf conjecture.

The lower bound for α_k had been made more precise first by K.C. Tong [6192] in 1956, then by J.L. Hafner [2430], but the best known result is due to K. Soundararajan [5852], who in 2003 showed

$$\Delta_k(x) = \Omega((x \log x)^{1/2-1/2k} (\log \log x)^a (\log \log \log x)^{-b}),$$

with $a = (1 + 1/2k)(k^{2k/(k+1)} - 1)$, $b = 1/2 + (k-1)/4k$.

The mean value of $|\Delta_k(x)|$ was first evaluated in 1922 by H. Cramér [1270], who for $k \geq 3$ got

$$\int_1^x |\Delta_k(t)| dt \ll x^{2-1/2k+\varepsilon}$$

for every $\varepsilon > 0$.

In the case $k = 3$ A. Walfisz [6525] got $\alpha_3 \leq 43/87 = 0.4942\dots$ in 1926, and several years later F.V. Atkinson²⁵⁵ [168] proved $\alpha_3 \leq 37/75 = 0.4933\dots$. This was slightly improved by R.A. Rankin [5115] and further improvements followed:

- $\alpha_3 \leq 14/29 = 0.4827\dots$ (M.I. Yüh [6804]),
- $\alpha_3 \leq 25/52 = 0.4807\dots$ (W.L. Yin [6779]),
- $\alpha_3 \leq 8/17 = 0.4705\dots$ (M.I. Yüh, F. Wu [6805]),
- $\alpha_3 \leq 5/11 = 0.4545\dots$ (J.R. Chen [1019]),
- $\alpha_3 \leq 43/96 = 0.4479\dots$ (G. Kolesnik [3455]).

For larger values of k , upper bounds were given by H.-E. Richert [5207] who showed that for a_k one can take any number exceeding $1 - ck^{-2/3}$ with a certain constant $c > 0$. Later A.A. Karatsuba [3251] made this more precise by establishing

$$\alpha_k \leq 1 - \frac{1}{2(200k)^{2/3}}$$

for large k . Improvements were later provided by A. Ivić [3037], D.R. Heath-Brown [2631], A. Ivić and M. Ouellet [3039, 3046] and K. Ford [2032], who obtained

$$\alpha_k \leq 1 - \frac{0.195\dots}{k^{2/3}}.$$

The mean value of the error term was evaluated by I. Kiuchi [3347] and T. Meurman [4276].

The Piltz problem in arithmetical progressions was considered in 1966 by A.F. Lavrik [3734], who obtained an asymptotical formula for the sum

$$\sum d_k(n)$$

extended of $n \leq x$, congruent to $a \bmod q$.

²⁵⁴This was slightly improved for $k \geq 5$ by A. Walfisz [6522].

²⁵⁵Frederick Valentine Atkinson (1916–2002), professor in Ibadan, Canberra and Toronto. See [4317].

The error term was later improved by A.F. Lavrik and Ž. Edgorov [3738], Ž. Edgorov [1686], M.M. Petečuk [4796] (for prime power q), R.A. Smith [5837], K. Matsumoto [4198], J.B. Friedlander and H. Iwaniec [2105, 2106], D.R. Heath-Brown [2641], C.E. Chace [977] and H. Li [3876].

One also considers the analogue of the Piltz problem in algebraic number fields, consisting of the evaluation of the difference between the sum of the coefficients a_n (with $n \leq x$) of an m th power of Dedekind zeta-function $\zeta_K(s)$ and the sum of residues at $s = 0$ and $s = 1$ of $\zeta_K^m(s)x^s/s$. This problem was studied by G. Szegő and A. Walfisz [6018, 6019, 6523, 6524]. The strongest known lower bounds for the error term are due to K. Girstmair, M. Kühleitner, W. Müller and W.G. Nowak [2240], who proved analogues of K. Soundararajan's [5852] bounds in the divisor problem. Upper bounds were provided by A. Ivić [3041] and W.G. Nowak [4642].

A recent survey of various questions connected with the divisor problem has been prepared by A. Ivić and E. Krätzel [3043].

A related problem was considered in 1932 by O. Hölder²⁵⁶ [2848], who considered the mean value of $t_k(n)$, the number of k -free divisors of n .

2.7 Diophantine Equations and Congruences

1. In 1887 a paper by C. Runge²⁵⁷ [5341] appeared in which certain necessary conditions were given for an equation of the form

$$F(x, y) = 0 \quad (2.91)$$

(where $F \in \mathbb{Z}[X, Y]$ is irreducible) to have an infinite number of integral solutions.

A new proof of Runge's result has been given by T. Skolem [5804]. For improvements see A. Schinzel [5440] and M. Ayad [182].

A quantitative version was given by D.L. Hilliker and E.G. Straus²⁵⁸ [2811] in 1983, and their bounds were later improved by P.G. Walsh [6536]. See also A. Grytczuk, A. Schinzel [2377], S. Tengely [6111], A. Sankaranarayanan, N. Saradha [5392].

Four years later D. Hilbert and A. Hurwitz published a joint paper [2793] in which they considered equations of the form

$$F(x, y, z) = 0,$$

where F is a homogeneous polynomial with integral coefficients, and the corresponding curve Γ in the projective plane is of genus²⁵⁹ zero. They showed that if

²⁵⁶Otto Ludwig Hölder (1859–1937), professor in Tübingen, Königsberg and Leipzig. See [6310].

²⁵⁷Carl David Tolmé Runge (1856–1927), professor in Hannover and Göttingen. See [1260].

²⁵⁸Ernst Gabor Straus (1922–1983), professor at the University of California in Los Angeles. See [889, 1826].

²⁵⁹The simplest way to define the genus of a projective curve Γ over a field k is to say that it is the \bar{k} -dimension of the linear space of holomorphic differential forms of Γ (see, e.g., [5791, Chap. 2]), \bar{k} denoting the algebraic closure of k .

such an equation has infinitely many rational solutions, then Γ is birationally equivalent to a line or a conic. The same result was also obtained by H. Poincaré [4936].

A fresh proof of the Hilbert–Hurwitz theorem was given by D. Poulakis [5002] in 1998.

2. The next important step forward occurred in 1909, when A. Thue [6142] proved his theorem on approximations by rationals and obtained as a corollary the following assertion.

If $F(X, Y) \in \mathbf{Z}[X, Y]$ is an irreducible form of degree $N \geq 3$ with rational integral coefficients, then for every fixed $a \in \mathbf{Z}$ the equation

$$F(x, y) = a \quad (2.92)$$

can have only finitely many integral solutions x, y .

(Such equations are called now *Thue equations*.)

Shortly afterwards E. Maillet [4112] filled some lacuna in Thue’s proof and used Thue’s theorem to show that if $F(X, Y)$ is an irreducible form of degree n with integral coefficients, and $G(X, Y)$ is a polynomial prime to F , of degree $m < n/2 - 1$, then the equation

$$F(x, y) = G(x, y) \quad (2.93)$$

can have only finitely many integral solutions.

Another consequence of Thue’s theorem was presented by its author in 1917 [6144], when he showed that the Diophantine equation

$$ax^2 + bx + c = dy^n$$

can have, for fixed $n \geq 3$, a, b, c, d , only finitely many integral solutions, provided $ad \neq 0$ and $b^2 \neq 4ac$ (cf. L.J. Mordell [4378] and E. Landau, A. Ostrowski [3681]).

An analogous result, with the quadratic polynomial replaced by a cubic one, was obtained by L.J. Mordell [4380], who conjectured in [4379] that the same happens also for polynomials of larger degrees. This was established in the anonymous paper [5746] (signed by “X”) of C.L. Siegel, who deduced from his strengthening of Thue’s theorem given in [5738] that if the polynomial f has no repeated roots, then the equation $y^n = f(x)$ has, for fixed $n \geq 3$, at most finitely many integral solutions. For effective results see Sect. 6.6.

Siegel’s thesis [5738] brought several applications to Diophantine equations. First of all he was able to show that equation (2.93) has finitely many solutions under less stringent assumptions about the degrees, and at the same time he showed the truth of the analogue of this assertion in the case that the rational integers are replaced by integers of a fixed algebraic number field K containing the coefficients of both F and G . He proved also that a polynomial over K , which has at least two different zeros, can represent only finitely many units (i.e., invertible integers of K) at algebraic integral arguments.

3. For a long time it has been known that the minimal solutions of the Pellian equation

$$x^2 - Dy^2 = 1 \quad (2.94)$$

(where D is positive and square-free) may be very large, even for relatively small values of D . The first such example seems to be that presented by J. Wallis²⁶⁰ in 1658, who showed that the minimal solution of the equation $x^2 - 151y^2 = 1$ is $x = 1\,728\,148\,040$, $y = 140\,634\,693$, and another resulted from the solution of the cattle problem attributed to Archimedes (see B. Krummhiesel, A. Amthor [3537], H.W. Lenstra, Jr. [3823], H.L. Nelson [4556]). The first upper bound for the minimal solution was given by R. Remak in 1913 [5158], who showed that in such a solution one has

$$\log y \ll D^{3/2} \log D.$$

In the following year Perron [4786] improved this to

$$\log y \leq (1 + o(1))D \log D,$$

using the observation that if $p(D)$ denotes the length of the period of the continued fraction of \sqrt{D} , then $p(D) \leq D + \sqrt{D}$ and

$$\log y \leq (p(D) + o(1)) \log D. \quad (2.95)$$

In 1916 T. Schmitz [5530] proved that $\log y \leq (8 + o(1))D$, and two years later I. Schur [5574] got

$$\log y \leq \frac{1}{2} \sqrt{D} \log D.$$

Note that minimal solutions of the equations $x^2 - Dy^2 = \pm 1$ and $x^2 - Dy^2 = \pm 4$ are closely related to fundamental units $\varepsilon > 1$ of the quadratic field $K = \mathbf{Q}(\sqrt{D})$, hence bounds for such solutions imply corresponding bounds for the regulator $R(K) = \log \varepsilon$ of K .

For integers D with large values of y in (2.94) see C. Reiter [5156], F. Halter-Koch [2483], Y. Yamamoto [6773].

Later stronger bounds for $p(D)$ were obtained. In 1927 T. Vijayaraghavan [6390] got $p(D) \ll D^{1/2+\varepsilon}$ and in 1942 L.K. Hua [2928] obtained $p(D) \ll \sqrt{D} \log D$. Thirty years later K. Hirst [2829] showed that for square-free D

$$p(D) < 2\sqrt{D} \log D + O(\sqrt{D}),$$

and D.R. Hickerson [2778] obtained for non-square D

$$p(D) \leq D^{1/2} \exp \left(\log 2 \frac{\log D}{\log \log D} + O \left(\frac{\log D \log \log \log D}{(\log \log D)^2} \right) \right).$$

Next, R.G. Stanton, C. Sudler, Jr. and H.C. Williams [5894] proved

$$p(D) < 0.72\sqrt{D} \log D$$

for every square-free $D > 7$, and for non-square D 's they showed

$$p(D) < 3.76\sqrt{D} \log \left(\frac{D}{s^2} \right),$$

²⁶⁰John Wallis (1616–1703), professor in Oxford. See [5587].

where s^2 is the maximal square factor of D . This estimate was improved in 1977 by J.H.E. Cohn [1163] to

$$p(D) < \frac{7}{2\pi^2} \sqrt{D} \log D + O(\sqrt{D})$$

for every non-square D . He showed also that $p(D) = \Omega(\sqrt{D}/\log \log D)$ (cf. J.C. Lagarias [3601]), and in 1986 H.W. Lu [4014] replaced the constant in Cohn's bound by 0.24 in the case of square-free D . The evaluation $p(D) \ll \sqrt{D} \log D$ was conjectured in 1962 by D. Shanks²⁶¹, and numerical support for it was provided by B.D. Beach and H.C. Williams [369]. Since for square-free D

$$p(D) < \frac{\log(x + y\sqrt{D})}{\log \alpha}$$

with $\alpha = (1 + \sqrt{5})/2$ (see [4767, 5894]), hence using Dirichlet's class-number formula jointly with a result of J.E. Littlewood [3945] one sees (E.V. Podsypanin [4925]) that the General Riemann Hypothesis implies

$$p(D) = O(\sqrt{D} \log \log D).$$

A survey of computational aspects was given by H.C. Williams [6674].

4. A formula for the number of solutions of a polynomial congruence modulo a prime was given in 1903 by A. Hurwitz [2959]. It is simpler than the formulas established earlier by J. König (see G. Rados²⁶² [5045] and L. Kronecker [3531, p. 363]), but nevertheless its applicability is limited. Generalizations to the case of equations in finite fields were later obtained by L.E. Dickson [1536] and H.S. Vandiver [6328].

Denote by $S_f(N)$ the number of solutions of the congruence

$$f(X) \equiv 0 \pmod{N},$$

where f is an irreducible polynomial with integral coefficients. If $k \geq 2$ is the degree of f , and $D(f)$ is its discriminant, then the bound

$$S_f(N) \leq k^{\omega(N)} D(f)^2$$

was established in 1921 by O. Ore²⁶³ [4699] in the case when $D(f) \neq 0$, and the leading coefficient of f is prime to N . This was later improved by G. Sándor [5389], and in 1979 M.N. Huxley [2979] established the bound $S_f(N) \leq k^{\omega(N)} \sqrt{|D(f)|}$.

The bound $S_f(N) \leq d^{k-1}(N)N^{1-1/k}$, which does not depend on the discriminant, was established in 1924 by E. Kamke [3230], and much later this was improved by S.V. Konyagin and S.B. Stečkin²⁶⁴ [3473] to

$$S_f(N) \leq \left(\frac{k}{e} + o(\log^2 k) \right) N^{1-1/k}.$$

²⁶¹Daniel Shanks (1917–1996), professor at the University of Maryland. See [6672].

²⁶²Gusztáv Rados (1862–1942), professor in Budapest.

²⁶³Oystein Ore (1899–1968), professor at Yale. See [4710].

²⁶⁴Sergei Borisovič Stečkin (1920–1995), professor in Moscow. See [480, 6252].

Later O.M. Fomenko [2023] obtained

$$\sum_{N \leq x} S_f(N) = C(f)x + O\left(\frac{x}{\log^c x}\right)$$

for every $c < 1/2$, and the error term was shown to be $O(x^{a(d)})$ with explicit $a(d) < 1$ by H.H. Kim [3333] and G. Lü [4013].

Fix a prime p . The *Poincaré series* $P_f(T)$ of a polynomial $f(X_1, \dots, X_N)$ with integral (or rational p -integral, i.e., with denominators not divisible by p) coefficients is defined by

$$P_f(T) = \sum_{n=0}^{\infty} a_n T^n,$$

where $a_0 = 1$ and a_n denotes the number of solutions of the congruence

$$f(x_1, \dots, x_N) \equiv 0 \pmod{p^n}.$$

It seems that this series appeared for the first time in 1964 in the book by Z.I. Borevič²⁶⁵ and I.R. Šafarevič [642], who conjectured that $P_f(T)$ is a rational function. This was confirmed later by J.-I. Igusa [3004, 3005], and a generalization to algebraic varieties was obtained by D. Meuser [4277]. Another proof, based on the elimination of quantifiers, was given by J. Denef [1466, 1467]. On this topic see also J. Denef [1468], A. Macintyre [4051], D. Meuser [4278], J. Pas [4754–4756].

5. The equation

$$\frac{x^m - 1}{x - 1} = \frac{y^n - 1}{y - 1} \quad (y > x \geq 2, m, n \geq 3) \quad (2.96)$$

has been considered in 1917 by R. Goormaghtigh²⁶⁶ [2281], who showed that the only solutions with $(x^m - 1)/(x - 1) \leq 10^6$ are $(m, n, x, y) = (5, 3, 2, 5)$ and $(13, 3, 2, 90)$. It is conjectured that there are no other solutions.

It was observed in 1956 by H.-J. Kanold [3241] that for fixed x, y there are at most finitely many solutions m, n of (2.96), and in 1986 T.N. Shorey [5722] gave the bound 17 for their number. In 2002 this bound was reduced to 2 by Y. Bugeaud and T.N. Shorey [824]. They also proved that if $y > 10^{11}$, then there is at most one solution and six years later B. He and A. Togbé [2623] proved that this holds for every y .

An effective bound for the solutions in the case when the maximal prime divisor of xy is bounded was found by R. Balasubramanian and T.N. Shorey [287] in 1980.

In 1961 H. Davenport, D.J. Lewis and A. Schinzel [1398] also showed that for fixed m, n there are only finitely many solutions x, y .

In the case $m = 3$ and n odd, P.Z. Yuan [6803] has shown that there are no new solutions. This had been known earlier for prime power y (M.H. Le [3749]). Yu.V. Nesterenko and T.N. Shorey [4573] got an explicit bound for the solutions of (2.96) in the case $d = (m - 1, n - 1) \geq 2$. This bound depends on $(m - 1)/d$ and $(n - 1)/d$.

²⁶⁵Zenon Ivanovič Borevič (1922–1995), professor in Leningrad.

²⁶⁶René Victor Goormaghtigh (1893–1960), director of a steel plant in Belgium. See [1418].

2.8 p -Adic Numbers

1. Right at the beginning of the new century K. Hensel had the brilliant idea of considering formal power series in which the role of the variable was played by a fixed prime number and the coefficients were digits $0, 1, \dots, p-1$. These entities were introduced in [2731, 2732] and although at the beginning were regarded rather as a curiosity, they were later to play an overwhelming role in the development of number theory and algebra. Hensel wrote in [2736] that the idea of this new class of numbers has its roots in the theory of algebraic functions, where one studies their behavior through expansions at points of the complex plane. In his new approach the role of points is played by prime numbers. His hope, expressed on page 3 of [2736], that his method would lead to a transcendence test for complex numbers was never fulfilled.

Hensel recapitulated his method in the book [2736], of which only the first volume appeared. He defined in it, for every prime p , the p -adic integers as finite or infinite sequences $C = (c_0, c_1, \dots)$ of digits $0, 1, \dots, p-1$ with properly defined arithmetical operations. He chose the form

$$C = c_0 + c_1 p + c_2 p^2 + \dots,$$

to represent these sequences, pointing out that these series do not converge in the usual sense, but have to be understood as a symbolical way to show that the sequence $c_0, c_0 + c_1 p, c_0 + c_1 p + c_2 p^2, \dots$ approximates the p -adic integer C . He wrote: “Die²⁶⁷ ... p -adischen Zahlen sind reine Symbole, mit denen nach bestimmten Vorschriften zu rechnen ist ...” Extending this definition by considering series of the form

$$c_{-n} p^{-n} + c_{-n+1} p^{-n+1} + \dots + c_0 + c_1 p + c_2 p^2 + \dots,$$

K. Hensel arrived at the field \mathbf{Q}_p of p -adic numbers²⁶⁸. The set \mathbf{Z}_p , consisting of series with $c_n = 0$ for negative n , forms a subring of \mathbf{Q}_p , its ring of integers.

Considering finite extensions of \mathbf{Q}_p , Hensel developed in a series of papers [2732, 2734, 2735, 2737, 2739–2748] all the main results of p -adic fields, as they are now called.

One of the first followers of Hensel’s new approach was G.E. Wahlin [6491–6494], who studied the structure of units in p -adic fields and applied Hensel’s theory to the factorization of prime ideals in extensions of the rationals.

An important tool in the elementary theory of p -adic and \mathfrak{p} -adic fields is *Hensel’s lemma*, proved by K. Hensel first [2733] for p -adic numbers (a simpler proof was given by L.E. Dickson [1541] in 1910), and then for their finite extensions [2734]. This lemma can be formulated in several ways. In its simplest form (which we state in the case of the field \mathbf{Q}_p) it asserts that if $F(X)$ is a polynomial with integral

²⁶⁷“The ... p -adic numbers are pure symbols, on which one has to perform calculations according to particular laws” [2736, p. 39].

²⁶⁸The second book [2738] by Hensel gave an exposition of elementary number theory based on the theory of p -adic numbers.

p -adic coefficients, $f \in \mathbb{F}_p[X]$ is its reduction mod p , and one has $f = gh$, where g, h are relatively prime non-constant polynomials, then one can write

$$F(X) = G(X)H(X),$$

where G, H are relatively prime polynomials with coefficients in \mathbb{Z}_p and g, h are their reductions mod p .

2. Hensel's method was not easily accepted, because its foundations were considered as being rather vague. This imposed the necessity of giving a sound basis for this theory. The first result in this direction came from A. Fraenkel²⁶⁹, who gave in [2065] an axiomatic definition of p -adic numbers, but his approach did not have any influence on the later development of number theory. The second approach to this problem, which turned out to be of utmost importance and exerted a big influence on a large part of commutative algebra, was due to J. Kürschak²⁷⁰ [3586], who in 1913 introduced *valuations*, as functions $v(x)$, defined in a field K , with non-negative real values, obeying the following conditions:

- (a) $v(x) = 0$ holds if and only if $x = 0$,
- (b) $v(xy) = v(x)v(y)$,
- (c) $v(x \pm y) \leq v(x) + v(y)$.

If v satisfies

- (d) $v(x \pm y) \leq \max\{v(x), v(y)\}$,

then it is called a *non-Archimedean valuation*.

This paper, which marks the start of valuation theory, which later became an important part of algebra, was followed by a sequence of three papers [4704–4706] by A. Ostrowski in which he determined all valuations of the rational field as well as of its finite extensions (a much simpler proof of this result was given later by E. Artin [143]). He also observed that the algebraic closure of the p -adic field \mathbb{Q}_p is not complete and showed that if a field K is complete under a non-archimedean valuation, L/K is a finite extension, β is algebraic and separable over K , and its distance from an element of L under the metrics $d(x, y) = w(x - y)$ (where w extends v to its separable closure) is sufficiently small, then β lies in K . This result is usually called *Krasner's lemma*, after M. Krasner²⁷¹, who rediscovered it in [3512]. One should also mention here the paper [5356] by K. Rychlik²⁷², where Hensel's lemma is extended to arbitrary complete fields.

The theory of valuated fields found its culmination in the work of H. Hasse and F.K. Schmidt [2609], published in 1934, where the structure of fields complete under a discrete valuation was determined. The rather complicated proof was later simplified by

²⁶⁹Adolf Abraham Halevi Fraenkel (1891–1965), professor in Marburg, Kiel and Jerusalem.

²⁷⁰József Kürschak (1864–1933), professor at the Technical University in Budapest.

²⁷¹Marc Krasner (1912–1985), professor in Clermont-Ferrand and Paris.

²⁷²Karel Rychlik (1885–1968), professor at the Technical University in Prague. See [2997].

O. Teichmüller²⁷³ [6098, 6099]. In the first of these papers, a mapping $\mathbf{Z}_p^* \mapsto \mathbf{Z}_p^*$ was defined, known today as the *Teichmüller character*, which turned out to be extremely useful.

The ideas of K. Hensel, J.Kürschak and A. Ostrowski were developed by M. Deuring, W. Krull²⁷⁴ [3536], A. Ostrowski [4709], F.K. Schmidt²⁷⁵ [5480] and others to form a sovereign branch of mathematics, the theory of valuations (see O.F.G. Schilling²⁷⁶ [5429], P. Ribenboim [5177, 5180], O. Endler²⁷⁷ [1763]). A broad exposition of its history was given by P. Roquette [5278].

²⁷³Oswald Teichmüller (1913–1943), student of Hasse, worked in Göttingen and Berlin. See [5423].

²⁷⁴Wolfgang Krull (1899–1971), professor in Freiburg, Erlangen and Bonn. See [5560].

²⁷⁵Friedrich Karl Schmidt (1901–1977), professor in Jena, Münster and Heidelberg. See [3584].

²⁷⁶Otto Schilling (1911–1973), professor at Purdue University.

²⁷⁷Otto Endler (1929–1988), professor in Rio de Janeiro.

Rational Number Theory in the 20th Century

From PNT to FLT

Narkiewicz, W.

2012, XIV, 654 p., Hardcover

ISBN: 978-0-85729-531-6