TRENDS IN RESEARCH: THE ANALYTIC NUMBER THEORY

HANS RADEMACHER

Ladies and Gentlemen: I wish to express my gratitude for the invitation to address this meeting and to thank you for granting me this opportunity to contribute a little part to the celebration of the anniversary of our host, this renowned institution of higher learning, the University of Chicago. The research work emanating from here has in its mathematical branch strongly emphasized analysis as well as number theory. The name "analytic number theory," indicating a union of these two fields of mathematical endeavor, is about as old as this celebrating Institution. In 1894 a book was published under the title Die Analytische Zahlentheorie, by Paul Bachmann. The name "analytic number theory" itself was a program. It said more than "diverse applications of infinitesimal calculus to number theory" as Dirichlet, the real founder of our discipline, had modestly called one of his great memoirs (1839). The name "analytic number theory," implies, as I take it, a thorough fusion of analysis and arithmetic, in which as we shall see, analysis is not necessarily subordinate to arithmetic. Incidentally, "analysis" stands here always for function theory, especially the theory of analytic functions.

What has the theory of functions to do with the theory of integers? Let me, to gain a starting point, begin with a few examples of well established results of analytic number theory:

1. If \( \pi(x) \) denotes as usual the number of prime numbers less than or equal to \( x \), then

\[
\lim_{x \to \infty} \frac{\pi(x)}{x \log x} = 1
\] as first proved by Hadamard and de la Vallée Poussin in the nineties of the last century.

2. The number of representations of a positive integer \( n \) as a sum of four squares is

\[
r_4(n) = 8 \left( \sum_{d|n} d - \sum_{d'|n} d' \right)
\] as Jacobi found as a corollary of his theory of elliptic functions.

An address delivered before the meeting of the Society in Chicago, Ill., on September 5, 1941, by invitation of the Program Committee; received by the editors January 6, 1942.

379
3. The number \( h(D) \) of classes of positive primitive binary quadratic forms of determinant \( D \equiv 7 \pmod{8} \) is given by Dirichlet's formula

\[
h(D) = \sum_{a} \left( \frac{a}{D} \right)
\]

where \( (a, D) = 1 \) and \( a \) runs through all positive integers less than \((1/2)D\).

Now, the first of these examples makes it quite obvious that analysis has to be applied, since the result does not only contain the continuous function \( x/\log x \), but moreover involves the notion of limit, so that the two fundamental concepts of infinitesimal analysis are represented in (1).

This is not so in the two other examples. All expressions appearing in the equations (2) and (3) have an arithmetical meaning and are defined in elementary number theory without any reference to analysis. Nevertheless both results appear as the goal of analytic proofs in one of which appear \( \vartheta \)-functions and in the other Dirichlet series. Both theorems can therefore be claimed by analytic number theory. However, there remains a big difference in these two cases: whereas the result (2) can also be proved by purely arithmetical methods, the equation (3) has defied all attempts of an elementary arithmetical proof.

This observation raises the question, which I will state in all its logical vagueness: what is the connecting link between arithmetic and analysis, or by what means can analysis take hold of arithmetical facts? In the steady flow of real numbers, called the continuum, which is the substratum of function theory, the integers are in no way distinguished from any other real numbers. The function \( e^z \) at first glance has no "affinity" to integers. We notice, however, the relation

\[
e^{2\pi iz} = e^{2\pi i(z+n)}
\]

for any integer \( n \) and all complex values \( z \). The function has the period \( n \) where \( n \) can be any integer. The fundamental fact is that the periods of an analytic, or for that matter, a continuous function form a discrete module or lattice. Or, speaking a little more generally: the ideas connected with period, invariance, and substitution group are basic for the application of analysis to number theory, and, as we can remark already here, also for the inverse process. Let me give another example, which is a little more involved. For the modular invariant \( J(\tau) \) we know that

\[
J(\tau) = J(\tau')
\]
implies and is implied by

$$(4b) \quad \tau' = \frac{a\tau + b}{c\tau + d}, \quad ad - bc = 1,$$

$a, b, c, d$ being integers. The function $J(\tau)$ appears thus as an embodiment of the discrete group of modular substitutions. This fact must have implications in both directions. Indeed, the group of modular transformations defines the classes of binary quadratic forms, and so we are led to the theory of singular moduli, the theory of complex multiplication, and finally to the Kronecker-Fueter theorem that any Abelian field over an imaginary quadratic field can be generated by the values of certain modular forms which they attain for special imaginary quadratic irrationalities. On the other side, equations (4a) and (4b) lead function-theoretically to the expansion (Petersson [33, 37])

$$(5a) \quad 12^3 J(\tau) = e^{-2\pi i \tau} + 744 + \sum_{n=1}^{\infty} c_n e^{2\pi i n \tau},$$

with

$$(5b) \quad c_n = \frac{2\pi}{n^{1/2}} \sum_{k=1}^{\infty} \frac{1}{k} I_1 \left( \frac{4\pi n^{1/2}}{k} \right) \sum_{h \text{ mod } k, (h,k)=1} e^{-2\pi i \left( \frac{h}{k} \right) \left( \frac{nk}{h} + \frac{h'}{k'} \right)}, \quad hh' \equiv -1(k),$$

where $I_1(z) = -i J_1(ix)$, the Bessel function of the first order.

You will always find such a group-invariance or periodicity, sometimes conspicuous, sometimes concealed, as underlying the applications of analysis to number theory. Fourier series, Fourier integrals, and Poisson sums are, therefore, natural and frequently used tools. But also the configuration of a point lattice can be taken as to express periodicity (especially in Minkowski’s work in the “geometry of numbers”), and even a power series is here often better understood as a series in $e^{2\pi i \tau}$, that is, a Fourier series with its obvious periodicity.

These analytic tools, developed in the 19th century, indicate sufficiently that our discipline must be a rather young one, so very much younger than elementary number theory, in whose history we meet the names of Euclid, Diophantos, Fermat. Indeed Lejeune Dirichlet can be regarded as the founder of our branch of research. Before him Euler, Gauss, and especially Jacobi, had found methods and results belonging to this field. After Dirichlet it was Riemann who with his epoch making memoir Ueber die Anzahl der Primzahlen unter einer gegebenen Grösse (1859) made the deepest mark in its history. In this brief survey I have also to mention the names of Hermite, Kronecker,
Hadamard, de la Vallée Poussin, and Minkowski, who all contributed works of lasting value.

The present standing of analytic number theory and its recognition as a fruitful branch of our science is, I think, entirely due to three mathematicians of this century: Landau, Hardy, and Littlewood. To Hardy and Littlewood we owe important progress in the theory of prime numbers and in our knowledge of the distribution of the complex zeros of the \( \zeta \)-function. Their greatest contribution, which they share with Ramanujan, lies, however, in the development of a fundamentally new method in additive number theory, a method which yielded their celebrated theorems concerning partitions, and about additive representations of numbers as sums of powers (Waring's problem) and as sums of primes (Goldbach's problem).

Landau has exerted a wide influence through his untiring mathematical enthusiasm and through his forceful advocacy of utter precision. The substance of his work has proved to be less permanent; his results were soon surpassed by deeper and more comprehensive ones, and his papers have very often been only second redactions of discoveries of others. How much we owe him nevertheless becomes evident if we compare a publication on analytic number theory of the the 1890's (for example, the above mentioned book of Bachmann, but also such substantial papers like those of Hadamard and de la Vallée Poussin not excepted) with a contemporaneous paper. Landau developed the technique of analytic number theory and prepared the tools; he found certain theorems about power series, Dirichlet series, Fourier integrals, which now are generally used as lemmas; and he made us familiar with the usefulness of a number of devices and lemmas discovered by others, as for example, Abel's partial summation, Mellin's formula, and Carathéodory's lemma. Landau's handbook on prime numbers will remain a classical treatise. Not a small merit of it is that it shaped our notation: It brought the symbol “\( O \)” into general use (it had been invented by Pringsheim), and Landau introduced there the symbol “\( o \)” (a constant source of quarrel between him and Pringsheim, which the German mathematicians used to watch with amusement). Both these symbols, now so well known and generally adopted, are particularly fit to express asymptotic relations which so frequently occur in analytic number theory.

Landau is no longer with us; Hardy and Littlewood about 10 years ago turned to other fields of investigation. Hence I understand it as my main task today to give a survey of developments in analytic number theory which took place after these three outstanding authors and independent of them.
This development has proceeded chiefly in two directions. One of them can roughly be characterized by words like "asymptotic formula" and "error term;" inequalities play an important part in the technique to "estimate" the error. I think here mainly of problems like the prime number theorem, lattice points in the circle, asymptotic expressions for the number of representations of a number as a sum of one or the other sort, investigations in which Hardy, Littlewood, and Landau have distinguished themselves, so that this pursuit of research can be understood as a direct continuation of their work. Investigations of this sort have attracted general attention, so much so, indeed, that the impression may have prevailed that analytic number theory deals foremost with asymptotic expressions for arithmetical functions. This view, however, overlooks another side of analytic number theory, which I may indicate by the words "identities," "group-theoretical arguments," "structural considerations." This line of research is not yet so widely known; it may very well be that methods of its type will lead to the "deeper" results, will reveal the sources of some of the results of the first direction of approach. Remarks like those which I made about applicability of analysis to arithmetic are especially pertinent here. The names Artin, Hecke, Mordell and Siegel would have to be mentioned in this connection.

The first type of analytic number theory is at present carried on in the Russian school with Vinogradoff as the leading name. Vinogradoff has become widely known for his great contributions to Waring's problem and Goldbach's problem. In this work he depends entirely on Hardy's and Littlewood's precedency; he introduced essentially two improvements of their method. One is of minor importance and merely an affair of convenience. He observed that for the additive representation of the number \( n \) you obviously do not need summands surpassing \( n \). This means that the power series which have been used by Hardy and Littlewood (and whose use in additive number theory really dates back to Euler) can be replaced by polynomials. This has certain advantages since it discards the difficulty of the natural boundary which the unit circle represents for those power series. Vinogradoff's second and decisive advance lies in his ingenious estimate of certain sums of roots of unity, as I shall now try to explain.

I begin with Waring's problem, in whose treatment Vinogradoff reaped his first success. For the discussion of

\[
(6) \quad f(x) = \sum_{n=0}^{\infty} x^{n^k}
\]

in the neighborhood of a root of unity \( \xi = e^{2\pi i (h/q)} \) Hardy and Little-
wood need expressions for the sums

\[ S_q(M) = \sum_{n=0}^{M} e^{2\pi i (h/q) n^k} \]

with the emphasis upon their dependence on \( q \) and \( M \) (for fixed given \( k \geq 3 \); \( k = 2 \) is in a different class since \( f(x) \) is then essentially a \( \vartheta \) function and \( S_q(M) \) essentially a Gaussian sum, both of which are well known from other connections). Now for an \( M \) which is large compared with \( q \) an expression with a useful error term is easily found by partial summation. The error term, however, becomes unmanageable for \( q \) comparatively large. This case, which appears on the so-called “minor arcs” proved first to be a serious obstacle to Hardy’s and Littlewood’s efforts. It is known that this difficulty delayed their final success for two years at a time when the required device had already been found and published by H. Weyl [58] but due to the interruption of communications during the first World War had not yet come to Hardy’s and Littlewood’s notice.

Now Vinogradoff recognized that a certain \( k \)-fold iteration in Weyl’s method could be dispensed with and replaced by one single step. Since that iteration was the source of a factor \( 2^k \) in the estimate for \( G(k) \), the smallest number of \( k \)th powers sufficing to express every sufficiently large number additively, this change meant an extraordinary diminution of the estimated order of \( G(k) \), a diminution as a matter of fact which was so considerable that it enabled Dickson to establish in many cases the true value \( g(k) \) of \( k \)th powers which suffice to represent additively all positive integers, simply by bridging the finite gap not covered by \( G(k) \) through a number of elementary computational steps [6, 7].

Vinogradoff’s lemma, which replaces Weyl’s lemma, can be enunciated as follows (in the form which was given to it by Heilbronn [21]): Let \( x \) run through \( X \) integers of an interval of length \( L \), \( y \) through \( Y \) integers on an interval of length \( M \), then

\[ \left| \sum_{x,y} e^{2\pi i (xy/q)} \right|^2 \leq \frac{XYML}{q} \left( 1 + \frac{q}{M} \right) \left( 1 + \frac{q \log q}{L} \right). \]

This lemma is not immediately applicable to (6a) and to (6). Vinogradoff employs the astonishing device of dropping certain Waring representations of the given number \( n \), by selecting \( k \)th powers of a certain factorization. This diminishes the chance of a Waring representation. Nevertheless he finds that the number of representations is different from null for \( s \geq 6k \log k + (4 + \log 216)k \) summands and sufficiently large \( n \) [50].
Vinogradoff’s most startling achievement was his proof in 1937 that every large odd number is the sum of three primes [52, 53], a result previously obtained by Hardy and Littlewood only under a generalized Riemann hypothesis. Vinogradoff’s result is so far the closest approach to Goldbach’s conjecture ever reached. The difficulties are here much greater than for the Waring problem, the distinction between major and minor arcs much subtler. The major arcs require for their treatment the classical theory of the distribution of primes founded on the \( \xi \)-function and the Dirichlet \( L \)-functions. In Vinogradoff’s paper, moreover, a deep theorem of Siegel about the class-number of quadratic fields [46] was used, which can be expressed in the statement

\[
\left| L(1, \chi) \right| > \frac{C}{k^e}
\]

where \( \chi \) is a real character modulo \( k \), a theorem which widens Heilbronn’s result [22] that the number of imaginary quadratic fields of class-number one is finite. Walfisz thereafter showed that Siegel’s theorem can be dispensed with, at the cost of some loss of precision in the error term [54].

The sum to be appraised in Goldbach’s problem is

\[
T_q(M) = \sum_{p \leq M} e^{2\pi i (h/q) p},
\]

again in particular for the minor arcs, that is, for comparatively high denominator \( q \). Now this sum does not fit into the scheme of Vinogradoff’s lemma (7) since \( p \) alone and not a product appears in the exponent. Vinogradoff resorts here to the sieve of Eratosthenes [53] which had been so successfully used by Viggo Brun [3]. The argument runs like this:

\[
T_q(M) = \sum_{r=2}^{M} e^{2\pi i (h/q) r} - \sum_{p_1 \leq M^{1/2}} \sum_{2 \leq m \leq M/p_1} e^{2\pi i (h/q) m p_1} + \sum_{p_1 < p_2 \leq M^{1/2}} \sum_{1 \leq m \leq M/p_1 p_2} e^{2\pi i ((h/q) m p_1 p_2)} + \cdots.
\]

The first sum is a trivial geometric sum, and in the following sums we do find the desired products in the exponents. This opens the way to an application of (7). Still, the completion is not quite simple but is handled by Vinogradoff with superb technique. I have already quoted his final result regarding Goldbach’s problem.

Before I drop this strand of my narration I wish to mention Tchudakoff’s application of Vinogradoff’s methods to the estimation of Riemann’s \( \xi \)-function on \( \Re(s) = 1 \) [49]. Tchudakoff uses Vinograd-
doff’s estimates [51] in the same way as Littlewood and Landau had used Weyl’s method for the improvement of the error term in the prime number theorem to $O(x \exp (-a(\log x \log \log x)^{1/2}))$. Tchudakoff obtains the prime number theorem in the form

$$\pi(x) = \int_2^x \frac{dt}{\log t} + O(x e^{-a(\log x)^{\alpha}})$$

with a certain $\alpha > 1/2$. Until then the remainder term had for three decades shown the value $\alpha = 1/2$. Of course, any $\alpha < 1$ is still far off from the Riemann hypothesis which is equivalent to $\alpha = 1, a = (1/2) - \epsilon$.

Appraisals of sums of roots of unity have recently played an important role in several parts of analytic number theory. Mordell [31], Davenport [4], and Hasse [5, 14] discussed sums of the form

$$S_q = \sum_{n \equiv a \mod q} e^{i2\pi f(n)}$$

where $f(n)$ is a polynomial in $n$ with integral coefficients. The aim is to give an estimate of $S_q$ with respect to $q$. The problem is a generalization of the order of magnitude of Gaussian sums, that is, $f(n)$ of the second degree, in which case we have

$$S_q = O(q^{1/2}).$$

It is of interest that the exponent 1/2 which appears here in a number of cases has something to do with the abscissa $\Re(s) = 1/2$ in the Riemann hypothesis, not for the ordinary $\zeta$-function, it is true, but for the $\zeta$-function belonging to a field of algebraic functions over a finite field of characteristic $p$; these $\zeta$-functions were introduced by E. Artin [1] in 1924 and later in a more general form defined by F. K. Schmidt [44]. The non-trivial zeros $\rho$ of such a $\zeta$-function turn out to be periodic and given by

$$\beta = \rho^p$$

where $\beta$ are the roots of certain polynomials; clearly $|\beta| = \rho^{1/2}$ means

(*)

$$\Re(\rho) = 1/2,$$

and the absolute value of $\beta$ depends on the number of solutions of certain congruences modulo $p$, or, which is equivalent to this, on the value of certain exponential sums. Relation (*) has been proved for the Artin $\zeta$-functions of the field of elliptic functions by Hasse [12, 13], who also outlined a program for further research. Modern algebraic concepts are fundamental in this work. Quite recently, in this year, André Weil [56, 57] published two sketches of proofs for the
Riemann hypothesis in all algebraic function fields over a finite field. We are looking forward to a complete account of his proof. Here still a wide field is open to research, a field attractive at the same time by its large generality and its richness of specific details.

A particularly interesting case of sums of roots of unity are the so-called Kloosterman sums

\[ S_q(u, v) = \sum_{h \mod q, (h, q) = 1} e^{(2\pi i/q) (uh + vh')} \]

with \( hh' \equiv 1 \pmod{q} \). Since these sums are multiplicative with respect to \( q \), they can be broken down to those with prime-number powers \( q \).

For \( q = p^a, a \geq 2 \), the order \( O(q^{1/2}) \) has been established by Salić [43], and moreover an explicit formula involving Legendre symbols and trigonometric functions has been found. Surprisingly, however, the case of a prime number \( q = p \) offers difficulties which so far have only permitted us to prove

\[ S_p(u, v) = O(p^{3/2}). \]

Weil’s above-mentioned results should establish here also \( O(p^{(1/2)+\varepsilon}) \).

The Kloosterman sums appear in the theory of partitions and in the study of the coefficients of modular functions. Recent work connected with these problems can also be understood as an extension of the Hardy-Littlewood-Ramanujan work. Whereas Hardy and Ramanujan obtained only an asymptotic expression for the number \( p(n) \) of partitions of \( n \), a refinement and at the same time a simplification of their method led to the equation [35, 36]

\[
\begin{align*}
p(n) &= \frac{1}{\pi 2^{1/2}} \sum_{q=1}^{\infty} A_q(n) \frac{d}{dn} \left[ \frac{\sin \frac{K}{q} \left( n - \frac{1}{24} \right)^{1/2}}{\left( n - \frac{1}{24} \right)^{1/2}} \right], \\
A_q(n) &= \sum_{h \mod q, (h, q) = 1} \omega_{h, q} e^{-2\pi (hn/q)}, \quad K = \pi(2/3)^{1/2},
\end{align*}
\]

where \( \omega_{h, q} \) are certain roots of unity taken from the theory of transformation of the modular form \( \eta(\tau) \), which have attracted the attention of quite a number of mathematicians since Hermite. The series in the equation just mentioned is absolutely convergent. It has been used successfully by D. H. Lehmer for the numerical computation of \( p(n) \) for high values of \( n \) [26, 27]. Analogous results for other problems of partitions with certain congruence conditions imposed on the summands have been obtained by Zuckerman [59], Niven [32], Hua [23], Miss Haberzetle [9], and Lehner [28].
These investigations form a natural bridge between the two different ways of investigation I mentioned before. Technically they require estimates of error terms, but also some group-theoretical arguments. And they lead to identities, which in turn invite group-theoretical treatment and thus point in the second direction in our field.

Identities can be used as sources of other identities. In this way the famous Ramanujan identities, of which I quote here only

\[ \sum p(5l + 4)x^l = 5\left[ \prod (1 - x^{5q^m})^5/\prod (1 - x^m)^6 \right], \]

can be proved by direct comparison of coefficients which are known in forms of series through the just mentioned methods. But the true source of the Ramanujan identities lies in the theory of transformation of modular forms, as it is seen at once if we rewrite the identity (**) 

\[ \sum_{\lambda=0}^{4} \frac{1}{\eta(\tau + 24\lambda)} = 5^z \frac{\eta(5\tau)^5}{\eta(\tau)^6} \]

[30, 39].

The formula (5) is an identity, which can also be derived by the Hardy-Littlewood-Ramanujan method. Here the problem arises to understand the invariance

\[ J\left(\frac{a\tau + b}{c\tau + d}\right) = J(\tau) \]

as an outcome of the Fourier series on the right-hand member [38].

Hardy himself has contributed a remarkable paper to similar investigations [10], showing that for example,

\[ \phi_8(0, \tau) = 1 + \frac{\pi^4}{3!} \sum_{n=1}^{\infty} n^8S_8(n)e^{2\pi i n\tau}, \]

(8a)

\[ S_8(n) = \sum_{q=1}^{\infty} \frac{1}{q^8} \sum_{h \mod q, (h,q)=1} \left( \sum_{j=1}^{q} e^{2\pi i (hn/q)} \right)^8 e^{-2\pi i (hn/q)}. \]

Here \( S_8(n) \) is the “singular series” of the problem of expressing a number as a sum of 8 squares. The proof of (8a) has to establish the fact that the Fourier series on the right of (8a) is a modular form of dimension \(-4\).

The “singular series,” first introduced into analytic number theory by Hardy and Littlewood, form objects of great mathematical interest of their own. They appear in problems of representation of integers in an additive way, for example, as \( n = x_1^2 + \cdots + x_r^2 \). For the
number of representations the Hardy-Littlewood method yields an asymptotic result of the form

\[ N_r(n) \sim f_r(n) \cdot \mathcal{S}_r(n), \]

where \( f_r(n) \) is a continuous function of \( n \), which can be interpreted as a density with respect to the \( r \)-dimensional point lattice. The other factor is the singular series \( \mathcal{S}_r(n) \), an arithmetical function of \( n \). A remarkable feature of all singular series is that they are factorable according to prime numbers:

\[ \mathcal{S}_r(n) = \prod_p A_p^{(r)}(n). \]

This fact finds its explanation in the meaning of \( A_p^{(r)}(n) \). Whereas for the problem

\[ n = x_1^k + \cdots + x_r^k \]

the function \( f_r(n) \) means the derivative

\[ f_r(n) = \frac{d}{dn} V_r(n) \]

of the volume

\[ V_r(n) = \int_{x_1 + \cdots + x_r \leq n; 0 \leq x_j} \cdots dx_r \]

or, in other words, a measure of the area of the surface

\[ n = x_1^k + \cdots + x_r^k, \quad 0 \leq x_j; j = 1, \ldots, r, \]

the \( A_p^{(r)}(n) \) give the density of solutions of the congruence

\[ n \equiv x_1^k + \cdots + x_r^k \pmod{p^i} \]

with respect to high powers of \( p \) as modulus, or explicitly:

\[ A_p^{(r)}(n) = \lim_{l \to \infty} \frac{b^{(r)}(n; p^l)}{g^{(r)}(p^l)} \]

where \( b^{(r)}(n; p^l) \) is the number of different solutions of (9) and \( g^{(r)}(p^l) \) is the average of the number of solutions of (9), distributed over \( p^l \) different \( n \)'s,

\[ g^{(r)}(p^l) = \frac{p^r l^r}{p^l} = p^{l(r-1)}. \]

The multiplicativity of the \( A_q^{(r)}(n) \) now becomes understandable, and
the product $(8b)$ means that $\mathcal{G}_r(n)$ is the density of solutions of the congruence for, let us say, $m!$ as modulus with $m \to \infty$.

Recently Siegel has emphasized this interpretation and used it with great success in his analytic theory of quadratic forms [47]. In that connection the singular series had appeared before, in the works of Smith and Minkowski, as measure of genera of quadratic forms. Through this connection it becomes clear why the Hardy-Littlewood method leads to an exact formula for the number of representations of $n$ as a sum of $r$ squares for $5 \leq r \leq 8$, whereas for higher $r$ it yields only an asymptotic result.

This interpretation of the singular series is possible in all those problems of additive number theory which preassign the number of summands or variables, as in Goldbach's problem, Waring's problem, or mixed problems, as for example, the problem of representation as a sum of a square and two primes (Estermann [8]), or as a sum of $r$ squares and $s$ cubes. It fails, however, for problems with an undetermined number of variables, as in the case of unrestricted partitions, since there the transition from equation to congruence destroys the boundedness of the number of variables for each $n$, so that the number of solutions modulo $p$ becomes meaningless. Indeed, the formula for $p(n)$, given above, is of quite a different structure.

Singular series appear as coefficients of Fourier series as in (8a). Siegel's analytic theory of quadratic forms can be regarded as a brilliant example of the study of such series. He shows that his series can be combined of $\vartheta$-functions

$$
\vartheta(r) = \sum_{m_1, \ldots, m_r} e^{2 \pi i r Q(m_1, \ldots, m_r)}
$$

where $Q$ is a positive quadratic form with integral coefficients; such a combination includes $\vartheta$-functions constructed with quadratic forms $Q$ of all classes of the same genus. It is known that such $\vartheta$-series are modular forms of dimension $-r/2$ and of a certain "level" (Stufe) depending essentially on the discriminant of the quadratic form $Q(m_1, \ldots, m_r)$ [45].

A general study of power series with singular series as coefficients has not yet been undertaken. It would be desirable to know more specific details about these functions than the general properties which can immediately be derived from Kac's, van Kampen's, and Wintner's remark [24, 25] that the singular series give rise to almost periodic arithmetical functions of $n$ and from Bochner's and Bohnenblust's [2] theorems about power series with almost periodic coefficients.
The modular functions have from the beginning of our discipline played an important part in additive problems; I need in this respect only point to Euler's formula, fundamental for the whole theory of partitions

\[ 1 + \sum_{n=1}^{\infty} p(n)x^n = \frac{1}{\prod_{l=1}^{\infty} (1 - x^m)} \]

in which the denominator is essentially the modular form

\[ \eta(\tau) = e^{\pi \imath \tau / 12} \prod_{1}^{\infty} (1 - e^{2\pi \imath m \tau}), \]

or to equation (2), obtained by Jacobi from an expression for the 4th power of \( \vartheta_3(0, \tau) \). Recently, however, they have also appeared in multiplicative number theory through the discovery of a surprising and most fruitful connection between modular functions and prime numbers. This connection is elaborated by Hecke in his beautiful theory, of which he published the first account in 1935 in the Royal Danish Academy [16]. As a matter of fact, a special result of Hecke’s theory was anticipated by Ramanujan [41, 11] in a conjecture which was then proved by Mordell in 1917 [29]. This is again an instance of Ramanujan’s gift of divination; not only that he foresaw or unveiled hitherto unknown facts, but most of his conjectures lead back to sources of great depth and abundant yield.

The “discriminant” in the theory of elliptic functions

\[ A(1, \tau) = g_2^2 - 27g_3^2 = (2\pi)^{12} x((1 - x)(1 - x^2) \cdots)^{24} \]

with \( x = e^{2\pi \imath r} \) is a modular form of dimension \(-12\), since for a modular substitution

\[ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \]

we have

\[ \Delta \left( 1, \frac{a\tau + b}{c\tau + d} \right) = (c\tau + d)^{12}\Delta(1, \tau). \]

The infinite product can be expanded into a power series

\[ x \prod_{1}^{\infty} (1 - x^m)^{24} = \sum_{n=1}^{\infty} \tau(n)x^n. \]

If we now, following Ramanujan, associate with this power series the Dirichlet series
it turns out that this series can be written as an infinite product

\[ F(s) = \prod_p \frac{1}{1 - \tau(p)p^{-s} + p^{1-2s}} \]

extended over all primes \( p \). It is appropriate to call such a product an “Euler product” in view of the formula

\[ \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \frac{1}{1 - p^{-s}} \]

first found and utilized by Euler. I shall have to make a remark about this latter product a little later. Not only the Euler product (10), but also a functional equation for \( F(s) \):

\[ (2\pi)^{-s}\Gamma(s)F(s) = (2\pi)^{s-12}\Gamma(12-s) \cdot F(12-s) \]

reminds us strongly of the \( \zeta \)-function and allied functions.

The coordination of a modular function on the one side and a Dirichlet series satisfying a functional equation on the other has now been systematized by Hecke [17, 18, 19]. Let us take an entire modular form \( F(\tau) \) of dimension \(-k\), \( k \) a positive even integer,

\[ F\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^k F(\tau) \]

having the expansion

\[ F(\tau) = c_0 + \sum_{n=1}^{\infty} c_n x^n, \quad x = e^{2\pi i \tau}, \]

which is everywhere convergent in the upper \( \tau \)-half-plane. Then let us put

\[ \phi(s) = \sum_{n=1}^{\infty} \frac{c_n}{n^s} \text{ (without } c_0). \]

Then the following statements are valid:

1. The series for \( \phi(s) \) is absolutely convergent in the half-plane \( \Re(s) > k \).
2. \( \phi(s) \) is an entire function if \( c_0 = 0 \); if \( c_0 \neq 0 \) then \( \phi(s) \) has a pole of the first order at \( s = k \) with the residue \(-1)^{k/2}c_0(2\pi)^k/\Gamma(k)\) and \((s - k)\phi(s)\) is an entire function.
3. \( \phi(s) \) satisfies a functional equation:

\[ (2\pi)^{-s}\Gamma(s)\phi(s) = (-1)^{k/2}(2\pi)^{s-k}\Gamma(k - s)\phi(k - s). \]
(4) \((s-k)\phi(s)\) is of finite order.

Of these statements (1) is implied by \(c_n = O(n^{k-1+\epsilon})\), which in turn is a simple consequence of the dimension \(-k\). For (2) and (3) we have the pattern of Riemann’s classical proof for the continuation and the functional equation of the \(\zeta\)-function by means of a \(\vartheta\)-function. In its application here the proof runs like this:

We have from Euler’s integral
\[
\frac{\Gamma(s)}{(2\pi i)^s} = \int_0^\infty e^{-2\pi ny} y^{s-1} dy
\]
and therefore for \(\Re(s) > k\)
\[
(2\pi)^{-s}\Gamma(s)\phi(s) = \int_0^\infty (F(iy) - c_0) y^{s-1} dy
\]
with
\[
F(iy) - c_0 = \sum_{n=1}^{\infty} c_n e^{-2\pi ny}.
\]
Since for the modular substitution
\[
\begin{pmatrix}
0 & -1 \\
1 & 0
\end{pmatrix}
\]
we have \(F(i/y) = (iy)^k F(iy)\) we can write
\[
(2\pi)^{-s}\Gamma(s)\phi(s)
\]

\[
= \int_1^\infty (F(iy) - c_0) y^{s-1} dy + \int_0^1 ((iy)^{-k} F(iy) - c_0) y^{s-1} dy
\]

\[
= \int_1^\infty (F(iy) - c_0) y^{s-1} dy + i^{-k} \int_1^\infty F(iw) w^{k-s-1} dw - \frac{c_0}{s}
\]

\[
= \int_1^\infty (F(iy) - c_0) y^{s-1} dy + (-1)^{k/2} \int_1^\infty (F(iw) - c_0) w^{k-s-1} dw
\]

\[
- (-1)^{k/2} c_0 \int_1^\infty w^{k-s-1} dw - \frac{c_0}{s}
\]

\[
= \int_1^\infty (F(iy) - c_0) (y^s + (-1)^{k/2} y^{k-s}) \frac{dy}{y}
\]

\[
- c_0 \left( \frac{1}{s} + (-1)^{k/2} \frac{1}{k-s} \right).
\]
So far our reasoning required $R(s) > k$. Now we have arrived at an expression which remains meaningful for any complex $s$. We have, therefore, obtained an analytic continuation over the whole $s$-plane for $\phi(s)$. Moreover, the substitution $s \to k - s$ changes the right-hand member by the factor $(-1)^{k/2}$, which proves (3). At the same time we infer the validity of statement (2).

The argument runs also in reverse, from the Dirichlet series of properties (1) to (4) to a modular form of dimension $-k$. Instead of the Euler integral we have only to apply Mellin’s formula.

Up to this point we have not encountered any trace of prime numbers. Hecke came to an Euler product by considering not a single modular form, but the whole set of all entire modular forms of dimension $-k$. They constitute a linear family of finite rank $\kappa$; the number $\kappa$ of linearly independent modular forms in this set is a known function of $k$. A linear operator $T$ will map the whole set on itself. If the system $F(\tau, \rho = 1, 2, \cdots, \kappa)$ forms a basis then there exists a matrix $(\lambda_{\rho \sigma})$ such that

$$T(F(\tau, \rho)) = \sum_{\rho = 1}^{\kappa} \lambda_{\rho \sigma} F(\tau, \sigma).$$

As linear operator Hecke takes, for any natural number $n$,

$$T_n(F) = n^{k-1} \sum_{d \mid n} \sum_{\max \mathfrak{a} \mathfrak{b}} F \left( \frac{a \tau + b}{d} \right) d^{-k},$$

for which it can be proved, by consideration of the subgroup

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{n}$$

and its factor-group in the full modular group, that it furnishes again a modular form of dimension $-k$.

Hence we have

$$T_m(F(\tau, \rho)) = \sum_{\rho = 1}^{\kappa} \lambda_{\rho \sigma}(m) F(\tau, \sigma).$$

The application of the operator $T_m$ on the Fourier expansion

$$F(\tau, \sigma) = \sum_{n=0}^{\infty} a(\sigma)(n) e^{2\pi i n \tau}$$

yields by comparison of coefficients,

$$\sum_{\sigma = 1}^{\kappa} \lambda_{\rho \sigma}(m) a(\sigma)(n) = \sum_{\delta \mid m, \delta \mid n} \delta^{k-1} a(\sigma) \left( \frac{mn}{\delta^2} \right), \quad m \geq 1, n \geq 1.$$
It is decisive that here the right-hand member shows symmetry in $m$ and $n$, which therefore must also prevail in the left-hand member:

$$\sum_{\sigma=1}^{\kappa} \lambda_{p\sigma}(m)a^{(\sigma)}(n) = \sum_{\sigma=1}^{\kappa} \lambda_{p\sigma}(n)a^{(\sigma)}(m).$$

The matrix $(\lambda_{p\sigma}(0))$, which appears here for the first time, can be uniquely determined as to fulfill also this relation. Now we obtain

$$T_m(F^{(q)}(\tau)) = \sum_{\sigma=1}^{\kappa} \lambda_{p\sigma}(m) \sum_{n=0}^{\infty} a^{(\sigma)}(n)e^{2\pi in\tau}$$

$$= \sum_{\sigma=1}^{\kappa} a^{(\sigma)}(m) \sum_{n=0}^{\infty} \lambda_{p\sigma}(n)e^{2\pi in\tau}. $$

This leads to the introduction of the functions

$$f_{p\sigma}(\tau) = \sum_{n=0}^{\infty} \lambda_{p\sigma}(n)e^{2\pi in\tau}$$

which span up the same linear set $\{F^{(1)}(\tau), \ldots, F^{(\kappa)}(\tau)\}$ and of which it is easily seen that they belong to the same set. With $\lambda(n) = (\lambda_{p\sigma}(n))$ we have in

$$B(\tau) = \sum_{n=0}^{\infty} \lambda(n)e^{2\pi in\tau}$$

a matrix of modular forms. In connection with (11) it is found that

(12a) \[ \lambda(m) \cdot \lambda(n) = \sum_{d \mid (m, n)} d^{k-1} \lambda \left( \frac{mn}{d^2} \right), \]

which in particular for $(m, n) = 1$ furnishes

(12b) \[ \lambda(m) \cdot \lambda(n) = \lambda(mn) \]

and also shows that the different matrices $\lambda(n)$ are commutative.

Now we go over with Hecke to a set of associated Dirichlet series

$$\Phi(s) = (\phi_{p\sigma}(s)) = \sum_{n=1}^{\infty} \frac{\lambda(n)}{n^s},$$

a matrix which, of course, stands for

$$\phi_{p\sigma}(s) = \sum_{n=1}^{\infty} \frac{\lambda_{p\sigma}(n)}{n^s}, \quad \rho, \sigma = 1, \ldots, \kappa.$$
\( f_{\rho \sigma}(\tau) \) we infer the validity of statements (1) to (4) for each element and hence the functional equation

\[
(2\pi)^{-s} \Gamma(s) \Phi(s) = (-1)^{k/2} (2\pi)^{-k} \Gamma(k - s) \Phi(k - s)
\]

in matrix notation. The relation (12b) makes it evident that we can write

\[
\Phi(s) = \prod_{p} \sum_{l=0}^{\infty} \frac{\lambda(p^l)}{p^{ls}}
\]

in which the summation of each infinite series can be effectuated by means of (12a) with the result:

\[
\Phi(s) = \prod_{p} (\lambda(1) - \lambda(p) p^{-s} + \lambda(1) p^{k-1-2s})^{-1},
\]

where \( \lambda(1) \), according to definition, is the unit matrix of order \( k \). Here we have the analogue of the Euler product.

If we would start the whole process with a new basis, obtained from the former one by a linear substitution \( A \), we would obtain the transformed matrices

\[
\lambda^*(n) = A \lambda(n) A^{-1}
\]

in our results. Such a transformation can be used to get matrices \( \lambda(n) \) of an especially simple type. Since the \( \lambda(n) \) are commutative they can simultaneously be transformed into matrices in which all elements beneath the principal diagonal are zeros. Beyond this H. Petersson [34] has shown that the \( \lambda \)'s can be brought simultaneously into diagonal form, which means that we can start the process with \( k \) linearly independent “eigen-functions” of all the linear operators

\[
T_n(F^{(\rho)}(\tau)) = \lambda^*_{\rho \rho}(n) F^{(\rho)}(\tau), \quad n = 1, 2, \ldots.
\]

Petersson proves this in a very elegant manner by introducing a definition of orthogonality of modular forms based on integrals extended over the fundamental region. The \( \lambda^*_{\rho \rho} \) are real algebraic numbers. We have now the Dirichlet series

\[
(13a) \quad \phi_{\rho \rho}(s) = \sum_{n=1}^{\infty} \frac{\lambda^*_{\rho \rho}(n)}{n^s}
\]

with an ordinary Euler product

\[
(13b) \quad \phi_{\rho \rho}(s) = \prod_{p} \frac{1}{1 - \lambda^*_{\rho \rho}(p) p^{-s} + p^{k-1-2s}}, \quad \rho = 1, \ldots, k,
\]
which is exactly of the form as it appears in Ramanujan's work on \( \Delta(1, \tau) \). Summarizing, we can roughly say that the Riemann functional equation of a Dirichlet series already implies the Euler factorization with respect to prime numbers, certainly a result in which analytic and arithmetic elements are inseparably welded together.

Unfortunately, Riemann's original coordination of a modular form and a Dirichlet series, namely,

\[
\eta(\tau) = \frac{1}{2} + \sum_{n=1}^{\infty} \frac{e^{\pi i n^2 \tau}}{n}, \quad \zeta(2s) = \sum_{n=1}^{\infty} \frac{1}{n^{2s}}
\]

with the Euler product

\[
\prod_{p} (1 - p^{-2s})^{-1}
\]

does not fit into the scheme, as already the comparison of this Euler product with (13b) shows; indeed, \( \eta(\tau) \) has the dimension \(-1/2\), and for fractional dimensions the complicated transformation formulae introduce multipliers which interfere with the definition of the operators \( T_n \).

Let us go back for a moment to the functions \( \phi_{pp}(s) \) in (13a) and (13b). We are here at once confronted with all the problems familiar from the theory of the Riemann \( \zeta \)-function: What is the distribution of the zeros of \( \phi_{pp}(s) \)? The critical strip is \( 0 \leq \Re(s) \leq k \); do all nontrivial zeros of \( \phi_{pp}(s) \) lie on the middle line \( \Re(s) = k/2 \)? In case \( \phi_{pp}(s) \) belongs to a modular form with \( c_0 = 0 \) ("cusp form") we know a few facts. The function \( \phi_{pp}(s) \) has no pole, of course, its series is absolutely convergent for \( \Re(s) > (k + 1)/2 \), \( \phi_{pp}(s) \) has no zeros on \( \Re(s) = (k + 1)/2 \) but infinitely many ones on \( \Re(s) = k/2 \), results all due to R. A. Rankin [42]. Ramanujan has for \( \phi_{pp}(s) = \Delta(1, \tau) \) made the conjecture

\[
|\tau(p)| \leq 2p^{11/2}
\]

and Petersson [34] has generalized it to

\[
|\lambda_{pp}(p)| \leq 2p^{(k-1)/2}
\]

or, which is equivalent, to the conjecture that the quadratic equation \( z^2 - \lambda_{pp}(p)z + p^{k-1} = 0 \) (derived from the denominator in (13b) with \( p^s = z \)) does not have two different real roots, which, since \( \lambda_{pp}(p) \) is real would mean that the roots have to be of absolute value \( p^{(k-1)/2} \). This conjecture has a close similarity to Hasse's theorem which confirms the Riemann hypothesis for elliptic function fields over finite fields.

Hecke has extended his theory also to modular forms of level (Stufe) \( Q \). The operators \( T_n \) with \( (n, Q) = 1 \) have the same behavior
as the operators for $Q=1$; the other ones, however, introduce complications on which I cannot dwell. Hecke applies this extension of his theory to a study of the $\vartheta$-functions generated by quadratic forms of several variables [20].

So far I have spoken only of the theory of rational integers on one side and of functions of one variable on the other. I would overstep the limits which I had to set myself in this discussion if I were to enter upon the problems presented by the fields of algebraic numbers. In many respects a full analogy with the rational field can act as guide. However, some new features appear here, as, for example, the group of units. An algebraic field of degree $n$ can be illustrated by an $n$-dimensional point lattice. Some problems, in particular additive ones, lead to analytic functions of $n$ complex variables; some other problems, in particular the multiplicative ones, are handled by means of a set of $\zeta$-functions with one complex variable $s$ and $(n-1)$ integer parameters (Hecke's $\zeta(s, \lambda)$-functions) [15]. The multiplicative theory of algebraic fields is, through Hecke's fundamental investigations, about as far advanced as that for the rational field; the additive number theory in algebraic fields, however, is still in its beginnings.

The theory of quadratic forms offers another way to come to functions of several variables, as Siegel has recently shown in his introduction of modular functions of several variables [48].

This report could, of course, mention only selected topics of analytic number theory. I do not wish to imply that no recent progress has been made in subjects which I did not discuss. There are, for example, the important contributions to the estimates of lattice points in the circle and in other areas due to van der Corput and his successors, and the investigations of Siegel and Gelfond concerning the transcendentality of certain types of numbers. I have purposely chosen such portions of analytic number theory which seemed to me to exhibit most clearly the present tendency, the trend, in contemporary research work. Our discipline has grown beyond the stage of mere application of analysis to number theory; we can characterize the present tendency as a deep mutual penetration of analysis and arithmetic. It is still so that the theory of analytic functions helps to solve arithmetical problems which otherwise appear as inaccessible; but number theoretical problems are the sources of new functions, and number theoretical arguments lead to a deeper understanding of the structure of known functions. I think that analytic number theory is a branch of mathematics that fascinates through its harmony and beauty and appeals to the working mathematician through its variety and fruitfulness.
BIBLIOGRAPHY


27. ———, An application of Schl"{a}fli's modular equation to a conjecture of Ramanujan, this Bulletin, vol. 44 (1938), pp. 84–90.


University of Pennsylvania