Contributions to Algebraic Number Theory from India

Dipendra Prasad

October 19, 2004

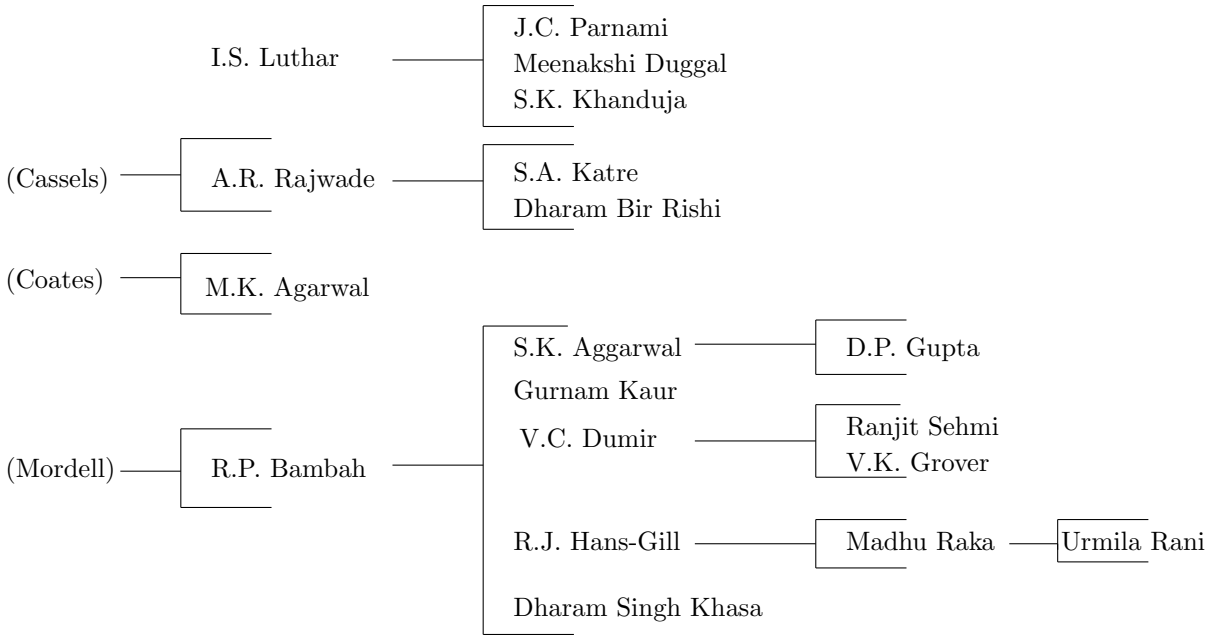
There was a conference organised at the Institite of Mathematical Sciences, Madras in 1997 on the occasion of the 50th anniversary of India's Independence to review contributions by Indians to various branches of mathematics since Independence. This is a written account of the lecture I gave then on some of the contributions by Indian mathematicians to Algebraic number theory for the period 1947-1997.

There has been a lot of work done in India during these years, and it will be impossible to report on all of it in limited space. We have therefore chosen some of the representative works from the vast literature reflecting to some extent the author's taste. Since this was a report about work done in the country, works of several very prominent mathematicians from India during this period who worked for most of their scientific career outside India has been omitted. In particular, we do not speak about the work of S. Chowla who has contributed so much to so many areas of Algebraic number theory. We have also restricted ourselves to areas very closely related to Algebraic number theory, and have therefore omitted topics in *transcendental* and *analytic number theory* which was reported by others in the conference. We have also omitted from our consideration the arithmetic theory of algebraic groups. In particular, we do not speak on the work of K.G. Ramanathan who initiated the study of arithmetic groups in the country which has flourished into a very strong area of research at the Tata Institute, Bombay.

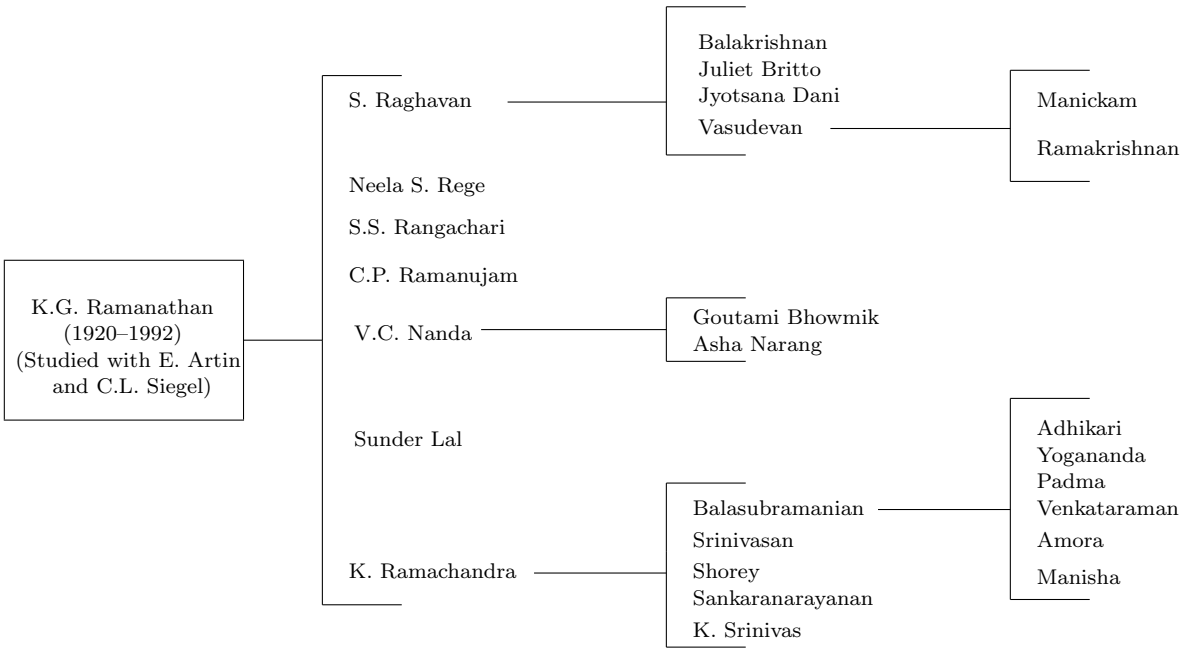
We begin the report by listing the two major schools in the country where algebraic number theory has been pursued, and in each case list some of the mathematicians from these schools. Limitation of knowledge on the part of the author has prevented him from a more complete list. In the list below, non-Indian mathematicians have been put in a bracket, and Y is on the immediate right of

X, if Y is a student of X.

Panjab University, Chandigarh



Tata Institute of Fundamental Research, Bombay



We now take up some specific topics in Algebraic number theory to which Indians have made a significant contribution.

1 Waring's Problem

The Waring's problem asks whether given any integer $k \geq 2$, there exists an integer $g(k) \geq 1$ such that any integer $n \geq 1$ is a sum of at most $g(k)$ kth powers of non-negative integers. The most classical result is for the exponent 2 in which case Lagrange proved that $g(2) = 4$.

Theorem 1 *(Lagrange) Any integer $n \geq 1$ can be written as $n = n_1^2 + n_2^2 + n_3^2 + n_4^2$ with integers $n_i \geq 0$.*

Theorem 2 *(Hilbert) Waring's problem has an affirmative answer for any exponent k, i.e., for any integer $k \geq 2$, there exists an integer $g(k)$ such that any integer $n \geq 1$ is a sum of at most $g(k)$ kth powers of non-negative integers.*

Theorem 3 *(Pillai-Dickson as completed by Balasubramanian, Deshouillers and Dress in the case $k = 4$ [BDD].)*

$$g(k) = 2^k + \left[\left(\frac{3}{2}\right)^k\right] - 2 \quad \text{if} \quad 2^k \left\{\left(\frac{3}{2}\right)^k\right\} + \left[\left(\frac{3}{2}\right)^k\right] \leq 2^k,$$

Otherwise,

$$g(k) = \begin{cases} 2^k + \left[\left(\frac{3}{2}\right)^k\right] + \left[\left(\frac{4}{3}\right)^k\right] - 2, \\ \text{Or}, \\ 2^k + \left[\left(\frac{3}{2}\right)^k\right] + + \left[\left(\frac{4}{3}\right)^k\right] - 3, \end{cases}$$

depending on whether

$$\left[\left(\frac{4}{3}\right)^k\right]\left[\left(\frac{3}{2}\right)^k\right] + \left[\left(\frac{4}{3}\right)^k\right] + \left[\left(\frac{3}{2}\right)^k\right] = 2^k, \quad \text{or} > 2^k,$$

where $\{x\}$ denotes the fractional part of x, and $[x]$ the integral part of x.

Remark : It is expected but not known (amazing as such a lack of knowledge might seem) that

$$2^k \left\{\left(\frac{3}{2}\right)^k\right\} + \left[\left(\frac{3}{2}\right)^k\right] \leq 2^k, \qquad (*)$$

and therefore only the first case in the statement of the theorem need be considered. Mahler has shown that $(*)$ holds for all but finitely many k.

1.1 Waring's problem for number fields

One can ask if Waring's problem has an affirmative answer in a number field too. However, one sees immediately that the problem may not have an affirmative answer because of local conditions. If for instance q is a power of prime and not itself a prime, then for any element x of $\mathbf{F}_q^*$, $x^{q-1} = 1$, and therefore sum of $(q-1)$-th powers of elements in $\mathbf{F}_q^*$ is not all of $\mathbf{F}_q^*$. The following theorem of C.P. Ramanujam [RCP1] is therefore the best (except for the explicit number of mth powers needed) one can hope for.

Theorem 4 *(C.P. Ramanujam) Any totally positive algebraic integer in any algebraic number field belonging to the order generated by the mth powers of algebraic integers in that number field is actually a sum of atmost max$(2^m + 1, 8m^5)$ mth powers of totally positive integers.*

Remark on the proof : The proof depends on a theorem of Birch that local to global principle holds in sufficiently large number of variables. Therefore it suffices to prove the above theorem for p-adic fields which is what C.P. Ramanujam does.

Generalising Waring's problem, one can ask about the set of values taken by a general form, or about the zero set of a general form: whether local to global principle holds, or whether the $weak\ approximation$ holds. Both these questions are an active area of research. Here is a theorem due to C.P. Ramanujam [RCP2], together with refinements due to Pleasant [Pl] and Hooley [Ho].

Theorem 5 *(C.P. Ramanujam) Any cubic form over any algebraic number field in ≥ 54 variables has a non-trivial zero.*

The strongest theorem in this direction is due to Pleasant obtained by refining the method of C.P. Ramanujam.

Theorem 6 *(Pleasant) Any cubic form over any algebraic number field in ≥ 16 variables has a non-trivial zero.*

Assuming the non-singularity of the cubic form, one has a much better theorem due to Hooley.

Theorem 7 *(Hooley) If $f(X)$ is a non-singular cubic form in 9 variables over $\mathbf{Q}$ which has a non-trivial zero in $\mathbf{Q}_p$ for all p, then $f(X)$ has a non-trivial zero.*

Remarks(a) The above theorem is due to Heath-Brown for 10 variables or more. In 10 variables, there are no local conditions: every cubic form in ≥ 10 variables over a p-adic field has a non-trivial zero.

(b) The theorem of Hooley is not yet available for number fields.

(c) It is expected that the theorem of Hooley is true without the non-singularity assumption.

2 Geometry of Numbers

This area was inaugurated by Minkowski in his work on discriminants and class numbers of number fields. R. P. Bambah and his school at Chandigarh have made several contributions to this area. We state below some of the questions in this subject in which this school has contributed. We begin by recalling the following basic and elementary theorem of Minkowski.

Theorem 8 *Let S be a convex, symmetrical domain in $\mathbf{R}^n$ containing the origin. Then S contains a point other than the origin from any lattice Λ whenever* $\mathrm{vol}(S) \geq 2^n \ \mathrm{vol}(\mathbf{R}^n/\Lambda)$.

Before proceeding further, we need to introduce the following definition.

Definition : A lattice $\Lambda \subset \mathbf{R}^n$ is called a covering lattice for a subset S in $\mathbf{R}^n$ if $\Lambda + S = \mathbf{R}^n$. The covering constant $c(S)$ of S is defined to be

$$c(S) = \sup \ \mathrm{vol}(\mathbf{R}^n/\Lambda),$$

where the supremum is taken over all latices Λ which form a covering lattice for S.

One also defines $\theta(S)$, the density of best covering lattice to be

$$\theta(S) = \frac{\mathrm{vol}(S)}{c(S)}.$$

Clearly, $\theta(S) \geq 1$. The following theorem is due to Bambah and Roth [BR].

Theorem 9 *For a closed convex symmetrical region S in $\mathbf{R}^n$ containing the origin,*

$$\theta(S) \leq \frac{\pi}{3\sqrt{3}} \frac{n^n}{n!}.$$

Remark: $\theta(D^n)$ even for the n-disc $D^n = \{x \in \mathbf{R}^n | |x| \leq 1\}$ in $\mathbf{R}^n$ is not known for $n \geq 6$!

Minkowski's Conjecture : Let $L_1, \cdots, L_n$ be linearly independent linear forms on $\mathbf{R}^n$ with $\Delta = \det(L_1, \cdots, L_n)$. Let $\alpha_1, \cdots, \alpha_n \in \mathbf{R}$. Then there exists $x \in \mathbf{Z}^n$ such that

$$\prod_{i=1}^{n} |L_i(x) + \alpha_i| \leq \frac{\Delta}{2^n}.$$

Bambah has proved this conjecture for $n = 4, 5$ in a joint paper with AC Woods, cf. [BW]. The conjecture is unknown for $n \geq 6$.

Oppenheim Conjecture : Given an indefinite quadratic form Q on $\mathbf{R}^n$ ($n \geq 3$) which is not a multiple of a rational quadratic form, and given $\epsilon > 0$, there exists $v \in \mathbf{Z}^n$, such that

$$0 < |Q(v)| < \epsilon.$$

Much work on this conjecture was done by Bambah, Raghavan and Ramanathan, cf.[RR2], besides Oppenheim, Davenport and Birch, and was finally proved by Margulis in 1986-87 who proved a conjecture of M.S. Raghunathan on the closure of orbits of unipotent flows on $\Gamma\backslash G$ where G is a Lie group, and Γ is an arithmetic subgroup. S.G. Dani and Gopal Prasad have also contributed to the Oppenheim Conjecture, see the papers [DM] and [BP]. Oppenheim conjecture is open to generalisation for forms of higher degree. Here we state the question in a rather crude form, cf. [RR1] for one case of such a conjecture.

Generalised Oppenheim Conjecture : Given a form Q of degree d on $\mathbf{R}^n$ ($n \geq n(d)$) which takes both positive and negative values and is not a multiple of a rational form, and given $\epsilon > 0$, there exists $v \in \mathbf{Z}^n$, such that

$$0 < |Q(v)| < \epsilon.$$

Here is another theorem relating to values of quadratic forms due to Blaney, cf. [Bl].

Theorem 10 *(Blaney, 1948) Let Q be an indefinite quadratic form in n variables and of discriminant $D \neq 0$. Then there exists a constant $\Gamma_{r,s}$ depending only on the signature (r, s) of Q at infinity, and not on Q itself, such that for any real numbers $c_1, \cdots, c_n$, there exists integers $x_1, \cdots, x_n$ such that*

$$0 < Q(x_1 + c_1, \cdots, x_n + c_n) < (\Gamma_{r,s}|D|)^{1/n}.$$

Much work has been done by Bambah, Hans-Gill, Dumir, Madhu Raka, Urmila Rani all from Chandigarh, to find the optimum $\Gamma_{r,s}$. The values of $\Gamma_{r,s}$ is now known for all r, s except $(r, s) = (1, 4)$. We refer to the survey paper [BDH] by Bambah, Dumir and Hans-Gill for a detailed account.

Examples :

(a) $\Gamma_{1,1} = 4$, due to Davenport and Heilbronn.
(b) $\Gamma_{2,1} = 4$, due to Blaney.
(c) $\Gamma_{1,2} = 8, \Gamma_{3,1} = \frac{16}{3}, \Gamma_{2,2} = 16$, due to Dumir.
(d) $\Gamma_{1,3} = 16$, due to Dumir and Hans-Gill.

3 Work on Elliptic curves and curves of higher genus

There has been a large number of papers by A.R. Rajwade, M.K. Agrawal, J.C. Parnami, D. B. Rishi, S.A. Katre, all from Chandigarh, cf. the bibliography at the end, and also by Padma and Venkataraman, cf. [PV], students of R. Balasubramanian from Mat. Science, Madras, on the explicit determination of the number of points on an elliptic curve with complex multiplication. Results have also been obtained for the number of points on curves of the form

$$y^2 = x^l + a.$$

Instead of stating various theorems obtained by the above mentioned mathematicians, we state one classical result of this kind due to Davenport and Hasse to give a flavour for the kind of the result that is obtained in this direction. The reader will easily notice that the problem one is really solving is one of signs.

Theorem 11 *(Davenport-Hasse) For the curve* $y^2 = x^3 - dx$,

$$N_p = \begin{cases} p+1 & \text{if} \quad p \equiv 3 \bmod 4 \\ p+1-\pi\left(\frac{d}{\bar{\pi}}\right)_4 - \bar{\pi}\left(\frac{d}{\pi}\right)_4 & \text{if} \quad p \equiv 1 \bmod 4. \end{cases}$$

Here $p = \pi\bar{\pi}$ *in* $\mathbf{Q}(i)$ *such that* $\pi, \bar{\pi}$ *are congruent to 1 modulo* $(2+2i)$*;* $\left(\frac{d}{\pi}\right)_4$ *is the 4th power residue symbol, and is defined to be the unique element* $x \in \{\pm 1, \pm i\}$ *such that*

$$d^{\frac{p-1}{4}} \equiv x \bmod \pi.$$

4 Siegel-Ramachandra-Robert Units

These are explicit units in abelian extensions of quadratic imaginary fields constructed using elliptic functions. After the initial work by Siegel, they were constructed by Ramachandra in [Ram], and then streamlined by Robert. These were called Siegel-Ramachandra-Robert units for some time, but are now called elliptic units and play a fundamental role in many works dealing with arithmetic of elliptic curves with complex multiplication as in the fundamental works of Coates-Wiles and Rubin.

Before we describe elliptic units, we describe the simpler case of cyclotomic units.

For $x \in \mathbf{Q}/\mathbf{Z}, x \neq 0$, let $g(x) = e^{2\pi i x} - 1$. Define the group of cyclotomic units to be the intersection of all units with the group generated by $g(x)$.

Theorem 12 *(a) If the denominator of x is composite, then $g(x)$ is a unit in the ring of algebraic integers. If the denominator of x is a power of p then $g(x)$ is a p-unit.*

(b) The mapping $x \to g(x)$ satisfies the distribution relation:

$$\prod_{Ny=x} g(y) = g(x),$$

for all integers $N \geq 1$.

(c) For $x \in \frac{1}{N}\mathbf{Z}/\mathbf{Z}$, $g(x) \in \mathbf{Q}(\zeta_N)$. For $a \in (\mathbf{Z}/N)^*$, let σ_a be the natural element in $\mathrm{Gal}(\mathbf{Q}(\zeta_N)/\mathbf{Q})$. Then

$$g(x)^{\sigma_a} = g(ax).$$

(d) The index of the cyclotomic units in all units is closely related to the class number of the real subfield. The index is equal to the class number in the case of prime power level.

Siegel Units: We will define Siegel units here which do not have as nice properties as the case of cyclotomic units described above, but are easier to define than the elliptic units which have properties much more analogous to cyclotomic units which we will be taking up next.

Let K be a quadratic imaginary field with H_K the Hilbert class field of K. We recall that H_K is the maximal unramified abelian extension of K and that its Galois group over K is canonically isomorphic to the class group of K. For an ideal $\mathcal{I}$ of K, we let $\sigma_{\mathcal{I}}$ denote the corresponding element of the Galois group of the Hilbert class field of K.

For an ideal $\mathcal{I}$ of K, define

$$u(\mathcal{I}) = \frac{\Delta(\mathcal{O}_K)}{\Delta(\mathcal{I}^{-1})},$$

where $\mathcal{O}_K$ is the ring of integers in K, and Δ is the Ramanujan delta function.

Theorem 13 *(Siegel)*

(a) $u(\mathcal{I}) \in H_K$.

(b) $u(\mathcal{I}\mathcal{J}) = u(\mathcal{I})^{\sigma_J} u(\mathcal{J})$.

(c) $(u(\mathcal{I})) = \mathcal{I}^{-12}$.

If h is the class number of K, then $\mathcal{I}^h$ is a principal ideal, say $\mathcal{I}^h = (\alpha), \alpha \in K^*$. Clearly, α is unique only up to a root of unity in K, and therefore α^{12} is well-defined. It follows that $\delta(\mathcal{I}) = u(\mathcal{I})^h \alpha^{12}$ is a well defined unit of H_K. The group generated by such units is called the group of Siegel units.

Elliptic Units: Let $L \subset \mathbf{C}$ be a lattice which is invariant under multiplication by elements of $\mathcal{O}_K$. For an integral ideal $\mathcal{I}$ of K, define

$$\begin{aligned} \Theta(z, L, \mathcal{I}) &= \frac{\theta(z,L)^{N\mathcal{I}}}{\theta(z,\mathcal{I}^{-1}L)} \\ &= \frac{\Delta(L)}{\Delta(\mathcal{I}^{-1}L)} \prod'_{u \in \mathcal{I}^{-1}L/L} \frac{\Delta(L)}{(\wp(z,L)-\wp(u,L))^6}. \end{aligned}$$

The prime over the product notation signifies that the product is to be taken over non-zero elements. (Since we do not define $\theta(z, L)$ here, one could take the second equality for the definition of $\Theta(z, L, \mathcal{I})$.) The numbers $\Theta(z, L, \mathcal{I})$ satisfy a 'distribution relationship' as in theorem 12(b):

$$\prod_{v \in \mathcal{J}^{-1}L/L} \Theta(z + v, L, \mathcal{I}) = \Theta(z, \mathcal{J}^{-1}L, \mathcal{I}),$$

which holds for any coprime ideals $\mathcal{I}, \mathcal{J}$ in $\mathcal{O}_K$.

Theorem 14 *Let m be a non-trivial integral ideal of K and v a primitive m-division point of L (i.e., $v \in m^{-1}L$ but $v \notin n^{-1}L$ for any proper divisor n of m). Then if $(\mathcal{I}, m) = 1$,*

(1) $\Theta(v, L, \mathcal{I})$ belongs to the m-ray class field of K.

(2) $\sigma_c(\Theta(v, L, \mathcal{I})) = \Theta(v, c^{-1}L, \mathcal{I})$.

(3) $\Theta(v, L, \mathcal{I})$ is a unit if m is not a power of a prime ideal. If $m = \wp^n$, it is a unit outside $\wp$.

5 Theta function associated to quadratic forms

Let $q : L \to \mathbf{Z}$ be a positive definite quadratic form on a lattice L in $\mathbf{R}^k$. The simplest theta function associated to q is

$$\begin{aligned} \theta_q(z) &= \textstyle\sum_{v \in L} e^{\pi i q(v) z} \\ &= \textstyle\sum_{n \geq 0} r_q(n) e^{\pi i n z} \end{aligned}$$

where $r_q(n) = \sharp\{v \in L | q(v) = n\}$.

It is known that $\theta_q(z)$ is a modular form of weight $k/2$ on the upper-half plane.

The Fourier coefficients of a theta function are all positive integers with 1 as its constant term. For many weights for the full modular group, Manickam, Ramakrishnan, Kalyan Chakraborty, Arbind Lal have determined all modular forms with these properties for their Fourier coefficients, cf. [CLR].

The space of modular forms is spanned by cusp forms and Eisenstein series. Eisenstein series have a simple Fourier expansion while cusp forms have nice estimates for their Fourier coefficients. Combining the two, one gets the following theorem.

Theorem 15 *(Hardy-Ramanujan)* $r_q(n) = \frac{\pi^{\frac{k}{2}} n^{\frac{k}{2}-1}}{\frac{k}{2}!}\sigma_k(n) + O(n^{\frac{k}{4}})$, *where* $k \geq 4$, *and* $\sigma_k(n)$ *is the 'singular series'.*

Such a theorem has been generalised by Raghavan in [RS1] who obtained an asymptotic formula for the number of integral representations of an n rowed positive semi-definite integral matrix T by an m rowed positive definite integral matrix S, i.e., the cardinality of the set of integral matrices X of size (n, m) with

$$XS^tX = T.$$

We will denote the cardinality of this set of X's by $r_S(T)$.

The estimate on $r_S(T)$ is via an association of Siegel modular form to S. We therefore fix some notation regarding Siegel modular forms.

Let

$$\mathbf{H}^n = \{Z = X + iY \in M_n(\mathbf{C}) | {}^tZ = Z, Y > 0\}$$

be the Siegel upper half space. The symplectic group $Sp(2n, \mathbf{R})$ operates on $\mathbf{H}^n$ and one has the notion of a Siegel modular form of genus n and weight k analogous to modular forms in one variable. A Siegel modular form has Fourier expansion

$$F(Z) = \sum_{{}^tA=A\geq 0} f(A)e^{\pi i \mathrm{tr}(AZ)}.$$

We now state Raghavan's theorem which estimates the Fourier coefficients of a Siegel modular form in terms of the Fourier coefficients of a linear combination of Eisenstein series. The difficulty in the proof of this theorem arises because unlike the one variable case, it is not true that a Siegel modular form is up to a cusp form, a linear combination of Eisenstein series. Raghavan has to use Siegel's

generalisation of the 'Farey dissection' to matrix spaces to obtain an estimate on the Fourier coefficient of the difference.

Theorem 16 *(Raghavan) Given a Siegel modular form*

$$F(Z) = \sum_{T \geq 0} a(T) e^{\pi i \mathrm{tr}(TZ)},$$

one can associate to $F(Z)$ a linear combination of Eisenstein series

$$\phi(Z) = \sum_{T \geq 0} b(T) e^{\pi i \mathrm{tr}(TZ)},$$

such that

$$a(T) - b(T) = 0([\mathrm{min}T^{-1}]^{\frac{n(n+1-2k)}{2}} [\mathrm{min}T]^{\frac{n+1-k}{2}})$$

for $|T| \geq \nu$, for some constant ν, and where $\mathrm{min}T$ denotes the minimum value taken by T at a non-zero vector.

Singular modular forms: A Siegel modular form F given by $F(Z) = \sum_{T \geq 0} f(T) e^{\pi i \mathrm{tr}(TZ)}$ is called a cusp form if $f(A) = 0$ whenever A is singular. At the other extreme we have the notion of a singular modular form which are Siegel modular forms which have the property that $f(A) = 0$ whenever A is non-singular. Certain theta functions constructed below provide examples of singular modular forms.

To a positive definite quadratic form $q : L \to \mathbf{Z}$, define $\theta_q(Z)$ to be the function on the Siegel upper-half plane $\mathbf{H}^n$ defined by

$$\theta_q(Z) = \sum_{{}^t A = A \geq 0} r_q(A) e^{\pi i \mathrm{tr}(AZ)}.$$

The function $\theta_q(Z)$ is called the theta function of genus n associated to the quadratic form q generalising the theta function in one variable defined at the beginning of this section. This Siegel modular form is singular if $k < n$. The first of the following two theorems, due to Resnikoff, states that the weights of singular modular forms is exactly like this, and the second due to Raghavan, cf. [RS2], states that singular modular forms are linear combinations of theta functions.

Theorem 17 *(Resnikoff): Singular modular forms of genus n exist only for weights $< n/2$.*

Theorem 18 *(Raghavan) A singular modular form is a linear combination of theta series.*

Remark : Raghavan proved the above theorem for the full modular group. The general case is due to Resnikoff and Freitag.

Raghavan also has several papers, some jointly with others, in which he studies estimates on the Fourier coefficients of Siegel modular forms, cf. [BR], for one such work.

6 Modular forms of half-integral weight

There has been an extensive study by Vasudevan of Vivekananda College, Chennai together with his former students Manickam and Ramakrishnan on the theory of new forms for half-integral weight modular forms and its relation to Jacobi forms. They have also made an explicit construction of the so called Shintani lifting which gives a connection between modular forms of integral and half-integral weights and have thereby obtained an explicit version of Waldspurger's theorem. We mention only one of their papers [MRV] out of several that they have written.

7 Henselian Rings

There has been several contributions from mathematicians at Chandigarh on Henselian rings.

The classical result of Hasse and Arf on higher ramification groups in a cyclic Galois extension of a complete discrete rank 1 valued field states that the jumps in the Herbrand upper indexing occur at integers. In a paper by Ram Avtar and N. Sankaran, cf. [AS], an analogous result has been proved for higher rank valued fields which are Henselian. They extend a result of S. Sen conjectured by A. Grothendieck, on wildly ramified automorphisms of a complete discrete rank 1 valued field.

Sudesh K. Khanduja has several papers around Hensel's lemma. We only mention [KS] here.

8 Brauer-Siegel theorem

There is the famous theorem in Algebraic number theory which tells how the various basic invariants of a number field (class number, regulator and the discriminant) vary as we vary the number field. In an interesting work, Sudesh K. Gogia (now Sudesh K. Khanduja after marriage!) and IS Luther prove the analogue for function fields.

9 Some more recent works

In this section we briefly mention about some of the recent works done in Algebraic number theory. All these mathematicians have been associated with the Tata Institute of Fundamental Research, Bombay.

Kirti Joshi : He has constructed coverings of the affine line using Drinfeld modules, cf. [J].

C. Khare : He has proved several results about congruences of modular forms, cf. [Kh1]. He also has proved that Artin's conjecture is a consequence of Serre's conjecture on modularity of certain Galois representations, cf. [Kh2].

Madhav Nori : He has a very beautiful construction for unramified coverings of the affine line in positive characteristic by finite Chevalley groups in that characteristic, cf. [N1]. He also has a new proof of the algebraicity of values of L-functions associated to Grössencharacters on totally real number fields which is due originally to Siegel and Klingen, cf. [N2].

Dipendra Prasad : According to conjectures of Langlands which have been proved in many cases, representation theory of p-adic algebraic groups is closely related to the representation theory of the Galois group of the p-adic field. Several of my works, some done in collaboration with B.H.Gross, cf. [GP], use this parametrization to give a description of "branching laws": explicit description of the decomposition of representations of a group restricted to a subgroup. In particular, there is a p-adic analogue of a theorem of Clebsch and Gordan about the tensor product of representations of $GL(2)$, cf. [P1],[P2].

C S Rajan : He has studied estimates on the orders of the Tate-Shafarevich group for elliptic curves over function field of curves over finite fields, cf. [Raj].

He also has proved multiplicity one theorem for ℓ-adic representations.

Nimish Shah : Counting integral points on Algebraic varieties of bounded height is a basic and important problem in number theory. Nimish Shah together with his collaborators have an impressive paper dealing with this problem when the variety in question is a closed subvariety of the affine n-space which is acted upon transitively by a reductive algebraic group, and for more general such homogeneous varieties. The proofs depend on the 'unipotent flows' on measures, see [EMS], for a paper in this direction.

Acknowledgement: The author would like to thank A. Raghuram and C.S.Yogananda, and Prof. R.J.Hans-Gill for their help.

10 Bibliography

[AS] Ram Avtar and N. Sankaran, Higher ramification in Hensel fields. *J. Reine Angew. Math.* 306 (1979), 185–191.

[BDD] R. Balasubramanian, J-M Deshouillers, F. Dress, Probleme de Waring pour les bicarres, I and II, *CR Acad. Sci. Paris Series I, Math.* 303(1986) 85-88 and 161-163.

[BDH] R.P. Bambah, V.C. Dumir, and R.J. Hans-Gill, Non-homogeneous problems: conjectures of Minkowski and Watson. *Number theory,* 15–41, Trends Math., Birkhuser, Basel, 2000.

[BR] R.P. Bambah and K.F. Roth, A note on lattice coverings, *Journal of Indian Mathematical Society*, 16(1952), 7-12.

[BW] R.P. Bambah, A.C. Woods, Minkowski's conjecture for $n = 5$; a theorem of Skubenko, *J. of Number theory* 12 (1980) 27-48.

[Bl] H. Blaney, Indefinite quadratic forms in n variables, *Journal of London Mathematical Society*, 23(1948), 153-160.

[BR] S. Bocherer, S. Raghavan, On Fourier coefficients of Siegel modular forms, *J. Reine Angew. Math* 384 (1988) 8-101.

[BP] A. Borel and G. Prasad, Values of isotropic quadratic forms at S-integral points,*Compositio Math.* 83 (1992), no. 3, 347–372.

[CLR]K. Chakraborty, A.K. Lal, B. Ramakrishnan, Modular forms which behave like theta functions, *Math. Computations* 66(1997) 1169-1183.

[DM] S.G. Dani and G.A. Margulis, Values of quadratic forms at integral points: an elementary approach, *Enseign. Math.* (2) 36 (1990), no. 1-2, 143–174.

[EMS] A. Eskin, S. Mozes, and N. Shah, Unipotent flows and counting lattice points on homogeneous varieties, *Ann. of Math.* (2) 143 (1996), no. 2, 253–299.

[GL]Sudesh K. Gogia and I.S. Luthar, The Brauer-Siegel theorem for algebraic function fields. *J. Reine Angew. Math.* 299/300 (1978), 28–37.

[GP1] B.H. Gross and D. Prasad, On the decomposition of a representation of SO(n) when restricted to SO(n-1), *Canadian J. of Maths* 44, 974-1002 (1992).

[H] C. Hooley, On nonary cubic forms, *J. Reine Angew. Math.* 386(1988) 32-98.

[J] K. Joshi, A family of etale coverings of the Affine Line, *Journal of Number Theory*, 59(1996), 414-418.

[KR] S.A. Katre and A.R. Rajwade, Resolution of sign ambiguity in the determination of the cyclotomic numbers of order 4 and corresponding Jacobsthal sum, *Math Scand.* 60 (1987) 52-62.

[KS] Sudesh K. Khanduja and Jayanti Saha, Generalized Hensel's lemma. *Proc. Edinburgh Math. Soc.* (2) 42 (1999), no. 3, 469–480.

[Kh1] C. Khare, Congruences between cusp forms, *Duke Mathematical Journal*, 80(1995) 631-667.

[Kh2]C. Khare, Remarks on mod p forms of weight one, *International Mathematics Research Notices*, 3(1997), 127-133.

[MRV] M. Manickam, B. Ramakrishnan, TC Vasudevan, The theory of new forms of half integral weight, *J. of Number theory* 34 (1990) 210-224.

[N1] M.V.Nori, Unramified coverings of the affine line in positive characteristic, *Algebraic Geometry and its applications (West Lafayette, IN, 1990), Springer-Verlag* (1994) 209-212.

[N2] M.V.Nori, Some Eisenstein cohomolgy classes, *Proceedings of the International Congress of Mathematicians, Zurich* 1994, Birkhauser (1995) 690-696.

[PAR] J.C. Parnami, M.K. Agrawal, A.R. Rajwade, The number of points on the curve $y^2 = x^5 + a$ in $\mathbf{F}_q$ and applications to local zeta functions, *Math. Student* 48 (1980) 205-211.

[Pl] P.A.B. Pleasant, Cubic polynomials over algebraic number fields, *J. of Number Theory* 7(1975), 310-344.

[PV] R. Padma and S. Venkataraman, Elliptic curves with complex multiplication and a character sum, *Journal of Number Theory* 61 (1996) 274-282.

[P1] D. Prasad, Trilinear forms for representations of GL(2) and local epsilon factors, *Compositio Math* 75, 1-46 (1990).

[P2] D. Prasad, Invariant linear forms for representations of GL(2) over a local field, *American J. of Maths* 114, 1317-1363 (1992).

[RS1] S. Raghavan, Modular forms of degree n and representation by quadratic forms, *Annals of Mathematics*, 70 (1959) 446-470.

[RS2] S. Raghavan, Singular modular forms of degree s, *in C.P. Ramanujam: A tribute, published by Springer Verlag for Tata Institute of Fundamental Research* (1978) 263-272.

[RR1] S. Raghavan and K.G. Ramanathan, Solvability of Diophantine inequality in Algebraic number fields, *Acta Arithmetica* (1972) 299-315.

[RR2] S. Raghavan and K.G. Ramanathan, Values of quadratic forms, *J. of Indian Math. Society 34*(1970), 253-257.

[Raj] C.S. Rajan, On the size of the Shafarevich-Tate group of elliptic curves over function fields, *Compositio Math. 105*(1997) 29-41.

[R1] A.R.Rajwade, The number of solutions of the congruence $y^2 \equiv x^6 - a \bmod p$, *Indian J. of pure and applied Math.* 4(1973) 325-332.

[R2] A.R.Rajwade, On the congruence $y^2 \equiv x^5 - a \bmod p$, *Proc. Cambridge Philosophical society*, 74(1973) 473-475.

[R3] A. R.Rajwade, Notes on the congruence $y^2 \equiv x^5 - a \bmod p$, *l'Enseignement Math* 21 (1975) 49-56.

[RR] Madhu Raka and Urmila Rani, Positive values of inhomogeneous indefinite ternary quadratic forms of type $(2, 1)$, *Hokkaido Math. J.* 25(1996) 215-230.

[RCP1]C.P. Ramanujam, Sums of mth powers in p-adic rings, *Mathematika*, 10(1963), 137-146.

[RCP2] C.P. Ramanujam, Cubic forms over algebraic number fields, *Proceedings of Cambridge Philosophical society*, 59(1963), 683-705.

[Ram] K. Ramachandra, Some applications of Kronecker limit formula, *Annals of Mathematics*, vol. 80, 1964, 104-148.

[Re] H.L.Resnikoff, Automorphic forms of singular weight are singular forms, *Math. Annalen* 215(1975) 173-193.

Mehta Research Institute,
Chhatnag Road, Jhusi,
Allahabad-211019.