Peter Sarnak
Princeton University, Department of Mathematics, Princeton, NJ 08544-1000
Institute for Advanced Study, Princeton, NJ 08540
sarnak@math.princeton.edu

Kloosterman Centennial Celebration

Kloosterman, quadratic forms and modular forms

This is the extended text of the lecture given by Peter Sarnak at the Kloosterman Centennial Celebration in Leiden on 7 April 2000. Sarnak describes Kloosterman's seminal contributions to the theories of both quadratic and modular forms, as well as the impact of these works on modern developments.

It is an honor and pleasure for me to give this lecture at this centennial celebration of Kloosterman's birth. I will discuss Kloosterman's foundational and far reaching contributions to the theory of quadratic and modular forms and related number theory. I also follow some of the themes introduced by Kloosterman through to present day research, showing his remarkable influence on the subject. Some of what I say intersects with the reports of Springer and Heath-Brown; this is quite natural since these works of Kloosterman are of wide interest.

Representing integers by quadratic forms

A basic problem concerning the arithmetic of quadratic forms is Hilbert's problem 11. It asks which integers in a number field K are represented by a given integral quadratic form F defined over K? For example, if $K = \mathbf{Q}$ and $F(x)$ is $A(x) = x_1^2 + x_2^2$ or $B(x) = x_1^2 + x_2^2 + x_3^2$ or $C(x) = x_1^2 + x_2^2 + x_3^2 + x_4^2$, the answer has been known for a long time (Fermat, Legendre, Lagrange). For $B(x)$ an integer $m > 0$ is represented by B iff $m \neq 4^a(8b+7)$ iff $B(x) \equiv m (\mathrm{mod}\ \ell)$ is solvable for every $\ell \geqslant 1$ (or as we will say the equation $F(x) = m$ is solvable locally integrally). For $C(x)$ there are no congruential obstructions and every positive m is a sum of four squares.

Hardy and Littlewood introduced the so called 'circle method' to study asymptotically the number of solutions to certain diophantine equations and, in particular, the sum of 5 (or more) squares:

$$F(x) = x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 = m. \tag{1}$$

Their answer takes the form

$$R_5(m) \sim \mu_\infty(m) \prod_p \delta(p,m) \qquad \text{as } m \to \infty. \tag{2}$$

Here $R_5(m)$ is the number of integral solutions in $(x_1, \ldots, x_5)$ to (1), and $\mu_\infty(m)$ measures the solutions over $\mathbf{R}$ to (1) while $\delta(p,m)$ measures the density of solutions to (1) modulo (p^ℓ), as $\ell \to \infty$ (i.e. the density of p-adic solutions).

Kloostermans Sums

In his 1924 dissertation [19] Kloosterman developed the circle method to deal with a general positive definite diagonal form $F(x)$ in 5 or more variables (i.e. $F(x) = a_1x_1^2 + \cdots + a_5x_5^2$, a_j positive integers). He obtains an asymptotic formula similar to (2) from which one concludes that given such an F there is a constant C_F (effectively computable) such that if $m \geqslant C_F$ then $F(x) = m$ has an integer solution x iff $F(x) = m$ is solvable locally integrally. For m small this local to global principle may fail, also note that this representation problem for any given m is clearly a finite one.

Kloosterman then turned to the case of four variable diagonal quadratic forms, which lies much deeper. His 1926 paper [20] is a landmark contribution to the circle method. Like many great papers it contains a number of novel ideas. Firstly he introduces the process of 'levelling' (a term introduced by Linnik [27]) which involves collecting the contributions of Farey arcs in the circle method, which have centers with a common denominator c (for a recent and useful variant of this process see [7]). Second, in order to achieve cancellations via the levelling process, Kloosterman introduced his famous 'Kloosterman Sum': For $m, n, c \geqslant 1$

$$S(m,n,c) := \sum_{\substack{x \bmod c \\ x\bar{x} \equiv 1 (c)}} e^{2\pi i\left(\frac{mx + n\bar{x}}{c}\right)}. \tag{3}$$

For $c = c_1c_2$, $(c_1, c_2) = 1$, he shows that

$$S(u, vc_2^2 + v'c_1^2, c) = S(u,v,c_1)S(u,v',c_2). \tag{4}$$

The estimation of S is then easily reduced to the case of c being a prime p. Finally, Kloosterman establishes the nontrivial estimate

$$|S(m,n,p)| \leqslant E\ p^{3/4} \tag{5}$$

for an absolute constant E and where we have assumed that not both m and n are divisible by p (here the trivial bound is $p-1$).

With these ingredients Kloosterman goes on and extends his results about positive definite diagonal integral forms in five variables to four variables — a striking achievement. It is perhaps worth recalling his method of proof of (5), which is elementary. He calculates explicitly the fourth moments $\sum_{m \bmod p} (S(m,1,p))^4$, which turn out to be a polynomial of degree 3 in p. From this (5) follows immediately. The fact that the exponent of $1/2$ is the sharpest possible in (5) (for general m and n), also follows. An attempt to improve on (5) by considering the higher moments

$$B(k,p) = \frac{1}{p} \sum_{m \bmod p} \left(\frac{S(m,1,p)}{\sqrt{p}} \right)^{2k} \tag{6}$$

was carried out by Salié [32]. He showed that $B(k,p)$ is related to counting the number of solutions over $\mathbf{F}_p$ (the field with p elements) to

$$\left.\begin{aligned} x_1 + x_2 + \cdots + x_k &= 1 \\ x_1^{-1} + x_2^{-1} + \cdots + x_k^{-1} &= 1 \end{aligned}\right\} \tag{7}$$

For $k \geqslant 8$ this is no longer elementary (see below).

Modular forms

Kloosterman was well aware that his results above are closely related to the problem of estimation of Fourier coefficients of cusp forms in the theory of modular forms. A holomorphic form of even integral weight $k \geqslant 2$ for a (congruence) subgroup Γ of the modular group $SL(2,\mathbf{Z})$, is a holomorphic function $f(z)$ defined on $\mathbf{H} = \{z = x + iy | y > 0\}$ satisfying

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z), \qquad \text{for } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma. \tag{8}$$

It has a Fourier expansion at infinity (and at the other cusps of $\Gamma\backslash\mathbf{H}$) taking the form

$$f(z) = \sum_{n=0}^{\infty} a_f(n) e^{2\pi i n z}. \tag{9}$$

f is a *cusp* form if $a_f(0) = 0$ (and similarly for expansions at the other cusps).

Now given the quadratic form F the theta function

$$\theta_F(z) = \sum_{m \in \mathbf{Z}^n} e^{2\pi i z F(m)} := \sum_{m=0}^{\infty} R_F(m) e^{2\pi i m z} \tag{10}$$

is a modular form of weight $n/2$ for a suitable congruence subgroup Γ. The asymptotic behavior of the representation numbers $R_F(m)$ is reduced to estimating the Fourier coefficients of cusp forms. The "trivial' bound for the coefficients of a cusp form in (9) is

$$|a_f(n)| \leqslant c_f n^{\frac{k}{2}} \tag{11}$$

with c_f a constant depending on f. The Ramanujan Conjecture [31] asserts that for $\varepsilon > 0$ there is $c_{f,\varepsilon}$ such that

$$|a_f(n)| \leqslant c_{f,\varepsilon} n^{\frac{k-1}{2}+\varepsilon}. \tag{12}$$

For forms F in five or more variables (i.e. $k > 2$) the trivial bound (11) suffices to settle the representation problem for F, however for four variables (11) does not suffice. Thus Kloosterman's 1926 paper involves obtaining a nontrivial estimate towards the Ramanujan Conjectures. In his 1927 paper [21] Kloosterman applied his method of levelling directly to a cusp form f, together with his bounds for the Kloosterman sums, to obtain the first estimates towards the Ramanujan Conjectures: For k even,

$$|a_f(n)| \leqslant c_f n^{\frac{k-1}{2}+\frac{3}{8}}. \tag{13}$$

This is perhaps one of the first instances in this subject (of which there have been numerous successors) where, while the sharp bound is not achieved, a nontrivial bound is established and it suffices to resolve the problem at hand.

The solution of the Ramanujan Conjecture above had to await developments by Eichler [10] (for weight 2) and Ihara [13] (for higher even weight) which reduced the problem to the Riemann Hypothesis for curves over finite fields (for weight 2) and the Weil Conjectures for varieties over finite fields (in general). The solution of these function field analogues of the Riemann Hypothesis were established by Weil [39] for curves and by Deligne [5] in general.

Similarly the sharp estimation of the Kloosterman sum

$$|S(m,n,p)| \leqslant 2\sqrt{p} \tag{14}$$

was shown by Hasse [11] and Weil [39] to follow from the Riemann Hypothesis for curves over finite fields. In particular the Kloosterman sum has an interpretation as a trace of Frobenius on a suitable cohomology group. With the developments by Deligne for counting points on varieties over finite fields one might try to analyze the Salié moments in (6) via the variety (7). However, the variety (7) is highly singular which makes this approach problematic. Another approach to this problem via monodromy of the 'Kloosterman Sheaf' was taken by Katz in [16]. He established that as $p \to \infty$ the moments $B(k,p)$ converge to the moments $B(k)$ of the so called 'Sato-Tate' measure. In other words he shows that if the 'Kloosterman angles', $\theta_{a,p} \in [0,\pi]$ are defined by

$$2\cos\theta_{a,p} = \frac{S(a,1,p)}{\sqrt{p}} \tag{15}$$

then their distribution, for $1 \leqslant a \leqslant p-1$ converges to $\frac{2}{\pi}\sin^2\theta d\theta$ as $p \to \infty$. An interesting conjecture about Kloosterman sums that has been confirmed with numerical experiments is that for a fixed, say $a = 1$, the angles $\theta_{1,p}$ are distributed according to the above Sato-Tate measure, as $p \to \infty$.

The general modular form connection

The story of the Kloosterman sum modular form connection does not end with these developments in arithmetical algebraic geometry. In fact there is a further powerful connection not only with holomorphic modular forms but also with the most general modular forms including Maass forms (which are eigenforms of the Laplacian on $\Gamma\backslash\mathbf{H}$). We note that the Kloosterman sum is to the Bessel function as the Gauss sum is to the Gamma function, that is to say it is the finite field analogue of the Bessel function. This is transparent from comparing the definition (3) and the representation

$$K_0(z) = \frac{1}{2}\int_0^{\infty} e^{-(t+z^2/4t)} \frac{dt}{t} \tag{16}$$

for the Bessel function. As is well known, Bessel functions arise in the context of the representations of $SL(2,\mathbf{R})$. The global connection has its roots in the trace like formula of Petersson [30] which gives a relation between sums of Kloosterman sums and sums of Fourier coefficients of modular forms over a basis of such forms. In Selberg [33] an extension of this relation to Maass forms is indicated. The precise identity in this case was given by Kuznietzov [25] and Bruggeman [2] in their extension of Petersson's formula. While algebraic geometry with its cohomological interpretation of the Kloosterman sum allows for the analysis of $S(m,n,p)$ for a fixed prime p, the above modular form connection allows one to study $S(m,n,c)$ with c varying over integers. The Petersson-Kuznietzov-Bruggeman formula also gives a direct connection between cancellations in sums of Kloosterman sums and the Ramanujan Conjectures for Maass forms (including the Selberg eigenvalue conjecture concerning the Laplace spectrum of $L^2(\Gamma\backslash\mathbf{H})$, [33]). Unlike the case of holomorphic forms of even integral weight, these conjectures have not been proven, though substantial progress has been achieved [28], [18]. This general Kloosterman Sum to modular form connection has, primarily through the work of Iwaniec and his coauthors Bombieri, Deshoulliers, Duke and Friedlander, became a fundamental tool in modern analytic number theory (see [15] for a survey of some of this theory). The theory they have developed (which some have termed 'Kloostermania') has many striking applications including the one to Artin's primitive root conjecture that Heath-Brown mentioned.

An important conjecture concerning Kloosterman sums and which has many applications, is that of Linnik [27] and Selberg [33]. It asserts that for $n,m,X \geqslant 1$, $\varepsilon > 0$ and $X \geqslant (m,n)^{1/2+\varepsilon}$,

$$\sum_{c \leqslant X} \frac{S(m,n,c)}{\sqrt{c}} \leqslant B_\varepsilon X^{1/2+\varepsilon} \tag{17}$$

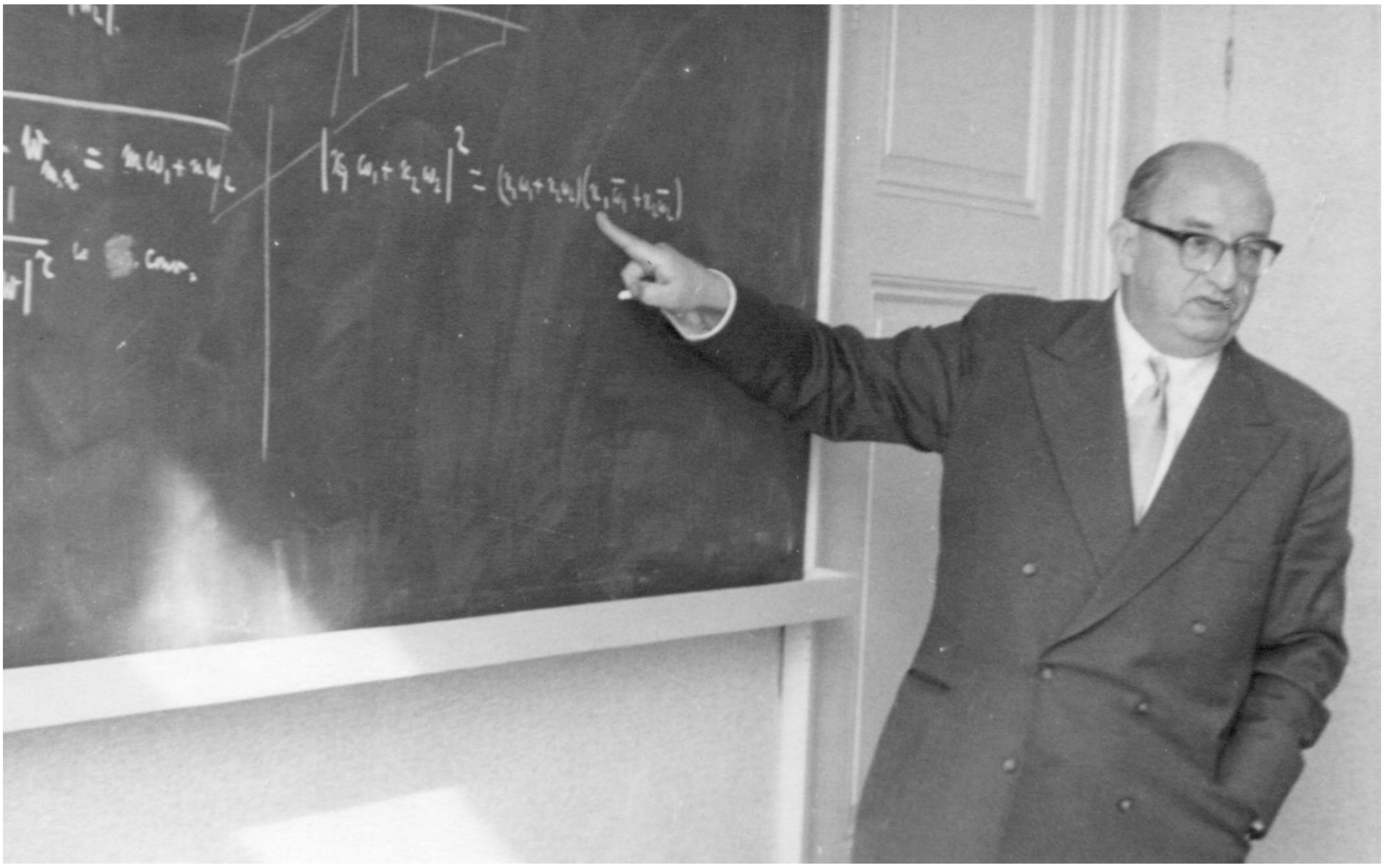
for B_ε a constant depending only on ε. There are similar Conjectures when c is restricted to arithmetic progressions. Note that Weil's bound (14) (which yields $S(m,n,c) = O_\varepsilon(c^{1/2+\varepsilon})$ for any $\varepsilon > 0$) gives the bound of $X^{1+\varepsilon}$ in (17). One seeks cancellations due to the signs of the Kloosterman sums. Kuznietzov [25] using his trace formula and the elementary fact that $SL(2,\mathbf{Z})\backslash\mathbf{H}$ has no exceptional Maass eigenvalues, established that for $m,n \geqslant 1$ fixed, there is $A = A(m,n)$ s.t.

$$\sum_{c \leqslant X} \frac{S(m,n,c)}{\sqrt{c}} \leqslant A\ X^{2/3}(\log X)^{1/3}. \tag{18}$$

The recent developments [28], [18] towards the Selberg eigenvalue conjecture show that there is also cancellation for such sums on progressions. For m,n,a,q fixed, there is $A = A(m,n,a,q)$ s.t.

$$\sum_{\substack{c \leqslant X \\ c \equiv a(q)}} \frac{S(m,n,c)}{\sqrt{c}} \leqslant AX^{13/18}. \tag{19}$$

Before leaving the topic of Kloosterman sums, I mention one other recent result. Katz [17] noticing that the numbers $a(p) = -\frac{S(1,1,p)}{\sqrt{p}}$ behave very much like the coefficients at primes of a Hecke eigenform (that is they obey the Ramanujan bound $|a(p)| \leqslant 2$ and apparently also the Sato-Tate law) asked whether they might in fact



H.D. Kloosterman

Kloosterman representing the Netherlands at a meeting of the IMU

be the coefficients of a cusp form. Such a form cannot be a holomorphic one since the numbers $S(1,1,p)$ do not lie in a fixed extension of $\mathbf{Q}$. So perhaps a Maass form? Booker [1] has shown that if such a form exists then either its Laplace eigenvalue or its level (as far as belonging to a congruence subgroups) would have to be at least 2^{24}. So there is no doubt (unfortunately) that such a juicy connection between Kloosterman sums and modular forms does not exist.

Representing integers in number fields

In 1929 Kloosterman returned to his investigations on Hilbert's 11^{th} problem. He addresses the problem for definite forms F over a totally real number field K. The circle method was extended to number fields by Siegel [34] who dealt with the question of representation of integers as a sum of five squares (in this case of number fields — the torus method would be a better description of the method). His work can be generalized to general quadratic forms in five (or more) variables. Unfortunately the levelling process of Kloosterman has resisted generalization to number fields. In [22] and [23] Kloosterman developed the modular form approach to the representation problem. He extends the theory of Eisenstein series and of theta functions to Hilbert modular forms and he reduces the representation problem to estimation of the Fourier coefficients of Hilbert modular forms (i.e. to bounds towards the Ramanujan Conjectures for these forms). As mentioned above, his levelling method does not extend easily to his setting, and so Kloosterman was not able to establish the desired 'non-trivial' bounds on the Fourier coefficients and this is the form in which he left the general problem, except for a further paper [24] in 1942 on the representations by inhomogeneous quadratic forms.

Since Kloosterman's work, there have been a series of developments on the problem of representations of integers by forms F. We review these briefly. Malyshev [29] extended Kloosterman's work to deal with the general (i.e. nondiagonal) form F in four (or more) variables over the rationals. The solution of Hilbert's problem in four (or more) variables over a number field is due to Kneser [26] (see also [12] and [3]). Using algebraic methods and, in particular, the Hasse principle (which in turn gave the solution of Hilbert's 11^{th} problem in the context of rational, rather than integral, representations) Kneser established the following local to global principle: Given a positive definite form F over a totally real field K, there is a constant C_F (effectively depending on F) such that if m is a positive integer with $\mathrm{Norm}(m) \geqslant C_F$, then F represents m primitively integrally (i.e. $F(x) = m$ with x_1, x_2, x_3, x_4 relatively prime — a technical condition which is needed in this four variable case) if and only if $F(x)$ represents m primitively integrally locally.

This leaves the cases of forms F in two or three variables. The binary case is equivalent to factorization of integers in quadratic extensions of K and as Hilbert already pointed out it can be analyzed by class field theory for relative quadratic extensions. In any event in this case, there is no local to global principle (in general when various class numbers are not equal to one) even for m large. So the situation for binary forms is very different to that of forms in four or more variables.

The investigation for forms in three variables is much more subtle and difficult and, in fact, is not completely understood. Neither the circle method (even over $\mathbf{Q}$ with Kloosterman's levelling process) nor the algebraic methods have been successful in this case. The approach through modular forms and theta functions leads to analogues of the Ramanujan Conjectures for $3/2$ weight forms. These have no known algebro-geometric interpretations. In fact, using the relation of Waldspunger [37] of the coefficients of such forms to the value at $s = \frac{1}{2}$ of corresponding automorphic L-functions, these half integral weight Ramanujan Conjectures turn out to be equivalent to versions of the 'Lindelöf Hypothesis' for these L-functions. For the problem at hand one needs to obtain estimates for these $3/2$ weight Fourier coefficients, which are better than what the sharp estimation of Kloosterman sums (to be precise in this case, these sums are variants known as Salié sums) yields. Duke [6] using an ingeneous embedding (into congruence subgroups) and positivity argument due to Iwaniec [14], was able to establish such 'non-trivial' bounds for the Fourier coefficients $a_f(m)$ of $3/2$ weight cusp forms f, when m is square free (all this being over $\mathbf{Q}$), (also see [8] for another proof of this which goes through estimating L-functions at $s = \frac{1}{2}$). This leads to the following result (see [9]): Given a definite form F in three variables over $\mathbf{Z}$, there is a constant C_F (*ineffective*) such that for $m \geqslant C_F$ and square-free, the equation $F(x) = m$ is solvable in $\mathbf{Z}$ iff it is solvable integrally locally. The square-free condition can be relaxed to m lying outside a given finite set of quadratic progressions (i.e. numbers of the form $t_j \nu^2$, $j = 1, \dots \ell, \nu \in \mathbf{Z}$) and in fact the local to global principle may fail along such a quadratic progression. The ineffectivity arises from the use of Siegel's ineffective lower bound for $L(1, \chi_d)$, see [35].

Extending these ideas as well as Kloosterman sum methods to number fields runs into basic problems not the least of which is caused by the units. In [4] an approach which directly uses the Maass spectral theory (and avoids Kloosterman sums) for Hilbert modular forms is developed and is used to establish nontrivial estimations of L-functions of Hilbert modular forms, at $s = \frac{1}{2}$. Using extensions of Waldpurger's formulas to this setting, these estimates translate to the desired nontrivial estimates for Fourier coefficients of Hilbert modular forms of half-integral weight. In particular one obtains the extension of the above result for quadratic forms in three variables over $\mathbf{Q}$ to definite forms F in three variables over K. We have only discussed definite forms because indefinite forms are easier to handle. The reason is that the general Siegel Mass Formula [36] gives an exact formula for the representation of m by the *genus* of F in terms of the Hardy-Littlewood densities in (2). In the case that the genus of F consists of a single class as is essentially the case when F is indefinite, the Mass Formula solves the representation problem explicitly in terms of local representability. Thus with the caveat of ineffectiveness, Hilbert's problem 11 is resolved.

My guess is that, if Kloosterman were alive today he would be happy to see that much progress has been made on what he set in motion, and he might well be even more delighted to see the extent to which his ideas and inventions are still at the forefronts of research.

References

1 A. Booker, *A test for identifying Fourier coefficients of automorphic forms and an application to Kloosterman sums* (2000).

2 R. Bruggeman, *Fourier coefficients of cusp forms*, Invent. Math. **45** (1978) 1–18.

3 J. Cassels, *Rational quadratic forms*, (1978) Academic Press.

4 J. Cogdell, I. Piatetsky–Shapiro, P. Sarnak, in preparation (2000).

5 P. Deligne, *La conjecture de Weil I*, I.H.E.S. **43** (1974) 273–307.

6 W. Duke, *Hyperbolic distribution problems and half integer weight Maass forms*, Invent. Math. **92** (1988), 73–90.

7 W. Duke, J. Friedlander and H. Iwaniec, *A quadratic divisor problem*, Invent. Math. **115** (1994), 209–217.

8 —, *Bounds for L–functions*, Invent. Math. **112** ((1993) 1–8.

9 W. Duke and R. Schulze-Pillot, *Representations of integers by positive definite quadratic forms and equidistribution of lattice points on ellipsoids*, Invent. Math. **90** (1990), 49–57.

10 M. Eichler, *Quaternäre quadratische Formen und die Riemannsche Vermuting für die kongruentz Zetafunktion*, Archiv. der Math. **5** (1954), 355–36.

11 H. Hasse, *Theorie der relativ-zyklischen algebraischen Funktionkörper, insbesondere bei eindichen Konstantenkörper*, Jnl. für die Reine **172** (1934), 37–54.

12 J. Hsia, M. Kneser and Y. Kitaoka, *Representations of positive definite quadratic forms*, J. Reine Angew Math. **301** (1978), 132–141.

13 Y. Ihara, *Hecke polynomials as congruence zeta functions in elliptic modular case*, Ann. Math. **85** (1967), 267–295.

14 H. Iwaniec, *Fourier coefficients of modular forms of half integral weight*, Invent. Math. **87** (1987), 385-401.

15 —, *Spectral theory of automorphic functions and recent developments in analytic number theory*, (1986) Proc. ICM Berkeley.

16 N. Katz, *Gauss sums, Kloosterman sums, and monodromy groups*, Ann. Math. Studies **116** (1988).

17 —, *Sommes exponentielles* Astérisque **79** (1980).

18 H. Kim and F. Shahidi, "Cuspidality of symmetric power L-functions and applications", in preparation (2000).

19 H. Kloosterman, *Over het splitsen van geheele positieve getallen in een some van kwadraten*, Thesis (1924) Universiteit Leiden.

20 —, *On the representation of numbers in the form $ax^2 + by^2 + cz^2 + dt^2$*, Acta. Math. **49** (1926), 407–464.

21 —, *Asymptotische Formeln für die Fourierkoeffizienten ganzer Modulformen*, Abh. Math. Sem Hamburg **5** (1927), 337–352.

22 —,*Theorie der Eisensteinshen Reihen von meheren Veränderlichen*, Abh. Math. Sem. Hamburg **6** (1928), 163–188.

23 — , *Thetareihen in total-reelen algebraischen Zahlkörpern*, Math. Ann. **103** (1930), 279–299.

24 —, *Simultane darstellung zweier ganzen zahlen als einer summe von ganzen zahlen und deren quadratsumme*, Math. Ann. **118** (1942), 319–364.

25 N. Kuznietzov, *Petersson's conjecture for cusp forms of weight zero and Linnik's conjecture, sums of Kloosterman sums*, Mat. SB. (NS) **39** (1981), 299-342.

26 M. Kneser, *Quadratische formen*, Lecture Notes, Göttingen (1974).

27 Y. Linnik, *Additive problems and eigenvalues of modular operators*, Proc I.C.M. Stockholm (1962), 270–284.

28 W. Luo, Z. Rudnick, P. Sarnak, *On the generalized Ramanujan conjectures for $GL(n)$* Proc. Symp. Pure Math. 66, Part 2, AMS. (1999).

29 A. Malyshev, *On the representations of integers by positive definite forms*, Mat. Steklov **65** (1962).

30 H. Petersson, *Zur analytischen Theorie der Grenzkreisgruppen*, I–IV Math. Ann. **115** (1938), 23–67, 175–204, 518–572, 670–709.

31 S. Ramanujan, *On certain arithmetical functions*, Trans. Camb. Phil. Soc. **XXII**, No. 9 (1916), 159–184.

32 H. Salié, *Zur Abschätzung der Fourierkoeffizienten ganzer Modulformen*, Math. Z. **36** (1931), 263–278.

33 A. Selberg, *On the estimation of Fourier coefficients of modular forms*, Proc. symp. Pure Math. **8** (1965), 1–15.

34 C. Siegel, *Additive theory der zahlkörper II*, Math. Ann. **88** (1923), 184–210.

35 —, *Uber die Klassenzahl quadraticher Zahlkörper*, Acta Arith. **83–86** (1935).

36 —, *Lectures on the analytic theory of quadratic forms*, Robert Peppermüller, Göttingen (1963).

37 L. Waldspurger, *Sur les coefficients de Fourier des formes modulaires de poids demi-entier*, J. Math. Pures Appl. **60** (1981), 375–484.

38 A. Weil, *On the Riemann hypothesis in function fields*, Proc. Nat. Acad. Sci. **27** (1941), 345–349.

39 —, *On some exponential sums*, Proc. Nat. Acad. Sci. **34** (1948), 204–207.