Lectures on Siegel Modular Forms and Representation by Quadratic Forms

By

Y. Kitaoka

Tata Institute of Fundamental Research
Bombay
1986

Lectures on Siegel Modular Forms and Representation by Quadratic Forms

By

Y. Kitaoka

Published for the

Tata Institute of Fundamental Research
Springer–Verlag
Berlin Heidelberg New York Tokyo
1986

Author
Y. Kitaoka
Department of Mathematics
Faculty of Science
Nagoya University
Chikusa–Ku, Nagoya, 464
JAPAN

ISBN 3-540-16472-3 Springer–Verlag, Berlin. Heidelberg.
New York. Tokyo
ISBN 0-387-16472-3 Springer–Verlag, New York.
Heidelberg. Berlin. Tokyo

Printed by K. M. Aarif at Paper Print India, Worli,
Bombay 400 018 and published by H. Goetze,
Springer–Verlag, Heidelberg, West Germany,

Printed In India

Preface

These are based on my lectures at the Tata Institute of Fundamental Research in 1983-84. They are concerned with the problem of representation of positive definite quadratic forms by other such forms.

§ 1.6 and Chapter 2 are added, besides lectures at the Institute, by Professor Raghavan (who also wrote up §§ 1.1–1.4) and myself respectively.

I would like to thank Professor Raghavan and the Tata Institute for their hospitality.

Y. Kitaoka

Contents

Chapter 1

Fourier Coefficients of Siegel Modular Forms

Introduction

1

The problem of the representation of a natural number t as the sum of a given number m of squares of integers is quite classical and although its history goes back to Diophantus, it may be said to have begun effectively with Fermat's theorem that every prime number congruent to 1 modulo 4 is a sum of two squares of integers. Practically, every mathematician of repute since Fermat has made a contribution to problems of this type in the theory of numbers. One has, thanks to Jacobi, a formula for the number $r_m(t)$ of representations of t as a sum of m squares of integers, with $m = 2, 4, 6$ and 8; for example,

$$r_2(t) = 4 \sum_{\substack{d|t \\ d \text{ odd}}} (-1)^{(d-1)/2},$$

$$r_4(t) = \begin{cases} 8 \sum\limits_{d|t} d & (t \text{ odd}) \\ 24 \sum\limits_{\substack{d|t \\ d \text{ odd}}} d & (t \text{even}). \end{cases}$$

Analogously, one can ask for the determination of (m, n) integral matrices G or of the *number* $r(A, B)$ of all *such* G, for which

$$(A[G] :=)^t GAG = B \qquad (*)$$

2 where A and B are given (m, m) and (n, n) integral positive definite matrices. As a first step, one can seek suitable conditions under which $(*)$ has a solution. A recent result in this direction is given by

Theorem A ([8])**.** *If $m \geq 2n + 3$ and if, for every prime number p, there exists a matrix G_p with entries in the ring $\mathbb{Z}_p$ of p-adic integers with ${}^tG_pAG_p = B$, then we have an integral matrix G satisfying the equation ${}^tGAG = B$, provided that for the minimum of B, viz.* $\min(B) := \inf_{0 \neq X \in \mathbb{Z}^n} {}^tXBX$*, we have* $\min(B) > \mathscr{X}(A)$ *for a suitable constant* $\mathscr{X}(A)$*.*

The proof of this theorem is arithmetical in nature and is given in Chapter 2. §2.4.

Remarks 1. If, on the other hand, A is *indefinite* with $m \geq n + 3$ and if, for every prime p including ∞, $(*)$ admits a solution G with entries in $\mathbb{Z}_p$, then it is known that $(*)$ has a solution G with entries in $\mathbb{Z}$. The proof is given in Chapter 2, § 2.4.

2. In the case $n = 1$ and $m \geq 5$, under the solvability of $(*)$ with G over $\mathbb{Z}_p$ for every prime p (including ∞), Theorem A, in this case, is well-known ([27], [4]). For $n = 1$ and $m = 4$, however, if, in addition, to the solvability of $(*)$ in G over $\mathbb{Z}_p$ for every prime p, one assumes further that for every prime q dividing $2 \det A$, the power of q dividing B does not exceed a fixed integer t, then for all $B > \mathscr{X} = \mathscr{X}(t)$, the equation $(*)$ is solvable over $\mathbb{Z}$. The proof of a stronger form of this assertion viz. A is anisotropic over q instead of "q dividing $2 \det A$", is purely arithmetic in nature and may be found in Kneser's Lectures [15]. An analytic proof
3 using the decomposition of theta series into Eisenstein series and a cusp form is also possible. If $m = 3$ and $n = 1$, assuming conditions as for $m = 4$ above, $(*)$ is solvable over $\mathbb{Z}$ for all $B > \mathscr{X} = \mathscr{X}(t)$, provided that B does not belong to a finite number

of "exceptional spinor classes" and further that the Generalized Riemann Hypothesis holds; the proof is arithmetical in nature. The case $m = 2$ and $n = 1$ reduces to a problem of representation over quadratic fields.

There is an analytic approach to Theorem A, based on the asymptotic behaviour of $r(A, B)$ or, more precisely, on an asymptotic formula for $r(A, B)$ as B "goes to infinity". Clearly $r(A, B) > 0$ if and only if $(*)$ is solvable for G over $\mathbb{Z}$. One first looks for a generating function for $r(A, B)$. Let $\mathscr{G}_n = \{Z \in \mathscr{M}_n(\mathbb{C}) | Z = {}^tZ,\ i^{-1}(Z - \overline{Z}) > 0\}$, the Siegel upper half space of degree n (or "genus n"). For the given $A > 0$ and any Z in $\mathscr{G}_n$, let

$$\vartheta(Z) = \vartheta(Z; A) := \sum_B e(\mathrm{tr}({}^tGAGZ))$$

where $e(\alpha) := \exp(2\pi i\alpha)$, tr denotes the trace and G runs over all (m, n) integral matrices. Then it is clear that $\vartheta(Z) = \sum\limits_{B \geq 0} r(A, B)e(\mathrm{tr}(BZ))$ where B now runs over all (n, n) non-negative definite integral matrices. It turns out that the theta series $\vartheta(Z)$ is a Siegel modular form of degree n, weight $m/2$ and level N (some N depending on A). Thus the problem now reduces to studying the asymptotic behaviour of Fourier coefficients of Siegel modular forms which is in the very centre of the analytic approach referred to.

If $A_1 = {}^tUAU$ for U in $GL_m(\mathbb{Z})$, then obviously $\vartheta(Z; A_1) = \vartheta(Z; A)$ **4**
i.e. $\vartheta(Z)$ is a class-invariant associated with A, depending only on the class (of matrices A_1 "equivalent" to A as above). The genus of A consists of all positive-definite matrices A^* such that for every prime number p, $A^* = {}^tU_pAU_p$ for U_p in $GL_m(\mathbb{Z}_p)$; it is known from the reduction theory of quadratic forms, that the genus of A consists of finitely many classes. Let $A_1, A_2, \ldots, A_h$ be a complete set of representatives of the classes in the genus of A and let $o(A_i)$ be the order of the unit group of A_i, consisting of all U in $GL_m(\mathbb{Z})$ with ${}^tUA_iU = A_i$. Then we have the genus - invariant $E(Z) := \{\sum_i \vartheta(Z; A_i)/o(A_i)\}/\{\sum\limits_i 1/o(A_i)\}$ associated with A, having the Fourier expansion $\sum\limits_{B \geq 0} a(B)e(\mathrm{tr}(BZ))$. From Siegel

[23], we know that, for $B > 0$,

$$a(B) = \pi^{n(2m-n+1)/4} \prod_{k=0}^{n-1} \{1/\Gamma\left(\frac{m-k}{2}\right)\} |\det A|^{-n/2} |\det B|^{\frac{m-n-1}{2}} \prod_p \alpha_p(A, B)$$

the product $\prod\limits_p$ being extended over all prime numbers p and $\alpha_p(A, B)$, the p-adic density of representation of B by A is defined as

$$\lim_{t\to\infty} p^{tn(n+1-2m)/2} \sharp\{G \in \mathscr{M}_{m,n}(\mathbb{Z}/p^t\mathbb{Z}) | {}^tGAG \equiv B(\mathrm{mod\ p^t})\}.$$

We note that $a(B) \neq 0$ if and only if for every prime p, ${}^tGAG = B$ is solvable for G over $\mathbb{Z}_p$. One then defines the modular form g by $g(Z) = \vartheta(Z) - E(Z)$ so that, denoting the Fourier coefficients of g by $b(B)$, we have

$$r(A, B) = a(B) + b(B).$$

One expects this to be an asymptotic formula for $r(A, B)$, with $a(B)$ as the "main term" and $b(B)$ as the "error term", one needs to estimate $a(B)$ i.e. essentially $\prod\limits_p \alpha_p(A, B)$, from below, as indeed shown to be possible by

Theorem B. *If $m \geq 2n + 3$ and if ${}^tGAG = B$ is solvable for G over $\mathbb{Z}_p$ for every prime p, then $\prod\limits_p \alpha_p(A, B) > \mathscr{X}(A) > 0$, for a constant $\mathscr{X}(A)$.*

Remarks 3. The condition $m \geq 2n + 3$ in Theorem B is best possible. (Likewise in Theorem 1 too, this condition seems best possible; however, no counter examples are available to establish the same).

4. Let $m > n$ and $P : \{p \,|\, p \nmid 2\det A\}$. Then if $B = {}^tX_pAX_p$ for every prime p with primitive X_p (i.e. with $(X_p *) \in GL_m(\mathbb{Z}_p)$), then $\prod\limits_{p\in P} \alpha_p(A, B) > \mathscr{X}(A) \prod\limits_{p\in P(B)} (1 + \varepsilon_p p^{-1})$ for a constant $\mathscr{X}(A) > 0$. Here $P(B)$ is defined as the set of primes p for which $m - 2n + t_p = 2$ and ε_p is the Legendre symbol $\left(\dfrac{(-1)^{m-n-1} dN_0 \det A}{p}\right)$; if $B \equiv ((v_i, v_j))(\mathrm{mod\ p})$ for a basis $\{v_i, \ldots, v_n\}$ of the associated quadratic space N over $\mathbb{Z}/p\mathbb{Z}$ with the orthogonal decomposition

$N = \mathrm{Rad}\, N \perp N_0$, $t_p = \dim N_0$ and dN_0 the discriminant of N_0. For almost all p, B is unimodular and $t_p = n$.

If $m > n + 2$, $P(B)$ is a finite set. If $m = 2n + 2$, $B = {}^tX_p A X_p$ for a primitive X_p, whenever $p \in P$; in that case, $\prod\limits_{p \in P(B)} (1 + \varepsilon_p p^{-1}) > \prod\limits_{p|e(B)} (1 - p^{-1}) \gg e(B)^{-\varepsilon}$ for every $\varepsilon > 0$, with $e(B)$ denoting the first elementary divisor of B. For $m = 2n + 2$,

$$p \in P(B) \Longleftrightarrow t_p = 0 \Longleftrightarrow N = \mathrm{Rad}\, N \Longleftrightarrow B = 0(\text{mod p}) \Longleftrightarrow \text{p|e(B)}.$$

5. The next step is naturally to get upper estimates for the Fourier coefficients $b(B)$ of $g(Z)$ which, by its very construction, has the property that for every modular substitution $Z \to M < Z >$ $(:= (AZ + B)(CZ + D)^{-1})$, of degree n, the constant term in the Fourier expansion $g(M < Z >) \det(CZ + D)^{-m/2} = \sum\limits_B b(B, M) e(\mathrm{tr}(BZ)/N)$ vanishes. For $n = 1$, this property characterises a cusp form; however, g is not a cusp form for $n > 1$, in general, preempting an appeal to the estimation of Fourier coefficients of cusp forms of degree n. 6

Using Hecke's estimate $b(B) = O(B^{m/4})$ for the Fourier coefficients of cusp forms (of degree 1 and weight $m/2$), we have for $m \geq 5$ an asymptotic formula $r(A, B) = a(B) + O(B^{m/4})$, noting that $a(B) \gg B^{(m/2-1)}$, whenever $a(B) \neq 0$. For $n = 1$ and $m = 4$, we can say that $a(B) \gg B^{1-\varepsilon} \prod\limits_{p|2 \det A} \alpha_P(A, B) \gg B^{1-\varepsilon}$ for every $\varepsilon > 0$, whenever $a(B)$ is non-zero, provided that an additional restriction that the power of primes p dividing $2 \det A$ does not exceed p^t for a fixed t; the implied constants in $\gg$ depend on t. Using Kloosterman's method, the "error term" $b(B)$ in this case has the estimate $b(B) = O(B^{(m/4)-1/4+\varepsilon})$ for every $\varepsilon > 0$ and thus we have again a genuine asymptotic formula for $r(A, B)$. Very little is known, in this respect, for $n = 1$ and $m = 3$.

Coming to the general case $n \geq 1$ and $m \geq 2n + 3$, we shall prove the following theorems, using Siegel's generalized circle method

Theorem C ([10],[19]). *For* $n \geq 1$, $m \geq 2n + 3$ *and* $B > 0$ *with* $\det B \ll$ 7

$(\min(B))^n b(B) = O(\min(B)^{(n+1-m/2)/2}(\det B)^{(m-n-1)/2})$. *(For* $n = 2$, *the condition* $\det B \ll (\min(B))^2$ *is unnecessary).*

Theorem D ([10],[20])**.** *For* $n \geq 1$ *and even* $m \geq 4n + 4$, $b(B) = O(\min(B)^{1-m/4}(\det B)^{(m-n-1)/2})$

Remarks 6. Since $\prod_p \alpha_p(A, B) \gg 1$, $1 - m/4 < 0$ and $1 - m/2 + n < 0$, both Theorems C and D yield asymptotic formulae for $r(A, B)$, as the 'minimum' $\min(B)$ of B goes to infinity. The condition $\det B \ll (\min B)^n$ for $n \geq 3$ in Theorem C is substantially the same as insisting that $\min(B)^{-1}B$ lies in a compact set.

The case when $m \leq 2n + 2$ and in particular $n = 2$, $m = 6$ is difficult and a conditional result can be obtained in this special case, by using a generalization of Kloosterman's method (involving the estimation of exponential sums).

For $m = 6$ and $n = 2$, let $\mathfrak{g} = \{Z \in \mathscr{G}_2 | \operatorname{abs}\det(CZ + D) \geq 1$ for every modular matrix $M = \begin{pmatrix} * & * \\ C & D \end{pmatrix}$ of degree $2\}$. Let us *make the following*

Assumption. Let c_1, c_2 be natural numbers, $c_1 | c_2$ and $Z \in \mathscr{G}_2$. Then, for

$$\sum_{\substack{g_1, g_2 \bmod c_1 \\ g_4 \bmod c_2}} \Big| \sum_{\substack{u_1, u_2 \bmod c_1 \\ u_4 \bmod c_2}} e((u_1 g_1 + u_2 g_2)/c_1 + u_4 g_4/c_2) \Big| = O(c_1^{2+a_1+\varepsilon} c_2^{1+a_2})$$

$$\begin{pmatrix} u_1/c_1 & u_2/c_1 \\ u_2/c_1 & u_4/c_2 \end{pmatrix} + Z \in \mathfrak{g}$$

where $0 \leq a_1 \leq 3/2$, $0 \leq a_2 < 1/2$ and the O-constant is independent of Z. Then we can prove

8 **Theorem E.** *For* $m = 6$, $n = 2$ *and Minkowski-reduced* $B = \begin{pmatrix} * & * \\ * & b_{22} \end{pmatrix} > 0$, *with* $\min(B) \geq$ *an absolute constant* $\mathscr{X} > 0$, *we have*

$$b(B) = O(((\min(B))^{(2a_2-1)/4+\varepsilon} + (\min(B))^{-1} \log \frac{\sqrt{\det B}}{\min(B)})(\det B)^{3/2})$$

under the assumption above, where $\omega(b_{22})$ *is the number of distinct prime divisors of* b_{22}.

Notation and Terminology.

For any matrix A, the transpose is denoted by ${}^tA$. By $\mathscr{M}_{r,s}(R)$ we mean the set of (r, s) matrices with entries in a commutative ring R with identity. If $A \in \mathscr{M}_{r,r}(R) = \mathscr{M}_r(R)$, then the determinant and the trace of A are denoted by $\det A$ and $\mathrm{tr}(A)$ respectively. For given matrices A, B we abbreviate ${}^tBAB$ (when defined) by $A[B]$. Superscripts r, s on a matrix $A^{(r,s)}$ indicate that it has r rows and s columns; by $A^{(r)}$, we mean an (r, r) matrix A. By $GL_n(R)$ we mean the group of (n, n) matrices with entries in R and $\det R$ invertible in R. For two matrices A, B in $\mathscr{M}_{r,s}(\mathbb{Z})$, we say $A \equiv B (\mathrm{mod\ q})$ if all the entries of $A - B$ are divisible by q. The (n, n) identity matrix is denoted by E_n and 0 represents a matrix, of the appropriate size, with all entries equal to 0. We write $A > B$ (respectively $A \geq B$) to say that $A - B$ is a symmetric positive-definite (respectively non-negative-definite) matrix; $A < B$ (respectively $A \leq B$) if $B > A$ (respectively $B \geq A$). We use the O and o notation of Hardy-Littlewood as well as the notation $\ll$ or $\gg$ (due to Vinogradov). When $f \ll g$ as well as $f \gg g$, we simply write $f \asymp g$; a similar notation applies to matrices. By $GL_m(\mathbb{Z}; q)$, we mean the congruence subgroup **9**
$\{U \in GL_m(\mathbb{Z}) | U \equiv E_m (\mathrm{mod\ q})\}$ of level q. A matrix $F^{(n,r)}$ in $\mathscr{M}_{n,r}(\mathbb{Z})$ with $r \leq n$ is called primitive, if there exists $U = (F*)$ in $GL_n(\mathbb{Z})$. By $[a_1, \ldots, a_n]$ we mean a diagonal matrix with $a_1, \ldots, a_n$ as diagonal elements. By an integral matrix, we mean a matrix with entries from $\mathbb{Z}$. For a complex matrix $W = (w_{ij})$, the matrix $(\overline{w}_{ij})$ with the complex conjugates $\overline{w}_{ij}$ as corresponding entries is denoted by $\overline{W}$.

Let $\Lambda_n = \{S = {}^tS \in \mathscr{M}_n(\mathbb{Z})\}$ and Λ_n^*, the dual of Λ_n, viz. $\{S = {}^tS = (s_{ij}) \in \mathscr{M}_n(\mathbb{Q}) | s_{ii}, 2s_{ij} \in \mathbb{Z}\} = \{S = {}^tS \,|\, \mathrm{tr}(ST) \in \mathbb{Z}$ for every T in $\Lambda_n\}$.

1.1 Estimates for Fourier Coefficients of Cusp Forms of Degree 1

10

We first give an elaborate description of the case of modular forms of one variable, which is quite typical, in a sense but not entirely so, since the higher dimensional cases are fairly difficult. We have already remarked that the modular form g introduced earlier is a cusp form for

$n = 1$ but not so, in general, for $n > 1$.

Let $H = \{z \in \mathbb{C} | \operatorname{Im} z > 0\}$ and k, N be natural numbers. The principal congruence subgroup $\Gamma(N) = \{\sigma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}) | \sigma \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) (\text{mod N})\}$ of the modular group $\Gamma = \Gamma(1)$ acts on H via the conformal mappings of H given by $Z \mapsto \sigma(z) = (az+b)(cz+d)^{-1}$ for $\sigma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in $\Gamma(N)$. We recall that $e(\alpha) = \exp(2\pi i\alpha)$ for $\alpha \in \mathbb{C}$.

Definition. *A holomorphic function $f : H \to \mathbb{C}$ is called a cusp form (respectively a modular form) of weight k and level N if, for every*

$$\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(N),\ f((az + b)(cz + d)^{-1})(cz + d)^{-k} = f(z)$$

and further for every

$$\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma,\ f(\sigma(z))(cz + d)^{-k} = \sum_{m>0} a_m e(mz/N)$$

(respectively $= \sum\limits_{m\geq 0} a_m e(mz/N)$).

For $\sigma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$ and $f : H \to \mathbb{C}$, we abbreviate $f(\sigma(z))(cz + d)^{-k}$ by $f|\sigma$. It is easy to verify that, for σ_1, σ_2 in Γ, we have $f|\sigma_1\sigma_2 = (f|\sigma_1)|\sigma_2$.

The following two theorems give estimates for the Fourier coefficients of cusp forms.

11 **Theorem 1.1.1** (Hecke [7]). *For the Fourier coefficients a_m of a cusp form $f(z) = \sum\limits_{m>0} a_m e(mz)$ of weight $k (\geq 2)$ and level N, we have $a_m = O(m^{k/2})$.*

Theorem 1.1.2. *For f as in Theorem 1.1.1, $a_m = O(m^{k/2-1/4+\varepsilon})$ for every $\varepsilon > 0$.*

We fix some notation and prove a few lemmas, before going on to the proofs of these two theorems.

We know that $\mathfrak{F} = \{z = x+iy \in H | \ |x| \leq 1/2, |z| \geq 1\}$ is a fundamental domain for the modular group Γ in H.

Let

$$\sigma < \mathfrak{F} >= \{\sigma(z)|z \in \mathfrak{F}\}, \Gamma_\infty \left\{ \begin{pmatrix} \pm 1 & n \\ 0 & \pm 1 \end{pmatrix} \in \Gamma | n \in \mathbb{Z} \right\} \text{ and } \mathfrak{g} = \bigcup_{\sigma \in \Gamma_\infty} \sigma < \mathfrak{F} > .$$

For any fixed m as in the assertion of Theorem 1.1.1 or 1.1.2 and for $\sigma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in Γ, let $\beta(\sigma) := \{x \in [0, N] | \sigma(x + \mathrm{im}^{-1}) \in \mathfrak{g}\}$. We also write $\beta(c, d)$ for $\beta(\sigma)$, as may be seen to be appropriate.

Since $H = \bigcup\limits_{\sigma \in \Gamma_\infty \backslash \Gamma} \sigma < \mathfrak{g} >$, we have $I_{N,m} = \{x + \mathrm{im}^{-1} | 0 \leq x \leq N\} = \bigcup\limits_{\sigma \in \Gamma_\infty \backslash \Gamma} \beta(\sigma)$, this being indeed a finite union, in view of the compactness of $I_{N,m}$. Further $I_{N,m} \cap \mathfrak{g} = \emptyset$ for $m > 2/\sqrt{3}$, since for $z = x + iy \in \mathfrak{g}$, $y \geq \sqrt{3}/2$. Thus $I_{N,m} = \bigcup\limits_{\substack{\sigma \in \Gamma_\infty \backslash \Gamma \\ \sigma \notin \Gamma}} \beta(\sigma)$. Further, measure $(\beta(\sigma_1) \cap \beta(\sigma_2)) = 0$, for $\sigma_1 \notin \Gamma_\infty \sigma_2$.

Now

$$\begin{aligned} N a_m &= \int\limits_0^N f(x + \mathrm{im}^{-1}) e(-m(x + \mathrm{im}^{-1})) dx \\ &= e^{2\pi} \sum_{\substack{\sigma \in \Gamma_\infty \backslash \Gamma \\ \sigma \notin \Gamma_\infty}} \int\limits_{\beta(\sigma)} f(z) e(-mx) dx \end{aligned}$$

$$\text{i.e.} \qquad a_m = \frac{e^2 \pi}{N} \sum_{\substack{(c,d)=1 \\ c \geq 1}} \alpha(c, d), \tag{1}$$

writing $\alpha(c, d)$ for the integral over $\beta(\sigma) = \beta(c, d)$. If $\beta(\sigma) = \emptyset$, then the corresponding $\alpha(c, d)$ is 0. On the other hand, if $\beta(\sigma) \neq \emptyset$, there exists x in $\mathbb{R}$ with $\sigma(x + \mathrm{im}^{-1}) \in \mathfrak{g}$ implying that **12**

$$\mathrm{Im}(\sigma(x + \mathrm{im}^{-1})) = m^{-1}/((cx + d)^2 + c^2/m^2) \geq \sqrt{3}/2.$$

Hence, in this case $m/c^2 = m^1/(c^2 m^{-2}) \geq m^{-1}/((cx + d)^2 + c^2/m^2) \geq \sqrt{3}/2$ i.e. $\beta(\sigma \neq \emptyset$ implies that $c = O(\sqrt{m})$. Thus in the sum over (c, d) in (1) with $(c, d) = 1$, we may restrict c to satisfy the condition $1 \leq c \ll \sqrt{m}$.

Lemma 1.1.3. *If f is a cusp form of weight k and level N and if* $(f|\sigma)(z) = \sum_{n\geq 1} a'_n e(nz/N)$ *for $\sigma \in \Gamma$, then*

$$\sum_{n>0} |a'_n||e(nz/N)| = O(\exp(-\mathscr{X}_1 \operatorname{Im} z)) \ \ \textit{for} \ \ \operatorname{Im} z \geq \mathscr{X} > 0$$

where $\mathscr{X}_1 = \pi/N$ and the O-constant depends only on $\mathscr{X}$ and on f in general.

Proof. Since $[\Gamma(1) : \Gamma(N)] < \infty$, the set $\{f|\sigma, \sigma \in \Gamma\}$ is finite, even for any modular form which is not necessarily a cusp form. Since $(f|\sigma)(i\mathscr{X}/2) = \Sigma a'_n \exp(-\pi n\mathscr{X}/N)$ is convergent, we obtain $|a'_n| \exp(-\pi n\mathscr{X}/N) = O(1)$. Hence, for any σ in $\Gamma(1)$ and $\operatorname{Im} z \geq \mathscr{X}$, we have

$$\begin{aligned}
\sum_{n\geq 1} |a'_n||e(nz/N)| &= \sum_{n\geq 1} |a'_n| \exp(-\pi n \operatorname{Im} z/N) \exp(-\pi n \operatorname{Im} z/N) \\
&< \sum_{n} |a'_n| \exp(-\pi n\mathscr{X}/N) \exp(-\pi n \operatorname{Im} z/N) \\
&\ll \sum_{n} \exp(-\pi n \operatorname{Im} z/N) \\
&= \exp(-\pi \operatorname{Im} z/N)/(1 - \exp(-\pi \operatorname{Im} z/N)) \\
&\ll \exp(-\pi z/N)/(1 - \exp(-\pi\mathscr{X}/N)).
\end{aligned}$$

The finiteness of $\{f|\sigma; \sigma \in \Gamma\}$ now completes the proof. □

13 **Lemma 1.1.4.** *If $b > a > 0$ and $r < -1/2$, then*

$$J(b, r) := \int_{-\infty}^{\infty} (x^2 + 1)^r \exp(-b/(x^2 + 1))dx = O_{a,r}(b^{r+1/2})$$

Proof. Splitting up the integral as the sum of integrals over $A = \{x \in \mathbb{R}|x^2 + 1 > 2b/a\}$ and $B = \{x \in \mathbb{R}|x^2 + 1 \leq 2b/a\}$, we have

$$J(b, r) = \int_A \ldots dx + \int_B \ldots dx = J_1 + J_2, \ \ \text{say. Now}$$

$$J_1 \leq \int_A (x^2+1)^r dx < \int_A x^{2r} dx \text{ (since } r < 0)$$

i.e.

$$\begin{aligned} J_1 &< \int_{x^2 > b/a} x^{2r} dx \ \text{ (since} b > a) \\ &= \frac{2}{2r+1} x^{2r+1} |_{\sqrt{b/a}}^{\infty} \\ &= O(b^{r+1/2}) \end{aligned}$$

with the constants in O involving a and r. □

For x in B, we use the estimate $\exp(-y) \ll y^r$ and obtain

$$J_2 \leq \int_B (x^2+1)^r (b/(x^2+1))^r = 2b^r \sqrt{2(b/a)-1} = O(b^{r+1/2})$$

which proves the lemma.

For the proof of Theorem 1.1.1, we use the well-known circle method.

Proof of Theorem 1.1.1. For given $(c, d) = 1$ with $1 \leq c \ll \sqrt{m}$, 14

$$\sum_{d_1 \in \mathbb{Z}} |\alpha(c, d+cd_1)| \ll \sum_{d_1 \in \mathbb{Z}} \int_{\beta(c,d+cd_1)} |cz+d+cd_1|^{-k} \exp(-\mathscr{X}_1/(m|cz+d+cd_1|^2))dx$$

using Lemma 1.1.3 with $\mathscr{X} = \sqrt{3}/2$ for $\sigma = \begin{pmatrix} * & * \\ c & d+cd_1 \end{pmatrix}$, $x + \mathrm{im}^{-1} c\beta(\sigma)$ and

$$f(x+\mathrm{im}^{-1}) = (c(x+\mathrm{im}^{-1}) + d + cd_1)^{-k} \sum_n a'_n e(n\sigma(x+\mathrm{im}^{-1})/N).$$

Thus

$$\sum_{d_1 \in \mathbb{Z}} |\alpha(c, d+cd_1)| \leq \sum_{d_1 \in \mathbb{Z}} \int_{d_1}^{d_1+N} ((cx+d)^2 + c^2/m^2)^{-k/2}$$

$$\exp\left(-\frac{\mathscr{X}_1}{m((cx+d)^2+c^2/m^2)}\right)dx$$
$$\leq N\int_{-\infty}^{\infty}(c^2x^2+c^2/m^2)^{-k/2}\exp\left(-\frac{\mathscr{X}_1/m}{c^2x^2+c^2/m^2}\right)dx$$
$$= Nc^{-k}m^{k-1}\int_{-\infty}^{\infty}(x^2+1)^{-k/2}\exp\left(-\frac{\mathscr{X}_1 m/c^2}{x^2+1}\right)dx$$
$$\ll c^{-k}m^{k-1}(m/c^2)^{-k/2}+1/2$$
$$\text{(by Lemma 1.4, for } k\geq 2)$$

i.e.
$$\sum_{d_1\in\mathbb{Z}}(\alpha(c,d+cd_1)|\leq c^{-1}m^{k/2-1/2}.$$

This leads us, for fixed c, to
$$|\sum_{\substack{(d,c)=1\\ c \text{ fixed}}}\alpha(c,d)|\ll(\varphi(c)/c)m^{k/2-1/2}\ll m^{k/2-1/2}$$

where φ is Euler's function. The theorem now follows, since
$$a_m\ll\sum_{1\leq c\ll\sqrt{m}}m^{k/2-1/2}\ll m^{k/2}.$$

For the proof of Theorem 1.1.2, we use a variation of the usual method of Kloosterman [14], by rendering it suitable for a generaliza-
15 tion to the case of modular forms of degree 2. First we need to fix some notation. Let m and f be as given in Theorem 1.2. For $z = x + im^{-1}$ in $\beta(\sigma) = \beta(c, d)$ with $\sigma = \left(\begin{smallmatrix} a & b\\ c & d\end{smallmatrix}\right)$ in Γ and $c \geq 1$, we have

$$\sigma(z)=\frac{az+b}{cz+d}=\frac{a}{c}-\frac{1}{c^2(z+d/c)}=\frac{a}{c}-\frac{1}{c^2(x+im^{-1}+d/c)}=\frac{a}{c}+\tau,\quad\text{say}$$

$\tau = \tau(\theta, c) = -1/\{c^2(\theta + i/m)\}$ with $\theta := x + d/c$. Now if $(f|\sigma^{-1})(w) = \sum_n a'_n e(nw/N)$ for $w \in H$, then by the definition of $\alpha(\sigma)$, we have

$$\alpha(\sigma)=\alpha(c,d)=\int_{\beta(\sigma)}(cz+d)^{-k}(f|\sigma^{-1})(\sigma(z))e(-mx)dx$$

$$
\begin{aligned}
&= c^{-k} \int\limits_{\substack{d/c \le \theta \le N + d/c \\ a/c+\tau \in \mathfrak{g}}} (\theta + i/m)^{-k} \sum_n a'_n e(n(a/c+\tau)/N) e(-m(\theta - d/c)) d\theta \\
&= c^{-k} \int\limits_{\substack{d/c \le \theta \le N + d/c \\ a/c+\tau \in \mathfrak{g}}} (\theta + i/m)^{-k} \sum_{n \ge 1} a'_n e(n\tau/N) e(-m\theta) e\left(\frac{na + mNd}{cN}\right) d\theta. \quad (2)
\end{aligned}
$$

For the proof of Theorem 1.1.2, we need to estimate $\sum\limits_{c,d} \alpha(c,d)$ afresh. But, as one may notice, in the expression (2) for $\alpha(\sigma)$, we have also the element a of σ featuring along with c and d. This calls for the following variation of the usual Kloosterman sums and estimates for the same.

For a, c in $\mathbb{Z}$ with $c \ge 1$ and for $z \in H$, let

$$
g(a,c,z) = \begin{cases} 1 & \text{if } a/c + z \in \mathfrak{g} \\ 0 & \text{otherwise.} \end{cases}
$$

Then $g(a+nc,c,z) = g(a,c,z)$ for every $n \in \mathbb{Z}$. Thus we have a finite Fourier expansion 16

$$
g(a,c,z) = {}_{t \bmod \mathrm{c}}\, b_t(c,z)\, e(ta/c). \quad (3)
$$

Lemma 1.1.5. $\sum\limits_{t \bmod \mathrm{c}} |b_t(c,z)| = O(c^{\varepsilon})$ *for every* $\varepsilon > 0$, *with an O-constant independent of z.*

Proof. Clearly $b_t(c,z) = c^{-1} \sum\limits_{\ell \bmod \mathrm{c}} g(\ell,c,z) e(-t\ell/c)$. The boundary of $\mathfrak{g}$ in H consists of the union of the translates $w \mapsto w+n$ of the arc $\{(x,y) | x^2 + y^2 = 1, -1/2 \le x \le 1/2\}$. Hence for any z in H, the intersection of the line $\{u + z | 0 \le u \le 1\}$ with $\mathfrak{g}$ has at most *two* connected components say $[a_1, b_1]$, $[a_2, b_2]$. Using the definition of $g(\ell,c,z)$ in the expansion for $b_t(c,z)$ above, we have the estimate

$$
|b_t(c,z)| \le c^{-1} \Big| \sum_{\frac{\ell}{c} \epsilon [a_1,b_1]} e(-t\ell/c) \Big| + c^{-1} \Big| \sum_{\frac{\ell}{c} \epsilon [a_2,b_2]} e(-t\ell/c) \Big|
$$

But $\ell/c \in [a_j, b_j]$ means that $0 \le u_j \le \ell \le v_j \le c$ for suitable integers u_1, v_1, u_2, v_2 with $0 \le u_1 \le v_1 \le u_2 \le v_2 \le c$. Now

$$
\Big| \sum_{\ell/c \in [a_j,b_j]} e(-t\ \ell/c) \Big| = \Big| \sum_{\ell = u_j}^{v_j} e(-t\ell/c) \Big| = \Big|\Big| \sum_{\ell=0}^{v_j - u_j} e(-t\ell/c) \Big|
$$

$$= |(e(-t(v_j - u_j + 1)/c) - 1)/(e(-t/c) - 1)|$$
$$\leq 1/(\sin \pi t/c) \text{ for } 1 \leq t < c \text{ and } j = 1, 2.$$

17 Hence, for $1 \leq t < c$, we have $|b_t(c, z)| \leq 2/(c \sin(\pi t/c))$. □

Clearly $|b_c(c, z)| \leq 1$. Combining these estimates

$$\begin{aligned}
\sum_{t \bmod c} |b_t(c, z)| &\leq 1 + \frac{2}{c} \sum_{t=1}^{c-1} 1/\sin \frac{t\pi}{c} \\
&\leq 1 + \frac{4}{c} \sum_{1 \leq t \leq c/2} \operatorname{cosec}(t\pi/c) \\
&\leq 1 + \frac{4}{c} \sum_{1 \leq t \leq c/2} 2c/(t\pi) \\
&= 1 + \frac{8}{\pi} \sum_{t=1}^{[c/2]} 1/t \\
&\leq 1 + \frac{8}{\pi} \log c \\
&= O(c^{\varepsilon}), \text{ proving the lemma.}
\end{aligned}$$

Our object now is to estimate first $\sum\limits_{\substack{(c,d)=1 \\ d \equiv d_0 (\text{mod N})}} \alpha(c, d)$ where $c \geq 1$ is fixed and the summation is over all $(c, d) = 1$ with d lying in a given residue class modulo N, say $d \equiv d_0(\text{mod N})$. Let cr = least common multiple of c and N; so that $r \geq 1$ and $r|N$. We fix, once for all, $\sigma_0 = \left(\begin{smallmatrix} \alpha & \beta \\ c & \delta \end{smallmatrix}\right)$ in Γ with some $\delta \equiv d_0(\text{mod N})$. If $X := \{x \text{ in } \mathbb{Z} \text{ modulo } cr | (x, c) = 1 \text{ and } x \equiv d_0(\text{mod N})\}$ then $\{d \in \mathbb{Z} | (c, d) = 1, d \equiv d_0(\text{mod N})\} = \bigcup\limits_{\text{x} \in \text{X}} \{\text{d} \in \mathbb{Z} | \text{d} \equiv \text{x}(\text{mod cr})\}$, as can be readily verified. Hence, for the fixed $c \geq 1$, d_0 modulo N and σ_0,

$$\begin{aligned}
\sum_{\substack{(c,d)=1 \\ d \equiv d_0 (\text{mod N})}} \alpha(c, d) &= \sum_{x \in X} \sum_{d \equiv x (\text{mod cr})} \alpha(c, d) \\
&= \sum_{x \in X} \sum_{y \bmod \text{N/r}} \sum_{d \equiv x + cry (\text{mod cN})} \alpha(c, d) \qquad (4)
\end{aligned}$$

18 **Lemma 1.1.6.** *For x in X and y, t in $\mathbb{Z}$, there exists $\sigma_x = \begin{pmatrix} a_x & b_x \\ c & x \end{pmatrix} \equiv \sigma_0 (\text{mod N})$ in Γ. Moreover, we have an element $\sigma = \begin{pmatrix} a_x - a_x^2 \text{ cry} & * \\ c & x + \text{cry} + cNt \end{pmatrix}$ in Γ, congruent to σ_0 modulo N.*

Proof. Since $x \in X$, we have $(c, x) = 1$ and $x \equiv d_0 \equiv \delta (\text{mod N})$. Hence there exists $\sigma_1 = \begin{pmatrix} a & b \\ c & x \end{pmatrix}$ in Γ. Now $\sigma_1 \sigma_0^{-1} \equiv \begin{pmatrix} a' & h \\ 0 & 1 \end{pmatrix} (\text{mod N})$ so that $a' \equiv 1 (\text{mod N})$ necessarily. Thus $\begin{pmatrix} 1 & -h \\ 0 & 1 \end{pmatrix} \sigma_1 \equiv \sigma_0 (\text{mod N})$, so that we can take $a_x = a - ch$, $b_x = b - hx$. Next, Γ clearly contains

$$\begin{pmatrix} 1 & -a_x^2 ry \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a_x & b_x \\ c & x \end{pmatrix} \begin{pmatrix} 1 & ry + tN \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a_x - a_x^2 \text{ryc} & b' \\ c & x + \text{cry} + ctN \end{pmatrix} = \sigma$$

and further $\sigma = \sigma_0 (\text{mod N})$, since $N | cr$ and

$$b' = (a_x - a_x^2 \text{ryc})(ry + tN) + b_x - x a_x^2 ry \equiv a_x ry + b_x - a_x^2 ry\, x (\text{mod N})$$

i.e.

$$b' \equiv a_x ry (1 - a_x x) + b_x \equiv b_x \text{mod N},$$

on noting that $c | (1 - a_x x)$ and $N | cr$. □

For the given cusp form f (and indeed for any modular form) of level N, we have $f | \sigma = f | \sigma_0$ since $\sigma \equiv \sigma_0 (\text{mod N})$. Let

$$(f | \sigma^{-1})(w) = (f | \sigma_0^{-1})(w) = \sum_n a'_n e(nw/N) \quad \text{for} \quad w \in H.$$

Then for any $x \in X$, we have, with the notation as in (2) and (4), 19

$$\sum_{y \bmod N/r} \sum_{d \equiv x + \text{cry} (\text{mod cN})} \alpha(c, d)$$
$$= \sum_{\substack{y \bmod \text{N}/\text{r} \\ t \in \mathbb{Z}}} \int\limits_{\substack{c^{-1} x + ry + Nt \leq \theta \leq c^{-1} x + ry + N(t+1) \\ c^{-1}(a_x - a_x^2 \text{ cry}) + \tau \in \mathfrak{g}}} \sum_n a'_n e(n\tau/N)$$
$$e(-m\theta) e\left(\frac{n(a_x - a_x^2 \text{ cry}) + mN(x + \text{cry} + cNt)}{cN} \right) d\theta$$
$$= c^{-k} \int\limits_{c^{-1} a_x + \tau \in \mathfrak{g}} (\theta + i/m)^{-k} \sum_n a'_n e(n\tau/N) e(-m\theta)$$

$$\sum_{y \bmod Nr^{-1}} e(y(-na_x^2 r/N) e\left(\frac{na_x + mNx}{cN}\right) d\theta. \tag{5}$$

We claim now that $(a_x, N/r) = 1$. for, cr is the least Common multiple of c and N and if a prime p divides N/r, then p necessarily divides c, and so p cannot divide a_x, since $\sigma_x \in \Gamma$. Hence

$$\sum_{y \bmod N/r} e(y(-na_x^2 r/N)) = \begin{cases} N/r & \text{if } N/r \text{ divides } n \\ 0 & \text{otherwise.} \end{cases}$$

The expression in (5) now reduces to

$$\frac{N}{rc^k} \int\limits_{c^{-1}a_x + \tau \varepsilon \mathfrak{g}} (\theta + i/m)^{-k} \sum_{\substack{(N/r)|n \\ n>0}} a'_n e(n\tau/N) e(-m\theta) e\left(\frac{na_x + mNx}{cN}\right) d\theta$$

$$= \frac{N}{rc^k} \int\limits_{\operatorname{Im}\tau \geq \sqrt{3}/2} (\theta + i/m)^{-k} g(a_x, c, \tau)$$

$$\sum_{\substack{(N/r)|n \\ n>0}} a'_n e(n\tau/N) e(-m\theta) e\left(\frac{na_x + mNx}{cN}\right) d\theta$$

$$= \frac{N}{rc^k} \int\limits_{\operatorname{Im}\tau \geq \sqrt{3}/2} (\theta + i/m)^{-k} \sum_{(N/r)|n} a'_n e(n\tau/N) e(-m\theta)$$

$$\sum_{t \bmod c} b_t(c, \tau) e\left(\frac{(tN + n)a_x + mNx}{cN}\right) d\theta \quad \text{(by (3))}$$

20 As a consequence, for fixed $c \geq 1$ and d_0 in $\mathbb{Z}$, we obtain, from (4),

$$\sum_{\substack{(c,d)=1 \\ d \equiv d_0 (\bmod N)}} \alpha(c, d) = \frac{N}{rc^k} \int\limits_{\operatorname{Im}\tau \geq \sqrt{3}/2} (\theta + i/m)^{-k} \sum_{\substack{n>0 \\ (N/r)|n}} a'_n e(n\tau/N) e(-m\theta)$$

$$\sum_{t \bmod c} b_t(c, \tau) \sum_{x \in X} e\left(\frac{(tN + n)a_x + mxN}{cN}\right) d\theta$$

Let us assume for a moment, that the inner most exponential sum, for every $n > 0$ divisible by N/r, has the estimate

$$\sum_{x \in X} e\left(\frac{(tN + n)a_x + mxN}{cN}\right) = O(c^{\frac{1}{2}+\varepsilon}(c, m)^{\frac{1}{2}}). \tag{6}$$

for every $\varepsilon > 0$, with an O-constant independent of t and N. Then using (6) and Lemmas 1.1.3 and 1.1.5, we may conclude form above, that

$$\left| \sum_{\substack{(c,d)=1 \\ d \equiv d_0 (\text{mod N})}} \alpha(c,d) \right| \ll c^{-k} \int\limits_{\text{Im}\, \tau \geq \sqrt{3}/2} (\theta^2 + m^{-2})^{-k/2} \exp\left(-\mathscr{X}_1 \frac{m^{-1}}{c^2(\theta^2 + m^{-2})} \right) c^{\varepsilon} c^{\frac{1}{2}+\varepsilon} (c,m)^{\frac{1}{2}} d\theta \tag{7}$$

(recalling that $\tau := -1/\{c^2(\theta + i/m)\}$. Making the change of variable $\theta \mapsto \theta/m$ on the right hand side of (7), it is

$$\ll c^{-k+1/2+2\varepsilon} (c,m)^{\frac{1}{2}} m^{k-1} \int\limits_{-\infty}^{\infty} (\theta^2 + 1)^{-k/2} \exp(-\mathscr{X}_1 m/(c^2(1+\theta^2))) d\theta$$

with $c \ll \sqrt{m}$ and now by Lemma 1.1.4, we have a majorant

$$\ll c^{-k+1/2+2\varepsilon} (c,m)^{\frac{1}{2}} m^{k-1} (m/c^2)^{-k/2+1/2} \ll c^{-\frac{1}{2}+2\varepsilon} m^{k/2-1/2} (c,m)^{\frac{1}{2}}.$$

Thus we have finally, as in the proof of Theorem 1.1.1,

$$a_m = O\left(\sum_{c \ll \sqrt{m}} \alpha(c,d) \right) \ll \sum_{1 \leq c \ll \sqrt{m}} c^{-1/2+2\varepsilon} (c,m)^{1/2} m^{k/2-1/2}$$

But now writing $(c,m) = u$, $c = uv \ll \sqrt{m}$, we have $v \ll \sqrt{m}/u$ so that **21**

$$\begin{aligned} \sum_{1 \leq c \ll \sqrt{m}} c^{-1/2+2\varepsilon} (c,m)^{1/2} &\ll \sum_{u|m} \sqrt{u} \sum_{v \ll \sqrt{m}/u} (uv)^{-1/2+2\varepsilon} \\ &= \sum_{u|m} u^{2\varepsilon} \sum_{v \ll \sqrt{m}/u} v^{-1/2+2\varepsilon} \\ &\ll \sum_{u|m} u^{2\varepsilon} (\sqrt{m}/u)^{\frac{1}{2}+2\varepsilon} \\ &= m^{1/4+\varepsilon} \sum_{u|m} 1/\sqrt{u} \end{aligned}$$

$$= m^{1/4+\varepsilon} \sum_{u|m} 1$$
$$\ll m^{1/4+2\varepsilon}$$

and hence

$$a_m = O(m^{k/2-1/4+2\varepsilon}) \tag{8}$$

proving Theorem 1.1.2, *under the assumption of the estimate* (6).

Before proceeding to the proof of (6), we make a few remarks. Namely, any estimate $\sum_{t \bmod c} |b_t(c,z)| = O(c^f)$ with $f \leq 1/2$, may be seen to imply $a_m = O(m^{k/2-1/4+f/2+\varepsilon})$ in place of (8). Clearly and $f < 1/2$ represents an improvement over Hecke's estimate. A straightforward application of Schwarz's inequality immediately yields an estimate with $f = 1/2$ but then we are in no better position than in Theorem 1.1.1.

22 Let us denote by K the exponential sum in (6). For any x in X, $(x,c) = 1$ and so let us fix an integer a with $ax \equiv 1(\text{mod c})$. Now since $a_x x \equiv 1(\text{mod c})$, we have $a_x \equiv a(\text{mod c})$, so that $a_x = a + cs$ for some s in $\mathbb{Z}$, which is unique modulo r, since $a + cs = a_x \equiv \alpha(\text{mod N})$ by Lemma 1.1.6 and $N|cr$. We observe that $N|cf$ if and only if $r|f$. Indeed, if $r|f$, $cr|cf$ and so $N|cf$; on the other hand, if $N|cf$, then $cr|cf$ since $c|cf$ and so $r|f$. Since $a_x = a + cs \equiv \alpha(\text{mod N})$, we may write K as

$$K = \sum_{x\in X} \sum_{s \bmod r} e((tN+n)(a+cs)+m\times N)/cN)\cdot\frac{1}{N}\sum_{u \bmod N} e((a+cs-\alpha)u/N)$$

Now the coefficient of s in the expression above is $(tN + n)/N = t + (n/N(/r))/r$ and hence we are justified in taking s only modulo r. Thus

$$K = N^{-1} \sum_{\substack{x\in X\\ u \bmod N}} e((tN+n)a+mxN)/cN)e((a-\alpha)u/N)\sum_{s\in\mathbb{Z}/(r)} e((tN+n+cu)s/N)$$

and the inner sum over s modulo r is r or 0 according as $N|(n+cu)$ or not, if we note that $(n+cu)/N = (n/(N+r))/r + (cr/N)u/r$ has denominator dividing r. As a result,

$$K = (r/N) \sum_{\substack{u \bmod N\\ N|(n+cu)}} e(-\alpha u/N) \sum_{x\in X} e((a((tN+n)+cu)+mxN)/cN)$$

$$= (r/N) \sum_{\substack{u \bmod N \\ N|(n+cu)}} e(-\alpha u/N) \sum_{x \in X} e\left(a\left(t + \frac{n+cu}{N}\right) + mx\right)/c) \tag{9}$$

wherein the second sum may be recognised as nearly a Kloosterman sum, since $ax \equiv 1(\text{mod c})$. 23

We remark now that there is a bijective correspondence $x \mapsto x$ between $X = \{x \in \mathbb{Z}/(cr)|(x,c) = 1,\ x \equiv \delta(\text{mod N})\}$ and $X' = \{x \in \mathbb{Z}/(c)|(x,c) = 1,\ x + cs \equiv \delta(\text{mod N})$ for some s in $\mathbb{Z}\}$. First, the map is one-one, since, for $x_1, x_2 \in X$ with $x_1 \equiv x_2(\text{mod c})$, we have $x_1 = x_2 + cf$ which, in view of $x_1 \equiv \delta \equiv x_2(\text{mod N})$, implies that $N|cf$ i.e. $r|f$ (by the arguments in the preceding paragraph) and so $x_1 \equiv x_2(\text{mod cr})$. The mapping is onto, since for any $x \in X'$, we need only remark that $x + cs$ modulo cr (for the s involved in the definition of X') maps to x in X'. Suppose now $ad \equiv 1(\text{mod c})$. Then $d + cs_1 \equiv \delta(\text{mod N})$ for some s_1 in $\mathbb{Z} \iff a + cs_2 \equiv \alpha(\text{mod N})$ for an s_2 in $\mathbb{Z}$. We prove only the implication $\Longrightarrow$ (the proof for the reverse implication being similar). For $ad \equiv 1(\text{mod c})$, there exists $\sigma^* = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in Γ and $\sigma^* \left(\begin{smallmatrix} 1 & s_1 \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} a & as_1+b \\ c & cs_1+d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} a & * \\ c & \delta \end{smallmatrix}\right)(\text{mod N})$.

Hence

$$\sigma^* \begin{pmatrix} 1 & s_1 \\ 0 & 1 \end{pmatrix} \sigma_0^{-1} \equiv \begin{pmatrix} 1 & -s_2 \\ 0 & 1 \end{pmatrix} (\text{mod N}) \text{ for some } s_2 \text{ in } \mathbb{Z}.$$

$$\text{i.e. } \begin{pmatrix} 1 & s_2 \\ 0 & 1 \end{pmatrix} \sigma^* \begin{pmatrix} 1 & s_1 \\ 0 & 1 \end{pmatrix} \equiv \sigma_0(\text{mod N}), \text{ implying that}$$

$a + cs_2 \equiv \alpha(\text{mod N})$, since $\sigma_0 = \left(\begin{smallmatrix} \alpha & \beta \\ c & \delta \end{smallmatrix}\right)$. Writing $t + (n + cu)/N$ in (9) as $\bar{u}$ and using the bijection between X and X', the inner sum over x in (9) becomes now 24

$$\sum_{x \in X} e\left(\frac{a\bar{u} + mx}{c}\right) = \sum_{\substack{a \bmod c \\ (a,c)=1, a+cs_2 \equiv \alpha(\text{mod N}) \text{ for some } s_2 \in \mathbb{Z}}} e\left(\frac{a\tilde{u} + md}{c}\right)$$

$$= \sum_{\substack{a \bmod c \\ (a,c)=1}} e\left(\frac{a\tilde{u} + md}{c}\right) \times \frac{1}{N} \sum_{s_2 \bmod r} \sum_{v \bmod N} e((a + cs_2 - \alpha)v/N),$$

by arguments as before,

$$
\begin{aligned}
&= N^{-1} \sum_{\substack{a \bmod c\\ (a,c)=1}} e\left(\frac{a\tilde{u} + md}{c}\right) \sum_{v \bmod N} e((a-\alpha)v/N) \sum_{s_2 \bmod r} e(cs_2 v/N)\\
&= rN^{-1} \sum_{\substack{v \bmod N\\ N|cv}} e(-\alpha v/N) \sum_{\substack{a \bmod c\\ (a,c)=1\\ ad\equiv 1 (\bmod c)}} e\left(\frac{a(\tilde{u} + cv/N) + md}{c}\right) \qquad (10)
\end{aligned}
$$

since the inner sum over s_2 modulo r is r or 0 according as N divides cv or not. The inner sum over a modulo c in (10) is a genuine Kloosterman sum (Note that $\tilde{u} + cv/N \in \mathbb{Z}$) and is $O(c^{1/2+\epsilon}(c,m)^{1/2})$, by Weil's well-known estimate [28]). This finally proves (6) and hence establishes Theorem 1.1.2 as well.

1.2 Reduction Theory

25 In this section, we give a quick survey of Minkowski's reduction theory for positive definite quadratic forms, as carried over to the general linear group $GL_m(\mathbb{R})$.

Let

$$G = GL_m(\mathbb{R}), A = \left\{\begin{pmatrix} a_1 & \dots & 0\\ \vdots & \ddots & \vdots\\ 0 & \dots & a_m\end{pmatrix} \in G | \text{all } a_i > 0\right\}$$

and

$$N = \left\{\begin{pmatrix} 1 & \dots & *\\ 0 & \ddots & \\ 0 & \dots & 01\end{pmatrix} \in G\right\}.$$

For any $g \in G$, the matrix ${}^t gg$ is positive definite and we have the Babylonian decomposition ${}^t gg = {}^t PP$ where $P = \begin{pmatrix} p_1 & \dots & p_{ij}\\ \vdots & \ddots & \vdots\\ 0 & \dots & p_m\end{pmatrix}$ with all $p_i > 0$ and $p_{ij} = 0$ for $i > j$. Thus if $\mathcal{O}(m)$ denotes the orthogonal group of degree m, then $gp^{-1} \in \mathcal{O}(m)$ and further $G = \mathcal{O}(m)AN$ i.e. for every g in G, $g = kan$ with $k \in \mathcal{O}(m)$, $a \in A$ and $n \in N$. This decomposition

$G = KAN$ is known as the Iwasawa decomposition and is unique, for every g in G. For given $t, u > 0$, let

$$A_t = \left\{ \begin{pmatrix} a_1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & a_m \end{pmatrix} \in A | \text{all } a_i > 0, a_i \leq t a_{i+1} \text{ for } 1 \leq i \leq m-1 \right\} \text{ and}$$

$$N_u = \left\{ \begin{pmatrix} 1 & \dots & n_{ij} \\ \vdots & \ddots & \vdots \\ 0 & \dots & 1 \end{pmatrix} \in N | \ |n_{ij}| \leq u \text{ for all } n_{ij} \right\}. \text{ Then}$$

$\mathfrak{S} = \mathfrak{S}^{(m)}_{t,u} := O(m) A_t N_u$ is a so-called Siegel domain; note that while $O(m)$ and N_u are compact, A_t is not compact. The following theorem shows that $\mathfrak{S}^{(m)}_{2/\sqrt{3},1/2}$ is almost a fundamental domain $G/GL_m(\mathbb{Z})$ for **26**
$GL_m(\mathbb{Z})$ in G;

Theorem 1.2.1. *$GL_m(\mathbb{R}) = \mathfrak{G}_{2/\sqrt{3},1/2} GL_m(\mathbb{Z})$.*

We prove first a few lemmas necessary for this theorem.

Lemma 1.2.2. *If $N_{\mathbb{Z}} := N \cap GL_m(\mathbb{Z})$, then $N = N_{1/2} \cdot N_{\mathbb{Z}}$.*

Proof. If $x = \begin{pmatrix} 1 & \dots & x_{ij} \\ \vdots & \ddots & \vdots \\ 0 & \dots & 1 \end{pmatrix} \in N$ and $y = \begin{pmatrix} 1 & \dots & y_{ij} \\ \vdots & \ddots & \vdots \\ 0 & \dots & 1 \end{pmatrix} \in N_{\mathbb{Z}}$, then $z = xy = \begin{pmatrix} 1 & \dots & z_{ij} \\ \vdots & \ddots & \vdots \\ 0 & \dots & 1 \end{pmatrix}$ with $z_{ij} = y_{ij} + \sum_{i<k<j} x_{ik} y_{kj} + x_{ij}$. In the order $(m-1, m)$, $(m-2, m-1)$, $(m-2, m), \dots, (i, i+1), \dots (i, m)$, choose $y_{ij} \in \mathbb{Z}$ such that $|z_{ij}| \leq 1/2$ for $i < j$ (Note that for $i = m-1$, $j = m$, the sum over $i < k < j$ is empty). This proves the lemma. $\square$

Let, for any column $x := {}^t(x_1, \dots, x_m)$, its norm $\sqrt{x_1^2 + \cdots + x_m^2}$ be denoted by $\|x\|$. For g in G, we now put $\varphi(g) = \|g e_1\|$ where e_1 is the unit vector ${}^t(1, 0 \dots 0)$. Using the Iwasawa decomposition $g = kan$ for g in G, we have

$$\varphi(g) = \|kane_1\| = \|ane_1\| = a_1 = \varphi(a)$$

where a_1 is the leading entry of the diagonal matrix a.

Remark. For g in G and γ in $GL_m(\mathbb{Z})$, clearly $g\gamma e_1 \in g\mathbb{Z}^m$ and $\inf\limits_{\gamma\in GL_m(\mathbb{Z})} \varphi(g\gamma) = \inf\limits_{0\neq x\in\mathbb{Z}^m} \|gx\|$ is attained at some x in $\mathbb{Z}^m$.

27 **Lemma 1.2.3.** *Let $g = kan$ be the Iwasawa decomposition of g in G and let further* $\inf\limits_{\gamma\in GL_m(\mathbb{Z})} \varphi(g\gamma) = \varphi(g)$. *Then, for the first two (diagonal) entries a_1, a_2 of a, we have $a_1/a_2 \leq 2/\sqrt{3}$.*

Proof. By lemma (1.2.2), we can find n' in $N_{\mathbb{Z}}$ such that $nn' \in N_{1/2}$. Our hypothesis tells us that $\varphi(gn'\gamma) \geq \varphi(g)$ for every γ in $GL_m(\mathbb{Z})$. But, from the form of n' and the definition of φ, we have $\varphi(g) = \varphi(gn')$. Writing $t = nn' = \begin{pmatrix} 1 & \ldots & t_{ij} \\ \vdots & \ddots & \vdots \\ 0 & \ldots & 1 \end{pmatrix}$, we have, by our choice of n', $|t_{ij}| \leq 1/2$. If $J_0 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and E_{m-2} is the $(m-2)$-rowed identity matrix, we take $\gamma_0 = \begin{pmatrix} J_0 & 0 \\ 0 & E_{m-2} \end{pmatrix}$. Then

$$gn'\gamma_0 e_1 = gn'{}^t(010\ldots0) = ka^t(t_{12}10\ldots0) = k^t(a_1t_{12}a_20\ldots0)$$

Thus $\sqrt{a_1^2t_{12}^2 + a_2^2} = \varphi(gn'\gamma_0) \geq \varphi(g) = a_1$, implying that $|t_{12}|^2 \leq 1/4$ i.e. $a_2^2 \geq a_1^2(1 - t_{12}^2) \geq (3/4)a_1^2$ and establishing our lemma. □

Theorem 1.2.1 is now seen to be immediate from

Lemma 1.2.4. *For g in G, there exists γ_0 in $GL_m(\mathbb{Z})$ such that* $\varphi(g\gamma_0) = \int\limits_{\gamma\in GL_m(\mathbb{Z})} \varphi(g\gamma)$. *Moreover $g\gamma_0 \in \mathfrak{S}_{2/\sqrt{3},1/2}$.*

Proof. For $m = 2$, we know that for some γ_1 in $GL_2(\mathbb{Z})$, we have $\varphi(g\gamma_1) = \inf\limits_{\gamma\in GL_2(\mathbb{Z})} \varphi(g\gamma)$. We can then evidently find n' in $N_{\mathbb{Z}}$ such that,
28 with $\gamma_0 = \gamma_1 n'$, we have $g\gamma_0 \in \mathfrak{S}_{2/\sqrt{3},1/2}$. Hence the Lemma is true for $m = 2$ and let us suppose that, for $m \geq 3$, the Lemma has been upheld with $m - 1$ in place of m. Now $\inf\limits_{0\neq x\in\mathbb{Z}^m} \|gx\|$ is attained at an $x' \neq 0$ in $\mathbb{Z}^m$ and such an x' is necessarily ('primitive' and hence) of the form $\gamma_1 e_1$ for some γ_1 in $GL_m(\mathbb{Z})$. Thus we have (by the Remark following Lemma 1.2.2),

$$\varphi(g\gamma_1) = \inf_{\gamma\in GL_m(\mathbb{Z})} \varphi(g\gamma). \tag{11}$$

Let $g\gamma_1 = kan$ be the Iwasawa decomposition, so that

$$k^{-1}g\gamma_1 = an = \begin{pmatrix} a_1 & * \\ 0 & g' \end{pmatrix} \quad \text{with} \quad g' \text{ in } GL_{m-1}(\mathbb{R}).$$

By the induction hypothesis, there exists γ_0' in $GL_{m-1}(\mathbb{Z})$ such that $g'\gamma_0'$ is in $\mathfrak{S}^{(m-1)}_{2/\sqrt{3},1/2}$. Consider the Iwasawa decomposition $g'\gamma_0' = k'a'n'$ with $a' = \begin{pmatrix} a_2 & & 0 \\ & \vdots & \\ 0 & & a_m \end{pmatrix}$. Then we have

$$g_1 := k^{-1}g\gamma_1 \begin{pmatrix} 1 & 0 \\ 0 & \gamma_0' \end{pmatrix} = \begin{pmatrix} a_1 & * \\ 0 & k'a'n' \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & k' \end{pmatrix} \begin{pmatrix} a_1 & & 0 \\ & \vdots & \\ 0 & & a_m \end{pmatrix} \begin{pmatrix} 1 & \cdot & * \\ \cdot & \cdot & \cdot \\ 0 & \cdot & 1 \end{pmatrix}$$

Now

$$\begin{aligned} &\varphi(g_1) = \varphi(k^{-1}g\gamma_1 \begin{pmatrix} 1 & 0 \\ 0 & \gamma_0' \end{pmatrix} = \varphi\left(g\gamma_1 \begin{pmatrix} 1 & 0 \\ 0 & \gamma_0' \end{pmatrix}\right) = \\ &\|g\gamma_1 \begin{pmatrix} 1 & 0 \\ 0 & \gamma_0' \end{pmatrix} e_1\| = \|g\gamma_1 e_1\| = \varphi(g\gamma_1) = \inf_\gamma \varphi(g\gamma) \text{ by (11)}, \\ &= \inf_\gamma \varphi(k^{-1}g\gamma) = \inf_\gamma \varphi\left(k^{-1}g\gamma_1 \begin{pmatrix} 1 & 0 \\ 0 & \gamma_0' \end{pmatrix}\gamma\right) = \inf_\gamma \varphi(g_1\gamma) \end{aligned}$$

since $\gamma_1 \left(\begin{smallmatrix} 1 & 0 \\ 0 & \gamma_0' \end{smallmatrix}\right)\gamma$ runs over $GL_m(\mathbb{Z})$ along with γ. Lemma 1.2.3 now applies to g_1 and so we have $a_1/a_2 \le 2/\sqrt{3}$. Already, by induction, we know that $a_i/a_{i+1} \le 2/\sqrt{3}$ for $2 \le i \le m$. Now for some

$$n_1 \in N_{\mathbb{Z}}, g_1 n_1 = k^{-1}g\gamma_1 \begin{pmatrix} 1 & 0 \\ 0 & \gamma_0' \end{pmatrix} n_1 \text{ is in } \mathfrak{S}^{(m)}_{2/\sqrt{3},1/2}$$

in view of Lemma 1.2.2 and so Lemma 1.2.4 is proved. $\square$ **29**

Corollary. *For g in $GL_m(\mathbb{R})$,* $\inf_{0 \neq x \in \mathbb{Z}^m} \|gx\| \le (2/\sqrt{3})^{(m-1)/2}(abs(\det g))^{1/m}$

Proof. In view of Theorem 1.2.1, we may assume that g is in a Siegel domain $\mathfrak{S}^{(m)}_{2/\sqrt{3},1/2} = O(m)A_{2/\sqrt{3}}N_{1/2}$ since both $\inf\limits_{0\neq x} \|gx\|$ and $abs(\det g)$ depend only on the coset $gGL_m(\mathbb{Z})$. Let then $g = kan$ with

$$k \in O(m), a = \begin{pmatrix} a_1 & \cdot & 0 \\ . & \vdots & . \\ 0 & \cdot & a_n \end{pmatrix} \in A_{2/\sqrt{3}} \text{ and } n \in N_{1/2}.$$

Clearly $a_1/a_i = \prod_{1\leq j\leq i-1}(a_j/a_{j+1}) \leq (2/\sqrt{3})^{i-1}$ and so $a_1^m = \prod\limits_{1\leq j\leq m} (a_1/a_j)\times \det a \leq \prod\limits_{1\leq j\leq m}(2/\sqrt{3})^{j-1} \det a = (2/\sqrt{3})^{m(m-1)/2} abs(\det g)$. This gives us

$$\varphi(g) = a_1 \leq (2/\sqrt{3})^{(m-1)/2}(abs \det g)^{1/m} \tag{12}$$

As we know, $\inf\limits_{0\neq x\in\mathbb{Z}^m} \|gx\|$ is attained at a primitive vector x' in $\mathbb{Z}^m$ and
30 such an x' is of the form $\gamma' e_1$ with some γ' in $GL_m(\mathbb{Z})$. Thus

$$\inf_{0\neq x\in\mathbb{Z}^m} \|gx\| = \inf_{\gamma\in GL_m(\mathbb{Z})} \|g\gamma e_1\| = \inf_{\gamma} \varphi(g\gamma) \leq \varphi(g)$$

which proves the Corollary, in view of (12). ◻

Definition. *For P in the space $\mathscr{P}_m$ of real m-rowed symmetric positive definite matrices, the minimum* $\min(P_: = \inf\limits_{0\neq x\in\mathbb{Z}^m} P[x]$.

If we define in the space $\mathscr{P}_m$, the domain $S_{t,u}$ corresponding to the Siegel domain $\mathfrak{S}_{t,u}$, by $S_{t,u} = \{a[n] | a \in A_t, n \in N_u\}$, then $S_{t^2,u}$ is just the image of $\mathfrak{S}_{t,u}$ under the mapping $g \mapsto {}^t gg$ from GL_m onto $\mathfrak{P}_m$. Theorem 1.2.1 and its corollary give us immediately.

Theorem 1.2.5. $\mathscr{P}_m = \bigcup\limits_{\gamma\in GL_m(\mathbb{Z})} S_{4/3,1/2}[\gamma]$ *and* $\mu_m := \sup\limits_{p\in\mathscr{P}_m} \dfrac{\min(P)}{(\det P)^{1/m}} \leq (4/3)^{\frac{m-1}{2}}$.

Proof. Writing P in $\mathscr{P}_m$ as ${}^t gg$ with g in $GL_m(\mathbb{R})$, we know from Theorem 1.2.1 that, for some $g\gamma$ in $GL_m(\mathbb{Z})$, $r = kan \in \mathfrak{S}_{2/\sqrt{3},1/2}$. Then

$P[\gamma] = a^2[n]$ which is clearly in $S_{4/3,1/2}$, proving the first assertion of the theorem. Now

$$\min(P) = \inf_{0\neq x\in\mathbb{Z}^m} p[x] = \inf_{0\neq x\in\mathbb{Z}^m} \|gx\|^2 \leq (4/3)^{(m-1)/2}(\det g)^{2/m}$$

by the Corollary. Hence $\min(p) \leq (4/3)^{(m-1)/2}(\det P)^{1/m}$ giving the required upper bound for μ_m. $\square$

Remark. The constant μ_m known as Hermite's constant is known explicitly for all $m \leq 8$ (e.g. $\mu_2 = 2/\sqrt{3}$, being also the best possible value). It is related to constants in the packing of spheres and also to the first eigenvalue of the Laplacian on some spaces.

For two positive definite matrices P_1, P_2 we use the notation $P_1 \asymp$ **31**
P_2 to indicate the existence of constants c_1, c_2 for which $P_1 - c_1P_2 > 0$ and $c_2P_2 - c_2P_1 > 0$, i.e. to say that P_1 and P_2 are of the same order of magnitude.

Theorem 1.2.6. *For $t, u > 0$ and any $P(= (p_{ij})) = a[n]$ in $S_{t,u}$, we have* $P \asymp a \asymp \begin{pmatrix} p_{11} & \cdot & 0 \\ \cdot & \cdot & \cdot \\ 0 & \cdot & p_{mm} \end{pmatrix}$.

Proof. Writing $a = \begin{pmatrix} a_1 & \cdot & 0 \\ \cdot & \cdot & \cdot \\ 0 & \cdot & a_m \end{pmatrix}$, $n = \begin{pmatrix} 1 & \cdot & n_{ij} \\ \cdot & \cdot & \cdot \\ 0 & \cdot & 1 \end{pmatrix}$ and $x = \begin{pmatrix} x_1 \\ \cdot \\ x_m \end{pmatrix} \neq 0$, we have for $y := nx = \begin{pmatrix} y_1 \\ \cdot \\ y_m \end{pmatrix}$.

$$\frac{a_i y_1^2}{a[x]} = \frac{a_i}{a[x]}\left(x_i + \sum_{k>i} n_{ik}x_k\right)^2 \leq \left[\frac{\sqrt{a_i}|x_i|}{\sqrt{a[x]}} + \sum_{k>i}\frac{\sqrt{a_i}|x_k||n_{ik}|}{\sqrt{a[x]}}\right]^2.$$

Now $a[x] \geq a_i|x_i|^2$ gives $(\sqrt{a_i}|x_i|/\sqrt{a[x]}) \leq 1$ while, for $k > i$,

$$\sqrt{a_i}|x_k| = \sqrt{\frac{a_i}{a_k}}\sqrt{a_k|x_k|^2} \leq \sqrt{\frac{a_i}{a_k}}\sqrt{a[x]} \leq t^{(k-i)/2}\sqrt{a[x]}.$$

Hence $\dfrac{a_i y_i^2}{a[x]} \leq \left(1 + \sum_{k>i} t^{(k-i)/2}u\right)^2 \ll 1$ where $\ll$ involves constants depending on t and u. We see therefore that $a[nx] = a[y] \ll a[x]$ for

every x i.e. $P \leq c_1 a$. On the other hand, $n \in N_u$ implies at once $n^{-1} \in N_u$, for some $u' > 0$ depending on u(and m). Hence $a[n^{-1}] \in S_{t,u'}$. By the arguments above, we have $a[n^{-1}] \leq c_2^{-1} a$ i.e. $P \geq c_2 a$, so that $P \asymp a$. Taking $x = e_i$, the unit vector with 1 at the i^{th} place and 0 elsewhere, 32
we have now $c_2 a_i = c_2 a[e_i] \leq P[e_i] = p_{ii} \leq c_1 a[e_i] = c_1 a_i$ so that $P_{ii} \asymp a_i$ for every i. In other words, $a \asymp \begin{pmatrix} p_{11} & \cdot & 0 \\ \cdot & \cdot & \cdot \\ 0 & \cdot & p_{mm} \end{pmatrix}$ and the theorem is proved. $\square$

The following theorem shows that any Siegel domain $S_{t,u}$ in $\mathscr{P}_m$ intersects at most finitely many $S_{t,u}[\gamma]$ for $\gamma \in GL_m(\mathbb{Z})$ and so a "fundamental domain" F for $GL_m(\mathbb{Z})$ in $\mathscr{P}_m$ can have at most finitely many "neighbours" $F[\gamma]$.

Theorem 1.2.7. *For any $d \geq 1$ and given $S = S_{t,u} \subset \mathscr{P}_m$, the number of X in $\mathscr{M}_m(\mathbb{Z})$ with $1 \leq abs(\det X) \leq d$ and $S[X] \cap S \neq \emptyset$ is finite.*

Proof. We use induction on m, for the proof. Let first $X = \begin{pmatrix} X_1 & X_{12} \\ 0 & X_2 \end{pmatrix}$ with $X_i \in \mathscr{M}_{m_i}(\mathbb{Z})$, $i = 1, 2$, $1 \leq m_1, m_2$ and $m_1 + n_2 = m$. Then writing $\|M\|$ for $abs(\det M)$, $\|X\| = \|X_1\| \, \|X_2\| \leq d$ implies that $1 \leq \|X_i\| \leq d$ for $i = 1, 2$. Take $a[n]$ in S with $(a[n])[X] = a'[n'] \in S$. Using the obvious decompositions

$$a = \begin{pmatrix} a_1^{(m_1)} & 0 \\ 0 & a_2^{(m_2)} \end{pmatrix}, n = \begin{pmatrix} n_1^{(m_1)} & n_{12} \\ 0 & n_2^{(m_2)} \end{pmatrix}, a' = \begin{pmatrix} a'_1 & 0 \\ 0 & a'_2 \end{pmatrix}, n' = \begin{pmatrix} n'_1 & n'_{12} \\ 0 & n'_2 \end{pmatrix}$$

we have

$$a[n] = \begin{pmatrix} a_1[n_1] & 0 \\ 0 & a_2[n_2] \end{pmatrix} \left[\begin{pmatrix} E & n_1^{-1} n_{12} \\ 0 & E \end{pmatrix} \right],$$
$$a'[n'] = \begin{pmatrix} a_1[n'_1] & 0 \\ a & a'_2[n'_2] \end{pmatrix} \left[\begin{pmatrix} E & n'^{-1} n'_{12} \\ 0 & E \end{pmatrix} \right]$$

33 where E now stands for the identity matrix of the appropriate size. Then, for X in the form given above, we see that

$$a[nX] = \begin{pmatrix} a_1[n_1 X_1] & 0 \\ 0 & a_2[n_2 X_2] \end{pmatrix} \left[\begin{pmatrix} E & X^{-1} X_{12} + X_1^{-1} n_1^{-1} n_{12} X_2 \\ 0 & E \end{pmatrix} \right]$$

By definition, $a_i, a'_i \in A_t^{(m_i)}$ and $n_i, n'_i \in N_u^{(m_i)}$ for $i = 1, 2$.

Now

$$\begin{aligned} a'_1[n'_1] &= a_1[n_1X_1], \\ n'^{-1}_1 n'_{12} &= X_1^{-1}X_{12} + X_1^{-1}n_1^{-1}n_{12}X_2, \\ a_2[n'_2] &= (a_2[n_2])[X_2]. \end{aligned}$$

Since m_1 and m_2 are both less than m, the induction hypothesis yields the finiteness of the number of such X_1 and X_2 and hence their boundedness as well. Further, $X_{12} = X_1 n'^{-1}_1 n'_{12} - n_1^{-1} n_{12} X_2$ wherein n_{12}, n'_{12} are bounded by virtue of n, n' being in N_u and moreover the inverses of the bounded unipotent matrices n_1, n'_1 are again (unipotent and) bounded. Thus the integral matrix X_{12} is bounded and the number of such X_{12} is finite. Consequently, we have shown that the number of integral $X = \begin{pmatrix} X_1 & X_{12} \\ 0 & X_2 \end{pmatrix}$ with $1 \leq \|X\| \leq d$ and $S[X] \cap S \neq \emptyset$ is finite. Let us now take the case of $X = (x_{ij})$ not necessarily in any such simple form (for some m_1, m_2) but with $S[X] \cap S \neq \emptyset$ and $1 \leq \|X\| \leq d$. In fact, for $1 \leq i \leq m - 1$, there exist then integers h_i, k_i with $x_{k_i,h_i} \neq 0$ and $h_i \leq i < k_i$. Denote the column ${}^t(x_{1i} \ldots x_{mi})$ of X by $x^{(i)}$, for $1 \leq i \leq m$. Let, as before, $p = a[n] \in S$ with $(p'_{ij}) = p' = (a[n])[X] = a'[n] \in S$. From Theorem 1.2.6, we have (for fixed $S_{t,u}$),

$$a'_i \asymp p'_{ii} = a[n][x^{(i)}] \asymp a[x^{(i)}] = \sum_j a_j x_{ji}^2.$$

Hence 34

$$a'_i \gg a'_{h_i} \asymp \sum_j a_j x_{j,h_i}^2 \geq a_{k_i} x_{k_i,h_i}^2 \geq a_{k_i} \quad \text{since} \quad x_{k_i,h_i} \neq 0.$$

$$\text{i.e.} \quad a'_i \gg a_i \quad (\text{some } k_i > i). \tag{13}$$

Writing $\|X\| = d_1$, we have $d_1 X^{-1} \in \mathscr{M}_m(\mathbb{Z})$. Some $P \in S_{t,u}$ implies that $\lambda p \in S_{t,u}$ for $\lambda > 0$, we have $p'[d_1X^{-1}] = d_1^2 P$ belongs to $S_{t,u}$ along with P'. Moreover, the integral matrix d_1X^{-1} is not in any simple (block) form as above, since, otherwise, X itself would then take such a simple (block) form. Applying now to P', $P'[d_1X^{-1}]$ in $S_{t,u}$ the same arguments as we used to derive (13), we find that $d_1^2 a_i \gg a'_i$. But since

$d_1 \le d$, we may conclude that $a_i \asymp a'_i$. Further $a_{i+1} \ll a_{k_i}$ (since $k_i > i$) and $a_{k_i} \ll a'_i$, as we have noted prior to deriving (13).

Hence $a_{i+1} \ll a_{k_i} \ll a'_i \asymp a_i \ll a_{i+1}$ i.e. $a_i \asymp a_{i+1}$ for every i. □

In other words, we have the chain of orders of magnitude:

$$\begin{array}{ccccc} a_1 & \asymp & a_2 & \asymp \ldots \asymp & a_m \\ )(& &)(& &)(\\ a'_1 & \asymp & a'_2 & \asymp \ldots \asymp & a'_m \end{array}$$

But then $\sum_i a'_j x_{ji}^2 \ll \sum_i a_j x_{ji}^2 \asymp (a[n])[x^{(i)}] = a'_i \asymp a'_j$ yields immediately that $x_{ji} \ll 1$ for all i and j and the theorem as well.

1.3 Minkowski Reduced Domain

35

For any $P = (p_{ij})$ in $\mathscr{P}_m$, we can introduce in $\mathbb{Z}^m$ an inner product (,) by defining $(x, y) = {}^t xPy$ whenever x, y are in $\mathbb{Z}^m$ and give it the structure of a quadratic module over $\mathbb{Z}$. If $e_i = {}^t(0, \ldots, 0, 1, 0, \ldots, 0)$ is the standard unit vector with 1 at the i^{th} place (and 0 elsewhere), then $\{e_1, \ldots, e_m\}$ is a natural basis for this quadratic module, with $(e_i, e_j) = p_{ij}$. We define, however, a new basis $\{f_1, \ldots, f_m\}$ as follows. Since P is positive-definite, the number of integral vectors with $(x, x) \le \mu$ for any given μ, is necessarily finite. Hence we can find f_1 in $\mathbb{Z}^m$ to satisfy the condition $(f_1, f_1) = \inf_{0 \ne x \in \mathbb{Z}^m} (x, x)$; of course, f_1 is not unique (since one can take, for example, $-f_1$ instead of f_1). Assuming that $f_1, \ldots, f_i$ have been chosen already, we can proceed to find f_{i+1} in $\mathbb{Z}^m$ meeting the requirements: $f_1, \ldots, f_{i+1}$ can be extended to a basis of $\mathbb{Z}^m$ and moreover, $(f_{i+1}, f_{i+1}) = \inf_x (x, x)$ where the infimum is taken over all x in $\mathbb{Z}^m$ for which $f_1, \ldots, f_i, x$ can be extended to a basis of $\mathbb{Z}^m$. By picking $-f_{i+1}$ instead of f_{i+1}, if necessary, we impose the additional restriction that $f_{i,i+1} \ge 0$; still, f_{i+1} is not unique but certainly exists. In this manner, we can find a $\mathbb{Z}$-basis $\{f_1, \ldots, f_m\}$ for the above quadratic module. Writing $f_i = \sum_{1 \le j \le m} u_{ji} e_j$ with u_{ji} in $\mathbb{Z}$ (for $1 \le i \le m$), we find that $U := (u_{ij})$ is in $GL_m(\mathbb{Z})$; further, if $q_{ij} := (f_i, f_j)$, then $Q := (q_{ij}) = {}^t UPU$ is in the same 'class' as the given P in $\mathscr{P}_m$, besides being *"Minkowski-reduced"*

in the following sense. Indeed, for any $x = {}^t(x_1, \ldots, x_m)$ in $\mathbb{Z}^m$ with the last $m-k+1$ elements $x_k, x_{k+1}, \ldots, x_m$ having 1 as greatest common divisor, the matrix $\begin{pmatrix} E_{k-1} & x \\ 0 & \end{pmatrix}$ is easily seen to be "primitive" i.e. capable of 36
being completed to an element of $GL_m(\mathbb{Z})$. Thus $f_1, \ldots, f_{k-1}, \sum\limits_{1\leq i\leq m} x_i f_i$ can be completed to a $\mathbb{Z}$-basis of $\mathbb{Z}^m$. Therefore, by our definition of f_k, we have

$$Q[x] = \left\{\sum_{1\leq i\leq m} x_i f_i, \sum_{1\leq i\leq m} x_i f_i\right\} \geq (f_k, f_k) = q_{kk}(1\underline{\leq}k\underline{\leq}m)$$

Thus the matrix Q in the same class as P satisfies the "reduction conditions":

(1) $Q[x] \geq q_{kk}(1 \leq k \leq m)$, for every $x = {}^t(x_1, \ldots, x_m)$ with the g.c.d. $(x_k, x_{k+1}, \ldots, x_m)$ equal to 1 and

(2) $q_{k,k+1} \geq 0$.

Definition. *Any positive definite matrix in $\mathscr{P}_m$ satisfying the "reduction conditions"* (1) - (2) *above is called Minkowski-reduced (or merely M-reduced).*

Let us first note that $q_{11} = \min(Q) = \inf\limits_{0\neq x\in\mathbb{Z}^m} Q[x]$. For any M-reduced Q, taking x in (1) to be e_ℓ with $\ell\underline{\geq}k$, we see that

$$q_{k,k} \leq q_{\ell,\ell}(k \leq \ell) \tag{14}$$

If, on the other hand, we take x in (1) to be $e_k \pm e_\ell$ for $\ell \neq k$, then condition (1) reads

$$q_{k,k} \pm 2q_{k\ell} + q_{\ell\,\ell} \geq q_{k,k}$$

i.e. 37

$$|q_{k\ell}| \leq 1/2 \cdot q_{\ell\,\ell} \quad \text{for} \quad k \neq \ell. \tag{15}$$

Let $\mathscr{R}_m = \mathscr{R}$ denote the set of all M-reduced matrices in $\mathscr{P}_m$. We have just shown that in every $GL_m(\mathbb{Z})$-orbit $\{P[U] | U \in GL_m(\mathbb{Z})\}$ in $\mathscr{P}_m$, there exists an element Q in $\mathscr{R}$. We may then state the following theorem presenting the reduction theory due to Minkowski and Siegel for positive-definite matrices.

Theorem 1.3.1. (i) $\mathscr{P}_m = \bigcup_{U \in GL_m(\mathbb{Z})} \mathscr{R}[U]$;

(ii) *$\mathscr{R}$ is contained in a Siegel domain $S_{t,u}$ for some t, u (depending only on m) and*

(iii) *For any $U \neq \pm E_m$ in $GL_m(\mathbb{Z})$, $\mathscr{R} \cap \mathscr{R}[U]$ is contained in the boundary of $\mathscr{R}$ (relative to $\mathscr{P}_m$).*

Actually, $\mathscr{R}$ is a fundamental domain for $GL_m(\mathbb{Z})$ in $\mathscr{P}_m$ for the action $p \mapsto P[U]$ with P in $\mathscr{P}_m$ and U in $GL_m(\mathbb{Z})$. It is a convex cone with vertex at 0 and its boundary is contained in a finite union of hyperplanes. Moreover, $\mathscr{R}$ has only finitely many neighbours (i.e. $\mathscr{R} \cap \mathscr{R}[U] \neq \emptyset$, only for finitely many U in $GL_m(\mathbb{Z})$). For all this, a detailed treatment may be found, for example, in Maass ([17], § 9).

Only the assertions (ii) and (iii) in Theorem 1.3.1. are to be proved and we need some lemmas for that purpose.

38 **Lemma 1.3.2.** *For any $R = (r_{ij})$ in $\mathscr{R}$, $r_{11} \dots r_{mm} \underset{m}{\ll} \det R$.*

Proof. The leading (ℓ, ℓ) principal minor $R_\ell = R[\begin{smallmatrix} E_\ell \\ 0 \end{smallmatrix}]$ in R is also M-reduced (in $\mathscr{P}_\ell$) for $1 \leq \ell \leq m$. Let us assume the lemma proved with $m-1$ in place of m; then writing r_j for $r_{jj} (1 \leq j \leq m)$, we have

$$r_1 r_2 \dots r_{m-1} \ll \det R_{m-1} \tag{16}$$

where the constant in $\ll$ depends only on $m-1$. Defining $\rho_{k\ell}$ by $(\rho_{k\ell}) = (\det R_{m-1}) R_{m-1}^{-1}$, we have on using the inequalities (14) corresponding to R_{m-1}, $|\rho_{k\ell}| r_\ell \ll r_1 r_2 \dots r_{m-1}$ and hence

$$|\rho_{k\ell}|/(\det R_{m-1}) \ll (r_1 r_2 \dots r_{m-1})/(r_\ell \det R_{m-1})$$

i.e.

$$|\rho_{k\ell}|/(\det R_{m-1}) \ll 1/r_\ell. \tag{17}$$

If, now, we write

$$R = \begin{pmatrix} R_{m-1} & r \\ t_r & r_m \end{pmatrix} = \begin{pmatrix} R_{m-1} & 0 \\ t_0 & s \end{pmatrix} \left[\begin{pmatrix} E_{m-1} & R_{m-1}^{-1} r \\ t_0 & t \end{pmatrix} \right] \tag{18}$$

with $s := r_m - R_{m-1}^{-1}[r]$, we have, on applying (14), (15) and (17),

$$R_{m-1}^{-1}[r] \ll \sum_{1 \le i,j \le m-1} (1/r_i) r_i r_j \ll r_{m-1}.$$

Thus

$$r_m = s + R_{m-1}^{-1}[r] \ll s + r_{m-1}. \tag{19}$$

Since $\det R = (\det R_{m-1}) \cdot s$ from (18), we obtain from (16) and (19) that **39**
$r_1 r_2 \dots r_m \ll (\det R_{m-1}) \cdot r_m \ll ((\det R)/s) \cdot r_m \ll (1 + r_{m-1}/s) \cdot \det R$. Once we establish that

$$r_{m-1} \ll s \tag{20}$$

the lemma will follow. In order to prove (20), let us assume that for some integer $k \le m-1$,

$$r_{\ell+1} < 4(m-1)^2 r_\ell \quad (\text{for } \ell = m-2, m-3, \dots, k+1, k \text{ but } \underline{\text{not}}\ k-1). \tag{21}$$

Here (21) is to be properly interpreted whenever k equals $m-1$ or 1. Writing z for ${}^t(x_1, \dots, x_{m-1})$, (18) gives, for $x = {}^t(x_1, \dots, x_m)$,

$$R[x] = R_{m-1}[x + x_m R_{m-1}^{-1} r] + s x_m^2. \tag{22}$$

Let $c = (2m-2)^{m-1}$ and let $x_i + a_i x_m (1 \le i \le m-1)$ denote the entries of the column $z + x_m R_{m-1}^{-1} r$. Now, given an integer x'_m in the closed interval $[0, c^{m-k}]$, we can certainly find integers $x'_k, x'_{k+1}, \dots, x'_{m-1}$ to satisfy $0 \le x'_i + a_i x'_m < 1$, for $k \le i \le m-1$. Dividing the closed interval $[0,1]$ into c closed subintervals of equal length, we can get a decomposition of the $(m-k)$-dimensional unit cube (in $\mathbb{R}^{m-k}$) into c^{m-k} cubes of equal volume. By Dirichlet's pigeonhole principle, at least two of the $1 + c^{m-k}$ vectors, say, $(x'_k + a_k x'_m, \dots, x'_{m-1} + a_{m-1} x'_m)$, $(x''_k + a_k x''_m, \dots, x''_{m-1} + a_{m-1} x''_m)$ must be contained in one of these c^{m-k} cubes; in other words, $|x'_i - x''_i + a_i(x'_m - x''_m)| \le 1/c$ for $k \le i \le m-1$. Hence there exist integers $x_k, x_{k+1}, \dots, x_m$, which we may indeed even assume to have greatest common divisor 1, such that **40**

$$|x_i + a_i x_m| \le 1/c, 0 < x_m \le c^{m-k} (k \le i \le m-1).$$

Trivially, there exist integers $x_1, \ldots, x_{k-1}$ satisfying the conditions

$$|x_i + a_i x_m| < 1 (i = 1, 2, \ldots, k-1).$$

For the corresponding column $x = {}^t(x_1, \ldots, x_m)$, we have $R[x] \geq r_k$, since R is M-reduced. But then (22) gives

$$\begin{aligned} r_k (\leq R[x]) \leq (k-1)^2 r_{k-1} + (k-1)(m-k) r_{k-1}/c \\ + (m-k)^2 (4(m-1)^2)^{m-k-1} r_k / c^2 + c^{2(m-k)} s \end{aligned}$$

if we use the inequalities

$$\begin{aligned} &|r_{ij}| \leq r_{k-1} (1 \leq i, j \leq k-1), |r_{pq}| \leq \frac{1}{2} r_{k-1} (p \leq k-1 < q-1) \\ &|r_{uv}| \leq (4(m-1)^2)^{m-k-1} r_k (k+1 \leq u, v \leq m-1) \end{aligned}$$

(the last one arising from (21)). Again $r_k \geq 4(m-1)^2 r_{k-1}$, by (21) and therefore finally

$$r_k \leq \frac{1}{4} r_k + \frac{1}{4} r_k + \frac{1}{4} r_k + c^{2(m-k)} s = \frac{3}{4} r_k + c^{2(m-k)} s \quad \text{i.e.} \quad r_k \ll s.$$

Since $r_{m-1} \leq (4(m-1)^2)^{m-k-1} r_k$, (20) is immediate and so is our lemma. □

Remark. The (reverse) inequality

$$\det R \leq r_1 \ldots r_m \tag{23}$$

for any R in $\mathscr{P}_m$ follows at once from the relation $\det R = (\det R_{m-1}) s$ implied by (18), the obvious inequality $s \leq r_m$ and the inequality, corresponding to (23), for R_{m-1} viz. $\det R_{m-1} \leq r_1 \ldots r_{m-1}$ from an inductive hypothesis.

41 For any $R = (r_{ij})$ in $\mathscr{P}_m$, we denote by R_0, the diagonal matrix with (the same) diagonal elements $r_{11}, r_{22}, \ldots, r_{mm}$ (as R).

Lemma 1.3.3. *For any R in $\mathscr{R}$, we have $c_1 R_0 < R < c_2 R_0$ with constants c_1, c_2 depending only on m.*

Proof. Let $R_0^{1/2}$ denote the positive square root $[\sqrt{r}_{11}, \ldots, \sqrt{r}_{mm}]$ of the diagonal matrix $R_0 = [r_{11}, \ldots, r_{mm}]$. For the eigenvalues $\rho_1, \ldots, \rho_m$ of $R[R_0^{-1/2}]$, we have $\rho_1 + \cdots + \rho_m = \text{trace}\ (R[R_0^{-1/2}]) = \text{trace}\ (RR_0^{-1}) = m$. While $\rho_1 \ldots \rho_m = \det R / \det R_0 \geq c'$ for some constant $c' = c'(m)$, by the preceding lemma. Hence $c_1 := m^{-(m-1)}c' < \rho_i < c_2 := m$, for $1 \leq i \leq m$ which means that $c_1 E_m < R[R_0^{-1/2}] < c_2 E_m$ i.e. $c_1 R_0 < R < c_2 R_0$, on transforming both sides of the inequalities by $R_0^{1/2}$. ◻

The Iwasawa decomposition $g = $ kan for g in GL_m implies at once that every $R (= {}^t gg)$ in $\mathscr{P}_m$ has the (unique) Jacobi decomposition $R = D[B]$ where $D = [d_1, \ldots, d_m]$ is diagonal with positive diagonal entries d_i and $B = (b_{ij})$ is upper triangular with $b_{ii} = 1$ for all i. The entries $d_1, \ldots, d_m$ and $b_{ij} (i < j)$ are called the *Jacobi coordinates* of $R = (r_{ij})$ in $\mathscr{P}_m$. Denoting r_{ii} by r_i as before, the relation $R = D[B]$ gives $r_i = d_i + \sum\limits_{1 \leq j \leq i-1} d_j b_{ji}^2$ for $1 \leq i \leq m$ (so that $r_i \geq d_i$ always) and further $\det R = d_1 \ldots d_m$. (Thus $\det R \leq r_1 \ldots r_m$, giving another proof for (23)).

Suppose now that R is M-reduced. Then $\prod\limits_{j=1}^{m} (r_j/d_j) = (r_1 \ldots r_m)/ \det R \leq c'' = c''(m)$, by Lemma 1.3.2. On the other hand, for any $R = D[B]$ in $\mathscr{P}_m$, we have $1 \leq (r_i/d_i) \leq \prod\limits_{j=1}^{m} (r_j/d_j)$. Hence for R in $\mathscr{R}$, $1 \leq r_i/d_i \leq c''$ and so $(1 \leq) r_i/d_i \ll r_j/d_j$ for all i, j. Consequently for R in $\mathscr{R}$, we 42
conclude, in view of (14), that

$$0 < \frac{d_j}{d_i} \ll \frac{r_j}{r_i} (\leq 1) \quad \text{for} \quad j \leq i.$$

Now, to prove that all b_{ij} are bounded (in absolute value) by a constant depending only on m, we use induction on m. In fact, let us assume that for $1 \leq p < i$ and $\ell > p$, we have $|b_{p\ell}| \leq c_1$. Then from the relation

$$r_{ij} = d_i b_{ij} + \sum_{1 \leq p \leq i-1} d_P b_{pi} b_{pj} (i < j).$$

we obtain that

$$d_i |b_{ij}| \leq |r_{ij}| + \sum_p d_p |b_{pi}| |b_{pj}|$$

$$\leq \frac{1}{2} r_i + \sum_P d_p c_1^2$$

(in view of (15) and the bound for $|b_{p\ell}|$)

$$\text{i.e.} \qquad |b_{ij}| \leq \frac{1}{2}(r_i/d_i) + \sum_{1\leq p\leq i} c_1^2 d_p/d_i \ll 1 \quad (\text{for } i < j).$$

We have thus proved assertion (ii) of Theorem 1.3.1. Along with Theorem 1.2.7, this gives us the important.

Corollary . *If R and $R[U]$ are both in $\mathscr{R}$ for some U in $GL_m(\mathbb{Z})$, the number of such U is finite.*

Before we proceed to prove assertion (iii) of Theorem 1.3.1, we make a few remarks about the interior $\mathscr{R}^0$ and the boundary $\partial(\mathscr{R})$ of $\mathscr{R}$. Among the "reduction conditions" (1) and (2), some are trivial; for example, if $x = \pm e_k$, then $R[x] = r_k$ for *every* R in $\mathscr{P}_m$. We therefore omit those inequalities which impose no condition on $\mathscr{R}$. Then $\mathscr{R}^0$
43 consists of points of $\mathscr{R}$ for which the "nontrivial" reduction conditions among (1) and (2) hold good with strict inequality. Hence $\partial(\mathscr{R})$ consists precisely of those points of $\mathscr{R}$ at which even one of these nontrivial reduction conditions holds with an equality (in place of $\geq$).

Let now both R_1 and $R_2 = R_1[U]$ for some U in $GL_m(\mathbb{Z})$ belong to $\mathscr{R}$. In view of the Corollary above, the matrix U belongs to a finite set of matrices (in $GL_m(\mathbb{Z})$) depending only on m. First let us suppose $U = (u_1 u_2 \ldots u_m)$ with columns $u_1, \ldots, u_m$ be no diagonal matrix, so that we have a first column, say u_k, which is different from $\pm e_k$. Then the column v_k of $U^{-1} = (v_1 \ldots v_m)$ is again $\neq \pm e_k$. Since $U = \begin{pmatrix} W & \\ 0 & u_k \ldots u_m \end{pmatrix}$ with a diagonal $(k-1, k-1)$ matrix W having ± 1 as its diagonal entries, we find, on expanding $\det U (= \pm 1)$ along the k^{th} column, that the last $m - k + 1$ elements of u_k have necessarily 1 as the greatest common divisor. From the reduction conditions (1) for $R_1 = \left(r_{ij}^{(1)}\right)$, we have $R_1[u_k] \geq r_{kk}^{(1)}$ i.e. if $R_2 = \left(r_{ij}^{(2)}\right)$, then $r_{kk}^{(2)} \geq r_{kk}^{(1)}$. Similarly, from $R_1 = R_2[U^{-1}]$, it follows that $r_{kk}^{(1)} \geq r_{kk}^{(2)}$. Thus we have

$$R_1[u_k] = r_{kk}^{(1)} = r_{kk}^{(2)} = R_2[v_k]$$

and so R_1, R_2 belong to the boundary $\partial(\mathscr{R})$ with u_k, v_k belonging to a finite set of possible columns. We consider next the case when U is a diagonal matrix with ± 1 as diagonal entries but $U \neq \pm E_m$. Suppose the first change of sign among the diagonal entries occurs, as we pass from the k^{th} diagonal entry to the next one (on the diagonal). Then $r^{(2)}_{k,k+1} = {}^t u_k R_1 u_{k+1} = -r^{(1)}_{k,k+1}$. By (2), $r^{(1)}_{k,k+1}$ and $r^{(2)}_{k,k+1}$ are non-negative and so necessarily, $r^{(1)}_{k,k+1} = 0 = r^{(2)}_{k,k+1}$.

It follows again that both R_1 and R_2 are on the boundary of $\mathscr{R}$ (We **44**
have also proved incidentally that the points of $\mathscr{P}_m \cap \partial(\mathscr{R})$ lie on a finite set of hyperplanes. We remark, without proof that $\mathscr{R}^0 \neq \emptyset$). All the assertions in Theorem 1.3.1 have now been established.

Example. In the special case when $m = 2$, $P = \left(\begin{smallmatrix} a & b \\ b & c \end{smallmatrix}\right)$ is M-reduced, if and only if $0 \leq b \leq a/2 \leq c/2$ and $a > 0$. These conditions imply that $ac \leq (4/3)\det P$. The reduced domain $\mathscr{R}$ is contained in $S_{4/3,1/2}$ and $\mu_2 = 4/3$.

1.4 Estimation for Fourier Coefficients of Modular Forms of Degree n

Let $\mathscr{G}_n$ denote the Siegel half-space of degree n, consisting of all (n,n) **45**
complex symmetric matrices $Z = X + iY$ with $\mathrm{Im}(Z) = Y := \dfrac{1}{2i}(Z - \overline{Z}) > 0$. The modular group $\Gamma_n = \mathrm{Sp}(2n, \mathbb{Z}) = \left\{M = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \mathscr{M}_{2n}(\mathbb{Z}) | M\ J^t_n M = J_n = \left(\begin{smallmatrix} 0 & E_n \\ E_n & 0 \end{smallmatrix}\right)\right\}$ acts on $\mathscr{G}_n$ as a discontinuous group of holomorphic automorphisms $Z \mapsto M < Z >:= (AZ + B)(CZ + D)^{-1}$ of $\mathscr{G}_n$, where A, B, C, D are (n,n) matrices constituting M in Γ; observe that $M\{Z\} := CZ + D$ is invertible. Also note that whenever $M = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$ is in Γ, ${}^t M$ is also in Γ and further $M^{-1} = \left(\begin{smallmatrix} {}^t D & {}^t B \\ {}^t C & {}^t A \end{smallmatrix}\right)$; $M = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$ is in Γ if and only if $A^t D - B^t C = E_n$, $A^t B = B^t A$ and $C^t D = D^t C$. The subgroup of $M = \left(\begin{smallmatrix} A & B \\ O & D \end{smallmatrix}\right) \in \Gamma$ with A, $D = {}^t A^{-1}$ in $GL_n(\mathbb{Z})$ and symmetric integral $S = A^{-1}B$ is denoted by $\Gamma_{n,\infty}$; if $M = \left(\begin{smallmatrix} & * \\ C & D \end{smallmatrix}\right)$ and $N = \left(\begin{smallmatrix} & * \\ C & D \end{smallmatrix}\right)$ are both in Γ, then $M = \left(\begin{smallmatrix} E_n & S \\ 0 & E_n \end{smallmatrix}\right) N \Gamma_{n,\infty} N$. For $Z \in \mathscr{G}_n$ and $M = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$ in Γ, $\mathrm{Im}(M < Z >) = {}^t(C\overline{Z} + D)^{-1}\,\mathrm{Im}(Z)(CZ + D)^{-1} > 0$.

A fundamental domain $\Gamma\backslash\mathscr{G}_n$ for the discontinuous action of Γ on $\mathscr{G}_n$ is given by

$$\mathfrak{g}_n := \left\{ Z \in \_n \,\middle|\, \begin{array}{ll} (1) & \text{Abs}\det(CZ+D) \geq 1 \text{ for every primitive} \\ & \ \text{integral } (CD) \text{ with } C^tD = D^tC \\ (2) & \text{Im}(Z) \text{ is } M\text{-reduced} \\ (3) & \text{The elements of } X := \frac{1}{2}(Z+\overline{Z}) \\ & \text{are} \leq 1/2 \text{ in absolute value.} \end{array} \right.$$

Introducing

$$\mathfrak{g}_n = \bigcup_{M\in\Gamma_{n,\infty}} M < \mathcal{F}_n >= \bigcup_{\substack{U\in GL_n(\mathbb{Z})\\ S={}^tS\in\mathscr{M}_n(\mathbb{Z})}} (\mathcal{F}_n[U]+S), \quad \text{we remark}$$

$$Z \in \mathfrak{g}_n \Longrightarrow \min(\text{Im(Z)}) \geq \sqrt{3}.2. \tag{24}$$

46 Indeed, $\min(\text{Im}(Z[U]+S)) = \min(\text{Im}(Z[U])) = \min(\text{Im}(Z))$ for every U in $GL_n(\mathbb{Z})$ and $S = {}^tS$ in $\mathscr{M}_n(\mathbb{Z})$. We may therefore assume, without loss of generality, that Z is already in $\mathfrak{F}_n$. Taking $M = \left(\begin{smallmatrix} A & B \\ C & D\end{smallmatrix}\right)$ in Γ_n

$$\text{with } A = \begin{pmatrix} 0 & 0 \\ {}^t0 & E_{n-1}\end{pmatrix}, \qquad B = \begin{pmatrix} -1 & 0 \\ t_0 & 0\end{pmatrix}$$
$$C = \begin{pmatrix} 1 & 0 \\ t_0 & 0\end{pmatrix} \text{ and } \qquad D = \begin{pmatrix} 0 & 0 \\ t_0 & E_{n-1}\end{pmatrix}, \text{ and}$$

inequality $\text{abs}(\det(CZ+D)) > 1$ for $Z = (z_{pq}) = (x_{pq}+iy_{pq})$, gives $|z_{11}| \geq 1$, $|x_{11}| \leq 1/2$ and so $y_{11} \geq \sqrt{3}/2$. Since Im(Z) is reduced, $\min(\text{Im}\, Z) = y_{11} \geq \sqrt{3}/2$. Conversely, it can be shown that a constant $\mathscr{X}_n$ exists such that $Z \in \mathfrak{g}_n$ whenever $\min(\text{Im(Z)}) > \mathscr{X}_n$. Let us fix a natural number q and a number k with $2k$ integral once for all; q will serve as the "level" and k as the "weight" of the modular forms to be considered in the sequel. Let $\Gamma_n(q)$ denote the principal congruence subgroup of level q in Γ_n, consisting of all M in Γ_n with $M \equiv E_{2n}(\text{mod q})$.

Definition. *For any $f : \mathscr{G}_n \mapsto \mathbb{C}$ and $M \in \Gamma_n$, we define $f|_kM = f|M$ by $(f|M)(Z) = f(M < Z >)\det(CZ+D)^{-k}$, with a fixed determination of the branch.*

For $M_1, M_2 \in \Gamma_n$, we have $f|M_iM_2 = \pm(f|M_1)|M_2$.

Definition. *By a Siegel modular form of degree n, weight k and level q, we mean a holomorphic function* $f : \mathscr{G}_n \to \mathbb{C}$ *such that* $f|M = u(M)f$ for *every* M *in* $\Gamma_n(q)$ *with a constant* $u(M)$ *of absolute value* 1 *and which, for* $n = 1$, *satisfies the condition* $f|M$ *is bounded in* $\mathscr{F}_1$ *for every* M *in* Γ_1.

It is known (see [16]) that for every M in Γ_n, $f|M$ has the Fourier expansion 47

$$\sum_{0\leq T\in\Lambda_n^*} a_M(T)e(\mathrm{tr}(TZ)/q).$$

Example. are given by the theta series $\sum\limits_{G^{(m,n)}} e(\pi i\,\mathrm{tr}(S[G]Z))$ for even integral $S^{(m)} > 0$ and the Eisenstein series of $\Gamma_n(q)$.

Definition. *A Siegel modular form of degree n, weight k and level q is said to vanish at every cusp, if for every M in* Γ_n, *the constant term* $a_M(0)$ in *the Fourier expansion of* $f|M$ *is zero. (Note that this definition is independent of the choice of the branch* $\det(CZ + D)^{-k}$*).*

Definition. *A Siegel modular form of degree n, weight k and level q is called a cusp form, if for every M in* Γ_n, *the Fourier coefficients* $a_M(T)$ *of* $f|M$ *corresponding to all* T *in* Γ_n^* *with* $\det T = 0$ *vanish.*

(This definition coincides for $n = 1$ with the preceding definition. For $n > 1$, however, a modular form vanishing at every cusp, is not a cusp form in general).

One of our main objective is to estimate the Fourier coefficients $a(T)$ of a Siegel modular form of degree n, weight k and level q, vanishing at every cusp. Replacing $f(Z)$ by $f(qZ)$ (of level q^2), if necessary, we *assume* that the Fourier expansion of f is given by $f(Z) = \sum\limits_{0\leq P\in\Lambda_n^*} a(P)e(\mathrm{tr}(PZ))$, *in the sequel*. Now, for given $T > 0$, we know that $T_1 = T[U]$ is M-reduced for some U in $GL_m(\mathbb{Z})$. But, if $f(Z) = \sum\limits_P a(P)e(\mathrm{tr}(PZ))$, then

$$(\det U)^{-k} f(Z[{}^tU]) = (\det U)^{-k} \sum_P a(P)e(\mathrm{tr}(P[U]Z)$$

$$= (\det U)^{-k} \sum_{P} a(P[U^{-1}])e(\mathrm{tr}(PZ)).$$

Denoting $(\det U)^{-k}a(P[U^{-1}])$ by $b(P)$, we see that $a(T)(\det U)^{-k}$ occurs as the Fourier coefficient, corresponding to the M-reduced matrix T_1,
48 for $f|\left(\begin{smallmatrix} U & 0 \\ 0 & {}^tU^{-1} \end{smallmatrix}\right)$. Since f is of level q and since $(GL_m(\mathbb{Z}) : GL_m(\mathbb{Z}; q)) < \infty$, we have only finitely many distinct functions of this form, as U varies over $GL_m(\mathbb{Z})$. *We shall therefore assume in the sequel that*, for the estimation of the Fourier coefficient $a(T)$, T is *M-reduced* and *further* $\min(T) \gg 0$ (i.e. $\min(T)$ is large enough).

The following lemma is essential for later applications.

Lemma 1.4.1. *If the series* $\sum_{0 \le P = {}^tP \in \mathscr{M}_n(\mathbb{Z})} a(P)e(\mathrm{tr}(PZ))$ *converges absolutely for every Z in $\mathscr{G}_n$ and if $a(P) = 0$ for all p with* $\mathrm{rank}(P) < \ell(\le n)$, *then for $\gamma = \mathrm{Im}(Z)$ in $S_{t,u}$ with* $\min(Y) \ge \varepsilon > 0$, *we have*

$$\mathscr{S}(Z) := \sum_{P} |a(P)||e(\mathrm{tr}(PZ)| = O_{\varepsilon}(\exp(-\mathscr{X}\ \mathrm{tr}(Y_\ell))$$

where $\mathscr{X}$ is a positive constant and Y_ℓ is the leading (ℓ, ℓ) minor of Y.

Proof. Since Y is in $S_{t,u}$, we see exactly as in Lemma 1.3.3, that $Y \asymp Y_0 = \begin{pmatrix} y_{11} & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & y_{nn} \end{pmatrix}$ and since $\min(Y) \ge \varepsilon$, we also have $Y \ge \varepsilon' E_n$ for some $\varepsilon' > 0$ depending on ε, t and u. The given series converges absolutely for $Z = i(\varepsilon'/2)E_n$ and hence $a(P)\exp(-\pi\varepsilon'\ \mathrm{tr}(P)) = O(1)$. Thus

$$\begin{aligned}\mathscr{S}(Z) &= \sum_{P} |a(P)| \exp(-\pi\,\mathrm{tr}(PY)) \\ &\le \sum |a(P)| \exp(-\pi\varepsilon'\ \mathrm{tr}(P)) \exp(-\pi\,\mathrm{tr}(PY)) \\ &\ll \sum_{\substack{P={}^tP \ge 0 \\ \mathrm{rank}\, P \ge \ell}} \exp(-\pi\,\mathrm{tr}(PY)) = \mathscr{T}, \quad \text{say.}\end{aligned}$$

Since $Y \asymp Y_0$ and $tr(Y_\ell) = y_{11} + \cdots + y_{\ell\ell}$, we may assume that $Y = Y_0$,
49 without loss of generality. For any h with $\ell \le h \le n$, we set

$$\alpha_0(h) = \sum_{\substack{0 \le p = {}^tp \in \mathscr{M}_n(\mathbb{Z}) \\ \mathrm{rank}(P) = h}} \exp(-\pi\,\mathrm{tr}(PY))$$

so that $\mathscr{T} = \sum_{\ell \leq h \leq n} \alpha_0(h)$. In order to prove the lemma, it suffices clearly to show that

$$\alpha_0(h) = O(\exp(-\mathscr{X}\ \mathrm{tr}(Y_\ell)) \quad \text{for a constant} \quad \mathscr{X} > 0. \tag{25}$$

□

Since $P \geq 0$ and $\mathrm{rank}(P) = h$, there exists U in $GL_n(\mathbb{Z})$ such that $P = \begin{pmatrix} P_1 & 0 \\ 0 & 0 \end{pmatrix}[U]$ for an integral $P_1^{(h)} > 0$. Suppose now that for U_1, U_2 in $GL_n(\mathbb{Z})$ and $P_2^{(h)} > 0$, we have $\begin{pmatrix} P_1 & 0 \\ 0 & 0 \end{pmatrix}[U_1] = \begin{bmatrix} P_2^{(h)} & 0 \\ 0 & 0 \end{bmatrix}[U_2]$. Then $\begin{bmatrix} P_1 & 0 \\ 0 & 0 \end{bmatrix}[U_1 U_2^{-1}] = \begin{bmatrix} P_2 & 0 \\ 0 & 0 \end{bmatrix}$ implying that $U_1 U_2^{-1} = \begin{bmatrix} W_1 & 0 \\ W_3 & W_4 \end{bmatrix}$ with W_1 in $GL_h(\mathbb{Z})$, W_4 in $GL_{n-h}(\mathbb{Z})$, $W_3 \in \mathscr{M}_{h,h-h}(\mathbb{Z})$ and $P_1[W_1] = P_2$. Since the number of W_1 in $GL_n(\mathbb{Z})$ with $P_1[W_1] = P_1$ is at least 2 (e.g. $P_1[\pm E_h] = P_1$), we have the inequality

$$\alpha_0(h) < \sum_{P_1} \sum_{U \in GL_n^{(h)}(\mathbb{Z}) \backslash GL_n(\mathbb{Z})} \exp\left(-\pi\, \mathrm{tr} \begin{pmatrix} P_1 & 0 \\ 0 & 0 \end{pmatrix} [U] Y\right) \tag{26}$$

where now P_1 runs over M-reduced integral matrices in $\mathscr{P}_h$ (representing the various $GL_h(\mathbb{Z})$-orbits of positive-definite integral matrices in $\mathscr{P}_h$) and U runs over a complete set of representatives of right cosets of

$$GL_n^{(h)}(\mathbb{Z}) := \left\{ \begin{pmatrix} E_h & 0 \\ * & * \end{pmatrix} \in GL_n(\mathbb{Z}) \right\} \quad \text{in} \quad GL_n(\mathbb{Z}).$$

Any such U can be written as $U = \begin{pmatrix} {}^tF \\ * \end{pmatrix}$ with primitive $F^{(n,h)}$ in $\mathscr{M}_{n,h}(\mathbb{Z})$. **50**

Further, $\mathrm{tr}\left(\begin{pmatrix} p_1 & 0 \\ 0 & 0 \end{pmatrix}[U]Y\right) = \mathrm{tr}(P_1 Y[P])$. Thus (26) becomes

$$\alpha_0(h) < \sum_{P_1 \in \mathscr{R}_h \cap \mathscr{M}_h} \sum_{(\mathbb{Z}) F^{(n,h)} \text{ primitive}} \exp(-\pi\, \mathrm{tr}(P_1 Y[F])). \tag{27}$$

From the reduction conditions, the number of M-reduced integral P_1 with given diagonal elements $p_1, p_2, \ldots, p_h$ is seen to be $\ll p_1^{h-1} p_2^{h-2} \ldots p_{h-1}$ (Actually, it is not hard to verify that the number of ($GL_h(\mathbb{Z})$-equivalence) classes $\{P_1\}$ of integral symmetric matrices P_1 with det

$P_1 \leq d$ is $\ll d^{(h-1)/2+\varepsilon}$ for any $\varepsilon > 0$. We, however, do not need to use this fact). From (27), we are led to the simple estimate

$$\alpha_0(h) \ll \sum_{p_1,\ldots,p_h \in \mathbb{N}} \sum_{F^{(n,h)}_{\text{primitive}}} \sum_{(p_1 p_2 \ldots p_h)^{h-1}} \exp\left(-\mathscr{X}' \operatorname{tr}\left(\begin{pmatrix} p_1 & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & p_h \end{pmatrix} Y[F]\right)\right) \tag{28}$$

with a constant $\mathscr{X}' = \mathscr{X}'(h) > 0$. Writing $P^* = \begin{pmatrix} p_1 & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & p_h \end{pmatrix}$ and $F = (f_1 \ldots f_h)$, we have $P^* \geq E_h$, $\operatorname{tr}(P^* Y[F]) \geq \operatorname{tr}(Y[F])$ and $\operatorname{tr}(P^* Y[F]) \geq \varepsilon' \operatorname{tr}(P^* E_h[F]) = \varepsilon' \sum_{1 \leq i \leq h} p_i {}^t f_i f_i \geq \varepsilon' \operatorname{tr}(P^*)$ since ${}^t f_i f_i \geq 1 (1 \leq i \leq h)$ in view of F being primitive. Thus

$$\exp(-\mathscr{X}' \operatorname{tr}(P^* Y[F])) \leq \exp(-\frac{1}{2}\mathscr{X}' \operatorname{tr}(Y^*[F])) \exp(-\frac{1}{2}\mathscr{X}' \varepsilon' \operatorname{tr}(P^*)).$$

Now since

$$\sum_{p_1,\ldots,p_h \in \mathbb{N}} (p_1 p_2 \ldots p_h)^{h-1} \exp(-\frac{1}{2}\mathscr{X}' \varepsilon' \operatorname{tr}(p_1 + \cdots + p_h)) < \infty,$$

we obtain from (28) that

$$\alpha_0(h) \ll \sum_{F^{(n,h)}_{\text{primitive}}} \exp(-\frac{1}{2}\mathscr{X}' \operatorname{tr}(Y[F])) \tag{29}$$

51 If, for $1 \leq i_1 < i_2 < \ldots < i_p \leq n$, the non-zero rows of any F in (29) have indices $i_1, \ldots, i_p$, then $p \geq h$ and $i_p \geq h$.

Hence

$$\operatorname{tr}(Y[F]) = \sum_{\substack{1 \leq i \leq h \\ 1 \leq k \leq n}} f_{ki} y_k f_{ki} \geq \sum_{1 \leq r \leq p} y_{i_r} \left(\sum_{1 \leq j = \leq h} f^2_{i_r, j}\right) \geq \sum_{1 \leq r \leq p} y_r$$
$$\geq \operatorname{tr}(Y_h) \geq \operatorname{tr}(Y_\ell)$$

and further

$$\operatorname{tr}(Y[F]) \geq \varepsilon' \operatorname{tr}({}^t F F) = \varepsilon' \sum_{\substack{1 \leq i \leq n \\ 1 \leq j \leq h}} f^2_{ij}.$$

It is now immediate that (for some $\mathscr{X} > 0$)

$$\begin{aligned}\exp(-\frac{1}{2}\mathscr{X}' \operatorname{tr}(Y[F] &= \exp(-\frac{1}{4}\mathscr{X}' \operatorname{tr}(Y[F])\exp(-\frac{1}{4}\mathscr{X}' \operatorname{tr}(Y[F])) \\ &\leq \exp(-\mathscr{X} \operatorname{tr}(Y_\ell))\exp\left(-\mathscr{X}\varepsilon' \sum_{\substack{1\leq i\leq n\\ 1\leq j\leq h}} f_{ij}^2\right)\end{aligned}$$

and as a result,

$$\begin{aligned}\alpha_0(h) &\ll \exp(-\mathscr{X} \operatorname{tr}(Y_\ell))\left(\sum_{g\in\mathbb{Z}}\exp(-\varepsilon'\mathscr{X} g^2)\right)^{hn} \\ &\ll \exp(-\mathscr{X} \operatorname{tr}(Y_\ell))\end{aligned}$$

proving (25) and the lemma.

Let

$$\mathfrak{t} = \mathfrak{t}_n(q) := \{X = (x_{ij}) \in \mathscr{M}_n(\mathbb{R}) | X = {}^tX, 0 \leq x_{ij} < q\}$$

and, for any given M in Γ_n and M-reduced $T \to 0$ in Λ_n^* with $\min T \gg 0$ (as we have assumed prior to the statement of Lemma 1.4.1),

$$\tilde{\beta}(M) := \{X \in \mathfrak{t} | M < X + iT^{-1} > \varepsilon\mathfrak{g}_n\}$$

so that $\tilde{\beta}(M) = \tilde{\beta}(NM)$ for every N in $\Gamma_{n,\infty}$. Let $M_1 = E_{2n}$, $M_2, \ldots,$ **52**
$M_r, \ldots$ be a complete set of representatives of the right cosets of $\Gamma_{n,\infty}$ in Γ_n. Now since $T = (t_{ij})$ is M-reduced, $T \asymp \begin{pmatrix} t_{11} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & t_{nn}\end{pmatrix}$ and so the assumption $\min T \gg 0$ yields that $t_{ii} \gg 0$ for every $i \geq 1$. Thus t_{ii}^{-1} is sufficiently small; for $T^{-1} \asymp \begin{pmatrix} t_{11}^{-1} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & t_{11}^{-1}\end{pmatrix}$, $\min(T^{-1})$ is also sufficiently small.

Hence if $\tilde{\beta}(E_{2n}) \neq \emptyset$, then $X + iT^{-1} \in \mathfrak{g}_n$ for some X and as a consequence, $\min(T^{-1}) \geq \sqrt{3}/2$, which gives a contradiction. For all but finitely many i, $\tilde{\beta}(M_i) = \emptyset$. Defining $\beta(M_2) = \tilde{\beta}(M_2)$ and $\beta(M_i) = \tilde{\beta}(M_i) \cap \{\tilde{\beta}(M_2) \cup \ldots \cup \tilde{\beta}(M_{i-1})\}^c$ inductively for $i \geq 3$, where $\{\quad\}^c$ denotes set complementation, the following lemma is immediate.

Lemma 1.4.2. $\mathfrak{t} = \coprod_{i\geq 2} \beta(M_i)$

For $n = 2$, the measure of the intersection of two distinct $\tilde{\beta}(M_i)$'s is 0 (and presumably this is true for $n = 3$ as well).

For $M = \left(\begin{smallmatrix} * & * \\ C & D \end{smallmatrix}\right) \in \Gamma_n$ and a modular form f of degree n, weight k and level q and T as above, let

$$\alpha(C, D) = \alpha(M) = \alpha(\Gamma_{n,\infty} M) = \int\limits_{\beta(M)} f(X + iT^{-1}) e(-\operatorname{tr}(TX)) dX$$

53 where $dX := \prod_{1\leq i\leq j\leq n} dx_{ij}$ denotes the volume element in $\mathfrak{t}$. Then if

$$\begin{aligned} f(Z) &= \sum_{0\leq T\in\Lambda_n^*} a(T) e(\operatorname{tr}(TZ)), \\ a(T) &= q^{-n(n+1)/2} e^{2\pi n} \int\limits_{\mathfrak{t}} f(X + iT^{-1}) e(-\operatorname{tr}(TX)) dX \\ &= q^{-n(n+1)/2} e^{2\pi n} \sum_{i\geq 2} \alpha(M_i), \quad \text{by Lemma 1.4.2.} \\ &= O\left(\sum_{i\geq 2} \alpha(M_i)\right). \end{aligned} \tag{30}$$

Lemma 1.4.3. *For f as above vanishing at all cusps and $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Gamma_n$ with $M < Z > \in \mathfrak{g}_n$,*

$$f(Z) = \operatorname{abs}(\det(CZ + D)^{-k}) O(\exp(-\mathscr{X} \min(\operatorname{Im}(M < Z >)),$$

for a constant $\mathscr{X}$.

Proof. (a) Since $[\Gamma_n : \Gamma_n(q)] < \infty$ and further $f|M_1M_2 = (f|M_1)|M_2$ along with $f|M = v(M)f$, for all M in $\Gamma_n(q)$, where $|v(M)| = 1$, the number of functions $\operatorname{abs}(f|N)$ for N in Γ_n is finite.

(b) If $N = \left(\begin{smallmatrix} * & * \\ C' & D' \end{smallmatrix}\right) \in \Gamma_n$, then $|f| = |f|(N^{-1}N)| = (\operatorname{abs}\det(C'Z + D'))^{-k}|(f|N^{-1})(N < Z >)|$.

(c) If Z is in the fundamental domain $\mathcal{F}_n$ for Γ_n in $\mathscr{G}_n$, $Y = (y_{ij}) :=$ $\mathrm{Im}(Z)$ is M-reduced and hence belongs to $S_{t,u}$ for some t, u depending only on n, by Theorem 1.3.1 (ii). We also know from (24) that $\min Y \geq \sqrt{3}/2$. Since f vanishes at all cusps,

$$(f|N)(Z) = \sum_{\substack{0 \leq p \in \Lambda_n^* \\ \mathrm{rank}\, P \geq 1}} a(p; N) e(\mathrm{tr}(PZ)/q)$$

for every N in Γ_n. Applying Lemma 1.4.1. we have then, for every N in Γ_n, $|(f|N)(Z)| = O(\exp(-\mathscr{X} y_{11})) = O(\exp(-\mathscr{X}$ $\min(\mathrm{Im}(Z))))$. 54

(d) Let $M < Z > \in \mathfrak{g}_n$; then there exist U in $GL_n(\mathbb{Z})$ and integral symmetric S such that ${}^tUM < Z > U + S \in \mathscr{F}_n$. For $N = \begin{pmatrix} {}^tU & SU^{-1} \\ 0 & U^{-1} \end{pmatrix} M$, we have $\min(\mathrm{Im}\, N < Z >) = \min(\mathrm{Im}(M < Z >)) \geq$ $\sqrt{3}2$ and further $N < Z >$ is M-reduced. From b), c) and a), it is immediate that

$$\begin{aligned} |f(Z)| &= \mathrm{abs}(\det(CZ + D)^{-k})|(f|N^{-1})(N < Z >)| \\ &= \mathrm{abs}(\det(CZ + D)^{-k}) O(\exp(-\mathscr{X} \min(\mathrm{Im}(M < Z >))). \end{aligned}$$

Lemma 1.4.3 implies at once

□

Lemma 1.4.4. *For f, T and M as above,*

$$|\alpha(M)| \ll \int_{\beta(M)} \mathrm{abs}(\det(C(X + iT^{-1}) + D))^{-k}$$
$$\exp(-\mathscr{X} \min(\mathrm{Im}(M < X + iT^{-1} >)))dX.$$

Definition. *A pair of (n, n) matrices C, D is called a symmetric pair if $C^tD = D^tC$ and is said to be* coprime*, if, whenever GC and GD are both integral, G is necessarily integral.*

If $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Gamma_n$, then (CD) is a coprime symmetric pair. Conversely, it is not hard to prove that given any coprime symmetric pair C, D of (n, n) integral matrices, there exists $M = \begin{pmatrix} * \\ CD \end{pmatrix}$ in Γ_n.

Definition. *Two coprime symmetric pairs C, D and C_1, D_1 are called* associated *if there exists U in $GL_n(\mathbb{Z})$ such that $(CD) = U(C_1D_1)$.* 55

Let $\{C, D\}$ denote the equivalence class of all (n-rowed) coprime symmetric pairs associated with a given pair C, D. We wish to determine a special representative in each class $\{C, D\}$, where $r = \operatorname{rank} C$. If $r = 0$, then $C = 0$; then D is necessarily in $GL_n(\mathbb{Z})$ and we choose O, E as a representative. Let then $0 < r \leq n$. There exist U_1, U_2 in $GL_n(\mathbb{Z})$, such that

$$U_1C = \begin{pmatrix} C_1 & 0 \\ 0 & 0 \end{pmatrix} {}^tU_2 \text{ where } C_1 = C_1^{(r,r)} \text{ with } \det C_1 \neq 0.$$

If we write analogously

$$U_1D = \begin{pmatrix} D_1 & D_2 \\ D_3 & D_4 \end{pmatrix} U_2^{-1} \text{ with } D_1 = D_1^{(r,r)},$$

then $C^tD = D^tC$ implies U_1C, U_1D is symmetric and so

$$\begin{pmatrix} C_1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} {}^tD_1 & {}^tD_3 \\ {}^tD_2 & {}^tD_4 \end{pmatrix} = \begin{pmatrix} D_1 & D_2 \\ D_3 & D_4 \end{pmatrix}\begin{pmatrix} {}^tC_1 & 0 \\ 0 & 0 \end{pmatrix}$$

Thus $C_1{}^tD_1 = D_1{}^tC_1$ and $D_3 = 0$, so that C_1, D_1 is symmetric.

Since $\left(\begin{smallmatrix} C_1 & D_1 & D_2 \\ 0 & 0 & D_4 \end{smallmatrix}\right)$ is primitive, $D_4 \in GL_{n-r}(\mathbb{Z})$ and further (C_1D_1) is primitive. Thus the symmetric pair C_1, D_1 is also coprime.

If Q_1, Q_2 are primitive (n, r) matrices (i.e. capable of being completed to elements of $GL_n(\mathbb{Z})$), we say Q_1, Q_2 are *associated*, whenever
56 $Q_1 = Q_2U_3$ for some $U_3 \in GL_r(\mathbb{Z})$. We denote the class of matrices associated with Q_1 by $\{Q_1\}$. Hence replacing $U_2 = (Q^*)$ by $U_2\left(\begin{smallmatrix} U_3 & 0 \\ 0 & E_{n-r} \end{smallmatrix}\right)$ with $U_3 \in GL_r(\mathbb{Z})$, we can ensure that the primitive matrix $Q^{(n,r)}$ is a chosen representative in its class. Under $U_2 \mapsto U_2\left(\begin{smallmatrix} U_3 & 0 \\ 0 & E_{n-r} \end{smallmatrix}\right)$ with $U_3 \in GL_r(\mathbb{Z})$, the form of U_1C, U_1D is unchanged, except for the replacement of C_1, D_1, Q by $C_1{}^tU_3$, $D_1U_3^{-1}$, QU_3 respectively. Replacing now U_1 by $\left(\begin{smallmatrix} U_4 & 0 \\ 0 & E_{n-r} \end{smallmatrix}\right)U_1$ with U_4 in $GL_r(\mathbb{Z})$, we can replace C_1, D_1 by any representative in its class $\{C_1, D_1\}$. Let us fix, for $1 \leq r \leq n$, from the classes of r-rowed coprime symmetric pairs a complete set of representatives as well as a complete system of representatives F from the

classes $\{F\}$ of primitive (n, r) matrices and to each F, let us assign a matrix $U = (F*)$ in $GL(n, \mathbb{Z})$, once for all. Thus we have established already a part of

Lemma 1.4.5. *Let $F = F^{(n,r)}$ run over a complete set of representatives of the classes $\{F\}$ of primitive matrices and C_1, D_1 over a complete set of representatives of classes $\{C_1, D_1\}$ with C_1, D_1 coprime and* $\det C_1 \neq 0$. *To each such F, let $U = (F*) \in GL_n(\mathbb{Z})$ be assigned once for all. Then the pairs*

$$C = \begin{pmatrix} C_1 & 0 \\ 0 & 0 \end{pmatrix} {}^tU, D = \begin{pmatrix} D_1 & 0 \\ 0 & E_{n-r} \end{pmatrix} U^{-1}$$

form a complete set of representatives of the classes $\{C, D\}$ with C, D coprime symmetric and $\operatorname{rank} C = r$.

Proof. What remains to be proved is only that the different pairs C, D 57
obtained in this manner belong to different classes. If possible, let

$$C^* = \begin{pmatrix} C_1^* & 0 \\ 0 & 0 \end{pmatrix} {}^tU^*, D^* = \begin{pmatrix} D_1^* & 0 \\ 0 & E_{n-r} \end{pmatrix} U^{*-1}$$

satisfy $C^* = U_1 C$, $D^* = U_1 D$ for some U_1 in $GL_n(\mathbb{Z})$. From this, we get $C^{*t}D = D^{*t}C$ and so

$$\begin{pmatrix} C_1^* & 0 \\ 0 & 0 \end{pmatrix} {}^tU^{*t}U^{-1} \begin{pmatrix} {}^tD_1 & 0 \\ 0 & E_{n-r} \end{pmatrix} = \begin{pmatrix} D_1^* & 0 \\ 0 & E_{n-r} \end{pmatrix} U^{*^{-1}} U \begin{pmatrix} {}^tC_1 & 0 \\ 0 & 0 \end{pmatrix}$$

Writing

$${}^tU^{*t}U^{-1} = \begin{pmatrix} V_1 & V_2 \\ V_3 & V_4 \end{pmatrix}, U^{*^{-1}}U = \begin{pmatrix} W_1 & W_2 \\ W_3 & W_4 \end{pmatrix}$$

we obtain

$$\begin{pmatrix} C_1^* V_1 {}^tD_1 & C_1^* V_2 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} D_1^* W_1 {}^tC_1 & 0 \\ W_3 {}^tC_1 & 0 \end{pmatrix}. \tag{30}$$

Hence $V_2 = 0$, $W_3 = 0$ and from $U = U^* \left(\begin{smallmatrix} W_1 & W_2 \\ 0 & W_4 \end{smallmatrix}\right)$, it follows then that $W_1 \in GL_r(\mathbb{Z})$. If $U = (F\ G)$ and $U^* = (F^* G^*)$, then $F = F^* W$, i.e. $\{F\} = \{F^*\}$ and so $F = F^*$ giving $U = U^*$, since, corresponding to F, we have assigned U once for all. Hence

$$U_1 \begin{pmatrix} C_1 & D_1 & 0 \\ 0 & 0 & E_{n-r} \end{pmatrix} = \begin{pmatrix} C_1^* & D_1^* & 0 \\ 0 & 0 & E_{n-r} \end{pmatrix} \text{ and so } U_1 = \begin{pmatrix} U_1' & 0 \\ * & * \end{pmatrix}.$$

But since U_1 is in $GL_n(\mathbb{Z})$, U'_1 is in $GL_r(\mathbb{Z})$ and so $\{C_1, D_1\} = \{C_1^* D_1^*\}$ i.e. $C_1 = C_1^*$, $D_1 = D_1^*$ and the lemma is proved. □

58 **Lemma 1.4.6.** *Between the family of classes $\{C, D\}$ of n-rowed coprime symmetric paris C, D with $\det C \neq 0$ and the set of all (n, n) rational symmetric matrices P, there exists a one - one correspondence given by $\{C, D\} \leftrightarrow p(= C^{-1}D)$.*

Proof. Clearly $\{C, D\}$ uniquely determines $P = C^{-1}D$. Suppose now $\{C_1, D_1\}$ and $\{C, D\}$ are mapped into the same P i.e. $C_1^{-1}D_1 = C^{-1}D = {}^tD{}^tC^{-1}$ so that $C_1{}^tD = D_1{}^tC$. This in turn means at once that for $M = \left(\begin{smallmatrix} * & * \\ C & D \end{smallmatrix}\right)$, $M_1 = \left(\begin{smallmatrix} * & * \\ C_1 & D_1 \end{smallmatrix}\right)$ in Γ_n, $M_1 M^{-1} = \left(\begin{smallmatrix} * & * \\ 0 & U \end{smallmatrix}\right)$ with $U \in GL_n(\mathbb{Z})$ and therefore $\{C, D\} = \{C_1, D_1\}$. We have thus shown that $\{C, D\} \mapsto P = C^{-1}D$ is well-defined and one-one and we need only to show that it is onto. For any given rational symmetric (n, n) matrix P, there exist U_3, U_4 in $GL_n(\mathbb{Z})$ such that $U_3 P U_4$ is a diagonal matrix with diagonal elements $a_i/b_i (1 \leq i \leq n)$, for a_i, b_i in $\mathbb{Z}$ with $(a_i, b_i) = 1$ and $b_i > 0$. If we now take $C_1 = B_0 U_3$, $D_1 = A_0 U_4^{-1}$ with diagonal matrices $A_0 = [a_1, \ldots, a_n]$ and $B_0 = [b_1, \ldots, b_n]$, then clearly $P = C_1^{-1}D_1$. Since $P = {}^tP$, we have $C_1{}^tD_1 = D_1{}^tC_1$. Since $(C_1 D_1)\begin{pmatrix} U_3^{-1} & 0 \\ 0 & U_4 \end{pmatrix} = (B_0\ A_0)$ is clearly primitive, it follows that C_1, D_1 is a coprime symmetric pair corresponding to $P(= C^{-1}D) = {}^tP$. □

As an immediate corollary of Lemma 1.4.6, we see that $\Gamma_{n,\infty} \backslash \{M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Gamma_n | \det C \neq 0\}$ is in one - one correspondence with $\{P = {}^tp \in \mathscr{M}_n(Q)\}$ via $C, D \mapsto (C^{-1}D =)P$.

Definition. *For $P = C^{-1}D = {}^tP \in \mathscr{M}_n(Q)$, define $\lceil P \rceil = \operatorname{abs}(\det C)$. (It is clear that if $C^{-1}D = P = C_1^{-1}D_1$, then abs $\det C = \operatorname{abs}\det C_1$ from above and so $\lceil P \rceil$ is well-defined).*

59 The following three lemmas have been reproduced from Siegel [25], for the sake of completeness.

Lemma 1.4.7. *Let K be an n-rowed diagonal matrix $[c_1, c_2, \ldots, c_n]$ with integers $c_1, \ldots, c_n$, $c_i | c_{i+1} (1 \leq i \leq n-1)$ as diagonal entries and $\mathscr{K} =$*

$\{U \in GL_n(\mathbb{Z}) | KUK^{-1}$ integral$\}$. *Then*

$$[GL_n(\mathbb{Z}) : \mathscr{K}] \leq \prod_{p|c_n} (1 - p^{-1})^{1-n} \prod_{1\leq k\leq n} c_k^{2k-n-1}$$

where p runs over the distinct primes dividing c_n.

Proof. Since $Q := GL_n(\mathbb{Z}; q)$ is a subgroup of $\mathscr{K}$ for every positive multiple q of c_n, we have $[GL_n(\mathbb{Z}) : \mathscr{K}] = [GL_n(\mathbb{Z})/Q : \mathscr{K}/Q]$. Now $GL_n(\mathbb{Z})/Q$ is isomorphic to the group of all n-rowed integral matrices V modulo q with $\det V \equiv \pm 1 (\text{mod q})$. In view of the Chinese Remainder Theorem, it suffices to show that

$$[\mathscr{U}^* : \mathscr{K}^*] \leq (1 - p^{-1})^{1-n} \prod_{1\leq k\leq n} c_k^{2k-n-1}$$

under the conditions that $q = c_n$ is a power of a fixed prime number p. $\mathscr{U}^*$ consists of all n-rowed integral matrices V modulo q with $\det V \equiv \pm 1 (\text{mod q})$ and $\mathscr{K}^*$ is the subgroup of all such V with integral KVK^{-1}.

Let $\mathscr{V}_n$ be the group of (n, n) integral V modulo q with $(\det V, q) = 1$ and $\mathscr{K}_n$ the subgroup of all V in $\mathscr{V}_n$ with integral KVK^{-1}. Then it is clear that $[\mathscr{V}_n : \mathscr{U}^*] = [\mathscr{K}_n : \mathscr{K}^*]$ and so $[\mathscr{V}_n : \mathscr{K}_n] = [\mathscr{U}^* : \mathscr{K}^*]$. If $\sharp\mathscr{V}_n$ and $\sharp\mathscr{K}_n$ denote the orders of $\mathscr{V}_n$ and $\mathscr{K}_n$ respectively, it suffices then to show that **60**

$$\sharp\mathscr{K}_n \geq (\sharp\mathscr{V}_n)(1 - p^{-1})^{n-1} \prod_{1\leq k\leq n} c_k^{n-2k+1}. \tag{31}$$

It is well-known that

$$\sharp\mathscr{V}_n = q^{n^2} \prod_{1\leq k\leq n} (1 - p^{-k}). \tag{32}$$

When $c_1 = c_n$, we have $K = c_1 E_n$, $\mathscr{K}_n = \mathscr{V}_n$ and (31) is true, since $\sum\limits_{1\leq k\leq n} (n + 1 - 2k) = 0$; in particular, this holds for $n = 1$. Let us apply induction on n and suppose that $c_1 < c_n$. Define h by the condition that $c_h < c_{h+1} = c_n$, then $1 \leq h \leq n - 1$. Let $V = (v_{k\ell}) = \begin{pmatrix} V_1 & V_2 \\ V_3 & V_4 \end{pmatrix}$ with $V_1 = V_1^{(h,h)}$. The matrices V and KVK^{-1} are both integral if and only if $v_{k\ell}$ and $c_k v_{k\ell} c_\ell^{-1}$ are in $\mathbb{Z}$ for k, $\ell = 1, 2, \ldots, n$. Then

V_3 and V_4 are arbitrary integral matrices, while V_1 and V_2 are integral matrices subject to the conditions $v_{k\ell} \equiv 0 (\mathrm{mod}\ c_\ell/c_k)$ for $k \leq h$, $k < \ell$. Since $p|(c_\ell/c_k)$ for $k \leq h < \ell$, we have $V_2 \equiv 0 (\mathrm{mod}\ p)$ and so $\det V \equiv (\det V_1)(\det V_4) (\mathrm{mod}\ p)$. Consequently, we get the elements V of $\mathscr{K}_n$ as follows: V_4 is any element of $\mathscr{V}_{n-h}$, V_3 is an arbitrary integral matrix modulo q, V_2 is any matrix modulo q satisfying the conditions $c_k^{-1} c_\ell | v_{k\ell}$ for $k \leq h < \ell$ and V_1 is any element of $\mathscr{K}_h$. It follows that $\sharp \mathscr{K}_n = a q^{h(n-h)} \cdot \sharp \mathscr{V}_{n-h} \cdot \sharp \mathscr{K}_h$, where a is the number of matrices V_2, namely $a = q^{h(n-h)} \prod\limits_{k \leq h < \ell} (c_k/c_\ell)$. Applying (31) with h instead of n and (32) with h, $n-h$ in place of n, we obtain

$$\sharp \mathscr{K}_n \geq q^{n^2} (1 - p^{-1})^{h-1} \prod_{1 \leq k \leq h} c_h^{h-2k+1} \prod_{k \leq h < \ell} (c_k/c_\ell)$$
$$\prod_{1 \leq k \leq h} (1 - p^{-k}) \prod_{1 \leq k \leq n-h} (1 - p^{-k})$$

61 Since

$$q^{n^2} \prod_{1 \leq k \leq h} (1 - p^{-k}) > \sharp \mathscr{V}_n, \prod_{1 \leq k \leq n-h} (1 - p^{-k}) \geq (1 - p^{-1})^{n-h}$$

and

$$\prod_{1 \leq k \leq h} c_k^{h-2k+1} \prod_{k \leq h < \ell} (c_k/c_\ell) = c_n^{-h(n-h)} \prod_{1 \leq k \leq h} c_j^{n-2k+1} = \prod_{1 \leq k \leq n} c_k^{n-2k+1}$$

the assertion (31) follows and the lemma is proved. □

The exact value of $[GL_n(\mathbb{Z}) : \mathscr{K}]$ can be obtained from the paper of A.N. Andrianov on 'Spherical functions for GL_n over local fields and summation of Hecke series, Math. Sbornik 12 (1970), 429-452.

Lemma 1.4.8. *Let $A(c_1, \ldots, c_n)$ denote the number of modulo 1 incongruent rational (n, n) symmetric matrices $P = C^{-1}D$ whose 'denominators' C have $c_1, \ldots, c_n$ as elementary divisors. Then*

$$A(c_1, \ldots, c_n) \leq \prod_{p|c_n} (1 - p^{-1})^{1-n} \prod_{1 \leq k \leq n} c_k^k.$$

Proof. Let C^* be any (n, n) integral matrix with $c_1, \ldots, c_n$ as elementary divisors and let $C^* = U_0 K U$ with U_0, $U \in GL_n(\mathbb{Z})$ and diagonal $K = [c_1, \ldots, c_n]$. If $A(C^*)$ is the number of modulo 1 incongruent symmetric R with integral $C^* R$ and if $R[{}^t U] = R_1 = (r_{k\ell})$ say, then $C^* R^t U = U_0 K R_1$ and so $A(C^*) = A(K)$. The matrix KR_1 is integral if and only if $c_k r_{k\ell}$ is in $\mathbb{Z}$ for $1 \leq k$, $\ell \leq n$. Since $r_{k\ell} = r_{\ell k}$ and $c_1 | c_2 | \ldots | c_n$, we obtain

$$A(K) = \prod_{1 \leq k \leq n} c_k^{n-k+1} \tag{33}$$

Now, the number of modulo 1 incongruent symmetric R with the same denominator C^* is at most $A(C^*)$. On the other hand, $C^* = U_0 K U$ and $C_1 = U_1 K U_2$ with U_1, $U_2 \in GL_n(\mathbb{Z})$ are denominators of the same rational symmetric matrix R, if and only if $C^* C_1^{-1} \in GL_n(\mathbb{Z})$; the latter implies that $K U_2 U^{-1} K^{-1}$ is integral, $U_2 U^{-1}$ is in $\mathscr{K} := \{V \in GL_n(\mathbb{Z}) | K V K^{-1}$ is integral$\}$ and so U, U_2 are in the same right coset of $\mathscr{K}$ in $GL_n(\mathbb{Z})$. Thus $A(c_1, \ldots, c_n) \leq [GL_n(\mathbb{Z}) : \mathscr{K}] A(K)$ and the lemma is immediate from (33) and Lemma 1.4.7. □ **62**

We need one more lemma, for our later purposes.

Lemma 1.4.9. *Let R run over a complete set of modulo 1 incongruent (n, n) rational symmetric matrices. Then the Dirichlet series*

$$\psi(s) := \sum_{R \bmod 1} \lceil R \rceil^{-s-n}$$

converges for $s > 1$. If $u > 0$ and $s > 1$, then

$$u^{-s} \sum_{\lceil R \rceil < u} \lceil R \rceil^{-n} + \sum_{\lceil R \rceil \geq u} \lceil R \rceil^{-n-s} < a \left(2 + \frac{1}{s-1} \right) u^{1-s}$$

where a depends only on n.

Proof. For two Dirichlet series $\alpha(s) = \sum\limits_n a_n \lambda_n^{-s}$ and $\beta(s) = \sum\limits_n b_n \lambda_n^{-s}$, we write $\alpha(s) < \beta(s)$ if $|a_n| \leq |b_n|$ for every n. From the definition of $A(c_1, \ldots, c_n)$ above, we have $\psi(s) = \sum\limits_{c_1 | c_2 | \ldots | c_n} A(c_1, \ldots, c_n)(c_1 \ldots c_n)^{-n-s}$ where $c_1, \ldots, c_n$ run over all systems of natural numbers with $c_1 | c_2 | \ldots$ **63**

$|c_n$. From Lemma 1.4.8, we obtain, on letting $c_1, \ldots, c_n$ run over all natural numbers, that

$$\begin{aligned}\psi(s) &< \sum_{c_1,\ldots,c_n} \prod_{p|c_n} (1-p^{-1})^{1-n} \prod_{1\le k\le n} c_k^{k-n-s} \\ &= \prod_p \left(1 + (1-p^{-1})^{1-n} \sum_{1\le \ell<\infty} p^{-\ell s}\right) \prod_{1\le k\le n-1} \zeta(s+n-k)\end{aligned}$$

Let

$$\nu = 2^n + n - 3, \gamma(s) = \zeta^\nu(s+1) \quad \text{and} \quad b_p := p((1-p^{-1})^{1-n} - 1).$$

Then $0 \le b_p \le 2^n - 2 = \nu - n + 1$ for all $p \ge 2$ and

$$1 + (1-p^{-1})^{1-n} \sum_{1\le\ell<\infty} p^{-\ell s} = (1 + b_p p^{-1-s})/(1-p^{-s})(1-p^{-1-a})^{n-\nu-1}/(1-p^{-s})$$

whence

$$\psi(s) < \gamma(s)\zeta(s) \tag{34}$$

proving the first assertion of the lemma. □

Let $\psi(s) = \sum_{1\le n<\infty} a_n n^{-s}$ and $\gamma(s) = \sum\limits_{1\le n<\infty} d_n n^{-s}$. Further, let $\sigma_k = \sum\limits_{1\le\ell\le k} a_\ell$, $\gamma(1) = \zeta^\gamma(2) = a$. Then, from (34), we have

$$\sigma_k \le \sum_{1\le\ell\le k} d_\ell [\frac{k}{\ell}] \le k \sum_{1\le\ell\le k} d_\ell/\ell < k \sum_{1\le\ell<\infty} d_\ell/\ell = ak (k = 1, 2, \ldots)$$

Hence, for all $u > 0$,

$$\sum_{\lceil R \rceil < u} \lceil R \rceil^{-n} = \sum_{\ell<u} a_\ell < au \tag{35}$$

64 Moreover, for

$$s > 1, \sum_{\lceil R \rceil \ge u} \lceil R \rceil^{-n-s} = \sum_{k\ge u} a_k k^{-s}$$

$$= \sum_{k \geq u} (\sigma_k - \sigma_{k-1})^{k^{-s}} \leq \sum_{k \geq u} \sigma_k (k^{-s} - (k+1)^{-s})$$
$$= s \sum_{k \geq u} \sigma_k \int_k^{k+1} x^{-s-1} dx < as$$
$$\sum_{k \geq u} \int_k^{k+1} x^{-s} dx \leq as \int_u^{\infty} x^{-s} dx$$
$$= asu^{1-s}/(s-1). \tag{36}$$

The second assertion of the lemma follows from (35) and (36).

It is known that $\psi(s) = \dfrac{\zeta(s)}{\zeta(s+n)} \prod_{r=1}^{n} \dfrac{\zeta(2s+n-r)}{\zeta(2s+2n-2r)}$ where ζ is Riemann's zeta function. This assertion may be found in H. Maass [17]. For a proof, see Kitaoka's paper 'Dirichlet series in the theory of Siegel modular forms, Nagoya Math.J. 35 (1984), 73-84 (cf. G. Shimura: On Eisenstein series, Duke Math.J.50(1983), 417-476).

Returning to the problem of estimating $\sum_M \alpha(M)$, we first state the following Propositions, which essentially go back to Siegel [25].

Proposition 1.4.10. *For f and T as above and half-integral $k > n+1/2$, we have*

$$\sum_{\substack{\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) = M \in \Gamma_{n,\infty} \backslash \Gamma_n \\ \det C \neq 0}} \alpha(M) \ll (\min T)^{(n+1-k)/2} (\det T)^{k-(n+1)/2} \tag{37}$$

if $\min T > \mathscr{X} > 0$ *for* $\mathscr{X}$ *depending only on n.*

Proposition 1.4.11. *For f and T as above and half-integral $k \geq n+1/2$, we have*

$$\sum_{\substack{\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) = M \in \Gamma_{n,\infty} \backslash \Gamma \\ \det C = 0}} \alpha(M) \ll (\min T)^{n-k} (\det T)^{k-(n+1)/2} \tag{38}$$

provided that $\det T \ll (\min T)^n$ *and* $\min T > \mathscr{X} > 0$ *as in Proposition 1.4.10.*

Remarks. Since $(n+1-k)/2 < 0$ for $k \geq n+3/2$, the right hand side of (37) is of a strictly lower order than the term $(\det T)^{k-(n+1)/2}$ occurring in the corresponding Fourier coefficient of Siegel's genus invariant for $S > 0$; therefore, for $\min T \gg 0$, we have a truly asymptotic formula
65 $r(S, T)$. We also note that the condition $\det T \ll (\min T)^n$ in Proposition 1.4.11 is *not* necessary for the proof of (37).

Lemma 1.4.12. *For* $M = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma_n$ *with* $\det C \neq 0$ *and real* $X = {}^tX$, *we have* $\mathrm{Im}(M < X+iT^{-1} >) = (T[X+C^{-1}D]+T^{-1})^{-1}[C^{-1}] \leq T[C^{-1}]$. *Further* $\beta(M) \neq \emptyset$ *implies that* $\min(T[C^{-1}]) \geq \sqrt{3}/2$.

Proof. Indeed for

$$Z = X + iY \in \mathscr{G}_n, \mathrm{Im}(M < Z >) = {}^t(C\overline{Z} + D)^{-1} Y (CZ + D)^{-1}$$

so that

$$\begin{aligned}(\mathrm{Im}(M < Z >))^{-1} &= (CX + D + iCY)Y^{-1}({}^t(CX + D) - iY^tC) \\ &= Y^{-1}[X^tC + {}^tD] + Y[{}^tC].\end{aligned}$$

Hence

$$\begin{aligned}\mathrm{Im}(M < X + iT^{-1} >) &= (T[X + C^{-1}D] + T^{-1})^{-1}[C^{-1}] \leq (T^{-1})^{-1}[C^{-1}] \\ &= T[C^{-1}].\end{aligned}$$

If $X_1 \in \beta(M)$, then $M < X_1 + iT^{-1} > \epsilon \mathfrak{g}_n$ and hence $\min T[C^{-1}] \geq \min(\mathrm{Im}(M < X_1 + iT^{-1} >)) \geq \sqrt{3}/2$.

For given $M = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma_n$ with $\det C \neq 0$, we now proceed to estimate the series $\sum\limits_{S \in \Lambda} \alpha\left(M\left(\begin{smallmatrix} E_n & S \\ 0 & E_n \end{smallmatrix}\right)\right) = \sum\limits_{S\in\Lambda} \alpha(C, D + CS)$. Applying Lemmas 1.4.4 and 1.4.12, we have $\sum\limits_{S\in\Lambda} \alpha(C, D + CS)$

$$\ll \sum_{S\in\Lambda} \int\limits_{\beta\left(M\left(\begin{smallmatrix} E_n & S \\ 0 & E_n \end{smallmatrix}\right)\right)} (\mathrm{abs}(\det(C(X + iT^{-1}) + D + CS))^{-k}$$
$$\exp(-\mathscr{X} \min((T[X + C^{-1}D + S] + T^{-1,-1}[C^{-1}]))dX$$

$$\ll q^{n(n+1)/2} \int\limits_{\mathscr{S}_n} (\operatorname{abs}(\det(C(X + iT^{-1})))^{-k}$$
$$\exp(-\mathscr{X} \min((T[X] + T^{-1})^{-1}[C^{-1}]))dX$$

where the integration is now over the $n(n+1)/2$-dimensional space $\mathscr{S}_n$ of all real $X = {}^tX$. For $X \in \mathscr{S}_n$, we define Θ by $\Theta = T^{1/2}XT^{1/2}$ **66**
where $T^{1/2}$ is the unique positive definite square root of T. Then $dX = (\det T)^{-(n+1)/2}d\Theta$ and

$$\sum_{S \in \Lambda} \alpha(C, D + CS) \ll (\det T)^{k-(n+1)/2} (\operatorname{abs} \det C)^{-k} \int\limits_{\varphi_n}$$
$$\det(\Theta^2 + E)^{-k/2} \exp(-\mathscr{X} \min(\Theta^2 + E_n)^{-1}|T^{\frac{1}{2}} C^{-1}])d\Theta$$

Writing

$$\Theta = \begin{pmatrix} w_1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & w_n \end{pmatrix} [V] \text{ with orthogonal } V^{(n,n)}$$
$$= (v_{ij}) \text{ and } |w_1| \geq \dots \geq |w_n|,$$

we have

$$\Theta^2 + E_n = \begin{pmatrix} w_1^2 + 1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & w_n^2 + 1 \end{pmatrix} [V] \leq (1 + w_1^2)E_n,$$
$$\det(\Theta^2 + E_n) = \prod_{1 \leq j \leq n} (1 + w_j^2), d\Theta = \prod_{k < \ell} |w_k - w_\ell| dw_1 \dots dw_n d\mu$$

where $d\mu$ is the Haar measure on the orthogonal group $O(n)$ and $|w_k - w_\ell| \leq (1 + w_k^2)^{1/2}(1 + w_\ell^2)^{1/2}$. Since the volume of $O(n)$ is finite, we see that the integral over φ_n above is

$$\ll \int\limits_{\mathbb{R}^n} \prod_{1 \leq j \leq n} (1 + w_j^2)^{-k/2} \exp(-\mathscr{X}(1 + w_1^2)^{-1} \min(T[C^{-1}]))$$

$$\prod_{1\le j\le n}(1+w_j^2)^{(n-1)/2}dw_1,\ldots dw_n$$

$$\ll \int_{\infty}^{\infty}(1+w_1^2)^{-k/2+(n-1)/2}\exp(-\mathscr{X}(1+w_1^2)^{-1}\min T[C^{-1}])dw_1$$

since $k// - (n-1)/2 > -1/2$

$\ll (\min T[C^{-1}])^{(n-k)/2}$ noting that $\min T[C^{-1}] \ge \sqrt{3}/2$,

by Lemma 1.4.12.

Now

$$\min(T[C^{-1}]) = |\det C|^{-2}\min(T[(\det C)C^{-1}]) \ge (\min T)/|\det C|^2$$

Hence we have

$$\sum_{S\in\Lambda}|\alpha(C,D+CS)| \ll (\det T)^{k-(n+1)/2}\begin{cases}|\det C|^{-k}\\ |\det C|^{-n}(\min T)^{(n-k)/2}\end{cases} \tag{39}$$

□

67 **Proof of Proposition 1.4.10.** From Lemma 1.4.6 and (39), we have

$$\begin{aligned}\left(\begin{smallmatrix}A & B\\ C & D\end{smallmatrix}\right) &= \sum_{\substack{M\in\Gamma_{n,\infty}\backslash\Gamma_n\\ \det C\ne 0}}\alpha(M) = \sum_{P=C^1 D \bmod 1}\ \sum_{S\in\Lambda}\alpha(C,D+CS)\\
&\ll (\det T)^{k-(n+1)/2}\left\{\sum_{\substack{P={}^tP\in\mathscr{M}_n(Q)\bmod 1\\ \lceil P\rceil<(\min T)^{1/2}}}\lceil P\rceil^n(\min T)^{(n-k)/2} + \sum_{\substack{P={}^tP\in\mathscr{M}_n(Q)\bmod 1\\ \lceil P\rceil\ge(\min T)^{1/2}}}\lceil P\rceil^k\right\}\\
&\ll (\det T)^{k(n+1)/2}(\min T)^{(n+1-k)/2},\end{aligned}$$

applying Lemma 1.4.9 with $u = (\min T)^{1/2}$ and $s = k-n(\ge 3/2)$, which proves (37) and Proposition 1.4.10.

We proceed now to the proof of Proposition 1.4.11. By Lemma 1.4.4, we have

$$|\alpha(M)| = |\alpha(C,D)| \ll \int_{\beta(M)}(\text{abs}\det((C(X+iT^{-1})+D))^{-k}dX \tag{39}$$

since for $X \in \beta(M)$, $\min(\operatorname{Im}(M < X + iT^{-1} >)) \geq \sqrt{3}/2$. We should remark, however, that estimate (39) is rather crude and deserves to be improved with a better knowledge of the geometry of $\mathscr{F}_n$, in order to obtain sharper estimates for $a(T)$. Using the form of C, D in Lemma 1.4.5 with $1 \leq r < n$, we have

$$\begin{aligned} \operatorname{abs}(\det(C(X + iT^{-1}) + D)) &= \operatorname{abs}\det(C_1(X[F] + iT^{-1}[F]) + D_1) \\ &= |\det C_1||\det((X[F] + iT^{-1}[F] + C_1^{-1}D_1)|. \end{aligned}$$

Thus **68**

$$\sum_{S={}^tS\in\Lambda_r} |\alpha\left(\begin{pmatrix} C_1 & 0 \\ 0 & 0 \end{pmatrix} {}^tU, \begin{pmatrix} D_1 + C_1 S & 0 \\ 0 & E_{n-r} \end{pmatrix} U^{-1}\right)| \ll$$

$$(\det C_1)^{-k} \sum_{S\in\Lambda_r} \int\limits_{X\in\beta\begin{pmatrix} A_1 & 0 & B_1 & 0 \\ A & E_{n-r} & 0 & 0 \\ C_1 & 0 & D_1 & 0 \\ 0 & 0 & 0 & E_{n-r} \end{pmatrix}\begin{pmatrix} E_n & S & 0 \\ & 0 & 0 \\ 0 & & E_n \end{pmatrix}\begin{pmatrix} {}^tU & 0 \\ 0 & U^{-1} \end{pmatrix}}$$

$$|\det(X[F] + C_1^{-1}D_1 + S + iT^{-1}[F])|^{-k} dX$$

$$|\det C_1|^{-k} \int\limits_{Q\in\bigcup\limits_{S\in\Lambda_r}(\mathrm{t}[U] + \begin{pmatrix} S & 0 \\ 0 & 0 \end{pmatrix})} |\det|(Q_1 + C_1^{-1}D_1 + iT^{-1}[F])|^{-k} dQ \tag{40}$$

under the change of variables $X \mapsto Q := X[U] = \begin{pmatrix} Q_1^{(r,r)} & Q_2 \\ * & Q_4 \end{pmatrix}$, noting that $dX = dQ$ and $Q_1 = X[F]$. For a real symmetric (r, r) matrix S', $\bigcup\limits_{S\in\Lambda_r} \left(\mathrm{t}[U] + \begin{pmatrix} qS + S' & 0 \\ 0 & 0 \end{pmatrix}\right)$ is a complete set of representations of $\mathscr{S}_n$ modulo $\{q\begin{pmatrix} 0 & S_2 \\ {}^tS_2 & S_4 \end{pmatrix} | S_2 \in \mathscr{M}_{r,n-r}(\mathbb{Z}), S_4 = {}^tS_4 \in \mathscr{M}_{n-r}(\mathbb{Z})\}$ and

$$\{\begin{pmatrix} S_1 & S_2 \\ {}^tS_2 & S_4 \end{pmatrix} | S_1 \in \varphi_r, S_2 \in \mathscr{M}_{r,n-r}(\mathbb{R}/q\mathbb{Z}), S_4 = {}^tS_4 \in \mathscr{M}_{n-r}(\mathbb{R}/q\mathbb{Z})\}$$

is another system of representatives. Suppose now that

$$Q = \begin{pmatrix} Q_1^{(r,r)} & Q_2 \\ {}^tQ_2 & Q_4 \end{pmatrix} \in \mathfrak{t}[U] + \begin{pmatrix} S & 0 \\ 0 & 0 \end{pmatrix} \quad \text{and}$$

$$Q' = \begin{pmatrix} Q_1 & Q_2' \\ {}^tQ_2' & Q_4 \end{pmatrix} \in \mathfrak{t}[U] + \begin{pmatrix} S' & 0 \\ 0 & 0 \end{pmatrix}$$

with $S \equiv S'(\text{mod q})$, $Q_2 \equiv Q_2'(\text{mod q})$ and $Q_4 \equiv Q_4'(\text{mod q})$. Then $Q - \left(\begin{smallmatrix} S & 0 \\ 0 & 0 \end{smallmatrix}\right)$ and $Q' - \left(\begin{smallmatrix} S' & 0 \\ 0 & 0 \end{smallmatrix}\right)$ are both in $\mathfrak{t}[U]$ and further are congruent
69 modulo q. Since U is in $GL_n(\mathbb{Z})$ and $\mathfrak{t}$ is the standard cube with sides of length q, we have then necessarily $Q - \left(\begin{smallmatrix} S & 0 \\ 0 & 0 \end{smallmatrix}\right) = Q' - \left(\begin{smallmatrix} S' & 0 \\ 0 & 0 \end{smallmatrix}\right)$ implying that $Q_2 = Q_2'$, $Q_4 = Q_4'$ and $S = S'$. For any given $Q_1 = X[F]$ and equivalence class in Λ_r modulo q, Q_2, Q_4 run at most modulo q. Hence, after absorbing constants, we see that the expression in (40) is

$$\ll [\Lambda_r : q\Lambda_r] q^{r(n-r)} q^{(n-r)(n-r+1)/2} |\det C_1|^{-k} \int\limits_{Q_1={}^tQ_1 \in \mathscr{M}_r(\mathbb{R})} |\det(Q_1 + iT^{-1}[F])^{-k} dQ_1 \tag{41}$$

the integrand being now independent of Q_2 and Q_4. It is easy to see again that the expression in (41) is

$$\begin{aligned} &\ll |\det C_1|^{-k} (\det T^{-1}[F])^{(r+1)/2-k} \int\limits_{X_1={}^tX_1 \in \mathscr{M}_r(\mathbb{R})} |\det(X_1 + iE_r)|^{-k} dX_1 \\ &\ll |\det C_1|^{-k} (\det T^{-1}[F])^{(r+1)/2-k}. \end{aligned} \tag{42}$$

For fixed r with $1 \leq r < n$, we know (by Lemmas 1.4.5 and 1.4.6) that there exists a one - one correspondence

$$\begin{aligned} &\Gamma_{\eta,\infty} \backslash \{M = \begin{pmatrix} * & * \\ C & D \end{pmatrix} \in \Gamma_n | \operatorname{rank} C \\ &\qquad = r\} / \{ \begin{pmatrix} E_n & \begin{pmatrix} S & 0 \\ 0 & 0 \end{pmatrix} \\ 0 & E_n \end{pmatrix} \in \Gamma_n\} \longleftrightarrow \{C_1^{-1} D_1 \text{mod } 1\}, \{\text{F}\} \end{aligned}$$

where $C_1^{-1}D_1$ runs over a complete set of modulo 1 incongruent (r,r) rational symmetric matrices and $F^{(n,r)}$ over a complete set of (n,r) primitive matrices described in Lemma 1.4.5. By assumption, $T \asymp \begin{pmatrix} t_1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & t_n \end{pmatrix}$ with $t_i := t_{ii}$ and it is not hard to see that

$$(\det T^{-1}[F]) \gg t_n^{-1} \dots t_{n-r+1}^{-1} \det E_n[F].$$

In fact, if $\begin{pmatrix} i_1 & i_2 & \dots i_r \\ 1 & 2 & \dots r \end{pmatrix} F$ is the determinant of the (r,r) submatrix of F formed by the rows with indices $i_1, i_2, \dots, i_r$, then **70**

$$\det T^{-1}F \gg \det \begin{pmatrix} t_1^{-1} & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & t_n^{-1} \end{pmatrix} [F] = \sum_{1 \le i_1 < i_2 < \dots i_r \le n}$$
$$= \begin{pmatrix} i_1 & i_2 & \dots & i_r \\ 1 & 2 & \dots & r \end{pmatrix}_F^2 t_{i_1}^{-1} \dots t_{i_r}^{-1}$$
$$\gg t_n^{-1} \dots t_{n-r+1}^{-1} \sum \begin{pmatrix} i_1 & i_2 & \dots & i_r \\ 1 & 2 & \dots & r \end{pmatrix}_F^2 = t_n^{-1} \dots t_{n-r+1}^{-1} \det E_n[F].$$

Using now the estimate (42), we conclude that

$$\sum_{S \in \Lambda_r} |\alpha\left(\begin{pmatrix} C_1^{(r)} & 0 \\ 0 & 0 \end{pmatrix} t_U, \begin{pmatrix} D_1 + C_1 S & 0 \\ 0 & E_{n-r} \end{pmatrix} U^{-1}\right)$$
$$| \ll |\det C_1|^{-k} (t_n^{-1} \dots t_{n-r+1}^{-1})^{\frac{r+1}{2}-k} \det(E_n[F])^{\frac{r+1}{2}-k}$$

From the last estimate and the one - one correspondence referred to in the preceding paragraph, it follows at once that

$$M = \sum_{\begin{pmatrix} * & * \\ C & D \end{pmatrix} \in \Gamma_{n,\infty} \backslash \Gamma_n, \operatorname{rank} C = r} \alpha(M) \ll \sum_{R = {}^t R \in \mathscr{M}_r(\mathbb{Q}) \bmod 1} \lceil R \rceil^{-k}$$
$$\sum_{\substack{F \in \mathscr{M}_{n,r}(\mathbb{Z})/GL_r\mathbb{Z} \\ F \text{ primitive}}} (\det E_n[F])^{\frac{r+1}{2}-k} (t_n \dots t_{n-r+1})^{k-\frac{r+1}{2}}. \tag{43}$$

The representatives F in the summation in (43) can be assumed to have been chosen already to satisfy the condition that $E_n[F]$ is M-reduced. If

$F = (f_1 \dots f_r)$, then, by Lemma 1.3.2, $\det E_n[F] \gg \prod_{1\le i\le r} E_n|f_i|$. Since $(r+1)/2 - k \le n/2 - k < 0$, we have

$$\sum_F (\det E_n[F])^{(r+1)/2-k} \ll \left\{ \sum_{0\neq x\in\mathbb{Z}^n} (E_n[x])^{(r+1)/2-k} \right\}^r . \tag{44}$$

If $x_1 \dots x_n \neq 0$, then $\sum_{1\le i\le n} x_i^2 \ge n|x_1 \dots x_n|^{2/n}$. Therefore the series over x on the right hand side of (44) is $\ll \sum_{1\le s\le n} \sum_{y_i\in\mathbb{Z}\setminus\{0\}} (y_1^2 + \dots + y_s^2)^{-(k-\frac{r+1}{2})} \ll$
71 $\sum_{1\le s\le n} \zeta(2\{k-(r+1)/2)/s) \ll 1$ since $k-(r+1)/2 > n/2$ for $r < n$, in view of the hypothesis $k \ge n + 1/2$. Thus the series over F in (44) is $\ll 1$. On the other hand, since $k - r > 1$ for $r \le n$, we can apply Lemma 1.4.9 to conclude that $\sum_{R={}^tR\in\mathscr{M}_r(\mathbb{Q}) \bmod 1} \lceil R \rceil^{-k} \ll 1$. So we finally see that the left hand side of (43) is

$$\ll (t_n \dots t_{n-r+1})^{k-(r+1)/2} = (\det T)^{k-(n+1)/2} (t_1 \dots t_{n-r})^{\frac{n+1}{2}-k} (t_{n-r+1} \dots t_n)^{\frac{n-r}{2}}.$$

We now use the assumption that $(\det T) \ll (\min T)^n$ for the M-reduced $T \asymp \begin{pmatrix} t_1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & t_n \end{pmatrix}$. Then $t_1 \asymp t_2 \asymp \dots \asymp t_n \asymp t$, say.

For $1 \le r \le n-1$, $(\dfrac{n+1}{2} - k)(n-r) + \dfrac{n-r}{2} \cdot r \le n-k$ with equality taking place when $r = n-1$. Thus

$$(t_1 \dots t_{n-r})^{\frac{n+1}{2}-k} (t_{n-r+1} \dots t_n)^{\frac{n-r}{2}} \asymp t^{(\frac{n+1}{2}-k)(n-r)+\frac{n-r}{2}\cdot r} \le t^{n-k}$$

and the left hand side of (43) is $\ll (\det T)^{k-\frac{n+1}{2}} (\min T)^{n-k}$ for $1 \le r \le n-1$. Summing over (43) for $1 \le r \le n-1$, Proposition 1.4.11 is immediate. In view of the remarks preceding Lemma 1.4.1., we have the following theorem (and Theorem C in the Introduction) as an immediate consequence of Proposition 1.4.10 and 1.4.11.

Theorem 1.4.13 ([10],[19]). *If $k = n + 3/2$ and $f(Z) = \sum_{0\le T\in\Lambda^*} a(T)$ $e(\mathrm{tr}(TZ)/q)$ is a Siegel modular form of degree n, weight $k(\in 1/2\mathbb{Z})$, level q and with constant term vanishing at all cusps, then*

$$a(T) = O((\min T)^{(n+1-k)/2} (\det T)^{k-(n+1)/2})$$

72 *provided that* $\min T \geq \mathscr{X}_1 (\det T)^{1/n}$ *and* $\min T \geq \mathscr{X}_2 > 0$ *for constants* $\mathscr{X}_1$, $\mathscr{X}_2$ *independent of* f *(but depending only on n).*

Remarks. The condition $\min T \geq (\det T)^{1/n}$ seems unavoidable for general n. The next theorem giving an estimate for coefficients of modular forms of degree 2, weight $k \geq 7/2$ and level q vanishing at all cusps imposes no such condition. Sunder Lal (Math. Zeit. 88 (1965), 207-243) has considered an analogue of Theorem 1.4.13 for the Hilbert-Siegel modular forms.

For any m-rowed integral $S > 0$, the associated theta series $f(Z) = \sum_G e(\mathrm{tr}(S[G]Z))$ is a modular form of degree n, weight $m/2$ and level 4 $\det S$ and $f(Z) - \varphi(Z)$ vanished at every cusp, if we take $\varphi(Z)$ to be the analytic genus invariant associated with S. The Fourier coefficients $b(T)$ of $\varphi(Z)$ are of the form $*(\det T)^{\frac{m-n-1}{2}} \times \prod_p \alpha_p(S,T)$ where $\prod_p \alpha_p(S,T)$ is the product of the p-adic densities of representation of T by S. Thus, for $m \geq 2n+3$ and $\min T \gg (\det T)^{1/n}$, we have from Theorem 1.4.13 an asymptotic formula for $r(S,T)$:

$$r(S,T) = *(\det T)^{\frac{m-n-1}{2}} \prod_p \alpha_p(S,T) + O\left((\det T)^{\frac{m-n-1}{2}} (\min(T))^{\frac{2n+2-m}{4}}\right)$$

For the case $n = 2$, we have an improved version of Proposition 1.4.11, and even *not* involving the unsatisfactory condition $(\det T) \ll (\min(T))^2$ namely

Proposition 1.4.14. *For* f, T *as above with* $\min T > \mathscr{X}$ *(an absolute constant independent of* f*) and* $n = 2$*,*

$$\sum_{\substack{M=\begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Gamma_{2,\infty}\backslash\Gamma_2 \\ \mathrm{rank}\, C = 1}} \alpha(M) \ll (\min(T))^{2-k} (\det T)^{k-3/2}$$

$$\begin{cases} 1 \ \textit{if}\ k \geq 7/2 \\ \log(\sqrt{\det T}/\min(T)) \ \textit{if}\ k = 3 \\ ((\det T)^{1/2}/\min(T))^{1/2} \ \textit{if}\ k = \frac{5}{2} \end{cases}$$

As immediate consequences of the foregoing, we have 73

Theorem 1.4.15 ([10]). *Let* $f(Z) = \sum_{0 \le T \in \Lambda} {}^{*} a(T) e(\mathrm{tr}(TZ)/q)$ *be a Siegel modular form of degree* 2*, weight* $k \geq 7/2$ *(with* $2k \in \mathbb{Z}$*), level* q *and with constant term vanishing at all cusps. Then for* $T > 0$ *and* $\min T > \mathscr{X}$ *(an absolute constant independent of* f*), we have,*

$$a(T) = O((\min T)^{(3-k)/2} (\det T)^{k-3/2})$$

Corollary . *If* $A^{(m)} > 0$, $B^{(2)} > 0$ *and if* $A[X] = B$ *is solvable with* X *having entries in* $\mathbb{Z}_p$ *for every prime* p*, then for large* $\min(B)$ *and* $m \geq 7$*,* $A[X] = B$ *has a solution* X *with entries in* $\mathbb{Z}$*.*

The proof of Proposition 1.4.14 has to be preceded by several lemmas.

Definition. *For given* $T > 0$ *and* $C = \left(\begin{smallmatrix} c & 0 \\ 0 & 0 \end{smallmatrix}\right)^{t} U$ *with* $U = \left(\begin{smallmatrix} f_1 & * \\ f_2 & \end{smallmatrix}\right) \in GL_2(\mathbb{Z})$ *and* $c \neq 0$ *in* $\mathbb{Z}$*, let* $a_1 := T^{-1}\left[\left(\begin{smallmatrix} f_1 \\ f_2 \end{smallmatrix}\right)\right]$ *and*

$$P = P(x_1, x_2) = P_{T,U,c}(x_1, x_2) := \begin{pmatrix} (a_1 + x_1^2/a_1)^{-1} & \\ 0 & 1/(a_1 \det T) \end{pmatrix} \left[\begin{pmatrix} 1/c & x_2 \\ 0 & 1 \end{pmatrix}\right]$$

Lemma 1.4.16. *For* $M = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma_2$ *with* $C = \left(\begin{smallmatrix} c & 0 \\ 0 & 0 \end{smallmatrix}\right)^{t}$, $D = \left(\begin{smallmatrix} d & 0 \\ 0 & 1 \end{smallmatrix}\right) U^{-1}$*,* $c \neq 0$ *in* $\mathbb{Z}$*,* U *in* $GL_2(\mathbb{Z})$*, and* $T \in \mathscr{P}_2$*, we have*

$$\mathrm{Im}(M < X + iT^{-1} >) = P(q_1 + d/c, a_2(q_1 + d/c)/a_1 - q_2)$$

where a_1*,* a_2*,* q_1*,* q_2 *are given by* $T^{-1}[U] = \left(\begin{smallmatrix} a_1 & a_2 \\ a_2 & a_4 \end{smallmatrix}\right)$ *and* $X[U] = \left(\begin{smallmatrix} q_1 & q_2 \\ q_2 & q_4 \end{smallmatrix}\right)$*.*

74 *Proof.* We know that $(\mathrm{Im}(M < X + iT^{-1} >))^{-1} = T\{{}^{t}(CX + D + iCT^{-1})\}$ (using the abbreviation $A\{B\}$ for ${}^{t}\overline{B}AB$) $= T[{}^{t}(CX + D)] + T^{-1}[{}^{t}C]$

$$= (\det T)\begin{pmatrix} a_4(cq_1 + d)^2 - 2a_2cq_2(cq_1 + d) + a_1c^2q_2^2 & * \\ -a_2(cq_1 + d) + a_1cq_2 & a_1 \end{pmatrix} + \begin{pmatrix} a_1c^2 & 0 \\ 0 & 0 \end{pmatrix}$$

This is, on the other hand, the same as

$$p^{-1}(q_1 + c^{-1}d, a_1^{-1}a_2(q_1 + c^{-1}d) - q_2)$$
$$\begin{pmatrix} a_1 + (q_1 + d/c)^2/a_1 & 0 \\ 0 & a_1 \det T \end{pmatrix} \left[\begin{pmatrix} c & 0 \\ cq_2 - a_1^{-1}a_2(cq_1 + d) & 1 \end{pmatrix}\right]$$
$$\begin{pmatrix} (a_1 + a_1^{-1}(q_1 + d/c)^2)c^2 + a_1(\det T)(cq_2 - a_1^{-1}a_2(cq_1 + d))^2 & * \\ a_1 \det T(cq_2 - a_1^{-1}a_2(cq_1 + d)) & a_1 \det T \end{pmatrix}$$

□

Lemma 1.4.17. *With notation as in Lemma 1.4.16,* $U = \left(\begin{smallmatrix} f_1 & * \\ f_2 & * \end{smallmatrix}\right)$ *and M-reduced* $T = \left(\begin{smallmatrix} t_1 & 0 \\ 0 & t_2 \end{smallmatrix}\right)\left[\left(\begin{smallmatrix} 1 & u \\ 0 & 1 \end{smallmatrix}\right)\right]$*, we have* $|c| f_2^2 \le (8/3)\sqrt{t_2/t_1}$ *and* $|f_1 f_2 c| \le 4/3$*, whenever* $\min(P) \ge \sqrt{3}/2$*; moreover, under this condition,* $|f_1| = 0$ *or* 1 *and if* $|f_1| = 1$*, then* $|c| \le 3$*.*

Proof. Since **75**

$$
\begin{aligned}
T &= \begin{pmatrix} t_1 & t_1 u \\ t_1 u & t_1 u^2 + t_2 \end{pmatrix}, T^{-1} - \frac{1}{2}\begin{pmatrix} t_1^{-1} & 0 \\ 0 & t_2^{-1} \end{pmatrix} \\
&= \frac{1}{t_1 t_2}\begin{pmatrix} t_1 u^2 + t_2 & -t_1 u \\ -t_1 u & t_1 \end{pmatrix} - \frac{1}{2}\begin{pmatrix} t_1^{-1} & 0 \\ 0 & t_2^{-1} \end{pmatrix} \\
&= \begin{pmatrix} u^2/t_2 + 1/(2t_1) & -u/t_2 \\ -u/t_2 & 1/(2t_2) \end{pmatrix}
\end{aligned}
$$

has determinant

$$
\frac{1}{4t_2^2}\left[\frac{t_2}{t_1} - 2u^2\right] \ge \frac{1}{4t_2^2}\left[\frac{3}{4} - \frac{1}{2}\right] > 0
$$

since $t_1 \le \dfrac{4}{3} t_2$ and $|u| \le 1/2$. Hence $T^{-1} > \dfrac{1}{2}\left(\begin{pmatrix} 1/t_1 & 0 \\ 0 & 1/t_2 \end{pmatrix}\right)$. On the other hand, since $P \in \mathscr{P}_2$, $(\min(P))^2 \le (4/3) \det P$. If then $\min(P) \ge \sqrt{3}/2$, we have

$$
\begin{aligned}
(3/4)^2 &= (3/4)(3/4) \le (3/4)\cdot(\min(P))^2 \le \det P \\
&= \det P = 1/\{c^2 \det T(a_1^2 + x_1^2)\} \le 1/(a_1^2 c^2 \det T).
\end{aligned}
$$

But

$$
a_1 = T^{-1}\left[\begin{pmatrix} f_1 \\ f_2 \end{pmatrix}\right] > 1/2\left(\frac{1}{t_1} f_1^2 + \frac{1}{t_2} f_2^2\right)
$$

and as a result, we have

$$
\begin{aligned}
\frac{1}{4}\left(2\sqrt{\frac{f_1^2}{t_1}\frac{f_2^2}{t_2}}\right)^2 c^2 t_1 t_2 &\le \frac{1}{4}\left(\frac{1}{t_1} f_1^2 + \frac{1}{t_2} f_2^2\right)^2 c^2 t_1 t_2 \qquad (45) \\
&\le (4/3)^2
\end{aligned}
$$

i.e. $c^2 f_1^2 f_2^2 \leq (4/3)^2$ and so

$$|f_1 f_2| \leq |c f_1 f_2| \leq 4/3.$$

Hence if $f_1 f_2 \neq 0$, $|f_1| = |f_2| = 1$. If $f_1 f_2 = 0$, then (since U is in $GL_2(\mathbb{Z})$), either $f_1 = 0$, $f_2 = 1$ or $f_1 = 1$, $f_2 = 0$ (taking only one primitive column from each class). From (45), we have

$$\frac{1}{4}\left(\frac{1}{t_2} f_2^2\right)^2 c^2 t_1 t_2 \leq \frac{1}{4}\left(\frac{1}{t_1} f_1^2 + \frac{1}{t_2} f_2^2\right)^2 c^2 t_1 t_2 \leq (4/3)^2$$

76 which gives us $c^2 f_2^4 \leq 4(4/3)^2(t_2/t_1)$ i.e. $|c f_2^2| \leq (8/3)\sqrt{t_2/t_1}$. If $|f_1| = 1 = |f_2|$, then $(1 \leq) c^2 = c^2 f_1^2 f_2^2 \leq (4/3)^2$ implies $|c| = 1$. If $|f_1| = 1$ and $f_2 = 0$, then from (45), we get $c^2 f_1^4 t_2/t_1 \leq 4(4/3)^2$ i.e. $c^2 \leq 4(4/3)^2(t_1/t_2) \leq 4(4/3)^3 < 2^4$ i.e. $|c| \leq 3$. This proves all the assertions of our lemma. □

Remarks. 1) Under the conditions of Lemma 1.4.17, the number of U coming into play is at most 4, namely $U = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ if $f_1 = 0$, $U = \left(\begin{smallmatrix} 1 & 0 \\ n & 1 \end{smallmatrix}\right)$ with $n \in \mathbb{Z}$ and $|n| \leq 1$ if $f_1 \neq 0$ (i.e. $f_1 = 1$). Whenever $|f_1 f_2| = 1$, we have $c = 1$.

2) For P as in Lemma 1.4.17, if $\sqrt{3}/2 \leq \min(P) = P\left[\left(\begin{smallmatrix} b_1 \\ b_2 \end{smallmatrix}\right)\right]$ for some integral column ${}^t(b_1 b_2)$, we claim that $b_2 \neq 0$. Otherwise, we can take $b_1 = 1$ and then $\min(P) = P[\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)] = 1/(c^2(a_1 + a_1^{-1} x_1^2)) \leq (2/\sqrt{3})(\det P)^{1/2} = (2/\sqrt{3})/((a_1 + a_1^{-1} x_1^2) c^2 a_1 \det T)^{1/2} \leq \dfrac{2}{\sqrt{3}}$ $(\min P/(a_1 \det T))^{1/2}$ i.e. $\sqrt{3}/2)^{1/2} \leq (\min(P))^{1/2} \leq (2/\sqrt{3})/(a_1 \det T)^{1/2}$ so that $a_1 \det T \leq 8/(3\sqrt{3})$. Together with the inequality $a_1 > \dfrac{1}{2}\left(\frac{1}{t_1} f_1^2 + \frac{1}{t_2} f_2^2\right)$ derived in the course of the proof of Lemma 1.4.17, this leads us to $1/2(t_2 f_1^2 + t_1 f_2^2) < 8/(3\sqrt{3})$. Since either f_1 or f_2 is different from 0, we have $\min\left(\frac{1}{2} t_1, \dfrac{1}{2} t_2\right) < 8/(3\sqrt{3})$ which contradicts t_1 and t_2 being sufficiently large (in view of $\min T \gg 0$, by assumption). This contradiction shows that when $\sqrt{3}/2 \leq \min P = P\left[\left(\begin{smallmatrix} b_1 \\ b_2 \end{smallmatrix}\right)\right]$, $b_2 \neq 0$.

To any $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $SL_2(\mathbb{Z})$, let us associate $\tilde{\sigma} = \begin{pmatrix} a & 0 & b & 0 \\ 0 & 1 & 0 & 0 \\ c & 0 & d & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$ in $\mathrm{Sp}(2, \mathbb{Z}) = \Gamma_2$. Then $\sigma \mapsto \tilde{\sigma}$ is an injective homomorphism. If $c \neq 0$, then $\sigma = \begin{pmatrix} 1 & a/c \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & -c^{-1} \\ c & d \end{pmatrix}$. In this case, we have for $Z = \begin{pmatrix} z_1 & z_2 \\ z_2 & z_4 \end{pmatrix}$, 77

$$\tilde{\sigma} < Z >= \begin{pmatrix} a/c & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} -1/(c(cz_1 + d)) & z_2/(cz_1 + d) \\ z_2/(cz_1 + d) & z_4 - cz_2^2/(cz_1 + d) \end{pmatrix} \tag{46}$$

by straightforward verification.

Let $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ with $c \geq 1$ and $U \in SL_2(\mathbb{Z})$. The following lemma gives an estimate for $\alpha\left(\begin{pmatrix} c & 0 \\ 0 & 0 \end{pmatrix}\right)^t U, \begin{pmatrix} d & 0 \\ 0 & 1 \end{pmatrix} U^{-1}\Big)$ needed in connection with Proposition 1.4.14.

Lemma 1.4.18. *Let σ, U be as above and let $A = T^{-1}[U] = \begin{pmatrix} a_1 & a_2 \\ a_2 & a_4 \end{pmatrix}$. For given $\Theta := \begin{pmatrix} \theta_1 & \theta_2 \\ \theta_2 & \theta_4 \end{pmatrix}$, $A = T^{-1}[U]$ and $C = \begin{pmatrix} c & 0 \\ 0 & 0 \end{pmatrix}{}^t U$, let*

$$\tau = \tau(\Theta, A, C) := \begin{pmatrix} -c^{-2}/(\theta_1 + ia_1) & c^{-1}(\theta_2 + ia_2)/(\theta_1 + ia_1) \\ c^{-1}(\theta_2 + ia_2)/(\theta_1 + ia_1) & \theta_4 + ia_4 - (\theta_2 + ia_2)^2/(\theta_1 + ia_1) \end{pmatrix}$$

Then

$$|\alpha\left(\begin{pmatrix} c & 0 \\ 0 & 0 \end{pmatrix}{}^t U, \begin{pmatrix} d & 0 \\ 0 & 1 \end{pmatrix} U^{-1}\right)| \ll c^{-k} \int\limits_{\substack{\begin{pmatrix} a/c & 0 \\ 0 & 0 \end{pmatrix} + \tau \in \mathfrak{g}_2 \\ \Theta \in t[U] + \begin{pmatrix} d/c & 0 \\ 0 & 0 \end{pmatrix}}} (\theta_1^2 + a_1^2)^{-k/2}$$

$$\exp(-\mathscr{X} \min(P(\theta_1, a_1^{-1} a_2 \theta_1 - \theta_2)) d\theta_1 d\theta_2 d\theta_4.$$

Proof. In view of Lemma 1.4.4 for $M = \tilde{\sigma}\begin{pmatrix} {}^t U & 0 \\ 0 & U^{-1} \end{pmatrix} = \begin{pmatrix} * & * \\ C & D \end{pmatrix}$ in Γ_2, we see, on taking $\Theta = X[U] + \begin{pmatrix} c^{-1}d & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} q_1 + c^{-1}d & q_2 \\ q_2 & q_4 \end{pmatrix}$ and noting $dX = d\Theta(:= d\theta_1 d\theta_2 d\theta_4)$, $\mathrm{Im}(M < X + iT^{-1} >) = P_{T,U,c}(q_1 + c^{-1}d, a_1^{-1} a_2(q_1 + c^{-1}d) - q_2) = P(\theta_1, a_1^{-1} a_2 \theta_1 - \theta_2)$ (by Lemma 1.4.16) and $\mathrm{abs}\det(C(X + iT^{-1}) + D) = \mathrm{abs}(c\theta_1 + cia_1)$, that 78

$$|\alpha(M)| = |\alpha(C, D)| \ll c^{-k} \int (\theta_1^2 + a_1^2)^{-k/2} \exp(-\mathscr{X}$$

$$\min(P(\theta_1, a_1^{-1}a_2\theta_1 - \theta_2)))d\Theta$$

the domain of integration for Θ corresponding to $\beta(M)$ for X under $X \mapsto \Theta$. But $M < X + iT^{-1} >= \tilde{\sigma} < \Theta - \left(\begin{smallmatrix} c^{-1}d & 0 \\ 0 & 0 \end{smallmatrix}\right) + iT^{-1}[U] >= \left(\begin{smallmatrix} a/c & 0 \\ 0 & 0 \end{smallmatrix}\right) + \tau$, by (46) and so the lemma is proved. □

For $\sigma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in $SL_2(\mathbb{Z})$ with $c \geq 1$ and U equal to one of the four matrices

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} \quad \text{with} \quad n = 0, 1 \text{ or } -1,$$

let

$$\mathscr{R}^*(U) := \bigcup_{m \in \mathbb{Z}} \left\{ \mathfrak{t}(U) + \begin{pmatrix} c^{-1}d + mq & 0 \\ 0 & 0 \end{pmatrix} \right\} = \mathscr{S}_2 / \left\{ \begin{pmatrix} 0 & s_2 \\ s_2 & s_4 \end{pmatrix} | s_2, s_4 \in q\mathbb{Z} \right\}$$

79 An application of Lemma 1.4.18 with d_1 ($\equiv d$ modulo q, for a fixed d) in place of d, leads to

Lemma 1.4.19. *For σ, U as above and f, T as in Proposition 1.4.14, we have*

$$\sum_{d_1 \equiv d (\text{mod cq})} |\alpha\left(\left(\begin{smallmatrix} c & 0 \\ 0 & 0 \end{smallmatrix}\right){}^tU, \left(\begin{smallmatrix} d_1 & 0 \\ 0 & 1 \end{smallmatrix}\right)U^{-1}\right)|$$

$$\ll c^{-k} \int\limits_{\substack{\left(\begin{smallmatrix} a_c & 0 \\ 0 & 0 \end{smallmatrix}\right) + \tau \in \mathfrak{g}_2 \\ \theta_1 \in \mathbb{R}, 0 \leq \theta_2, \theta_4 < q}} (\theta_1^2 + a_1^2)^{-k/2} \exp(-\mathscr{X} \min(P(\theta_1, a_1^{-1}a_2\theta_1 - \theta_2)))d\Theta$$

Proof. We need only to note that $A := T^{-1}[U] = \left(\begin{smallmatrix} a_1 & a_2 \\ a_2 & a_4 \end{smallmatrix}\right)$, $\tau = \tau(\Theta, A, c)$ and $P = P_{T,U,c}(x_1, x_2)$ are all independent of d, taking an extension $\left(\begin{smallmatrix} a & * \\ c & d_1 \end{smallmatrix}\right)$ of $(c \ \ d_1)$ to $SL_2(\mathbb{Z})$ and that $\min(P(\theta_1, a_1^{-1}a_2\theta_1 - (\theta_2 + qn))) = \min(P(\theta_1, a_1^{-1}a_2\theta_1 - \theta_2)\left[\left(\begin{smallmatrix} 1 & cn \\ 0 & 1 \end{smallmatrix}\right)\right]) = \min(P(\theta_1, a_1^{-1}a_2\theta_1 - \theta_2))$ for every $n \in \mathbb{Z}$. □

Before we begin the proof of Proposition 1.4.14, we note that, for $\Theta = \left(\begin{smallmatrix} \theta_1 & \theta_2 \\ \theta_2 & \theta_4 \end{smallmatrix}\right)$ in the domain of integration referred to in Lemma 1.4.19, we have $P(\theta_1, a_1^{-1}a_2\theta_1 - \theta_2) = \operatorname{Im}\tau (= \operatorname{Im}(M < X + iT^{-1} >)$, by Lemma 1.4.16) $\geq \sqrt{3/2}$. Hence, by Remark 2 following Lemma 1.4.17, we have $\min(P(\theta_1, a_1^{-1}a_2\theta_1 - \theta_2)) = P[\binom{b_1}{b_2}]$ for an integral column ${}^t(b_1 b_2)$ with $b_2 \neq 0$. Thus, we can remove the condition $\begin{pmatrix} a/c & 0 \\ 0 & 0 \end{pmatrix} + \tau \in \mathfrak{g}_2$ on the domain of integration for Θ in Lemma 1.4.19, if we majorize $\exp(-\mathscr{X} \min(P(\theta_1, a_1^{-1}a_2\theta_1 - \theta_2)))$ by the series

$$\sum_{0 \neq b_2, b_1 \in \mathbb{Z}} \exp(-\mathscr{X} p(\theta_1, a_1^{-1}a_2\theta_1 - \theta_2) \begin{bmatrix} b_1 \\ b_2 \end{bmatrix}).$$

Proof of Proposition 1.4.14. In the light of the preceding paragraph, we see that 80

$$\sum_{d_1 \equiv d (\text{mod cq})} |\alpha \left(\begin{pmatrix} c & 0 \\ 0 & 0 \end{pmatrix} {}^t U, \begin{pmatrix} d_1 & 0 \\ 0 & 0 \end{pmatrix} U^{-1} \right)| \ll c^{-k}$$
$$\sum_{0 \neq b_2, b_1 \in \mathbb{Z}} \exp(-\mathscr{X} a_1^{-1} b_2^2 / \det T) \int_{\theta_1 \in \mathbb{R}, 0 \leq \theta_2, \theta_4 < q} (\theta_1^2 + a_1^2)^{-k/2} \times$$
$$\times \exp(-\mathscr{X} \frac{b_2^2 (c^{-1} b_2^{-1} b_1 + a_1^{-1} a_2 \theta_1 - \theta_2)^2}{a_1 + \theta_1^2 / a_1} d\Theta.$$

If $b_1 \in b_1' + cb_2 q\mathbb{Z}$, then $c^{-1}b_2^{-1}b_1 + a_1^{-1}a_2\theta_1 - \theta_2$ for any fixed θ_1, θ_4, $b_2 \neq 0$ (and *fixed* b_1' modulo $cb_2 q$) covers $\mathbb{R}$ as θ_3 runs over an interval of length q. Thus the right hand side of the preceding inequality is

$$\ll c^{-k} \sum_{0 \neq b_2 \in \mathbb{Z}} c|b_2| \exp(-\mathscr{X} a_1^{-1} b_2^2 / \det T)$$
$$\int_{-\infty}^{\infty} \int_{-\infty}^{\infty} (\theta_1^2 + a_1^2)^{-k/2} \exp(-\mathscr{X} b_2^2 \theta_2^2 / (a_1 + \theta_1^2 / a_1)) d\theta_1 d\theta_2$$
$$\ll c^{1-k} \sum_{0 \neq b_2 \in \mathbb{Z}} |b_2| \exp(-\mathscr{X} a_1^{-1} b_2^2 / \det T)$$
$$\int_{-\infty}^{\infty} (\theta_1^2 + a_1^2)^{-k/2} (a_1 + \theta_1^2 / a_1)^{1/2} |b_2|^{-1} d\theta_1$$

$$\ll c^{1-k} \sum_{0\neq m\in\mathbb{Z}} \exp(-\mathscr{X} a_1^{-1} m^2/\det T) a_1^{-k+3/2} \int_{-\infty}^{\infty} (1+x^2)^{(1-k)/2} dx$$

$$\ll c^{1-k} a_1^{-k+3/2} \sum_{m\in\mathbb{Z}} \exp(-\mathscr{X} a_1^{-1} m^2/\det T),$$

by the convergence of the last integral for $k \geq 5/2$,

$$\ll c^{1-k} a_1^{(3/2)-k} (a_1 \det T)^{1/2} \sum_{m\in\mathbb{Z}} \exp(-\mathscr{X}^{-1}\pi^2 a_1 \det T \cdot m^2)$$

(in view of the Poisson summation formula

$$\sum_{m\in\mathbb{Z}} e^{-\pi\lambda m^2} = \frac{1}{\sqrt{\lambda}} \sum_{m\in\mathbb{Z}} e^{-\frac{\pi}{\lambda}m^2}, \quad \text{for } \lambda > 0)$$

$$= c^{1-k} a_1^{2-k} (\det T)^{1/2} \sum_{m\in\mathbb{Z}} \exp(-\pi^2 \mathscr{X}^{-1} a_1 \det T m^2)$$

81 $\ll c^{1-k} a_1^{2-k} (\det T)^{1/2}$, on noting that the last series over m is ≤ 1, since $a_1 \det T = T^{-1}[u_1] \det T$ with $u_1 = {}^t(0\ 1)$ or ${}^t(1\ n)$ with $n = 0, 1, -1$ and, in view of $T^{-1} \asymp \begin{pmatrix} t_1^{-1} & 0 \\ 0 & t_2^{-1} \end{pmatrix} > t_2^{-1} E_2$, $a_1 \det T \gg t_1 \gg 0$. If now, for $c \geq 1$, we define

$$\mathscr{X}(c, U) := \sum_{(d,c)=1} \alpha\left(\begin{pmatrix} c & 0 \\ 0 & 0 \end{pmatrix} {}^t U, \begin{pmatrix} d & 0 \\ 0 & 0 \end{pmatrix} U^{-1}\right),$$

then the above estimate for the sub-series over $d_1 \equiv d (\mathrm{mod}\ \mathrm{cq})$ and summation over d modulo cq together yield the estimate

$$\mathscr{X}(c, U) \ll c^{2-k} a_1^{2-k} (\det T)^{1/2}.$$

Let us note here that $a_1 = T^{-1}\left[\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right] \asymp t_2^{-1}$ and $a_1 = T^{-1}\left[\begin{smallmatrix} 1 \\ n \end{smallmatrix}\right] \asymp t_1^{-1} + n^2 t_2^{-1}$ with $|n| \leq 1$ corresponding to the respective possibilities for U; in the former case $c \ll \sqrt{t_2/t_1}$ and in the latter case $0 < c \leq 3$. Hence

$$\sum_{1\leq c<\infty} \mathscr{X}\left(c, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\right) \ll \sum_{c \ll \sqrt{t_2/t_1}} c^{2-k} t_2^{k-2} (t_1 t_2)^{1/2}$$

$$= (\min(T))^{2-k} (\det T)^{k-3/2} \sum_{1\leq c\ll\sqrt{t_2/t_1}} c^{2-k}$$

$$\ll (\min(T))^{2-k}(\det T)^{k-3/2} = \begin{cases} 1 & \text{for } k \geq 7/2 \\ \log(t_2/t_1) & \text{for } k = 3 \\ \sqrt[4]{t_2/t_1} & \text{for } k = 5/2 \end{cases}$$

$$\ll \begin{cases} (\min(T))^{2-k}(\det T)^{k-3/2}, \ \text{for } k \geq 7/2 \\ (\min(T))^{2-k}(\det T)^{k-3/2} \log(\sqrt{\det T}/\min(T)), \ \text{for } k = 3 \\ (\min(T))^{2-k}(\det T)^{k-3/2}(\det T)^{1/4}/(\min(T))^{1/2}, \ \text{for } k = 5/2, \end{cases}$$

while **82**

$$\sum_{\substack{1 \leq c \leq 3 \\ |n| \leq 1}} \mathscr{X}(c, U) \ll \sum_{\substack{1 \leq c \leq 3 \\ n=0,1,-1}} c^{2-k}(t_1^{-1} + n^2 t_2^{-1})^{2-k}(\det T)^{1/2}$$
$$\ll t_1^{k-2}(t_1 t_2)^{1/2} = (\det T)^{k-3/2} t_2^{2-k}$$
$$\ll (\det T)^{k-3/2}(\min(T))^{2-k}, \ \text{since } t_2/t_1 \gg 1 \text{ and } k \geq 5/2.$$

These estimates prove Proposition 1.4.14 immediately.

Remark. The case of $U = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ is troublesome. If $f_1 \neq 0$, then $f_1 = 1 \leq c \leq 3$ and $a_1 \gg 1/t_1$,

$$\mathscr{X}\left(c, \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix}\right) \ll \int\limits_{\theta_1^2 + a_1^2 \ll 1/\det T} (\theta_1^2 + a_1^2)^{-k/2} d\theta_1$$

(from Lemma 1.4.19 and since

$\det \operatorname{Im} \tau = \det \operatorname{Im}(M < X + iT^{-1} >) \gg 1)$

$$= a_1^{1-k} \int\limits_{x^2+1 \ll 1/(a_1^2 \det T)(\ll (t_1/t_2) \ll 1)} (x^2+1)^{-k/2} dx$$
$$\ll t_1^{k-1}.$$

1.5 Generalization of Kloosterman's Method to the Case of Degree 2

83

In this section, we generalize Theorem 1.1.2 to the case of modular forms of degree 2 whose constant term vanishes at every cusp. But our result is conditional because we do not have a good estimate for a generalized Wey1 sum.

Let k, q be natural numbers with $k \geq 3$ and $f(z) = \sum\limits_{0 \leq p \in \Lambda_2^*} a(P)$ $e(\operatorname{tr} PZ)$ be a Siegel modular form of degree 2, weight k and level q whose constant term vanishes at every cusp, and in addition we require $f|M = f$ for every $M \in \Gamma_2(q)$. As before, we fix an M-reduced positive definite matrix T whose minimum is larger than an absolute constant $\mathscr{X}$ fixed later.

Let $\mathscr{F} = \mathscr{F}_2$ be a fundamental domain as in § 1.4 and $\mathscr{F}_0$ be a subset of $\mathscr{F}$ such that for every point in $\mathscr{G}_2$ there is a unique point in $\mathscr{F}_0$ which is mapped by Γ_2. Put $\mathfrak{g} = \bigcup\limits_{M \in \Gamma_{2,\infty}} M < \mathscr{F}_0 >$ and for $\mathfrak{t} := \{X \in \mathscr{M}_2(\mathbb{R}) | 0 \leq x_{ij} = x_{ji} < q (1 \leq i, j \leq 2)\}$ and $M \in \Gamma_2 \beta(M) := \{X \in \mathfrak{t} | M < X + iT^{-1} > \in \mathfrak{g}\}$.

Lemma 1.5.1. $\mathfrak{t} = \bigcup\limits_{\substack{M \in \Gamma_{2,\infty} \backslash \Gamma_2 \\ M \notin \Gamma_{2,\infty}}} \beta(M)$ *and the measure of*

$$\beta(M_1) \cap \beta(M_2) \textit{ equals } 0 \textit{ if } \Gamma_{2,\infty} M_1 \neq \Gamma_{2,\infty} M_2.$$

84 *Proof.* The first assertions is clear. Suppose $X \in \beta(M_1) \cap \beta(M_2)$. Then we have $N_1, N_2 \in \Gamma_{2,\infty}$ such that $N_j M_j < X + iT^{-1} > \varepsilon \mathscr{F}_0$. By definition of $\mathscr{F}_0$, we obtain $N_1 M_1 < X + iT^{-1} >= N_2 M_2 < X + iT^{-1} >$ and hence $(N_2 M_2)^{-1} N_1 M_1 < X + iT^{-1} >= X + iT^{-1}$. Thus $\beta(M_1) \cap \beta(M_2)$ is covered by a countable union of fixed points of the above type. If the measure of $\beta(M_1) \cap \beta(M_2)$ is not zero, then the above equation for some $N_1, N_2 \in \Gamma_{2,\infty}$ is trivial in X and hence $(N_2 M_2)^{-1} N_1 M_1 = \pm B_2$. This implies $\Gamma_{2,\infty} M_1 = \Gamma_{2,\infty} M_2$. □

Remark . As noted after Lemma 1.4.2, this lemma holds without the replacement of $\mathscr{F}$ by $\mathscr{F}_0$. But the proof is lengthy.

Lemma 1.5.2. *Let $C, D \in \mathscr{M}_2(\mathbb{Z})$ be a symmetric coprime pair with* $\det C \neq 0$*. Then there exists $A \in \mathscr{M}_2(\mathbb{Z})$ such that $\begin{pmatrix} A & * \\ C & D \end{pmatrix} \in \Gamma_2$ with* $(\det A, q) = 1$.

Proof. Since C, D is a coprime symmetric pair, there exists $A \in \mathscr{M}_2(\mathbb{Z})$ with $\begin{pmatrix} A & * \\ C & D \end{pmatrix} \in \Gamma_2$. Since $\begin{pmatrix} E_2 & S \\ 0 & E_2 \end{pmatrix} \begin{pmatrix} A & * \\ C & D \end{pmatrix} = \begin{pmatrix} A+SC & * \\ C & D \end{pmatrix}$, we have only to prove, for any prime p, $\det(A + SC) \not\equiv 0 \bmod p$ for some integral symmetric matrix S by using the Chinese remainder theorem. Let $c_1|c_2$ be elementary divisors of C and $UCV = [c_1, c_2] = \tilde{C}$ for U, $V \in GL_2(\mathbb{Z})$. Put ${}^tU^{-1}AV = \left(\begin{smallmatrix} a_1 & a_2 \\ a_3 & a_4 \end{smallmatrix}\right) = \tilde{A}$ and $S[U^{-1}] = \left(\begin{smallmatrix} s_1 & s_2 \\ s_2 & s_4 \end{smallmatrix}\right)$; then we have $\det(A + SC) = \det(UV) \left|\begin{smallmatrix} a_1+s_1c_1 & a_2+s_2c_2 \\ a_3+s_2c_1 & a_4+s_4c_2 \end{smallmatrix}\right| =$

$$\pm(a_1a_4 - a_2a_3 + s_4c_2(a_1 + s_1c_1) + a_4c_1s_1 - a_3c_2s_2 - c_1a_2s_2 - c_1c_2s_2^2).$$

We suppose that this is congruent to $0 \bmod p$ for every s_1, s_2, $s_4 \in \mathbb{Z}$. Then $a_1a_4 - a_2a_3$, c_2a_1, c_2c_1, a_4c_1, $a_3c_2 + c_1a_2$ are obviously congruent **85**
to $0 \bmod p$. Since ${}^tAC$ is symmetric, $a_3c_2 + c_1a_2 = 2c_1a_2$ follows. If p does not divide $c_1a_2 = a_3c_2$, then $p \nmid c_1c_2$. Thus c_1a_2 and so the determinant of every $(2, 2)$ submatrix of $({}^t\tilde{A}, {}^t\tilde{C})$ is divisible by p. This contradicts $({}^t\tilde{A}, {}^t\tilde{C})$ being primitive. □

Lemma 1.5.3. *Let C, D' be a symmetric coprime pair with* $\det C \neq 0$. *Then*

(i) *there exists* $\left(\begin{smallmatrix} A' & B' \\ C & D' \end{smallmatrix}\right) \in \Gamma_2$ *with* $(\det A', q) = 1$,

(ii) *for $D \in \mathscr{M}_2(\mathbb{Z})$ such that C, D form a symmetric coprime pair and $D \equiv D' \bmod q$, there exist A, $B \in \mathscr{M}_2(\mathbb{Z})$ such that* $\Gamma_2 \ni \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} A' & B' \\ C & D' \end{smallmatrix}\right) \bmod q$ *and*

(iii) *for $S \in \Lambda_2$ with $CS \equiv 0 \bmod q$, and for A, B, D in* (ii),

$$\Gamma_2 \ni \begin{pmatrix} A - AS\,{}^tCA & * \\ C & CS + D \end{pmatrix} \equiv \begin{pmatrix} A' & B' \\ C & D' \end{pmatrix} \bmod q.$$

Proof. First, (i) is nothing but the previous lemma.

Suppose $\left(\begin{smallmatrix} \tilde{A} & \tilde{B} \\ C & D \end{smallmatrix}\right) \in \Gamma_2$ for D in (ii); then $\left(\begin{smallmatrix} \tilde{A} & \tilde{B} \\ C & D \end{smallmatrix}\right) \left(\begin{smallmatrix} A' & B' \\ C & D' \end{smallmatrix}\right)^{-1}$

$$= \begin{pmatrix} \tilde{A}{}^tD' - \tilde{B}{}^tC & -\tilde{A}{}^tB' + \tilde{B}{}^tA' \\ C{}^tD' - D{}^tC & -C{}^tB' + D{}^tA' \end{pmatrix} \equiv \begin{pmatrix} E_2 & * \\ 0 & E_2 \end{pmatrix} \bmod q.$$

Thus

$$\begin{pmatrix} A' & B' \\ C & D' \end{pmatrix} \equiv \begin{pmatrix} E_2 & G \\ 0 & E_2 \end{pmatrix} \begin{pmatrix} \tilde{A} & \tilde{B} \\ C & D \end{pmatrix} \bmod q \ \text{ for some } \ G \in \Lambda.$$

Now $A = \tilde{A} + GC$, $B = \tilde{B} + GD$ satisfy the conditions in (ii). 86

Let S be as in (iii). Put

$$M = \begin{pmatrix} E_2 & -AS^tA \\ 0 & E_2 \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} E_2 & S \\ 0 & E_2 \end{pmatrix};$$

then it is easy to see

$$M = \begin{pmatrix} A - AS^tAC & AS(E_2 - {}^tAD) - AS^tACS + B \\ C & CS + D \end{pmatrix} \in \Gamma_2.$$

Further $S^tAC = S^tCA = {}^t(CS)A \equiv 0 \bmod \mathrm{q}$ and $S(E_2 - {}^tAD) = -S^tCB = -{}^t(CS)B \equiv 0 \bmod \mathrm{q}$ imply (iii). ◻

Lemma 1.5.4. *Let* $\begin{pmatrix} A' & B' \\ C & D' \end{pmatrix} \in \Gamma_2$ *with* $(\det A', q) = 1$ *and* $\det C \neq 0$. *Then we have*

$$\bigcup_{\tilde{D}} \Gamma_{2,\infty} \begin{pmatrix} * & * \\ C & \tilde{D} \end{pmatrix} = \bigcup_{D \in \mathscr{D}} \bigcup_{S \in \Lambda(C,q)} \Gamma_{2,\infty} \begin{pmatrix} A - AS^tCA & * \\ C & CS + D \end{pmatrix}.$$

where $\tilde{D}$ *runs over* $\tilde{D} \in \mathscr{M}_2(\mathbb{Z})$ *such that* $\tilde{D} \equiv D' \bmod \mathrm{q}$ *and* $(C, \tilde{D})$ *is a symmetric coprime pair,* $S \in \Lambda(C, q) := \{S = {}^tS \in \Lambda_2 | CS \equiv 0 \bmod \mathrm{q}\}$ *and* $\mathscr{D} := \{D \in \mathscr{M}_2(\mathbb{Z}) \bmod \mathrm{C}\Lambda(\mathrm{C}, \mathrm{q}) | (\mathrm{C}, \mathrm{D})$ *is a symmetric coprime pair and* $D \equiv D' \bmod \mathrm{q}\}$, *and coset representatives on the right are congruent to* $\begin{pmatrix} A' & B' \\ C & D' \end{pmatrix} \bmod \mathrm{q}$ *for some* $A \in \mathscr{M}_2(\mathbb{Z})$ *with* $\Gamma_2 \ni \begin{pmatrix} A & B \\ C & D \end{pmatrix} \equiv \begin{pmatrix} A' & B' \\ C & D' \end{pmatrix} \bmod \mathrm{q}$.

Proof. By the previous lemma, for $\tilde{D}$ above, there exists $\begin{pmatrix} \tilde{A} & \tilde{B} \\ C & \tilde{D} \end{pmatrix} \in \Gamma_2$, which is congruent to $\begin{pmatrix} A' & B' \\ C & D' \end{pmatrix} \bmod \mathrm{q} \cdot \mathscr{D}$ is a set of representatives of such $\tilde{D}$ modulo $C\Lambda(C, q)$, and so the rest follows from the previous lemma. ◻

Lemma 1.5.5. *Let* A, $C \in \mathscr{M}_2(\mathbb{Z})$ *satisfying* ${}^tAC = {}^tCA$, *det* $C \neq 0$,

87 $(\det A, q) = 1$. *Then, for* $P \in \Lambda_2^*$, *we have*

$$\sum_{S \in \Lambda(c,q) \bmod \mathrm{q}\Lambda} e(tr\ PAS\,{}^tA/q) = \begin{cases} [\Lambda(c, q) : q\Lambda] & \text{if } \boxed{*} \\ 0 & \text{otherwise,} \end{cases}$$

where the condition $\lceil * \rceil$ *on P is as follows:*

$$\lceil * \rceil : \operatorname{tr}(PS) \equiv 0 \bmod \mathrm{q} \ \ \textit{for every} \ \ \mathrm{S} \in \Lambda({}^t\mathrm{C}, \mathrm{q}),$$
$$\textit{i.e.} \ \ S \in \Lambda \ \ \textit{with} \ \ {}^tCS \equiv 0 \bmod \mathrm{q}.$$

Proof. It is clear that we have only to prove that the condition $\lceil * \rceil$ is equal to $\operatorname{tr}(PAS{}^tA) \equiv 0 \bmod \mathrm{q}$ for every $S \in \Lambda(C, q)$. Since $(\det A, q) = 1$, for $S \in \Lambda$ we have $S \in \Lambda(C, q) \Longleftrightarrow CS \equiv 0 (\bmod \mathrm{q}) \Longleftrightarrow$

$${}^tACS{}^tA \equiv 0 \bmod \mathrm{q} \Longleftrightarrow {}^\mathrm{t}\mathrm{CAS}{}^\mathrm{t}\mathrm{A} \equiv 0 \bmod \mathrm{q} \Longleftrightarrow \mathrm{AS}{}^\mathrm{t}\mathrm{A} \in \Lambda({}^\mathrm{t}\mathrm{C}, \mathrm{q}).$$

Since $S \equiv A(A_1 S{}^tA_1){}^tA \bmod \mathrm{q}$ for $A_1 \in \mathscr{M}_2(\mathbb{Z})$ with $AA_1 \equiv A_1A \equiv E_2 \bmod \mathrm{q}$, $AS{}^tA$ runs over $\Lambda({}^tC, q) \bmod \mathrm{q}\Lambda$ along with $S \in \Lambda(C, q)$. Thus we have proved the equality of two conditions. ◻

The following two propositions are proved at the end, in this section.

Proposition 1.5.6. *Let* $\left(\begin{smallmatrix} A' & B' \\ C & D' \end{smallmatrix}\right) \in \Gamma_2$ *with* $\det C \neq 0$, $(\det A', q) = 1$, *and* $P, G, T \in \Lambda^*$. *Suppose that p satisfies the condition* $\lceil * \rceil$ *in Lemma 1.5.5. We denote by* $S(G, P, T, C, \left(\begin{smallmatrix} A' & B' \\ C & D' \end{smallmatrix}\right))$ *the exponential sum*

$$\sum_{D \in \mathscr{D}} e(\operatorname{tr}(AC^{-1}(G + Pq^{-1}) + TC^{-1}D).$$

where A, D, $\mathscr{D}$ *are the same as in Lemma 1.5.4. Then we have* **88**

$$S(G, P, T, C, \begin{pmatrix} A' & B' \\ C & D' \end{pmatrix}) = O(c_1^2 c_2^{1/2+\varepsilon}(c_2, t)^{1/2}) \ \ \textit{for any} \ \ \varepsilon > 0,$$

where

$$C = U^{-1}\begin{pmatrix} c_1 & 0 \\ 0 & c_2 \end{pmatrix} V^{-1}, U, V \in GL_2(\mathbb{Z}), 0 < c_1 | c_2, T[V] = \begin{pmatrix} * & * \\ * & t \end{pmatrix}.$$

The implied constant depends only on q.

Proposition 1.5.7. *Let n be a natural number and* $S = \{{}^t(bd) | b, d \epsilon \mathbb{Z}$, $(b, d) = 1\}$. *We introduce the equivalence relation* ${}^t(b, d) \sim {}^t(b', d')$

by ${}^t(b\ \ d) \equiv w^t(b'd')\bmod \mathrm{n}$ *for some* $w \in \mathbb{Z}$, *with* $(w, n) = 1$ *and put* $S(n) = S/\sim$. *Then, for* $T = (t_{ij}) \in \Lambda_2^*$, *we have*

$$\sum_{S(n)\ni x} (T[x], n)^{1/2} = O(n^{1+\varepsilon}(e(T), n)^{1/2}) \text{ for any } \varepsilon > 0,$$

where $e(T) = (t_{11}, t_{22}, 2t_{12})$.

As before we *put, for* $M = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma_2$,

$$\alpha(M) = \alpha(C, D) := \int\limits_{\beta(M)} f(X + iT^{-1})e(-\operatorname{tr}(TX)dX.$$

Then we have

$$a(T) = e^{4\pi}a^{-3}\left\{\sum_{\substack{M\in\Gamma_{2,\infty}\backslash\Gamma_2 \\ \operatorname{rank} C=2}} \alpha(C, D) + \sum_{\substack{M\in\Gamma_{2,\infty}\backslash\Gamma_2 \\ \operatorname{rank} C=1}} \alpha(C, D)\right\}$$

Let $C \in \mathscr{M}_2(\mathbb{Z})$ with $\det C \neq 0$. For $S = {}^tS \in \mathscr{M}_2(\mathbb{Q})$ with $SC \in \mathscr{M}_2(\mathbb{Z})$ and for $W \in \mathscr{G}_2$, we put

$$g(S, C; W) = \begin{cases} 1 & \text{if } S + W \in \mathfrak{g}, \\ 0 & \text{otherwise.} \end{cases}$$

89 Then $g(S, C; W)$ has the Fourier expansion

$$\sum_{G\in\Lambda^*/\gamma(C)} b(G, C; W)e(\operatorname{tr}(SG)),$$

where $\gamma(C) := \{G \in \Lambda^* | \operatorname{tr}(SG) \in \mathbb{Z}$ for every $S = {}^tS \in \mathscr{M}_2(\mathbb{Q})$ with $SC \in \mathscr{M}_2(\mathbb{Z})\}$ and $b(G, C; W) = [\Lambda^* : \gamma(C)]^{-1} \sum\limits_S e(-\operatorname{tr}(SG))g(S, C; W)$ where S runs over $\{S = {}^tS \in \mathscr{M}_2(\mathbb{Q})\bmod \Lambda | \mathrm{SC} \in \mathscr{M}_2(\mathbb{Z})\}$. Now we have

Lemma 1.5.8. *Let* (C, D') *be a symmetric coprime pair with* $\det C \neq 0$. *Then we have*

$$\sum_D \alpha(C, D) = [\Lambda(c, q) : q\Lambda] \det c^{-k}$$

$$\int\limits_{\min(\operatorname{Im}\tau)\geq\sqrt{3}/2} \det(\theta+iT^{-1})^{-k}\sum_{0\leq P\in\Lambda^*} a'(P)e(\operatorname{tr}(P\tau)/q)\times$$
$$\times\, e(-\operatorname{tr}(T\theta))\sum_{G\in\Lambda^*/\gamma(C)} b(G,C;\tau)S(G,P,T,C,\begin{pmatrix}A' & B'\\ C & D'\end{pmatrix})d\theta$$

where D runs over $\{D\equiv D'\bmod q|\mathrm{C},\ D$ *are symmetric and coprime*$\}$, $\tau=\tau(\theta,C)=-{}^tC^{-1}(\theta+iT^{-1})^{-1}C^{-1}$, *and* $\left(\begin{smallmatrix}A' & B'\\ C & D'\end{smallmatrix}\right)\in\Gamma_2$ *with* $(\det A',q)=1$, *and $a'(P)$ are Fourier coefficients of*

$$f|\begin{pmatrix}A' & B'\\ C & D'\end{pmatrix}(Z)=\det(CZ+D')^{-k}f(A'Z+B')(CZ+D')^{-1})$$
$$=\sum a'(P)e(\operatorname{tr}(PZ/q)).$$

Proof. By Lemma 1.5.2, there exists $\left(\begin{smallmatrix}A' & B'\\ C & D'\end{smallmatrix}\right)\in\Gamma_2$ with $(\det A',q)=1$ and we put $f|\left(\begin{smallmatrix}A' & B'\\ C & D'\end{smallmatrix}\right)^{-1}(Z)=\sum a'(P)e(\operatorname{tr}PZ/q)$. For $D\in\mathscr{M}_2(\mathbb{Z})$ such that (C,D) is a symmetric coprime pair and $D\equiv D'\bmod q$, there exists $\left(\begin{smallmatrix}A & B\\ C & D\end{smallmatrix}\right)\in\Gamma_2$ with $\left(\begin{smallmatrix}A & B\\ C & D\end{smallmatrix}\right)=\left(\begin{smallmatrix}A' & B'\\ C & D'\end{smallmatrix}\right)\bmod q$. Hence we have $f|\left(\begin{smallmatrix}A & B\\ C & D\end{smallmatrix}\right)^{-1}=$ $f|\left(\begin{smallmatrix}A' & B'\\ C & D'\end{smallmatrix}\right)^{-1}=F$ (say). Then we have $\alpha(C,D)=\int\limits_{\beta(M)}\det(C(X+iT^{-1})+$ **90**
$D)^{-k}F(M<X+iT^{-1}>)e(-\operatorname{tr}(TX))dX$, where $M=\left(\begin{smallmatrix}A & B\\ C & D\end{smallmatrix}\right)$.

Since $\det C\neq 0$, we have $M<Z>=AC^{-1}-{}^tC^{-1}(Z+C^{-1}D)^{-1}C^{-1}$.

Putting $X=\theta-C^{-1}D$, $\tau=-{}^tC^{-1}(\theta+iT^{-1})^{-1}C^{-1}$,

$$\alpha(C,D)=(\det C)^{-k}\int\limits_{\substack{\theta\in\mathfrak{t}+C^{-1}D\\ AC^{-1}+\tau\in\mathfrak{g}}}(\theta+iT^{-1})^{-k}F(AC^{-1}+\tau)$$
$$e(-\operatorname{tr}(T(\theta-C^{-1}D)))d\theta.$$
$$=(\det C)^{-k}\int\limits_{\substack{\theta\in\mathfrak{t}+C^{-1}D\\ AC^{-1}+\tau\in\mathfrak{g}}}(\theta+iT^{-1})^{-k}\sum_{p}a'(P)e(\operatorname{tr}(P\tau)/q)$$
$$e(-\operatorname{tr}(T\theta))\times e(\operatorname{tr}(PAC^{-1}/q+TC^{-1}D))d\theta$$

$$= (\det C)^{-k} \int\limits_{\substack{\theta\in\mathfrak{t}+C^{-1}D \\ \min(\mathrm{Im}(\tau))\geq\sqrt{3}/2}} (\theta + iT^{-1})^{-k} \sum_{P} a'(P)$$

$$e(\mathrm{tr}(P\tau)/q) e(-\mathrm{tr}(T\theta))$$

$$\times \sum_{G\in\Lambda^*/\gamma(C)} b(G, C; \tau) e(\mathrm{tr}(AC^{-1}G + PAC^{-1}/q + TC^{-1}D)) d\theta$$

since $AC^{-1} + \tau \in \mathfrak{g}$ implies $\min(\mathrm{Im}\,\tau) \geq \sqrt{3}/2$. □

Applying Lemma 1.5.4, the sum $\sum\limits_{D} \alpha(C, D)$ referred to is equal to

$$|\det C|^{-k} \sum_{\substack{D\in\mathscr{D} \\ S\in\Lambda(C,q)}} \int\limits_{\substack{\theta\in\mathfrak{t}+C^{-1}D+S \\ \min(\mathrm{Im}\,\tau)\geq\sqrt{3}/2}} (\theta + iT^{-1})^{-k} \sum_{P} a'(P) e(\mathrm{tr}(P\tau)/q) e(-\mathrm{tr}\,T\theta) \times$$

$$\times \sum_{G\in\Lambda^*/\gamma(C)} b(G, C; \tau) e(\tau r((A - AS\,{}^tCA)C^{-1}G + P(A - AS\,{}^tCA)C^{-1}/q +$$

$$+ TC^{-1}(CS + D)) d\theta,$$

91 (noting that $\mathrm{tr}((A-AS\,{}^tCA)C^{-1}G+P(A-AS\,{}^tCA)C^{-1}/q+TC^{-1}(CS+D))$

$$\equiv \mathrm{tr}(AC^{-1}G + PAC^{-1}/q - PAS\,{}^tA/q + TC^{-1}D) \bmod 1$$

since ${}^tCAC^{-1} = {}^tA$,)

$$= (\det C)^{-k} \sum_{\substack{D\in\mathscr{D} \\ S\in\Lambda(C,q)/q\Lambda}} \int\limits_{\min(\mathrm{Im}\,\tau)\geq\sqrt{3}/2} (\theta + iT^{-1})^{-k} \sum a'(P)$$

$$e(\mathrm{tr}(P\tau/q)) e(-\mathrm{tr}(T\theta)) \times \sum_{G\in\Lambda^*/\gamma(C)} b(G, C; \tau) e(\mathrm{tr}(AC^{-1}G$$

$$+ PAC^{-1}/q - PAS\,{}^tA/q + TC^{-1}D)) d\theta$$

$$= [\Lambda(C, q) : q\Lambda] (\det C)^{-k} \int\limits_{\min(\mathrm{Im}\,\tau)\geq\sqrt{3}/2} (\theta + iT^{-1})^{-k}$$

$$\sum_{\lceil * \rceil} a'(P) e(\mathrm{tr}(P\tau/q)) e(-\mathrm{tr}(T\theta) \times$$

$$\sum_{G \in \Lambda^*/\gamma(C)} b(G, C; \tau) S\left(G, P, T, C, \begin{pmatrix} A' & B' \\ C & D' \end{pmatrix}\right) d\theta,$$

which proves our lemma.

Lemma 1.5.9. *Let* $M = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma_2$ *and* $f|M(Z) = \sum a'(P) e(\operatorname{tr}(PZ/q))$. *If* $\underline{\min}(\operatorname{Im} Z) \geq \sqrt{3}/2$, *then* $\sum |a'(P) e(\operatorname{tr}(PZ/q))| = O(\exp(-\mathscr{X}\, \underline{\min}(\operatorname{Im} Z))$ *for some* $\mathscr{X} > 0$.

Proof. Let $\Gamma_2 = \bigcup\limits_i M_i \Gamma_2(q)$ and $f|M_i(Z) = \sum a_i(P) e(\operatorname{tr}(PZ/q))$. Suppose $\operatorname{Im}(Z[U^{-1}])$ is M-reduced for $U \in GL_2(\mathbb{Z})$. Since $f|M\left(\begin{smallmatrix} {}^tU & 0 \\ 0 & U^{-1} \end{smallmatrix}\right) = f|M_i$ for some i, $(\det U)^k a'(P[{}^tU^{-1}]) = a_i(P)$ for every $0 \leq P \in \Lambda^*$, and then we have

$$\begin{aligned}
&\sum |a'(P) e(\operatorname{tr}(PZ/q)| \\
&= \sum |a'(P[{}^tU^{-1}]) e(\operatorname{tr}(PZ[U^{-1}]/q))| \\
&= \sum |a_i(P) e(\operatorname{tr}(PZ[U^{-1}]/q))| \\
&= O(\exp(-\mathscr{X} \min(\operatorname{Im}(Z[U^{-1}])))) \quad \text{(Lemma 1.4.1)} \\
&= O(\exp(-\mathscr{X} \min(\operatorname{Im} Z))).
\end{aligned}$$

This completes the proof, since $[\Gamma : \Gamma(q)] < \infty$. □ **92**

Here we make an assumption, namely

Assumption (*):

$$\sum_{G \in \Lambda^*/\gamma(C)} |b(G, C; \tau)| = O(c_1^{a_1+\varepsilon} c_2^{a_2}) \ \text{ for } \begin{cases} 0 \leq a_1 \leq 3/2 \\ \\ 0 \leq a_2 < 1/2 \end{cases} \quad \text{and any } \varepsilon > 0,$$

where $0 < c_1 | c_2$ are elementary divisors of C and the implied constant is independent of τ.

This is discussed later.

Let $C, D \in \mathscr{M}_2(\mathbb{Z})$ form a symmetric coprime pair with $\det C \neq 0$. Under Assumption $(*)$, we have, by virtue of Lemma 1.5.8, Proposition

1.5.6 and Lemma 1.5.9,

$$\begin{aligned} &|\sum_{D'\equiv D \bmod q} \alpha(C,D')| \\ &\ll |\det C^{-k}| \int\limits_{\min(\operatorname{Im}\tau)\geq\sqrt{3}/2} |\det(\theta+iT^{-1})|^{-k}\exp(-\mathscr{X}\min(\operatorname{Im}\tau))c_{c_2}^{a_1+\varepsilon a_2}\times \\ &c_1^2c_2^{1/2+\varepsilon}(c_2,t)^{1/2}d\theta \end{aligned}$$

where

$$C=U^{-1}\begin{pmatrix} c_1 & 0\\ 0 & c_2\end{pmatrix}V^{-1}, U,V\in GL_2(\mathbb{Z}), 0<c_1|c_2, T[V]=\begin{pmatrix} * & *\\ * & t\end{pmatrix},$$

since

$$\tau=-{}^tC^{-1}(\theta+iT^{-1})^{-1}C^{-1}, \operatorname{Im}\tau=(T[\theta]+T^{-1})^{-1}[C^{-1}],$$

and for $X=\sqrt{T}\theta\sqrt{T}$, we have $d\theta=\det T^{-3/2}dX$. Hence

$$\begin{aligned} &|\sum_{D'\equiv D \bmod q} \alpha(C,D')| \\ &\ll c_1^{a_1+2-k+\varepsilon}c_2^{a_2+1/2-k/\varepsilon}(c_2,t)^{1/2}(\det T)^{k-3/2}\int \det(X^2+1)^{-k/2}\times \\ &\quad\exp(-\mathscr{X}\min((X^2+1)^{-1}[\sqrt{T}C^{-1}]))dX, \\ &\ll c_1^{a_1+2-k+\varepsilon}c_2^{a_2+1/2-k+\varepsilon}(c_2,t)^{1/2}(\det T)^{k-3/2}(\min(T[c^{-1}]))^{1-k/2} \end{aligned}$$

(as for the proof of Proposition 1.4.10).

93 Thus we have proved

Lemma 1.5.10. *Let $C\in\mathscr{M}_2(\mathbb{Z})$ with $\det C\neq 0$. Then we have*

$$\left|\sum_D \alpha(C,D)\right| \ll (\det T)^{k-3/2}c_1^{a_1+2-k+\varepsilon}c_2^{a_2+1/2-k+\varepsilon}$$
$$(c_2,t)^{1/2}(\min(T[C^{-1}]))^{1-k/2}$$

under Assumption $(*)$*, where*

$$C = U^{-1}\begin{pmatrix} c_1 & 0 \\ 0 & c_2 \end{pmatrix} V^{-1}, U, V \in GL_2(\mathbb{Z}) 0 < c_1/c_2$$

and $T[V] = \left(\begin{smallmatrix} * & * \\ * & t \end{smallmatrix}\right)$.

For the above C, $\min(T[C^{-1}]) = \min(T[V\begin{pmatrix} c_1^{-1} & 0 \\ 0 & c_2^{-1} \end{pmatrix}]) = c_2^{-2}$ $\min T[V\begin{pmatrix} c_2/c_1 & 0 \\ 0 & 1 \end{pmatrix}] > c_2^{-2}\min(T)$ holds. In the decomposition $C = U^{-1}$ $\begin{pmatrix} c_1 & 0 \\ 0 & c_2 \end{pmatrix} V^{-1}$, V is uniquely determined in

$$GL_2(\mathbb{Z}) / \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z}) | b \equiv 0 \operatorname{mod} \mathrm{c}_2/\mathrm{c}_1 \right\}$$

so we have a bijection $V = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto^t (b\ d) \in S(c_2/c_1)$ defined in Proposition 1.5.7 and $(c_2, t) \leq c_1(c_2/c_1, t)$.

Thus we have, by Proposition 1.5.7.

Lemma 1.5.11. *Let* $0 < c_1 | c_2$*. Then, under Assumption* $(*)$*,*

$$\begin{aligned} |\sum \alpha(C, D)| \ll (\det T)^{k-3/2} c_1^{a_1+5/2-k+\varepsilon} c_2^{a_2+1/2-k+\varepsilon} \\ (c_2/c_1)^{1+2\varepsilon}(e(T), c_2/c_1)^{1/2} \times \\ \times \begin{cases} 1, \\ (c_2^{-2}\min T)^{1-k/2} & \text{for any } \varepsilon > 0 \end{cases} \end{aligned}$$

where C runs over representatives of left cosets by $GL_2(\mathbb{Z})$ of integral matrices with elementary divisors c_1, c_2, and D runs over all possible D with $\left(\begin{smallmatrix} * & * \\ C & D \end{smallmatrix}\right) \in \Gamma_2$. **94**

Now we can prove

Proposition 1.5.12. *Under Assumption* $(*)$ *we have, for any* $\varepsilon > 0$*,*

$$|\sum_{\operatorname{rank} C = 2} \alpha(C, D)| \ll (\min T)^{a|2+k/4-k/2+\varepsilon} (\det T)^{k-3/2}$$

if $\min(T) > \mathscr{X}$ *(= an absolute constant > 0) and* $k \geq 3$.

Remark. Since $a_2 < 1/2$, $a_2/2 + 5/4 - k/2 < 0$ and so $a_2/2 + 5/4 - k/2 + \varepsilon < 0$ for a sufficiently small positive ε.

Proof. Decompose the sum $|\sum \alpha(C,D)|$ as

$$|\sum_{c_2<(\min(T))^{1/2}} \alpha(C,D)| + |\sum_{c_2\geq(\min(T))^{1/2}} \alpha(C,D)| = \sum_1 + \sum_2 \quad \text{(say)}.$$

By virtue of Lemma 1.5.11, we have

$$\begin{aligned}
(\det T)^{3/2-k}\sum_1 &\ll \sum_{c_1|c_2<(\min(T))^{1/2}} c_1^{a_1+5/2-k+\varepsilon} c_2^{a_2+1/2-k+\varepsilon}(c_2/c_1)^{1+2\varepsilon}\\
&\qquad (e(T), c_2/c_1)^{1/2}(c_2^{-2}\min T)^{1-k/2}\\
&= (\min(T))^{1-k/2} \sum_{c_1|c_2<(\min(T))^{1/2}} c_1^{a_1+a_2+1-k+2\varepsilon}\\
&\qquad (c_2/c_1)^{a_2-1/2+3\varepsilon}(e(T), c_2/c_1)^{1/2}\\
&\leq (\min(T))^{1-k/2} \sum_{\substack{n,m\geq 1\\ nm<(\min(T))^{1/2}}} n^{a_1+a_2+1-k+2\varepsilon}\\
&\qquad m^{a_2-1/2+3\varepsilon}(e(T), m)^{1/2}.
\end{aligned}$$

95 The sum over m does not exceed

$$\begin{aligned}
&\sum_{r|e(T)} r^{1/2} \sum_{s<(\min(T))^{1/2}/nr} (sr)^{a_2-1/2+3\varepsilon}\\
&< \sum_{r|e(T)} r^{a_2+3\varepsilon} \sum_{s<(\min(T))^{1/2}/nr} s^{a_2-1/2+3\varepsilon}\\
&\ll \sum_{r|e(T)} r^{a_2+3\varepsilon}((\min(T))^{1/2}/nr)^{a_2+1/2+3\varepsilon} \quad (\text{since } a_2 + 1/2 + 3\varepsilon > 0)\\
&= (\min(T))^{a_2/2+1/4+3\varepsilon/2} n^{-a_2-1/2-3\varepsilon} \sum_{r|e(T)} r^{-1/2}\\
&\leqq (\min(T))^{a_2/2+1/4+3\varepsilon/2} n^{-a_2-1/2-3\varepsilon} \sum_{r|e(T)^1}\\
&\ll (\min(T))^{a_2/2+1/4+2\varepsilon} n^{-a_2-1/2-3\varepsilon} \quad (\text{since } e(T) \leq \min(T)).
\end{aligned}$$

Thus we have

$$
\begin{aligned}
(\det T)^{3/2-k}\sum_{1} &\ll (\min T)^{a_2/2+5/4-k/2+2\varepsilon}\sum_{n\geq 1} n^{a_1+1/2-k-\varepsilon}\\
&\ll (\min T)^{a_2/2+5/4-k/2+2\varepsilon} \quad (\text{since } \ a_1+1/2-k\leq -1).
\end{aligned}
$$

Similarly, we have

$$
\begin{aligned}
(\det T)^{3/2-k}\sum_{2} \ll &\sum_{\substack{c_1|c_2\\ c_2\geq(\min(T))^{1/2}}} c_1^{a_1+5/2-k+\varepsilon}c_2^{a_2+1/2-k+\varepsilon}\\
&(c_2/c_1)^{1+2\varepsilon}(e(T),c_2/c_1)^{1/2}\\
= &\sum_{\substack{c_1|c_2\\ c_2\geq(\min(T))^{1/2}}} c_1^{a_1+a_2+3-2k+2\varepsilon}(c_2/c_1)^{a_2+3/2-k+3\varepsilon}(e(T),c_2/c_1)^{1/2}\\
= &\sum_{\substack{n,m\geq 1\\ nm\geq(\min(T))^{1/2}}} n^{a_1+a_2+3-2k+2\varepsilon}m^{a_2+3/2-k+3\varepsilon}(e(T),m)^{1/2}.
\end{aligned}
$$

The sum over m is less than **96**

$$
\begin{aligned}
&\sum_{r|e(T)}\ \sum_{s\geq(\min(T))^{1/2}/(nr)} (sr)^{a_2+3/2-k+3\varepsilon}r^{1/2}\\
&= \sum_{r|e(T)} r^{a_2+2-k+3\varepsilon}\sum_{s\geq(\min(T))^{1/2}/(nr)} s^{a_2+3/2-k+3\varepsilon}\\
&\ll \sum_{r|e(T)} r^{a_2+2-k+3\varepsilon}((\min(T))^{1/2}/nr)^{a_2+5/2-k+3\varepsilon}\\
&\qquad (\text{since } \ a_2+5/2-k+3\varepsilon<0 \ \text{ for small } \ \varepsilon>0)\\
&= (\min(T))^{a_2/2+5/4-k/2+(3/2)\varepsilon}n^{-a_2-5/2+k-3\varepsilon}\sum_{r|e(T)} r^{-1/2}\\
&\ll (\min(T))^{a_2/2+5/4-k/2+2\varepsilon}n^{-a_2-5/2+k-3\varepsilon}.
\end{aligned}
$$

Thus we have

$$
(\det T)^{3/2-k}\sum_{2} \ll (\min(T))^{a_2/2+5/4-k/2+2\varepsilon}\sum_{n\geq 1} n^{a_1+1/2-k-\varepsilon}
$$

$$\ll (\min(T))^{a_2/2+5/4-k/2+2\varepsilon}$$

□

The proof of Proposition 1.5.12 is complete, but for the proof of Proposition 1.5.6 and 1.5.7.

Remark on Assumption (*). Let $C = U^{-1}\begin{pmatrix} c_1 & 0 \\ 0 & c_2 \end{pmatrix} V^{-1}$ with U, $V \in GL_2(\mathbb{Z})$, $0 \leq c_1 | c_2$, and put $C' = \begin{pmatrix} c_1 & 0 \\ 0 & c_2 \end{pmatrix}$. Then

$$\begin{aligned}
\gamma(C') &= \{G \in \Lambda^* |\, \mathrm{tr}(SG) \in \mathbb{Z} \ \text{ for every } \ S \\
&= {}^tS \in \mathscr{M}_2(\mathbb{Q}) \ \text{ with } \ SC' \in \mathscr{M}_2(\mathbb{Z})\} \\
&= \{G \in \Lambda^* |\, \mathrm{tr}(SG) \in \mathbb{Z} \text{ for every} \\
&\qquad S = {}^tS \in \mathscr{M}_2(\mathbb{Q}) \ \text{ with } \ S[U]C \in \mathscr{M}_2(\mathbb{Z})\} \\
&= \gamma(C)[{}^tU].
\end{aligned}$$

97 Hence

$$\begin{aligned}
b(G, C; W) &= [\Lambda^* : \gamma(C')]^{-1} \sum_{\substack{{}^tS = S \bmod \Lambda \\ SC \in \mathscr{M}_2(\mathbb{Z})}} e(-\mathrm{tr}(SG)) g(S, C; W) \\
&= [\Lambda^* \gamma(C')]^{-1} \sum_{\substack{S \bmod \Lambda \\ SC' \in \mathscr{M}_2(\mathbb{Z})}} e(-\mathrm{tr}(S[U]G)) g(S[U], C; W) \\
&= [\Lambda^* : \gamma(C')]^{-1} \sum_{S} e(-\mathrm{tr}(SG[{}^tU])) g(S, C'; W[U^{-1}]) \\
&= b(G[{}^tU], C'; W[U^{-1}]).
\end{aligned}$$

Thus we obtain

$$\sum_{G \in \Lambda^*/\gamma(C)} |b(G, C; \tau)| = \sum_{G \in \Lambda^*/\gamma(C')} |b(G, C' : \tau[U^{-1}])|.$$

For $S = \begin{pmatrix} s_1 & s_2 \\ s_2 & s_4 \end{pmatrix}$, it is clear that $SC' \in \mathscr{M}_2(\mathbb{Z})$ if and only if $s_1 = u_1/c_1$, $s_2 = u_2/c_1$, $s_4 = u_4/c_2$ for u_1, u_2, $u_4 \in \mathbb{Z}$.

For $G = \begin{pmatrix} g_1 & g_2/2 \\ g_2/2 & g_4 \end{pmatrix}$, $G \in \gamma(C')$ if and only if $c_1|g_1$, $c_1|g_1$, $c_1|g_2$, $c_2|g_4$. Hence we have

$$\sum_{G \in \Lambda^*/\gamma(C)} |b(G, C; \tau)|$$

$$= \sum_{\substack{g_1,g_2 \bmod c_1 \\ g_4 \bmod c_2}} c_1^{-2}c_2^{-1}\left|\sum_{\substack{u_1,u_2 \bmod c_1 \\ u_4 \bmod c_2 \\ \begin{pmatrix} u_1/c_1 & u_2/c_1 \\ u_2/c_1 & u_4/c_2\end{pmatrix}+\tau[U^{-1}]\in\mathfrak{g}}} e(u_1g_1/c_1 + u_2g_2/c_1 + u_4g_4/c_2)\right|.$$

Thus Assumption (∗) is the same as 98

$$(\sharp) \sum_{\substack{g_1,g_2 \bmod c_1 \\ g_4 \bmod c_2}}\left|\sum_{\substack{u_1,u_2 \bmod c_1 \\ u_4 \bmod c_2}} e((u_1g_1 + u_2g_2)/c_1 + u_4g_4/c_2)\right| = O(c_1^{2+a_1+\epsilon}c_2^{1+a_2})$$

$$\text{for } 0 < c_1|c_2 \text{ and any } \varepsilon > 0 \qquad \begin{pmatrix} u_1/c_1 & u_2/c_1 \\ u_2/c_1 & u_4/c_2\end{pmatrix} + W \in \mathfrak{g}$$

where $0 \le a_1 \le 3/2$, $0 \le a_2 < 1/2$ and the implied constant is independent of c_1, c_2, W.

Using Schwarz's inequality, the left hand side does not exceed

$$\sqrt{c_1^2c_2}\sqrt{\sum_{g_1,g_2,g_4}|\sum\ldots|^2} = \sqrt{c_1^2c_2}\sqrt{c_1^2c_2\sum 1_{\begin{pmatrix} u_1/c_1 & u_2/c_1 \\ u_2/c_1 & u_4/c_2\end{pmatrix}+W\in\mathfrak{g}}} \le c_1^3c_2^{3/2}.$$

Hence Assumption (∗) is true once we get a sharper estimate than the estimate via Schwarz's inequality. (cf. Remarks before the proof of (6) on page 21).

The left hand side of (♯) does not exceed

$$\sum_{u_1,u_2,g_1,g_2 \bmod c_1}\left\{\sum_{g_4 \bmod c_2}\left|\sum_{\substack{u_4 \bmod c_4 \\ \begin{pmatrix} u_1/c_1 & u_2/c_1 \\ u_2/c_1 & u_4/c_2\end{pmatrix}+W\in\mathfrak{g}}} e(u_4g_4/c_2)\right|\right\}.$$

Suppose the sum inside the curly brackets is $O(c_2^{3/2-\delta})$ for some $\delta > 0$ 99
(Actually it is $O(c_2^{3/2})$, from Schwarz's inequality); then Assumption (∗) holds for $a_1 = 3/2$, $a_2 = 1/2 - \delta/2$.

(**Proof.** If $c_2^\delta = O(c_1)$, then $c_1^3c_2^{3/2}/(c_1^{7/2}c_2^{3/2-\delta/2}) = c_1^{-1/2}c_2^{\delta/2} = O(1)$. If $c_1 = O(c_2^\delta)$, then $c_1^4c_2^{3/2-\delta}/(c_1^{7/2}c_2^{3/2-\delta/2}) = c_1^{1/2}c_2^{-\delta/2} = O(1)$.)

Combining Proposition 1.5.12 with Proposition 1.4.14, we have

Theorem 1.5.13. *Let* $f(z) = \Sigma a(T)e(\mathrm{tr}(TZ/q))$ *be a Siegel modular form fo (degree* 2*), level* q*, weight* $k = 3$ *and with zero as the constant term at all cusps. Then for* $T > 0$ *and* $\min T > \mathscr{X}$ (= absolute constant)

$$a(T) = O(((\min(T))^{a_2/2-1/4+\varepsilon} + (\min(T))^{-1} \log \frac{\sqrt{\det T}\min(T)}{)} \det T^{3/2})$$

under Assumption $(*)$.

Remark. If $\sqrt{\det T} = O(\min(T))$, then the above implies

$$a(T)/\det T^{3/2} \to 0 \ \text{ as } \ \min(T) \to \infty.$$

It remains to prove Proposition 1.5.6 and 1.5.7.

For P, $T \in \Lambda^*$ and $C \in \mathscr{M}_2(\mathbb{Z})$ with $\det C \neq 0$, we put

$$K(P, T; C) = \sum_D e(\mathrm{tr}(AC^{-1}P + C^{-1}DT)),$$

where D runs over the set $\{D \mathrm{mod}\ \mathrm{C}\Lambda | (\mathrm{C}, \mathrm{D})$ a symmetric coprime pair$\}$ and A is an integral matrix such that $\begin{pmatrix} A & * \\ C & D \end{pmatrix} \in \Gamma_2$. Another possible A is of the form $A + SC$, $S \in \Lambda_2$. Thus the generalized Kloosterman sum
100 $K(P, T; C)$ is well defined. To prove Proposition 1.5.6, we show that

i) $S(G, P, T, C, \begin{pmatrix} A' & B' \\ C & D' \end{pmatrix})$ is reduced to the sum of $K(P, T; C)$

ii) the same estimate for $K(P, T; C)$ holds as well as for $S(\cdot\cdot)$.

Reduction from $S(\cdot\cdot)$ to $K(\cdot\cdot)$

R1) The exponential sum $S(G, P, T, C, \begin{pmatrix} A' & B' \\ C & D' \end{pmatrix})$ is well-defined.

Proof. Suppose that

$$\begin{pmatrix} A_1 & B_1 \\ C & D_1 \end{pmatrix} \equiv \begin{pmatrix} A_2 & B_2 \\ C & D_2 \end{pmatrix} \mathrm{mod}\ \mathrm{q} \ \text{ and } \ \mathrm{D}_1 \equiv \mathrm{D}_2 \mathrm{mod}\ \mathrm{C}\Lambda(\mathrm{C}, \mathrm{q}).$$

There exists $S \in \Lambda$ such that $D_1 = D_2 + CS$ and $CS \equiv 0 \mathrm{mod}\ \mathrm{q}$, and then there exists $S_1 \in \Lambda$ such that

$$\begin{pmatrix} A_1 & B_1 \\ C & D_1 \end{pmatrix} = \begin{pmatrix} E_2 & S_1 \\ 0 & E_2 \end{pmatrix} \begin{pmatrix} A_2 & B_2 \\ C & D_2 \end{pmatrix} \begin{pmatrix} E_2 & S \\ 0 & E_2 \end{pmatrix}$$

and we have $A_1 = A_2 + S_1 C$. Hence $\mathrm{tr}(A_1 C^{-1}(G + Pq^{-1}) + TC^{-1} D_1) - \mathrm{tr}(A_2 C^{-1}(G + Pq^{-1}) + TC^{-1} D_2) = \mathrm{tr}(S_1(G + Pq^{-1}) + TS) \equiv \mathrm{tr}(S_1 Pq^{-1})$ mod 1. Since $A_1 = A_2 + S_1 C \equiv A_2 \text{mod q}$ implies $S_1 C \equiv 0 \text{mod q}$ and P satisfies the condition $\boxed{*}$, we have $\mathrm{tr}\, S_1 P = 0 \text{mod q}$. Thus the exponential sum $S(\cdot\cdot)$ is well-defined.

R2) For $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma_2$, $D \equiv D' \text{mod q}$, there exists a unique $S \in \Lambda$ mod $\Lambda({}^t\mathrm{C}, \mathrm{q})$ such that

$$\begin{pmatrix} E_2 & S \\ 0 & E_2 \end{pmatrix}\begin{pmatrix} A & B \\ C & D \end{pmatrix} \equiv \begin{pmatrix} A' & B' \\ C & D' \end{pmatrix} \text{mod q}.$$

□

Proof. Since 101

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}\begin{pmatrix} A' & B' \\ C & D' \end{pmatrix}^{-1} \equiv \begin{pmatrix} * & * \\ 0 & E_2 \end{pmatrix} \text{mod q},$$

there exists $S \in \Lambda$ such that

$$\begin{pmatrix} E_2 & S \\ 0 & E_2 \end{pmatrix}\begin{pmatrix} A & B \\ C & D \end{pmatrix} \equiv \begin{pmatrix} A' & B' \\ C & D' \end{pmatrix} \text{mod q}.$$

If

$$\begin{pmatrix} E_2 & S_1 \\ 0 & E_2 \end{pmatrix}\begin{pmatrix} A & B \\ C & D \end{pmatrix} \equiv \begin{pmatrix} E_2 & S_2 \\ 0 & E_2 \end{pmatrix}\begin{pmatrix} A & B \\ C & D \end{pmatrix} \text{mod q},$$

then $A + S_1 C \equiv A + S_2 C \text{mod q}$ and so $S_1 - S_2 \in \Lambda({}^t C, q)$. □

Therefore

$$S\left(G, P, T, C, \left(\begin{smallmatrix} A' & B' \\ C & D' \end{smallmatrix}\right)\right) = \sum_{D \in \mathscr{D}} \sum_{S \in \Lambda/\Lambda({}^t C, q)} e(\mathrm{tr}(A + SC)C^{-1}(G + Pq^{-1}) + TC^{-1}D)q^{-4} \sum_{M \text{mod q}} e((A + SC - A')M/q)),$$

where $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma_2$ is any extension of (C, D),

$$= q^{-4} \sum_{M \text{mod q}} \sum_{D \in \mathscr{D}} e(\mathrm{tr}(AC^{-1}(G + Pq^{-1}) + TC^{-1}D + (A - A')M/q))\times$$

$$\times \sum_{S\in\Lambda/\Lambda({}^tC,q)} e(\operatorname{tr}(S(P+CM)q^{-1})).$$

The last exponential sum is $[\Lambda : \Lambda({}^tC, q)]$ or O according as $(P+\frac{1}{2}(CM+{}^tM^tC))/q \in \Lambda^*$ or not. Thus it is equal to

$$q^{-4}[\Lambda : \Lambda({}^tC,q)] \sum_{\substack{M \bmod q\\ (P+\frac{1}{2}(CM+{}^tM^tC)/q\in\Lambda^*}} \sum_{D\in\mathscr{D}} e(\operatorname{tr}(AC^{-1}(G+(P+\frac{1}{2}(CM$$
$$+{}^tM^tC))/q)+TC^{-1}D))e(-\operatorname{tr}(A'M/q)).$$

Putting $N_M := G + (P+\frac{1}{2}(CM+{}^tM^tC))/q \in \Lambda^*, S(N_M) = \sum_{D\in\mathscr{D}} e(\operatorname{tr}(AC^{-1}N_M + TC^{-1}D))$, we have

$$S(G,P,T,C,\begin{pmatrix} A' & B' \\ C & D' \end{pmatrix}) = q^{-4}[\Lambda : \Lambda({}^tC,q)] \sum_{\substack{M \bmod q\\ N_M\in\Lambda^*}} S(N_M)e(-\operatorname{tr} A'M/q).$$

102 Note that $[\Lambda : \Lambda({}^tC,q)] \leq [\Lambda : q\Lambda]$ and the number of M does not exceed q^4.

R3) The mapping $D \mapsto D$ from $\mathscr{D}$ to $\mathscr{D}' := \{D \in \mathscr{M}_2(\mathbb{Z})/C\Lambda | C, D$ are a symmetric coprime pair such that $D + CS \equiv D' \bmod q$ for some $S \in \Lambda\}$ is bijective.

Proof. Suppose that $D_1 \equiv D_2 \bmod C\Lambda$ for $D_1, D_2 \in \mathscr{D}$. Since $D_1, D_2 \in \mathscr{D}$, $D_1 \equiv D_2 \equiv D' \bmod q$. Hence for $S \in \Lambda$ with $D_1 - D_2 = CS$ we have $CS \equiv 0 \bmod q$ and then $S \in \Lambda(C,q)$. This means $D_1 \equiv D_2 \bmod C\Lambda(C,q)$ and the mapping is injective. Since, for $D \in \mathscr{D}'$, $D + CS (\equiv D \bmod C\Lambda)$ for the S involved in the definition of $\mathscr{D}'$ is contained in $\mathscr{D}$, the mapping is surjective. ◻

R4) If $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma_2$, $D + CS \equiv D' \bmod q$ for $S \in \Lambda \Longleftrightarrow A + S_1C \equiv A \bmod q$ for $S_1 \in \Lambda$

Proof. $D + CS \equiv D' \bmod q$ for $S \in \Lambda$

$$\Longleftrightarrow \begin{pmatrix} A & B \\ C & D \end{pmatrix}\begin{pmatrix} E_2 & S \\ 0 & E_2 \end{pmatrix} \equiv \begin{pmatrix} * & * \\ C & D' \end{pmatrix} \bmod q$$

$$\iff \begin{pmatrix} E_2 & S_1 \\ 0 & E_2 \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} E_2 & S \\ 0 & E_2 \end{pmatrix} \equiv \begin{pmatrix} A' & B' \\ C & D' \end{pmatrix} \text{mod q.}$$

$$\iff \begin{pmatrix} E_2 & S_1 \\ 0 & E_2 \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} \equiv \begin{pmatrix} A' & * \\ C & * \end{pmatrix} \text{mod q}$$

$$\iff A + S_1 C \equiv A' \text{mod q.}$$

For $N = N_M$ we have, with $S(N_M)$ as in (R2) **103**

$$S(N_M) = \sum_{D \in \mathscr{D}'} e(\operatorname{tr}(AC^{-1}N + TC^{-1}D)) \quad \text{(by (R3))}$$

$$= \sum_{\substack{D: A + S_1 C \equiv A' \text{mod q} \\ \text{for } S_1 \in \Lambda^1, \left(\begin{smallmatrix} A & * \\ C & D \end{smallmatrix}\right) \in \Gamma_2}} e(\operatorname{tr}(AC^{-1}N + TC^{-1}D)) \quad \text{(by (R4))}$$

$$= \sum_{\substack{D \text{mod } C\Lambda \\ : \left(\begin{smallmatrix} A & * \\ C & D \end{smallmatrix}\right) \in \Gamma_2}} \sum_{S \in \Lambda \text{mod } \Lambda({}^tC, q)} e(\operatorname{tr}(A + SC)C^{-1}N + TC^{-1}D)) \times$$

$$q^{-4} \sum_{M \text{mod q}} e(\operatorname{tr}((A + SC - A')M)/q) \quad \text{(by (R2)).}$$

$$= q^{-4} \sum_{\substack{D \text{mod } C\Lambda \\ : \left(\begin{smallmatrix} A & * \\ C & D \end{smallmatrix}\right) \in \Gamma_2}} e(\operatorname{tr}(AC^{-1}N + TC^{-1}D)) \sum_{M \text{mod q}} e(\operatorname{tr}(A - A')M/q) \times$$

$$\times \sum_{S \in \Lambda \text{mod } \Lambda({}^tC, q)} e(\operatorname{tr}(SCM/q))$$

$$= q^{-4}[\Lambda : \Lambda({}^tC, q)] \sum_{\substack{\text{mod q} \\ (CM + {}^t(CM))/2\varepsilon q\Lambda^*}} e(-\operatorname{tr}(A'M/q)) \sum_{\substack{D \text{mod } C\Lambda \\ : \left(\begin{smallmatrix} A & * \\ C & D \end{smallmatrix}\right) \in \Gamma_2}}$$

$$e(\operatorname{tr}(AC^{-1}(N + (1/(2q))(CM + {}^tM^tC)) + TC^{-1}D))$$

$$= q^{-4}[\Lambda : \Lambda({}^tC, q)] \sum_{\substack{M \text{mod q} \\ (CM + {}^t(CM))/2 \in q\Lambda^*}}$$

$$e(-\operatorname{tr} A'M/q))K(N + 1/(2q)(CM + {}^t(CM)), T; C).$$

Hence Proposition 1.5.6 would follow immediately from □

Proposition 1.5.14. *Let $C = U^{-1} \left(\begin{smallmatrix} c_1 & 0 \\ 0 & c_2 \end{smallmatrix}\right) V^{-1}$, for $U, V \in GL_2(\mathbb{Z})$, $0 < c_1 | c_2$. For $P, T \in \Lambda^*$, we have, for any $\varepsilon > 0$.* **104**

$$K(P, T : C) = O(c_1^2 c_2^{1/2+\varepsilon}(c_2, t)^{1/2}),$$

where t is the $(2,2)$ *entry of* $T[V]$.

To prove this, we need several lemmas.

Lemma 1.5.15. *We have* $K(P,T;U^{-1}CV^{-1}) = K(P[{}^tU],T[V];C)$ *for* P, $T \in \Lambda^*$, U, $V \in GL_2(\mathbb{Z})$ *and* $C \in M_2(\mathbb{Z})$ *with* $\det C \neq 0$.

Proof. Since

$$\begin{pmatrix} {}^tU & 0 \\ 0 & U^{-1} \end{pmatrix}\begin{pmatrix} A & * \\ C & D \end{pmatrix}\begin{pmatrix} V^{-1} & 0 \\ 0 & {}^tV \end{pmatrix} = \begin{pmatrix} {}^tU & AV^{-1} & * \\ U^{-1} & CV^{-1} & U^{-1}D^tV \end{pmatrix},$$

$$D \mathrm{mod}\ \mathrm{C}\Lambda \Longleftrightarrow \mathrm{U^{-1}D^tV mod\ U^{-1}C\Lambda^tV} \Longleftrightarrow \mathrm{U^{-1}D^tVmod\ U^{-1}CV^{-1}\Lambda}.$$

Hence we have

$$\begin{aligned} K(P,T;U^{-1}CV^{-1}) &= \sum_{D \mathrm{mod}\ \mathrm{C}\Lambda} e(\mathrm{tr}({}^tUAV^{-1}(U^{-1}CV^{-1})^{-1}P \\ &\qquad + (U^{-1}CV^{-1})^{-1}U^{-1}D^tVT)) \\ &= \sum_{D \mathrm{mod}\ \mathrm{C}\Lambda} e(\mathrm{tr}(AC^{-1}P[{}^tU] + C^{-1}DT[V])) \\ &= K(P[{}^tU], T[V] : C). \end{aligned}$$

□

Lemma 1.5.16. *For the diagonal matrices* $C = [c_1, c_2]$, $F = [f_1, f_2]$, $H = [h_1, h_2]$, *suppose that* $f_1|f_2$, $h_1|h_2$, $c_i = f_ih_i$, f_i, $h_i > 0 (i = 1, 2)$ *and that* f_2, h_2 *are relatively prime. Put* $X_1 = sf_2^2F^{-1}$, $X_2 = th_2^2H^{-1}$ *for integers* s, t *with* $sf_2^2 + th_2^2 = 1$. *If then*

$$\begin{pmatrix} A_1 & B_1 \\ F & D_1 \end{pmatrix}, \begin{pmatrix} A_2 & B_2 \\ H & D_2 \end{pmatrix} \in \Gamma_2, \Gamma_2 \ni \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} X_2A_1 + X_1A_2 & * \\ HF & HD_1 + FD_2 \end{pmatrix}$$

and the mapping $\varphi : (D_1, D_2) \mapsto D$ *induces a bijection from*

$$\{D_1 \mathrm{mod}\ \mathrm{F}\Lambda | \begin{pmatrix} * & * \\ F & D_1 \end{pmatrix} \in \Gamma_2\} \times \{\mathrm{D_2 mod\ H}\Lambda | \begin{pmatrix} * & * \\ H & D_2 \end{pmatrix} \in \Gamma_2\}$$

$$to\ \{|D \mathrm{mod}\ \mathrm{C}\Lambda | \begin{pmatrix} * & * \\ C & D \end{pmatrix} \in \Gamma_2\}.$$

105 *Proof.* Let $\begin{pmatrix} A_1 & B_1 \\ F & D_1 \end{pmatrix}, \begin{pmatrix} A_2 & B_2 \\ H & D_2 \end{pmatrix} \in \Gamma_2$ and put

$$A = X_2A_1 + X_1A_2, D = HD_1 + FD_2, B = (HF)^{-1}({}^tAD - E_2).$$

Recall that, for $\begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathscr{M}_4(\mathbb{Z})$, $\begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Gamma_2$ if and only if ${}^tAD - {}^tCB = E_2$ and ${}^tAC$, ${}^tBD$ are symmetric. $\square$

Now

$$B = X_2B_1 + X_1B_2 + th_2^2H^{-1}A_1H^{-1}D_2 + sf_2^2F^{-1}A_2F^{-1}D_1$$

is integral and both

$${}^tAC = ({}^tA_1X_2 + {}^tA_2X_1)FH = th_2^{2t}A_1F + sf_2^{2t}A_2H$$

and

$$\begin{aligned} {}^tBD &= ({}^tDA - E_2)C^{-1}D = {}^tDAC^{-1}D - C^{-1}D \\ &= {}^tDAC^{-1}D - F^{-1}D_1 - H^{-1}D_2 \end{aligned}$$

are symmetric. Moreover, ${}^tAD - {}^tCB = E_2$ and so $\begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Gamma_2$. If $HD_1 + FD_2 \in C\Lambda$, then $F^{-1}D_1 + H^{-1}D_2 \in \Lambda$ and so $F^{-1}D_1, H^{-1}D_2 \in \Lambda$ since $(f_2, h_2) = 1$. Hence φ is injective. It is easy to see that for the above $\begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Gamma_2$, $\begin{pmatrix} HA & HB - X^tAD \\ F & X_2D \end{pmatrix}$ and $\begin{pmatrix} FA & FB - X_2{}^tAD \\ H & X_1D \end{pmatrix}$ are also in Γ_2. From $H(X_2D) + F(X_1D) = D$ follows the surjectivity of φ.

Lemma 1.5.17. *Let C, F, H, X_1, X_2 be as in the previous lemma. Then for P, $T \in \Lambda^*$, we have*

$$K(P, T; C) = K(tP[h_2H^{-1}]), T; F)K(sP[f_2F^{-1}], T; H).$$

Proof. By the previous lemma, we have

$$\begin{aligned} K(P, T; C) &= \sum_D e(\mathrm{tr}(AC^{-1}P + C^{-1}DT)) \\ &= \sum_{D_1, D_2} e(\mathrm{tr}((X_2A_1 + X_1A_2)F^{-1}H^{-1}P \\ &\qquad + F^{-1}H^{-1}(HD_1 + FD_2)T)) \end{aligned}$$

$$= \sum_{D_1} e(\mathrm{tr}(X_2A_1F^{-1}H^{-1}P + F^{-1}D_1T))$$
$$\sum_{D_2} e(\mathrm{tr}(X_1A_2F^{-1}H^{-1}P + H^{-1}D_2T))$$
$$= K(tP[h_2H^{-1}], T; F)K(sP[f_2F^{-1}], T; H).$$

106 By virtue of Lemmas 1.5.15 and 1.5.17, in order to prove Proposition 1.5.14, we have only to show

$$K(P, T; \begin{pmatrix} p^{e_1} & 0 \\ 0 & P^{e_2} \end{pmatrix}) = O(P^{2e_1+e_2/2}(P^{e_2}, t)^{1/2}),$$

where P is a prime number $0 \le e_1 \le e_2$, $T = \left(\begin{smallmatrix} * & * \\ * & t \end{smallmatrix}\right)$ and the implied constant is independent of p, e_1, e_2, P, T. Put $C = \left(\begin{smallmatrix} p^{e_1} & 0 \\ 0 & p^{e_2} \end{smallmatrix}\right)$, $D = \left(\begin{smallmatrix} d_1 & d_2 \\ d_3 & d_4 \end{smallmatrix}\right)$. $C^{-1}D$ is symmetric if and only if $d_3 = p^{e_2-e_1}d_2$. Hence C, D are symmetric and coprime if and only if $d_3 = p^{e_2-e_1}d_2$ and one of (i) - (iv) holds:

(i) $e_1 = e_2 = 0$, (ii) $e_1 = 0, e_2 > 0, p \nmid d_4$,

(iii) $0 < e_1 < e_2, p \nmid d_1d_4$, (iv) $0 < e_1 = e_2, d_1d_4 - d_2^2 \not\equiv 0 \bmod \mathrm{p}$.

D runs over classes mod C if and only if d_1, d_2, d_4 runs over classes mod p^{e_1}, mod p^{e_1}, mod p^{e_2} respectively. For a symmetric coprime pair C, D, we can take A satisfying the conditions ${}^tAC$ is symmetric and $B = C^1({}^tAD - E_2) \in \mathscr{M}_2(\mathbb{Z})$, so that $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma_2$.

Put

$$P = \begin{pmatrix} p_1 & p_2/2 \\ p_2/2 & p_4 \end{pmatrix}, \quad T = \begin{pmatrix} t_1 & t_2/2 \\ t_2/2 & t_4 \end{pmatrix}$$

(i) In case $e_1 = e_2 = 0$, we can take $A = D = 0$ and $K(P, T; C) = 1$.

(ii) In case $e_1 = 0$, $e_2 > 0$, we can take $\left(\begin{smallmatrix} 0 & 0 \\ 0 & d \end{smallmatrix}\right)$, with $d \bmod \mathrm{p}^{e_2}$ and $p \nmid d$ as D and then we may take $A = \left(\begin{smallmatrix} 0 & 0 \\ 0 & a \end{smallmatrix}\right)$ with $ad \equiv 1 \bmod \mathrm{p}^{e_2}$.

107 Now $K(P, T; C)$

$$= \sum_{\substack{d \bmod \mathrm{p}^{e_2} \\ p \nmid d}} e(\mathrm{tr}(\begin{pmatrix} 0 & 0 \\ 0 & a/p^{e_2} \end{pmatrix} p + \begin{pmatrix} 0 & 0 \\ 0 & d/p^{e_2} \end{pmatrix} T))$$

$$= \sum_{\substack{d \bmod p^{e_2} \\ p \nmid d}} e((ap_4 + dt_4)/p^{e_2}) \text{ is a genuine Kloosterman}$$

sum and we are through.

(iii) In case $0 < e_1 < e_2$, put $\delta = d_1 d_4 - p^{e_2 - e_1} d_2^2 (\not\equiv 0 \bmod p)$ and for an integer d with $d\delta \equiv 1 \bmod p^{e_2}$, we can take $A = d\begin{pmatrix} d_4 & -p^{e_2-e_1} d_2 \\ -d_2 & d_1 \end{pmatrix}$. Then we have

$$K(P, T; C) = \sum_{\substack{d_1, d_2 \bmod p^{e_1} \\ d_4 \bmod p^{e_2} \\ p \nmid d_1 d_4}} e(d(d_4 p_1 p^{-e_1} - d_2 p_2 p^{-e_1} + d_1 p_4 p^{-e_2}) +$$
$$+ d_1 t_1 p^{-e_1} + d_2 t_2 p^{-e_1} + d_4 t_4 p^{-e_2}),$$

taking a in $\mathbb{Z}$ with $ad_1 \equiv 1 \bmod p^{e_2} (\Longleftrightarrow d_4 \equiv a\delta + p^{e_2-e_1} a d_2^2 \bmod p^{e_2})$.

Hence

$$K(P, T; C) = \sum_{d_1, d_2 \bmod p^{e_1}, p \nmid d_1} e(d_1 t_1 p^{-e_1} + d_2 t_2 p^{-e_1}$$
$$+ a p_1 p^{-e_1} + a d_2^2 t_4 p^{-e_1})$$
$$\times \sum_{\delta \bmod p^{e_2}, p \nmid \delta} e(\{d(a d_2^2 p_1 p^{2(e_2-e_1)} - d_2 p_2 p^{e_2-e_1}$$
$$+ d_1 p_4) + \delta(a t_4)\}/p^{e_2})$$

where the last sum on δ is the ordinary Kloosterman sum, and since $p \nmid a$, we have

$$K(P, T; C) = p^{2e_1} O(p^{e_2/2} (t_4, p^{e_2})^{1/2}).$$

(iv) In case $0 < e_1 = e_2 = e$, d_1, d_2, d_4 runs over $\mathbb{Z}/p^e$ with $\delta = d_1 d_4 - d_2^2 \not\equiv 0 \bmod p$. Taking $A = d\begin{pmatrix} d_4 & -d_2 \\ -d_2 & d_1 \end{pmatrix}$ for an integer d with 108
$d\delta \equiv 1 \bmod p^e$, we have

$$K(P, T; C) = \sum_{\substack{d_1, d_2, d_4 \bmod p^e \\ \delta \not\equiv 0 \bmod p}} e(\{d\{d_4 p_1 - d_2 p_2 + d_1 p_4)$$

$$+ (d_1t_1 + d_2t_2 + d_4t_4)\}/p^e)$$
$$= \sum_{p|d_2} + \sum_{p\nmid d_2} = \sum_1 + \sum_2 \quad \text{(say)}.$$

We have $\sum_1 = O(p^{2e+e/2}(t_4, p^e)^{1/2})$ quite similarly to the previous case. For dealing with $\sum_2$, we define integers δ_1, δ_2 by $d_1 \equiv d_2\delta_1 \bmod p^e$ and $d_4 \equiv d_2\delta_4 \bmod p^e$; then $\delta := d_1d_4 - d_2^2 \equiv d_2^2(\delta_1\delta_4 - 1) \bmod p^e$ and $1 \equiv dd_2^2(\delta_1\delta_4 - 1) \bmod p^e$. Then $\sum_2$ is transformed to

$$\sum_2 = \sum_{\substack{d_2,\delta_1,\delta_4 \bmod p^e \\ p\nmid d_2 \\ \delta_1\delta_4 \not\equiv 1 \bmod p}} e(d_2\{d(\delta_4p_1 - p_2 + \delta_1p_4) + \delta_1t_1 + t_2 + \delta_4t_4\}/p^e);$$

noting that $dd_2 \cdot d_2(\delta_1\delta_4 - 1) \equiv 1 \bmod p^e$ and denoting by x' the inverse class of $x \bmod p^e$,

$$\sum_2 = \sum_{\substack{\delta_1,\delta_4 \bmod p^e \\ \delta_1\delta_4 \not\equiv 1 \bmod p}} \sum_{\substack{d_2 \bmod p^e \\ p\nmid d_2}} e(\{d_2'((\delta_1\delta_4 - 1)'(\delta_4p_1 - p_2 + \delta_1p_4)) +$$
$$+ d_2(\delta_1t_1 + t_2 + \delta_4t_4)/p^e)$$
$$= \sum_{\substack{\delta_1,\delta_4 \bmod p^e \\ \delta_1\delta_4 \not\equiv 1 \bmod p}} O(p^{e/2}(\delta_1t_1 + \delta_4t_4, p^e)^{1/2}).$$
$$= O(p^{e/2} \sum_{x \bmod p^e} (x, p^e)^{1/2} \sharp \left\{\delta_1, \delta_4 \bmod p^e \Big|_{x \equiv \delta_1t_1 + t_2 + \delta_4t_4 \bmod p^e}^{\delta_1\delta_4 \not\equiv 1 \bmod p}\right\}$$

$\square$

109 Put $(t_4, p^e) = p^s$; then $0 \le s \le e$. If $s = e$, then $\sum_2 = O(p^{3e})$ (by the trivial estimation) $= O(p^{2e+e/2}(p^e, t_4)^{1/2})$ is what we want. Suppose $s < e$ and $t_4 = up^s$ with $(u, p) = 1$; then

$$\sum_2 = O(p^{e/2} \sum_{x \bmod p^e} (x, p^e)^{1/2} \sharp \left\{\delta_1, \delta_4 \bmod p^e \Big|_{u\delta_4 \equiv (x - \delta_1t_1 - t_2)/p^s \bmod p^{e-s}}^{x \equiv \delta_1t_1 + t_2 \bmod p^s}\right\}$$

$$= O(p^{e/2}\sum_{0\le i\le e} p^{(e-i)/2}\sum_{\substack{v \bmod p^i\\ p\nmid v}} p^s \sharp$$

$$\left\{\begin{matrix}\delta_1 \bmod p^e | vp^{e-i} \equiv \delta_1 t_1 + t_2 \bmod p^s\\ (\text{taking } \ x = vp^{e-i})\end{matrix}\right\}$$

$$= p^{e+s}\sum_{0\le i\le e} p^{-i/2} O(\sharp\{\delta_1 \bmod p^e, v \bmod p^i | vp^{e-i}$$

$$\equiv \delta_1 t_1 + t_2 \bmod p^s \quad p\nmid v\}.$$

In case $p^s|t_1$ and $p^s|t_2$, we have

$$\sum_2 = p^{e+s}\sum_{\substack{0\le i\le e\\ e-i\ge s}} p^{i/2+e} O(1) = O(1)p^{5e/2+s/2}.$$

In case $p^s|t_1$ but $p^s\nmid t_2$, $vp^{e-i}\equiv \delta_1 t_1 + t_2 \bmod p^s$ if and only if $vp^{e-i}\equiv t_2 \bmod p^s$. Putting $a_2 = \operatorname{ord}_p t_2 < s$, we have $e-i = a_2$ and then

$$\sum_2 = p^{e+s-(e-a_2)/2} O\left(\sharp\left\{\delta_1 \bmod p^e, v \bmod p^{e-a_2}\left|\begin{matrix}vp^{a_2}\equiv t_2 \bmod p^s\\ p\nmid v\end{matrix}\right.\right\}\right)$$

$$= p^{e+s-(e-a_2)/2+e+(e-a_2-(s-a_2))} O(1).$$

$$= p^{5e/2+a_2/2} O(1) = p^{5e/2+s/2} O(1).$$

Thus, we are through in case $p^s|t_1$. In case $a_1 = \operatorname{ord}_p t_1 < s$ and $a_2 = \operatorname{ord}_p t_2 < a_1$, $vp^{c-i}\equiv \delta_1 t_1 + t_2 \bmod p^s (p\nmid v)$ implies $\operatorname{ord}(\delta_1 t_1 + t_2) = a_2 <$ **110**
s and so $e-i = a_2$, moreover, $v \equiv \delta_1 t_1 p^{-a_2} + t_2 p^{-a_2} \bmod p^{s-a_2}$. Hence $v \equiv t_2 p^{-a_2} \bmod p^{a_1-a_2}$ and the number of possible v is at most p^{e-a_1} and for each v, δ_1 satisfies $\delta_1 \equiv (v - t_2 p^{-a_2})(t_1 p^{-a_2})^{-1} \bmod p^{s-a_1}$ and so the number of possible δ_1 is not larger than p^{e-s+a_1}. Thus we have

$$\sum_2 = p^{e+s+(a_2-e)/2+e-s+a_1+e-a_1} O(1) = O(1)p^{5e/2+a_2/2} = O(1)p^{5e/2+s/2}.$$

Finally in case $a_1 = \operatorname{ord}_p t_1 < s$, $a_2 = \operatorname{ord}_p t_2 \ge a_1$, $\delta_1 t_1 + t_2 \equiv 0 \bmod p^{a_1}$ and $a_1 < s$ imply $e - i \ge a_1$, and from $\delta_1(t_1 p^{-a_1}) = vp^{e-i-a_1} - t_2 p^{-a_1} \bmod p^{s-a_1}$, it follows that the number of possible δ_1 is at most $p^{e-(s-a_1)}$ for each v. Hence we have

$$\sum_2 = O(1)p^{e+s}\sum_{0\le i\le e-a_1} p^{-i/2+i+e-s+a_1}$$

$$= O(1)p^{2e+a_1+\frac{1}{2}(e-a_1)} = O(p^{5e/2+s/2}).$$

Thus we have completed the proof of Proposition 1.5.14 and so of Proposition 1.5.6.

Now it remains to prove Proposition 1.5.7.

Let $T = \begin{pmatrix} t_1 & t_2/2 \\ t_2/2 & t_4 \end{pmatrix} \in \Lambda^*$. Since $T[x] = t_1x_1^2 + t_2x_1x_2 + t_4x_2^2$, the sum $\gamma(T, n) = \sum\limits_{x \in S(n)} (T[x], n)^{1/2}$ is well-defined.

Lemma 1.5.18. *For integers m, n with* $(m, n) = 1$ *we have* $\gamma(T, mn) = \gamma(T, m)\gamma(T, n)$.

Proof. For $x = {}^t(bd)$, $y = {}^t(b'd')$ with $(b, d) = (b', d') = 1$ we take
111 $z = {}^t(ac)$ with $(a, c) = 1$ so that $z \equiv x \mathrm{mod\ m}$, $z \equiv y \mathrm{mod\ n}$. It is easy to see that this induces a bijective mapping from $S(m) \times S(n)$ to $S(m, n)$. □

Hence the left hand side is equal to

$$\sum_{S(mn)\ni x} (T[x], m)^{1/2} (T[x], n)^{1/2}$$

$$= \sum_{\substack{S(m)\ni x \\ S(n)\ni x}} (T[z], m)^{1/2} (T[z], n)^{1/2} \begin{pmatrix} z \equiv x & \mathrm{mod\ m} \\ z \equiv y & \mathrm{mod\ n} \end{pmatrix}$$

$=$ The right hand side.

Thus we have only to give the proof for the case $n = p^e$ where p is a prime number and $e \geq 1$. Put $S' = \{({}^t(bd)|(b, d, p) = 1\}$ and define the equivalence ${}^t(bd) \approx {}^t(b'd')$ by ${}^t(bd) \equiv n\ {}^t(b'd') \mathrm{mod\ p^e}$ for some integer n; then we have

$$\gamma(T, p^e) = \sum_{S'/\approx\ni x} (T[x], p^e)^{1/2},$$

since $x \mapsto x$ induces a bijective mapping from $S(p^e)$ to $S'/\approx$. Since $V \in \mathscr{M}_2(\mathbb{Z})$ with $\det V \not\equiv 0 \mathrm{mod\ p}$ operates on $S'/\approx$, we have $\gamma(T, p^e) = \sum\limits_{S'/=\ni x} (T[V_x], p^e)^{1/2}$.

Hence we may suppose, without loss of generality that T has a canonical form mod $\mathrm{p^e}$ and more explicitly (i) T is the diagonal matrix $= [up^{a_1}, uvp^{a_2}]$ $O \leq a_1 \leq a_2$, $p \nmid uv$ (ii) $2^a \begin{pmatrix} 1 & 1/2 \\ 1/2 & 1 \end{pmatrix}$, $a \geq 0$

if $p = 2$ or (iii) $2^a \left(\begin{smallmatrix} 0 & 1/2 \\ 1/2 & 0 \end{smallmatrix}\right) a \geq 0$ if $p = 2$. Our aim is to prove $\gamma(T, p^e) = O(p^{e(1+\epsilon)}(e(T), p^e)^{1/2})$ where $e(T) = p^{a_1}, 2^a, 2^a$ according to (i), (ii), (iii) respectively. **112**

Lemma 1.5.19. (i) $\sum\limits_{\substack{n \bmod p^e \\ p \nmid n}} (n^2+v, p^{e-a_1})^{1/2} = O(p^e)$ *if* $p \nmid v$, $0 \leq a_1 < e$, *and*

(ii) $\sum\limits_{n \bmod p^{e-1}} (p^2n^2 + vp^{a_2-a_1}, p^{e-a_1})^{1/2} = O(p^{e(1+\varepsilon)})$ *for any* $\varepsilon > 0$, *if* $p \nmid v$, $0 \leq a_1 < a_2$ *and* $e \geq 1$.

Proof. First we prove (i). If $p \neq 2$ and $\left(\dfrac{-v}{p}\right) = -1$, then (i) is trivial since $p \nmid (n^2+v)$. Suppose $p \neq 2$ and $\left(\dfrac{-v}{p}\right) = 1$. Take a p-adic integer g so that $g^2 + v = 0$. If $n^2 + v \equiv 0 \bmod p$, then $n = \pm g + mp^s$ with $m \in \mathbb{Z}_p^*$, $s \geq 1$ and so $n^2 + v = p^s(\pm 2gm + m^2p^s)$ is exactly divisible by p^s. Thus we have

$$\begin{aligned}
&\sum_{\substack{n \bmod p^e \\ p \nmid n}} (n^2 + v, p^{e-a_1})^{1/2} \\
&= \sum_{\substack{n \bmod p^e \\ p \nmid n, n^2+v \equiv 0 \bmod p}} (n^2 + v, p^{e-a_1})^{1/2} + \sum_{\substack{n \bmod p^e \\ p \nmid n, n^2+v \not\equiv 0 (p)}} 1 \\
&\leqq 2 \sum_{1 \leq s \leq e} \sum_{\substack{m \bmod p^{e-s} \\ p \nmid m}} (p^s, p^{e-a_1})^{1/2} + p^e \\
&= 2 \sum_{1 \leq s \leq e-a_1} p^{s/2}\varphi(p^{e-s}) + 2 \sum_{e-a_1 < s \leq e} p^{(e-a_1)/2}\varphi(p^{e-s}) + p^e
\end{aligned}$$

where φ is the Euler function. □

The first partial sum is equal to **113**

$$\sum_{1 \leq s \leq e-a_1-1} p^{s/2}p^{e-s}(1 - p^{-1}) + p^{(e-a_1)/2}\varphi(p^{a_1})$$

$$= p^{e-\frac{1}{2}}(1 - p^{-(e-a_1-1)/2})(1 + p^{-\frac{1}{2}}) + p^{(e-a_1)/2}\varphi(p^{a_1}) = O(p^e).$$

The second is $p^{(e-a_1)/2}(\varphi(p^{a_1-1}) + \cdots + \varphi(1)) = p^{(e+a_1)/2-1} = O(p^e)$. Thus, in this case, we are through.

Suppose $p = 2$ and $v \not\equiv 7 \bmod 8$; then $n^2 + V \not\equiv 0 \bmod 8$ for old n. Hence we have

$$\sum_{\substack{n \bmod 2^e \\ 2\nmid n}} (n^2 + v, 2^{e-a_1})^{\frac{1}{2}} \leq \sum (4, 2^{e-a_1})^{\frac{1}{2}} = O(2^e).$$

Lastly, we suppose $p = 2$, $v \equiv 7 \bmod 8$, and take $g \in \mathbb{Z}_2^*$ so that $g^2+v = 0$. Since, for $n = g + 2^r m$ with $r \geq 1$, $2 \nmid m$, $n^2 + v = 2^{r+1}m(g + 2^{r-1}m)$, we have

$$\begin{aligned}
&\sum_{\substack{n \bmod 2^e \\ 2\nmid n}} (n^2 + v, 2^{e-a_1})^{\frac{1}{2}} \\
&= \sum_{\substack{m \bmod 2^{e-1} \\ 2\nmid m}} (2^2 m(g+m), 2^{e-a_1})^{\frac{1}{2}} + \sum_{2\leq r\leq e} \sum_{\substack{m \bmod 2^{e-r} \\ 2\nmid m}} (2^{r+1}, 2^{e-a_1})^{\frac{1}{2}} \\
&= \sum_{\substack{n \bmod 2^{e-1} \\ 2\mid n}} (2^2 n, 2^{e-a_1})^{\frac{1}{2}} + \sum_{2\leq r\leq e} 2^{e-r-1}(2^{r+1}, 2^{e-a_1})^{\frac{1}{2}} \\
&= \sum_{1\leq r\leq e-1} 2^{e-2-r}(2^{2+r}, 2^{e-a_1})^{\frac{1}{2}} + \sum_{2\leq r\leq e} 2^{e-r-1}(2^{r+1}, 2^{e-a_1})^{\frac{1}{2}} \\
&= 2^e \sum_{2\leq r\leq e} 2^{-r}(2^{r+1}, 2^{e-a_1})^{\frac{1}{2}} = 2^e \sum_{2\leq r\leq e-a_1-1} 2^{\frac{1}{2}(1-r)} \\
&\qquad + 2^e \sum_{e-a_1\leq r\leq e} 2^{-r+\frac{1}{2}(e-a_1)} = O(2^e).
\end{aligned}$$

114 Thus (i) has been proved. Let us prove (ii). If $a_2 \geq e$, then we have

$$\begin{aligned}
&\sum_{n \bmod p^{e-1}} (p^2 n^2 + v p^{a_2-a_1}, p^{e-a_1})^{1/2} \\
&= \sum_{n \bmod p^{e-1}} (p^2 n^2, p^{e-a_1})^{1/2} = \sum_{0\leq r\leq e-1} \varphi(p^{e-1-r})(p^{2+2r}, p^{e-a_1})^{1/2}
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{0\le r\le (e-a_1)/2-1} \varphi(p^{e-1-r})p^{1+r} + \sum_{(e-a_1)/2\le r\le e-1} \varphi(p^{e-1-r})p^{(e-a_1)/2}\\
&= O(ep^e) = O(p^{e(1+\varepsilon)}).
\end{aligned}
$$

Suppose $a_2 < e$; then we have

$$
\begin{aligned}
&\sum_{n \bmod p^{e-1}} (p^2n^2 + vp^{a_2-a_1}, p^{e-a_1})^{1/2}\\
&\sum_{0\le r<(a_2-a_1-2)/2} \varphi(p^{e-1-r})p^{1+r} + \sum_{\substack{r=(a_2-a_1-2)/2\\ m \bmod p^{e-1-r}\\ p\nmid m}} p^{(a_2-a_1)/2}(m^2+v, p^{e-a_2})^{1/2} +\\
&\sum_{(a_2-a_1)/2\le r\le e-1} \varphi(p^{e-1-r})p^{(a_2-a_1)/2}(n = mp^r, p\nmid m)\\
&= O(ep^e) + p^{(a_2-a_1)/2} \sum_{\substack{r=(a_2-a_1-2)/2\\ m \bmod p^{e-1-r}\\ p\nmid m}} (m^2+v, p^{e-a_2})^{1/2}.
\end{aligned}
$$

The last partial sum vanishes if $a_2 \not\equiv a_1 \bmod 2$. Suppose $a_2 \equiv a_1 \bmod 2$ and put $E := e-1-r$, $A_1 = 0$. Then $E = e-(a_2-a_1)/2 > (a_2+a_1)/2 > 0 = A_1$ and $E \ge e-a_2$. Hence the last partial sum is not larger than **115**

$$
\begin{aligned}
&p^{(a_2-a_1)/2} \sum_{\substack{m \bmod p^E\\ p\nmid m}} (m^2+v, p^E)^{\frac{1}{2}}\\
&= p^{(a_2-a_1)/2} O(p^E), \quad \text{(by (i))} = O(p^e).
\end{aligned}
$$

Thus we have completed the proof of Lemma 1.5.19.

To prove $\gamma(T, p^e) = O(p^{e(1+\varepsilon)}(e(T), p^e)^{\frac{1}{2}})$, note that ${}^t(n,1)(n \bmod p^e)$, ${}^t(m, p^t)$ $(p \nmid m, m \bmod p^{e-t}, 1 \le t \le e)$ give a complete set of representatives of $S'/\approx$. Suppose T to be in diagonal form $[up^{a_1}, uvp^{a_2}]$, $0 \le a_1 \le a_2$, $p \nmid uv$; then

$$
\begin{aligned}
\gamma(T, p^e) = &\sum_{n \bmod p^e} (n^2up^{a_1} + uvp^{a_2}, p^e)^{\frac{1}{2}}\\
&+ \sum_{1\le t\le e} \sum_{\substack{m \bmod p^{e-t}\\ p\nmid m}} (m^2up^{a_1} + uvp^{a_2+2t}, p^e)^{\frac{1}{2}}.
\end{aligned}
$$

We want to show that $\gamma(T,p^e)=O(p^{e(1+\varepsilon)+\min(a_1,e)/2})$.

If $a_1\geq e$, then

$$\begin{aligned}\gamma(T,p^e)&=p^{e/2}\{p^e+\varphi(p^{e-1})+\cdots+\varphi(1)\}\\&=p^{e/2}\{p^e+p^{e-1}\}=O(p^{3e/2}).\end{aligned}$$

In case $a_1<e$, we have

$$\begin{aligned}\gamma(T,p^e)=p^{\frac{1}{2}a_1}&\sum_{\substack{n \bmod p^e\\ p\nmid n}}(n^2+vp^{a_2-a_1},p^{e-a_1})^{\frac{1}{2}}+\\&+p^{\frac{1}{2}a_1}\sum_{n \bmod p^{e-1}}(p^2n^2+vp^{a_2-a_1},p^{e-a_1})^{\frac{1}{2}}+\\&+p^{\frac{1}{2}a_1}\sum_{1\leq t\leq e}\sum_{\substack{m \bmod p^{e-t}\\ p\nmid m}}(m^2+vp^{a_2-a_1+2t},p^{e-a_1})^{\frac{1}{2}}\end{aligned}$$

116 Hence if $a_1=a_2<e$, then

$$\gamma(T,P^e)=p^{a_1/2}O(p^e)+p^{\frac{1}{2}a_1+e-1}+p^{a_1/2}\sum_{1\leq t\leq e}\varphi(p^{e-t})=O(p^{a_1/2+e}).$$

If $a_1<e$ and $a_1<a_2$, then

$$\begin{aligned}\gamma(T,P^e)&=p^{a_1/2}\varphi(p^e)+p^{a_1/2}O(p^{e(1+\varepsilon)})+p^{a_1/2}\sum_{1\leq t\leq e}\varphi(p^{e-t})\\&=O(p^{e(1+\varepsilon)+a_1/2}).\end{aligned}$$

Suppose $T=2^a\begin{pmatrix}1&\frac{1}{2}\\ \frac{1}{2}&1\end{pmatrix}$, $a\geq 0$ and $p=2$. Since

$$T\begin{pmatrix}x_1\\ x_2\end{pmatrix}=2^a(x_1^2+x_1x_2+x_2^2),\text{ord}\,T[x]=2^a\quad\text{if}\quad(x_1,x_2,2)=1.$$

Hence

$$\gamma(T,2^e)=\sum_{x\in S'/\approx}(2^a,2^e)^{\frac{1}{2}}=(2^e+2^{e-1})2^{|(a,e)/2}=O(2^{e+\min(a,e)/2}).$$

Suppose $T = 2^a \begin{pmatrix} 0 & \frac{1}{2} \\ \frac{1}{2} & 0 \end{pmatrix}$; then

$$\begin{aligned}
\gamma(T, 2^e) &= \sum_{n \bmod 2^e} (2^a n, 2^e)^{\frac{1}{2}} + \sum_{1 \le t \le e} \sum_{\substack{m \bmod 2^{e-t} \\ 2 \nmid m}} (2^{a+t} m, 2^e)^{\frac{1}{2}} \\
&= \sum_{0 \le t \le e} \varphi(2^{e-t})(2^{a+t}, 2^e)^{\frac{1}{2}} + \sum_{1 \le t \le e} \varphi(2^{e-t})(2^{a+t}, 2^e)^{\frac{1}{2}} \\
&= 2^{e-1+\min(a,e)/2} + 2 \sum_{1 \le t \le e-1} 2^{e-t-1+\min(a+t,e)/2} + 2^{e/2} \\
&\le 2^{e+\min(a,e)/2} + 2(e-1)2^{e+\min(a,e)/2} = O(2^{e(1+\epsilon)+\min(a,e)/2})
\end{aligned}$$

since $e - t - 1 + \min(a+t, e)/2 \le e + \min(a, e)/2$.

1.6 Estimation of Fourier Coefficients of Modular Forms

Let $\{n, k, s\}$ denote the space of modular forms of degree n, weight k and level s. In this section, we first obtain a Representation Theorem for $\{n, k, s\}$ with even $k \ge 2n + 2$ in terms of the Eisenstein series $E^k_{n,j}(Z; f)$ in the sense of Klingen [13] arising as 'lifts' of cusp forms f in $\{j, k, s\}$ for $j \le n$. Then we shall derive an estimate for the Fourier coefficients of modular forms in $\{n, k, s\}$ for even (integral) $k \ge 2n + 2$, following Kitaoka [10]. We first prove a few preparatory lemmas for the Representation Theorem, following H. Braun [3] and Christian [6]. **117**

Lemma 1.6.1. *For any $R \in \mathrm{Sp}(n, \mathbb{Q})$, there exist an upper triangular Q in $GL(n, \mathbb{Q})$ and an (n, n) rational symmetric S such that $M = R \begin{pmatrix} {}^tQ & {}^tQS \\ 0 & Q^{-1} \end{pmatrix}$ is in Γ_n.*

Proof. Let $R = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ with (n, n) matrices A, B, C, D. For some $d \ne 0$ in $\mathbb{Z}$, $(-d{}^tC, d{}^tA)$ is an integral symmetric pair and further $(-{}^tC{}^tA)$ has rank n. Hence, for some U in $GL(2n, \mathbb{Z})$, $(-d{}^tCd{}^tA)U = (G\ \ 0)$ with (n, n) invertible integral G. Clearly then $C' := -dG^{-1t}C$, $D' := dG^{-1t}A$ form a coprime symmetric pair and constitute therefore the last n rows of $N = (M')^{-1}$ for some M' in Γ_n, so that we have $NR =$

$\begin{pmatrix} * & * \\ dG^{-1}(-{}^tCA+{}^tAC) & * \end{pmatrix} = \begin{pmatrix} * & * \\ 0 & Q_1 \end{pmatrix}$ with Q_1 in $GL(n, \mathbb{Q})$. By easy induction, there exists V in $GL(n, \mathbb{Z})$ with $Q := VQ_1$ in upper triangular form. The lemma is now immediate with $M = M' \begin{pmatrix} {}^tV & 0 \\ 0 & V^{-1} \end{pmatrix}$. $\square$

Let us fix, in the sequel, $M_1, \ldots, M_t$ in Γ_n so that $\Gamma_n = \coprod\limits_{1 \leq i \leq t} \Gamma_n(s) M_i$.
118 Then, by Lemma 1, any $R \in \mathrm{Sp}(n, \mathbb{Q})$ can be written in the form $N' M_i \begin{pmatrix} {}^tQ & {}^tQS \\ 0 & Q^{-1} \end{pmatrix}$ for some N' in $\Gamma_n(s)$ and M_i with Q, S as in Lemma 1.6.1. For f in $\{n, k, s\}$, we have therefore

$$\begin{aligned} (f|_k R)(Z) &= (((f|_k N')|_k M_i \begin{pmatrix} {}^tQ & {}^tQS \\ 0 & Q^{-1} \end{pmatrix}) (Z) \\ &= (f|_k M_i)({}^tQ(Z+S)Q) \quad (\det Q)^k. \end{aligned}$$

Now, for any j with $1 \leq j \leq n$ and $Z_1 \in \mathscr{G}_{n-j}$, the j^{th}-iterate Φ^j of the Siegel operator on any $f : \mathscr{G}_n \to \mathbb{C}$ is defined by

$$(\Phi^j f)(Z_1) = \lim_{\lambda \to \infty} f\left(\begin{pmatrix} Z_1(n-j) & 0 \\ 0 & i\lambda E_j \end{pmatrix}\right);$$

it is known that for f in $\{n, k, s\}$, $\Phi_j f$ exists and is in $\{n-j, k, *\}$.

Definition. *We call f in $\{n, k, s\}$ a j-*cusp form*, if $\Phi^j(f|_k R) = 0$ for every R in* $\mathrm{Sp}(n, \mathbb{Q})$*. For $j = 1$, we call f just a* cusp form.

Lemma 1.6.2. *Any f in $\{n, k, s\}$ is a j-cusp form if any only if $\Phi^j(f|_k M_i) = 0$ for $1 \leq i \leq t$.*

Proof. To prove the lemma, it is enough to show that f is a j-cusp form if $\Phi^j(f|_k M) = 0$ for every M in Γ_n (or equivalently if $\Phi^j(f|_k M_i) = 0$ for $1 \leq i \leq t$). The limit as λ tends to ∞ in the definition of $\Phi^j(f|_k M_i)(Z_1)$ can be applied termwise to the Fourier expansion

$$(f|kM_i)\begin{pmatrix} Z_1 & 0 \\ 0 & i\lambda E_j \end{pmatrix} = \sum_{T = \begin{pmatrix} T_1^{(n-j)} & T_2 \\ * & T_3 \end{pmatrix} \geq 0} a(T; f; M_i) e^{2\pi i \operatorname{tr}(T \begin{pmatrix} Z_1 & 0 \\ 0 & i\lambda E_j \end{pmatrix})/s}$$

and hence

$$\Phi^j(f|_k M_i)(Z_1) = \sum_{T_1^{(n-j)} \geq 0} a(\begin{pmatrix} T_1 & 0 \\ 0 & 0 \end{pmatrix}; f; M_i) e^{2\pi i \operatorname{tr}((T_1 Z_1))/s}$$

119 The assumption $\Phi^j(f|_k M_i) = 0$ for $1 \leq i \leq t$ is equivalent then to $a(\left(\begin{smallmatrix} T_1 & 0\\ 0 & 0\end{smallmatrix}\right); f; M_i) = 0$ for all $T_1 \geq 0$ and $1 \leq i \leq t$. On the other hand, we know from Lemma 1.6.1 that for R in $\mathrm{Sp}(n; \mathbb{Q})$,

$$\begin{aligned}
\Phi^j(f|_k R)(Z_1) &= \Phi^j(f|M_i\begin{pmatrix} {}^tQ & {}^tQS\\ 0 & Q^{-1}\end{pmatrix})(Z_1)\\
&\qquad\qquad \text{for suitable } M_i \text{ and } Q, S \text{ as above}\\
&= \lim_{\lambda\to\infty}(f|M_i)({}^tQ(\begin{pmatrix} Z_1 & 0\\ 0 & i\lambda E_j\end{pmatrix} + S)Q)\\
&= \sum a(T; f; M_i) e^{\frac{2\pi i}{s}(\mathrm{tr}(T_1 Z_1[Q_1] + \mathrm{tr}(T_3 Z_1[Q_2]) + 2\,\mathrm{tr}(T_2 {}^tQ_2 Z_1 Q_1)))} \times\\
T &= \begin{pmatrix} T_1^{(n-j)} & T_2\\ * & T_3\end{pmatrix} \geq 0 \times e^{\frac{2\pi i}{s}\,\mathrm{tr}(TS')} \lim_{\lambda\to\infty} e^{\frac{-2\pi\lambda}{s}}\ \mathrm{tr}(T_3[{}^tQ_3]),
\end{aligned}$$

writing $Q = \left[\begin{smallmatrix} Q_1^{(n-j)} & Q_2\\ 0 & Q_3\end{smallmatrix}\right)$ and $S' = {}^tQSQ$. Now since $\det Q_3 \neq 0$, $\mathrm{tr}(Q_3 T_3 {}^tQ_3) \neq 0$ unless $T_3 = 0$ and therefore for every T with $T_3 = 0$ and therefore for every T with $T_3 \neq 0$, the limit of the corresponding term as λ tends to ∞, is zero. If $T_3 = 0$, then $T_2 = 0$ as well, in view of "$T \geq 0$". Thus in the limit as λ tends to ∞, at most the terms corresponding to $T = \left(\begin{smallmatrix} T_1^{(n-j)} & 0\\ 0 & 0\end{smallmatrix}\right)$ can survive. Our assumption "$\Phi^j(f|_k M_i) = 0$" above implies a $(T; f; M_i) = 0$ for these latter type of T are 0, leading to $\Phi^j(f|_k R) = 0$ for every R in $\mathrm{Sp}(n, \mathbb{Q})$ and also proving the lemma. □

For $0 < j \leq n$, let $\Delta_{n,n-j}(s) = \{M \in \Gamma_n(s)|$ the entries of the first $2n - j$ columns of the last j rows of M are $0\}$.

Then

$$\Delta_{n,n-j}(s) = \left\{ M = \begin{pmatrix} A & 0 & B & *\\ * & Q^{-1} & * & *\\ C & 0 & D & *\\ 0 & 0 & 0 & Q\end{pmatrix} \in \Gamma_n(s) \right\}$$

and is indeed a subgroup of $\Gamma_n(s)$; any M in $\Delta_{n,n-j}(s)$, $Q \equiv E_j (\mathrm{mod}\ s)$ in $GL(j, \mathbb{Z})$ and further $\underline{M} := \left(\begin{smallmatrix} A & B\\ C & D\end{smallmatrix}\right)$ is in $\Gamma_{n-j}(s)$. The mapping $M \mapsto \underline{M}$ 120 is a homomorphism of $\Delta_{n,n-j}$ onto $\Gamma_{n-j}(s)$, with kernel

$$\left\{\begin{pmatrix} E_{n-j} & 0 & 0 & * \\ * & E_j & * & * \\ & & E_{n-j} & * \\ 0 & & 0 & E_j \end{pmatrix} \in \Delta_{n,n-j}(s)\right\}$$

We denote $\Delta_{n,n-j}(1)$ simply as $\Delta_{n,n-j}$.

Definition. *For N_1, N_2 in Γ_n, we say $N_1 \widetilde{j,s}\, N_2$ if, for some M in $\Gamma_n(s)$, we have $N = N_1^{-1} M N_2 \in \Delta_{n,n-j}$.*

Lemma 1.6.3. *For N_1, N_2 in Γ_n with $N_1 \widetilde{j,s} N_2$ and f in $\{n, k, s\}$, we have $\Phi^j(f|N_1) = 0 \Longleftrightarrow \Phi^j(f|N_2) = 0$ for $0 \leq j \leq n$.*

Proof. Writing $Z = \begin{pmatrix} Z_1 & Z_2 \\ {}^tZ_2 & Z_3 \end{pmatrix}$ with $Z_1 \in \mathscr{G}_{n-j}$, we have, for $j < n$, $N < Z >= \begin{pmatrix} \underline{N}<Z_1> & * \\ * & * \end{pmatrix}$ and $\det N\{Z\} = \det \underline{N}\{Z_1\} \det Q$ for some Q in $GL(j, \mathbb{Z})$. Thus $\Phi^j(f|N_2) = \Phi^j(f|MN_2) = \Phi^j(f|N_1 N) = (\det Q)^k (\Phi^j(f|N_1))|\underline{N}$, for $0 \leq j < n$. □

The lemma follows on noting that for $j = n$, $\Phi^n(f|N_i) =$ the constant term in the Fourier expansion of $f|N_i$ and $|a(0, N_1)| = |a(0, N_2)|$.

121 For $T \geq 0$, let

$$\Gamma_n(s; T) = \left\{\begin{pmatrix} {}^tU & * \\ 0 & U^{-1} \end{pmatrix} \in \Gamma_n(S) | T[{}^tU] = T\right\}.$$

Then, for even (integral) $k > n + 1 + \operatorname{rank} T$, we define the Poincaré series g_k and p_k by

$$g_k(Z, T; \Gamma_n(s)) := \sum_{M \in \Gamma_n(s,T) \backslash \Gamma_n(s)} e^{\frac{2\pi i}{s} \operatorname{tr}(TM<Z>)} (\det M\{Z\})^{-k},$$

$$p_k(Z, T; N; \Gamma_n(s)) := \sum_{N^{-1}M \in \Gamma_n(s,T) \backslash N^{-1}\Gamma_n(s)} e^{\frac{2\pi i}{s} \operatorname{tr}(TN^{-1}M<Z>)} (\det N^{-1}M\{Z\})^{-k}$$

for N in Γ_n. These series converge absolutely, uniformly on compact subsets of $\mathscr{G}_n$ and belong to $\{n, k, s\}$ for $k > n + 1 + \operatorname{rank}(T)$. For $T = 0$, they are just Eisenstein series. Clearly $p_k(Z, T; E_{2j}; \Gamma_n(s)) = g_k(Z, T; \Gamma_n(s))$.

Lemma 1.6.4. *For $k > n + 1 + \operatorname{rank} T$ and N in Γ_n, we have*

$$p_k(Z, T; N; \Gamma_n(s)) = g_k(Z, T; \Gamma_n(s))|N^{-1}.$$

Proof. Suppose M' runs over a complete set of representatives of the right cosets of $\Gamma_n(s)$ modulo $\Gamma_n(s^*, T)$. Then $M : NM'N^{-1}$ is in $\Gamma_n(s)$ and $M'N^{-1} = N^{-1}M$. Further $M'N^{-1}$ runs over a complete set of representatives of elements in $N^{-1}\Gamma_n(s)$ such that, for *no* two such distinct elements, say $N^{-1}M_1$, $N^{-1}M_2$ we have $N^{-1}M_1 \in \Gamma_n(s, T)N^{-1}M_2$; otherwise, we will have for $M'_1 \neq M'_2$ with $M'_i N^{-1} := N^{-1}M_i$, $i = 1, 2$, $M'_1 \in \Gamma_n(s, T)M'_2$, a contradiction. □

Now 122

$$\begin{aligned} g_k(Z, T; \Gamma_n(s))|N^{-1} &= \sum_{M' \in \Gamma_n(s,T)\backslash\Gamma_n(s)} e^{\frac{2\pi i}{s} \operatorname{tr}(TM'<N^{-1}<Z>>)} \\ &\qquad \det M'\{N^{-1} < Z >\}^{-k} \det N^{-1}\{Z\}^{-k} \\ &= \sum_{M'} e^{\frac{2\pi i}{s} \operatorname{tr}(T(M'N^{-1})<Z>)} (\det(M'N^{-1})\{Z\})^{-k} \\ &= \sum_{N^{-1}M \in \Gamma_n(s,T)\backslash N^{-1}\Gamma_n(s)} e^{\frac{2\pi i}{s} \operatorname{tr}(T(N^{-1}M)<Z>)} \\ &\qquad (\det(N^{-1}M)\{Z\})^{-k} \\ &= p_k(Z, T; N; \Gamma_n(s)) \end{aligned}$$

Lemma 1.6.5. *For $T = \begin{pmatrix} T_0^{(n-j)} & 0 \\ 0 & 0 \end{pmatrix}$ with $T_0^{(n-j)} > 0$ and $Z = \begin{pmatrix} Z_0^{(n-j)} & * \\ * & * \end{pmatrix} \in \mathscr{G}_n$ we have $\Phi^j(g_k(Z, T; \Gamma_n(s)) = *g_k(Z_0, T_0; \Gamma_{n-j}(s))$ if $0 < j < n$ and $\Phi^n(g_k(Z, 0; \Gamma_n(s)) = 1$.*

Proof. The involved limit with $Z = \begin{pmatrix} Z_0 & 0 \\ 0 & i\lambda E_g \end{pmatrix}$ (as $\lambda \to \infty$) in Φ^j can be applied termwise to the series defining g_k, namely to each term

$$e^{\frac{2\pi i}{s} \operatorname{tr}(TM<Z>)} (\det M\{Z\})^{-k} = e^{\frac{2\pi i}{s} \operatorname{tr}(T_0(M<Z>)_0)} (\det M\{Z\})^{-k}$$

where $(M < Z >)_0$ denote the top (leftmost) $(n - j, n - j)$ submatrix of $M < Z >$. Let $\begin{pmatrix} C_1 & C_2 & D_1 & D_2 \\ C_3 & C_4 & D_3 & D_4 \end{pmatrix}$ with $(n - j, n - j)$ submatrices C_1, D_1 be the matrix formed by the last n rows of $M(\text{in } \Gamma_n(s))$ and $Y_0 = \mathrm{Im}(Z_0)$. As in Klingen (Math. Zeit. 102 (1967), p.35), we have **123**

$$\mathrm{abs}(\det M\{Z\})^{-2} = \det(\mathrm{Im}((M < Z >)_0)/(\det Y_0 P(\lambda) \text{ where } P(\lambda) := \det(\lambda Y_0^{-1}[[Z_0^t C_3 + {}^tD_3]] + E_j[[i\lambda^t C_4 + {}^tD_4]])$$

with ${}^t\overline{S}RS$ abbreviated as $R[[S]]$; we are using here the relations

$$\begin{pmatrix} (Y_M)_0 & Y_{M,2} \\ * & Y_{M,3} \end{pmatrix}^{-1} \{= \begin{pmatrix} * & * \\ * & (Y_{M,3} - (Y_M)_0^{-1}[Y_{M,2}])^{-1} \end{pmatrix}\}$$
$$= (\mathrm{Im}(M < Z >))^{-1} = (\mathrm{Im}(Z))^{-1}[[{}^t(CZ + D)]] =$$
$$= \begin{pmatrix} Y_0^{-1} & 0 \\ 0 & \frac{1}{\lambda}E_j \end{pmatrix} [[\begin{pmatrix} * & {}^t(C_3 Z_0 + D_3) \\ * & t(i\lambda C_4 + D_4) \end{pmatrix}]],$$

and

$$(\mathrm{abs}(\det((CZ + D)^2)/((\det Y_0)\lambda^j)$$
$$= 1/\det(\mathrm{Im}(M < Z >)) = 1/((\det(Y_M)_0)(\det(Y_{M,3} - (Y_N)_0^{-1}[Y_{M,2}])))$$
$$= (1/\det(\mathrm{Im}((M < Z >)_0))(\det(Y_0^{-1}[[{}^t(C_3 Z_0 + D_0))]]$$
$$+ \frac{1}{\lambda} E_j[[{}^t(i\lambda C_4 + D_4)]])$$

Now

$$\left| e^{\frac{2\pi i}{s} \mathrm{tr}(T_0(M<Z>)_0)} \det(\mathrm{Im}((M < Z >)_0))^{k/2} \right| \leq \prod_{1 \leq \ell \leq n-j} (\lambda_\ell^{k/2} e^{-c\lambda_\ell})$$

where $c = c(T_0) > 0$ and $\lambda_1, \ldots, \lambda_{n-j}$ are the eigenvalues of $\mathrm{Im}((M < Z >)_0)$; hence it is bounded for all M, uniformly as λ goes to infinity. We can now conclude from above that, for fixed Z_0,

$$\lim_{\lambda \to \infty} e^{\frac{2\pi i}{s} \mathrm{tr}(TM<Z>)} (\det M\{Z\})^{-k} = 0,$$

unless $P(\lambda)$ is a constant. Next we determine, for what M, $P(\lambda)$ can turn out to be a constant. The relation above connecting $P(\lambda)$ and abs $(\det M\{Z\})^{-2}$ shows that $P(\lambda) > 0$ while each of $\lambda Y_0^{-1}[[Z_0{}^tC_3 + {}^tD_3]]$ and
124 $E_j[[i\lambda^t C_4 + {}^tD_4]]$ is non-negative definite. Hence, for all λ,

$$\begin{aligned}\det(\lambda^2 C_4{}^tC_4 + D_4^t D_4) &= \det(E_j[[i\lambda{}^tC_4 + {}^tD_4]]) \\ &\leq \det(\lambda Y_0^{-1}[[Z_0^t C_3 + {}^tD_3]] + E_j[[i\lambda{}^tC_4 + {}^tD_4]]).\end{aligned}$$

If $P(\lambda)$ were constant, both sides have the constant value $\det D_4{}^tD_4$ and hence $C_4 = 0$; also $Y_0^{-1}[[Z_0{}^tC_3 + {}^tD_3]]$ is necessarily 0, implying that $C_3 = D_3 = 0$. Finally, therefore $M \in \Delta_{n,n-j}(s)$, under the assumption that $P(\lambda)$ is a constant. Thus, for $j < n$, $\lim\limits_{\lambda\to\infty} e^{\frac{2\pi i}{s}\operatorname{tr}(TM<Z>)} \det M\{Z\}^{-k} = 0$ unless M is in $\Delta_{n,n-j}(s)$; in that case, the limit is, in fact, $e^{\frac{2\pi i}{s}\operatorname{tr}(T_0\underline{M}<Z_0>)}$ $\det \underline{M}\{Z_0\}^{-k}$, since $\det M\{Z\}^{-k} = \det D_4^k \det(C_1Z_0 + D_1)^{-k} = \det \underline{M}\{Z_0\}^{-k}$ and $e^{\frac{2\pi i}{s}\operatorname{tr}(TM<Z>)} = e^{\frac{2\pi i}{s}\operatorname{tr}(T_0(M<Z>)_0)} = e^{\frac{2\pi i}{s}\operatorname{tr}(T_0\underline{M}<Z_0>)}$. To complete the proof for $j < n$, we need only observe that to any coset

$$\Gamma_n(s, \begin{pmatrix} T_0 & 0 \\ 0 & 0 \end{pmatrix}) \begin{pmatrix} A_1 & 0 & B_1 & * \\ * & U & * & * \\ C_1 & 0 & D_1 & * \\ 0 & 0 & 0 & {}^tU^{-1} \end{pmatrix},$$

if we make correspond the coset $\Gamma_{n-j}(s, T_0)\begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix}$, this mapping is clearly well-defined and surjective on $\Gamma_{n-j}(s, T_0)\backslash\Gamma_{n-j}(s)$; it is also easily checked to be injective, since

$$\begin{aligned}&\begin{pmatrix} A_1 & 0 & B_1 & * \\ * & U_1 & * & * \\ C_1 & 0 & D_1 & * \\ 0 & 0 & 0 & {}^tU_1^{-1} \end{pmatrix}\begin{pmatrix} A_1 & 0 & B_1 & * \\ * & U_2 & * & * \\ C_1 & 0 & D_1 & * \\ 0 & 0 & 0 & {}^tU_2^{-1} \end{pmatrix}^{-1} \\ &= \begin{pmatrix} E_{n-j} & 0 & 0 & * \\ * & U_1U_2^{-1} & * & * \\ & & E_{n-j} & * \\ 0 & & & {}^tU_1^{-1}{}^tU_2 \end{pmatrix} \in \Gamma_n(s, \begin{pmatrix} T_0 & 0 \\ 0 & 0 \end{pmatrix}).\end{aligned}$$

Thus

$$\Phi^j(g_k(Z, \begin{pmatrix} T_0 & 0 \\ 0 & 0 \end{pmatrix}; \Gamma_n(s))\Gamma_n(s)) = g_k(Z_0, T_0, \Gamma_{n-j}(s)), \quad \text{for } j < n.$$

$\square$

The proof for the case $j = n$ is immediate on putting $Z = i\lambda E_n$ in the **125**
Fourier expansion of the Eisenstein series $g_k(Z, 0; \Gamma_n(s))$ the only term surviving in the limit is the constant term 1.

Lemma 1.6.6. *For N_1, N_2 in Γ_n with $N_1 \underset{j,s}{\nsim} N_2$ and $j < n$, we have* $\Phi^j(p_k(Z, \begin{pmatrix} T_0^{(n-j)} & 0 \\ 0 & 0 \end{pmatrix}, N_1, \Gamma_n(s))|N_2)) = 0$.

Proof. Indeed $\Phi^j(p_k(Z, \begin{pmatrix} T_0^{n-j} & 0 \\ 0 & 0 \end{pmatrix}, N_1, \Gamma_n(s)|N_2) =$

$$\mathrm{Lim}_{\lambda\to\infty}\, g_k(\begin{pmatrix} Z_0 & 0 \\ 0 & i\lambda E_j \end{pmatrix}, T, \Gamma_n(s))|N_1^{-1}N_2) \quad (\text{with } T = \begin{pmatrix} T_0^{(n-j)} & 0 \\ 0 & 0 \end{pmatrix}).$$

$$= \sum_{M' \in \Gamma_n(s,T)\backslash\Gamma_n(s)} \mathrm{Lim}_{\lambda\to\infty}\, e^{\frac{2\pi i}{e^s}\operatorname{tr}(T(M'N_1^{-1}N_2)<\begin{pmatrix} Z_0 & 0 \\ 0 & i\lambda E_j \end{pmatrix}>)}$$

$$(\det(M'N_1^{-1}N_2)\{\begin{pmatrix} Z_0 & 0 \\ 0 & i\lambda E_j \end{pmatrix}\})^{-k}$$

$$= 0,$$

since, for no M' in $\Gamma_n(s)$, $M'N_1^{-1}N_2 = N_1^{-1} \cdot (N_1 M' N_1^{-1})N_2 \in \Delta_{n,n-j}$, by the hypothesis $N_1 \underset{j,s}{\nsim} N_2$ and so the limit of every term is 0, by the same arguments as in the proof of Lemma 1.6.5. ◻

We now recall the structure of the finite dimensional space γ of cusp
126 forms in (n, k, s). As we know, given f, g in $\{n, k, s\}$ at least one of which is a cusp from, the scalar product (f, g) is defined by

$$\frac{1}{v} \int_{T_n(s)\backslash\mathscr{G}_n} f(Z)\overline{g}(Z) \frac{dXdY}{(\det Y)^{n+1-k}}$$

with the customary (invariant) volume element $dv = (\det Y)^{-(n+1)}dX\, dY$. Corresponding to $Z = X + iY$ in $\mathscr{G}_n$ and $v := \int_{\Gamma_n(s)\backslash\mathscr{G}_n} dv < \infty$. If $f(Z) = \sum_{T>0} a(T)e^{\frac{2\pi i}{s}\operatorname{tr}(TZ)}$ is a cusp form in $\{n, k, s\}$, the scalar product $(f(Z), g_k(Z, S; \Gamma_n(s))$ is, upto a constant factor, equal to $(\det S)^{\frac{n+1}{2}-k}a(S)$ for $S > 0$ and 0 if $\det S = 0$. If $\mathcal{I}$ denotes the subspace of γ generated by $g_k(Z, T; \Gamma_n(s))$ for semi-integral $T^{(n)} > 0$. Then, using the (non-degenerate) scalar product (,) in γ, there exists an orthogonal complement $\mathfrak{n}$ for $\mathcal{I}$ in γ i.e. $\gamma = \mathcal{I} \oplus \mathfrak{n}$. We claim that $\mathfrak{n} = \{0\}$; in fact, any f in $\mathfrak{n}$ is orthogonal to $g_k(Z, S; \Gamma_n(s))$ for every semi integral $S > 0$ and hence the Fourier expansion of f has all coefficients equal to 0 i.e. $f = 0$.

Lemma 1.6.7. *Suppose that, for $f \in \{n, k, s\}$, $\Phi^j(f|R)$ is a cusp form for R in Γ_n, whenever $j < n$. Then there exists*

$$\varphi_{R,j}(Z) = \varphi_{R,j}(Z; f) := \sum_\nu C_\nu p_k(Z; \begin{pmatrix} T_{R,\nu} & 0 \\ 0 & 0 \end{pmatrix}; R; \Gamma_n(s))$$

such that $\Phi^j((f - \varphi_{R,j})|R) = 0$, for every R in Γ_n.

Proof. First, let $j < n$. Since $\Phi^j(f|R)$ is a cusp form, there exist, by the above remarks, finitely many $T_{R,\nu}^{(n-j)} > 0$ and constants $c_\nu = c_\nu(R; f)$ such that **127**

$$\begin{aligned}
(\Phi^j(f|R))(Z_0) &= \sum_\nu c_\nu g_k(Z_0; T_{R,\nu}; \Gamma_{n-j}(s)) \qquad (Z_0 \in \mathscr{G}_{n-j}) \\
&= \sum_\nu c_\nu \Phi^j(g_k(Z; \begin{pmatrix} T_{R,\nu} & 0 \\ 0 & 0 \end{pmatrix}; \Gamma_n(s))), \quad \text{by Lemma 5} \\
&= \sum_\nu c_\nu \Phi^j(p_k(Z; \begin{pmatrix} T_{R,\nu} & 0 \\ 0 & 0 \end{pmatrix}; R; \Gamma_n(s))|R), \quad \text{by Lemma 4}
\end{aligned}$$

which proves the lemma for $j < n$. For $j = n$, we need only to take $\varphi_{R,n}(Z) = a(0, R) p_k(Z, 0; R; \Gamma_n(s))$, since

$$\Phi^n(f|R) = \Phi^n(\sum a(T, R) e^{\frac{2\pi i}{s} \operatorname{tr}(TZ)}) = a(0, R) \quad \text{and}$$

$$\Phi^n(p_k(Z, 0; R; \Gamma_n(s))|R) = \Phi^n(g_k(Z, 0; \Gamma_n(s)) = 1. \qquad \square$$

From Lemma 1.6.2, we know that $\Phi^j(f|R) = 0$ for every R in $Sp(n, \mathbb{Q})$, if already $\Phi^j(f|M_i) = 0$ for finitely many $M_1, \ldots, M_t$ in Γ_n. From these M_i, we pick a maximal set of representatives, say $M_1', \ldots, M_{u_j}'$ which are mutually $\tilde{j, s}$-inequivalent. Let now f satisfy the conditions stated in Lemma 1.6.7. For fixed j, let us consider

$$\psi_j(Z) := \sum_{1 \le \ell \le u_j} \varphi_{M_\ell', j}(Z) = \sum_{1 \le \ell \le u_j} \sum_\gamma c_{\ell,\nu} p_k(Z; \begin{pmatrix} T_{M_\ell',\nu} & 0 \\ 0 & 0 \end{pmatrix}; M_\ell'; \Gamma_n(s))$$

with the same notation as in Lemma 1.6.7. Now any $M_i (1 \leq i \leq t)$ is
128 $\underset{j,s}{\sim} M'_m$ for some m with $1 \leq m \leq u_j$; we have then,

$$\Phi^j((f - \psi_j)|M_i) = \Phi^j(f|M_i - \varphi_{M'_m,j}|M_i) = \Phi^j((f - \varphi_{M'_m,j})|M_i) = 0,$$

in view of Lemmas 1.6.6, 1.6.7 and 1.6.3, giving us

Lemma 1.6.8. *For φ in $\{n, k, s\}$, suppose that, whenever $j < n$, $\Phi^j(\varphi|M)$ is a cusp form, for every M in Γ_n. Then there exists ψ_j in $\{n, k, s\}_{n-j} :=$ $\{$linear-combinations of $p_k(Z; \begin{pmatrix} T_0^{(n-j)} & 0 \\ 0 & 0 \end{pmatrix}, M, \Gamma_n(s))\}$ such that $\Phi^j((\varphi - \psi_j)|M) = 0$ for every M in Γ_n and $1 \leq j \leq n$.*

Finally we state and prove the following Representation Theorem for modular forms.

Theorem 1.6.9. *For even integral $k > 2n + 1$, every f in $\{n, k, s\}$ is a finite linear combination of the Poincaré series $p_k(Z, T, N, \Gamma_n(s))$ for semi-integral $T \geq 0$ and N in Γ_n.*

Proof. First we need to formulate an inductive statement, following H. Braun. Let $2 \leq j \leq n$ and $R = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Gamma_{n-j+1}$ with $(n - j + 1, n - j + 1)$ submatrices A, B, C, D. Then

$$R' := \begin{pmatrix} A & 0 & B & 0 \\ 0 & E_{j-1} & 0 & 0 \\ C & 0 & D & 0 \\ 0 & 0 & 0 & E_{j-1} \end{pmatrix}$$

is in Γ_n and further for any f' in $\{n, k, s\}$ $\Phi^j(f'|MR') = \Phi(\Phi^{j-1}(f'|MR'))$
129 for any M in Γ_n and from the special form of R', we have $\Phi^{j-1}(f|MR') =$ $(\Phi^{j-1}(f'|M))|R$. Thus we have, for any M in Γ_n and R in Γ_{n-j+1},

$$\Phi^j(f'|MR') = \Phi((\Phi^{j-1}(f'|M))|R). \tag{$*$}$$

Now, from Lemma 1.6.7, there exists ψ_n in $\{n, k, s\}$ such that

$$\Phi^n((f - \psi_n)|M) = 0 \quad \text{for every} \quad M \quad \text{in} \quad \Gamma_n.$$

Assume now that, for any fixed j with $1 \leq j \leq n$ and for the given f denoted as f_0, we have already constructed f_{n-j} in $\{n,k,s\}$ so that $\Phi^j(f_{n-j}|M))$ is a cusp form for every M in Γ_n. Then by Lemma 1.6.8, there exists ψ_j (corresponding to $\varphi = f_{n-j}$) such that

$$\Phi^j((f_{n-j} - \psi_j)|M) = 0 \quad \text{for every} \quad M \quad \text{in} \quad \Gamma_n, (**)_j$$

where $\psi_j \in \{n,k,s\}_{n-j}$, is a linear combination of the Poincaré series

$$p_k(Z; \begin{pmatrix} T^{(n-j)} & 0 \\ 0 & 0 \end{pmatrix}; M'; \Gamma_n(s)).$$

Note that for $j = n$, aψ_n with $\Phi^n((f_0 - \psi_n)|M) = 0$ for every M in Γ_n already exists. From $(**)_j$ and $(*)$, we obtain

$$\Phi((\Phi^{j-1})((f_{n-j} - \psi_j)|M))|R) = 0 \quad \text{for every} \quad M \quad \text{in} \quad \Gamma_n \quad \text{and every} \quad R \quad \text{in} \quad \Gamma_{n-j+1}$$

whenever $2 \leq j \leq n$. If we set $f_{n-j+1} = f_{n-j} - \psi_j$, the last relation means that, for every M in Γ_n, $\Phi^{j-1}(f_{n-j+1}|M)$ is a cusp form. Applying Lemma 1.6.8 to f_{n-j+1} in place of f and $j-1$ in place of j (for which we **130**
had the condition $2 \leq j \leq n$), there exists ψ_{j-1} in $\{n,k,s\}_{n-j+1}$ as defined above, such that $\Phi^{j-1}((f_{n-j+1} - \Psi_{j-1})|M) = 0$ for every M in Γ_n, which is just $(**)_{j-1}$. Thus the inductive argument is complete, giving us the validity of $(**)_1$, i.e.

$$0 = \Phi((f_{n-1} - \Psi_1)|M) = \Phi((f - \sum_{1 \leq \ell \leq n} \psi_\ell)|M) \quad \text{for every} \quad M \ \text{ in } \ \Gamma_n.$$

In other words, $f - \sum_{1 \leq \ell \leq n} \psi_\ell$ is a cusp form. Since the space of cusp forms is generated by $p_k(Z; T^{(n)}; E_{2n}; \Gamma_n(s))$ with semi-integral $T > 0$, the proof of the theorem is complete. □

Let us now identify the Poincaré series g_k in terms of "lifts" (i.e. Eisenstein series $E(Z; f)$, in the sense of Klingen, arising) from cusp forms f of degree $\leq n$. Let f be a cusp form in $\{r,k,s\}$. Then for every $k > n + r + 1$, we define, after Klingen,

$$E^k_{n,r}(Z; f) := \sum_{M \in \Delta_{n,r}(s) \backslash \Gamma_n(s)} f((M < Z >)^*)(\det M\{Z\})^{-k}$$

where, for any (n, n) matrix A, we denote its top(leftmost) (r, r) submatrix by A^*. The series is well-defined, since for M, N in $\Gamma_n(s)$ with M in $\Delta_{n,r}(s)N$, we can easily verify that $f(M < Z >^*)(\det M\{Z\})^{-k} = f(N < Z >^*)(\det N\{Z\})^{-k}$; further it represents an element of $\{n, k, s\}$. If
131 $T^{(n)} = \begin{pmatrix} T_0^{(r)} & 0 \\ 0 & 0 \end{pmatrix}$ with $T_0 > 0$, then we know already that the correspondence

$$\begin{aligned}\Gamma_n(s,T)M = \Gamma_n(s,T)\begin{pmatrix} A_0^{(r)} & 0 & B_0^{(r)} & * \\ * & U & * & * \\ C_0^{(r)} & 0 & D_0^{(r)} & * \\ 0 & 0 & 0 & {}^tU^{-1} \end{pmatrix} &\mapsto \Gamma_r(s,T_0)\begin{pmatrix} \Lambda_0 & B_0 \\ C_0 & D_0 \end{pmatrix} \\ &= \Gamma_r(s,T_0)\underline{M}\end{aligned}$$

from the coset space $\Gamma_n(s,T)\backslash\Delta_{n,r}(s)$ to the coset space $\Gamma_r(s,T_0)\backslash\Gamma_r(s)$ is a bijection. From the coset decompositions $\Gamma_n(s) = \coprod_{M_\ell} \Delta_{n,r}(s)M_\ell$, $\Delta_{n,r}(s) = \coprod_{N_j} \Gamma_n(s,T)N_j$, we get $\Gamma_n(s) = \coprod_{M_\ell, N_j} \Gamma_n(s,T)N_jM_\ell$.

Now

$$\begin{aligned} e^{\frac{2\pi i}{s}\operatorname{tr}(T(N_jM_\ell)<Z>)} &= e^{\frac{2\pi i}{s}\operatorname{tr}(T_0((N_jM_\ell)<Z>)^*)} = \\ = e^{\frac{2\pi i}{s}\operatorname{tr}(T_0(N_j<M_\ell<Z>>)^*)} &= e^{\frac{2\pi i}{s}\operatorname{tr}(T_0\underline{N_j}<(M_\ell<Z>)^*>)}\end{aligned}$$

with $\underline{N_j}$ in $\Gamma_r(s)$ corresponding to N_j in $\Delta_{n,r}(s)$ in the sense explained already. Moreover,

$$\begin{aligned}(\det(N_jM_\ell)\{Z\})^{-k} &= (\det N_j\{M_\ell < Z >\})^{-k} \times (\det M_\ell\{Z\})^{-k} \\ &= (\det \underline{N_j}\{(M_\ell < Z >)^*\})^{-k}(\det M_\ell\{Z\})^{-k}.\end{aligned}$$

132 Now we have

$$\begin{aligned} g_k(Z,T;\Gamma_n(s)) &= \sum_{M\in\Gamma_n(s,T)\backslash\Gamma_n(s)} e^{\frac{2\pi i}{s}\operatorname{tr}(TM<Z>)}(\det M\{Z\})^{-k} \\ &= \sum_{\substack{M_\ell\in\Delta_{n,r}(s)\backslash\Gamma_n(s) \\ N_j\in\Gamma_n(s,T)\backslash\Delta_{n,r}(s)}} e^{\frac{2\pi i}{s}\operatorname{tr}(T(N_jM_\ell)<Z>)}(\det(N_jM_\ell)\{Z\})^{-k} \\ &= \sum_{M_\ell}(\det M_\ell\{Z\})^{-k}\sum_{N_j} e^{\frac{2\pi i}{s}\operatorname{tr}(T_0\underline{N_j}<(M_\ell<Z>)^*>)}\end{aligned}$$

$$
\begin{aligned}
&(\det \underline{N_j}\{(M_\ell < Z >)^*\})^{-k}\\
&= \sum_{M_\ell \in \Delta_{n,r}(s)\backslash \Gamma_n(s)} (\det M_\ell\{Z\})^{-k} \sum_{\underline{N_j} \in \Gamma_r(s,T_0)\backslash \Gamma_r(s)} e^{\frac{2\pi i}{s}\operatorname{tr}(T_0 \underline{N_j}<(M_\ell<Z>)^*>)}\\
&\quad (\det \underline{N_j}\{(M_\ell < Z >)^*\})^{-k}\\
&= E^k_{n,r}(Z; g_k(*, T_0; \Gamma_r(s))).
\end{aligned}
$$

We may reformulate the theorem above as the following assertion: for even integral $k > 2n+1$, the space $\{n,k,s\}$ is generated by $E^k_{n,r}(Z;g)|M$ as g varies over cusp forms of degree $r(\leq n)$ and M over Γ_n.

Using the above Representation Theorem for $\{n,k,s\}$ in terms of the Eisenstein series $E^k_{n,j}(Z;f)$ constructed from cusp forms f in $\{j,k,s\}$ and the estimate for Fourier coefficients of cusp forms (analogous to Theorem 1.1.1), we proceed now to derive an estimate for the Fourier coefficients of modular forms in $\{n,k,s\}$ for even integral $k \geq 2n+2$. To this end, we shall prove, following Kitaoka [10], a series of lemmas and propositions.

We decompose any M in Γ_n as $M = \begin{pmatrix} A_M & B_M \\ C_M & D_M \end{pmatrix}$ with (n,n) submatrices **133**
A_M, B_M, C_M, D_M. For any (p,q) matrix F and any s with $1 \leq s \leq p$, we denote the (s,q) matrix formed from the last s rows of F by $\lambda_s(F)$. For $0 \leq r \leq n$, $\{M \in \Gamma_n |$ the first $n+r$ columns of $\lambda_{n-r}(M)$ are $0\}$ is just the group $\Delta_{n,r}(1)$ introduced earlier. Indeed, for any such M,

$$
A_M = \begin{pmatrix} A_1 & A_2 \\ A_3 & A_4 \end{pmatrix}, B_M = \begin{pmatrix} B_1 & B_2 \\ B_3 & B_4 \end{pmatrix}, C_M = \begin{pmatrix} C_1 & C_2 \\ 0 & 0 \end{pmatrix}, D_M = \begin{pmatrix} D_1 & D_2 \\ 0 & D_4 \end{pmatrix}
$$

with A_1, B_1, C_1, D_1 of size (r,r) and further D_4 is in $GL_{n-r}(\mathbb{Z})$, $A_4{}^tD_4 = E_{n-r}$, $A_2{}^tD_4 = 0$, $C_2{}^tD_4 = 0$, and therefore $A_2 = 0$, $C_2 = 0$, $A = \begin{pmatrix} A_1 & 0 \\ A_3 & A_4 \end{pmatrix}$. Moreover, $\Delta_{n,r}(s) = \Delta_{n,r} \cap \Gamma_n(s)$. If we write $M_1 = \begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix}$ for any (such) M in $\Delta_{n,r}$, then M_1 is in Γ_r. If Z_1 is the leading (r,r) submatrix of Z in $\mathscr{G}_n$, then it is easy to see that $M_1 < Z_1 >$ is the leading (r,r) submatrix of $M < Z >$ and further $\det M\{Z\} = (\det M_1\{Z_1\}).\ \det D_4$, where $N\{Z\} := C_N Z + D_N$ for any N in Γ_n.

Lemma 1.6.10. *For M, N in Γ_n, $\Delta_{n,r}M = \Delta_{n,r}N$ if and only if $\lambda_{n-r}(M) \in GL_{n-r}(\mathbb{Z})\lambda_{n-r}(N)$.*

Proof. From the form of the elements of $\Delta_{n,r}$, clearly $\Delta_{n,r}M = \Delta_{n,r}N$ **134**
implies that $\lambda_{n-r}(M) = V\lambda_{n-r}(N)$ for some V in $GL_{n-r}(\mathbb{Z})$. On the other hand, if $\lambda_{n-r}(M) \in GL_{n-r}(\mathbb{Z})\lambda_{n-r}(N)$, we may already suppose, without loss of generality, that $\lambda_{n-r}(M) = \lambda_{n-r}(N)$ after replacing M by $\left(\begin{smallmatrix} {}^tU^{-1} & 0 \\ 0 & U \end{smallmatrix}\right) M$ for $U = \left(\begin{smallmatrix} E_r & 0 \\ 0 & V \end{smallmatrix}\right)$ with a suitable V in $GL_{n-r}(\mathbb{Z})$. But then we have evidently $\lambda_{n-r}(MN^{-1}) = (0^{(n-r,n+r)}E_{n-r})$ and we are through. □

Lemma 1.6.11. *For any M in Γ_n with rank $(\lambda_s(C_M)) < s = n - r(< n)$, there exists N in $\Delta_{n,n-1}$ such that $\Delta_{n,r}M \ni N\left(\begin{smallmatrix} U & 0 \\ 0 & {}^tU^{-1} \end{smallmatrix}\right)$ for some U in $GL_n(\mathbb{Z})$.*

Proof. From the hypothesis, there exist V in $GL_s(\mathbb{Z})$ and W in $GL_n(\mathbb{Z})$ such that $\lambda_1(V\lambda_s(C_M)W) = 0$. Then, for $K := \left(\begin{smallmatrix} * & 0 & \\ & E_r & 0 \\ 0 & 0 & V \end{smallmatrix}\right) M \left(\begin{smallmatrix} W & 0 \\ 0 & {}^tW^{-1} \end{smallmatrix}\right)$, we have $\lambda_1(C_K) = 0$ and hence the elements of $\lambda_1(D_K)$ are relatively prime. It is clear that $D_K = \left(\begin{smallmatrix} * \\ 0\ldots 01 \end{smallmatrix}\right) F$ for some F in $GL_n(\mathbb{Z})$. If we set $N = K\left(\begin{smallmatrix} {}^tF & 0 \\ 0 & F^{-1} \end{smallmatrix}\right)$, then $\lambda_1(N) = (0\ldots 01)$ and consequently N is in $\Delta_{n,n-1}$. The lemma follows on taking $U = W^tF$. □

135 Let f be a cusp form in $\{r, k, \ell\}$ for fixed $r \leq n-1$ and even integral $k \geq n+r+2$. Let us denote, in the sequel, the leading (r,r) submatrix P_1 of $P^{(n,n)} = \left(\begin{smallmatrix} P_1 & P_2 \\ P_3 & P_4 \end{smallmatrix}\right)$, by P^*. For any M in Γ_n, let us abbreviate $f((M < Z >)^*)\,(\det(C_M Z + D_M))^{-k}$ as $(f|M)(Z)$. For any given R in Γ_n, we split the (absolutely convergent) Eisenstein series $E^k_{n,r}(Z; f)|R$ as the sum of two subseries $\sum\limits_i = \sum\limits_N (f||N)(Z)$, $i = 1, 2$ where N runs over a complete set of elements $N_1, N_2, \ldots$ in $\Gamma_n(\ell)R$ such that $N_i \notin \Delta_{n,r}(\ell)N_j$ for $i \neq j$ and the rank of $\lambda_{n-r}(C_N)$ is $n-r$ for N occurring in $\sum\limits_1$ and $< n-r$ for N in $\sum\limits_2$. Now $C_M = C_N$ for $M := N\left(\begin{smallmatrix} E_n & \ell S \\ 0 & E_n \end{smallmatrix}\right)$ and any integral symmetric $S^{(n,n)}$. Thus the subseries $\sum\limits_i$ represent functions invariant under all translations $Z \to Z + \ell S$ and admit Fourier expansions $\sum_{T \geq 0} a_i(T) \exp(2\pi i \operatorname{tr}(TZ)/\ell)$.

Lemmas 1.6.10, 1.6.11 lead to the following

Proposition 1.6.12. *For a cusp form f in $\{r, k, \ell\}$ as above and R in Γ_n,* *all the Fourier coefficients $a_2(T)$ for $T > 0$ of*

$$\sum_2 = \sum_{\substack{N \in \Delta_{n,r}(\ell)\backslash\Gamma_n(\ell)R \\ \operatorname{rank}(\lambda_{n-r}(C_N))<n-r}} (f \| N)(Z)$$

vanish.

Proof. By Lemma 1.6.11, there exist K in $\Delta_{n,r}$, M in $\Delta_{n,n-1}$ and U in $GL_n(\mathbb{Z})$ such that $N = KM\begin{pmatrix} U & 0 \\ 0 & {}^tU^{-1} \end{pmatrix}$. Let $K^* := \begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix}$ in Γ_r formed from the leading (r, r) submatrices of A_K, B_K, C_K, $D_K = \begin{pmatrix} * & * \\ 0 & D_4 \end{pmatrix}$. It is easy to verify that **136**

$$\begin{aligned}
\det N\{Z\} &= (\det(KM)\{UZ^tU\})/(\det U) \\
&= (\det((C_K A_M + D_K C_M)UZ^tU + C_K B_M + D_K D_M)) \det U \\
&= \det(C_K M < UZ^tU > + D_K) \det(C_M UZ^tU + D_M) \det U \\
&= \det(C_1 M < UZ^tU >)^* + D_1) \det D_4 \cdot \det(M\{UZ^tU\}) \det U \\
&= \det(K^*\{(M < UZ^tU >)^*\} \det(M\{UZ^tU\}) \det D_4 \cdot \det U
\end{aligned}$$

and moreover,

$$\begin{aligned}
(N < Z >)^* &= ((KM) < UZ^tU >)^* = (K < MUZ^tU >>)^* \\
&= K^*(M < UZ^tU >)^* > .
\end{aligned}$$

On the other hand, there exist constants $\alpha_1, \ldots, \alpha_m$ (depending on f and K) such that

$$f(K^* < W >)(\det K^*\{W\})^{-k} = \sum_{1 \le j \le m} \alpha_j f_j(W) \quad \text{for} \quad W \in \mathscr{G}_r$$

where $f_1, \ldots, f_m$ form a basis of the space of cusp forms in $\{r, k, \ell\}$. Hence $(f\|N)(Z) = f(K^* < (M < UZ^tU >)^* >)(\det K^*\{(M < UZ^tU >)^*\})^{-k}(\det M\{UZ^tU\})^{-k} = \sum_j \alpha_j f_j((M < UZ^tU >)^*)(\det M\{UZ^tU\})^{-k} = \sum_j \alpha_j (f_j\|M)(UZ^tU)$. Decomposing $Z = X + iY$ in $\mathscr{G}_n$ as $\begin{pmatrix} Z_1 & Z_2 \\ {}^tZ_2 & Z_3 \end{pmatrix}$ with Z_1 in $\mathscr{G}_{n-1}$ and writing

$$A_M = \begin{pmatrix} A_1' & 0 \\ A_3' & a_4 \end{pmatrix}, B_M = \begin{pmatrix} B_1' & B_2' \\ B_3' & b_4 \end{pmatrix}, C_M = \begin{pmatrix} C_1' & 0 \\ 0 & 0 \end{pmatrix}, D_M = \begin{pmatrix} D_1' & D_2' \\ 0 & d_4 \end{pmatrix}$$

with A'_1, B'_1, C'_1, D'_1 of size $(n-1, n-1)$, we have $\det M\{Z\} = \det(C'_1 Z_1 + D'_1)d_4$ and $M < Z >$ has $(A'_1 Z_1 + B'_1)(C'_1 Z_1 + D'_1)^{-1}$ as its leading $(n - 1, n-1)$ submatrix. Thus $(f_j \| M)(Z)$ is independent of the variables Z_2 and z_3. 137

For $Y = (y_{pq}) = \operatorname{Im} Z$, let us write $\dfrac{\partial}{\partial Y} = \left(\varepsilon_{pq} \dfrac{\partial}{\partial y_{pq}}\right)$ with $\varepsilon_{pq} = 1$ or $1/2$ according as $p = q$ or $p \neq q$ and denote by D_Y the differential operator $(\det Y)(\det \dfrac{\partial}{\partial Y})$ known to be invariant under $Y \mapsto VY{}^tV$ for all V in $GL_n(\mathbb{R})$. Then it is clear that

$$\begin{aligned} D_Y((f \| N)(Z)) &= \sum_j \alpha_j D_Y((f_j \| M)(UZ{}^tU)) \\ &= \sum_j \alpha_j D_Y((f_j \| M)(UX{}^tU + iY)) \quad (\text{using } \ Y \mapsto UY{}^tU) \\ &= 0 \end{aligned}$$

and so $D_Y(\sum_2) = 0$. On the other hand, we know that

$$(\det \frac{\partial}{\partial Y})(\exp(2\pi i \operatorname{tr}(TZ)/\ell) = \det(-(2\pi/\ell)T) \exp(2\pi i \operatorname{tr}(TZ)/\ell).$$

Thus, on applying D_Y termwise to the Fourier expansion of $\sum_2$ (as is indeed permissible), it follows that

$$\sum_{T \geq 0} a_2(T) \det(-(2\pi/\ell)T) \exp(2\pi i \operatorname{tr}(TZ)/\ell) = 0.$$

Consequently, for all $T > 0$, we have $a_2(T) = 0$ and the proposition is proved. $\square$

Our objective being to get an estimate for the Fourier coefficients of Eisenstein series for $T > 0$ or (indeed) for $a_1(T)$, in view of Proposition 1.6.12 above, we should first get a system of representatives of the right
138 cosets of $\Gamma_n(\ell)$ modulo $\Delta_{n,r}(\ell)$ containing N with $\operatorname{rank}(\lambda_{n-r}(C_N)) = n-r$. The next few lemmas tackle this question for $\ell = 1$.

Lemma 1.6.13. *For any n-rowed symmetric pair (C, D) there exists a coprime symmetric pair (P, Q) such that $C\,{}^tP + D\,{}^tQ = 0$.*

Proof. If $C = 0$, we can trivially take $P = E^{(n)}$, $Q = 0$. Let then $C \neq 0$ and first, let $\det C \neq 0$. Then there exist U in $GL_n(\mathbb{Z})$ and $V = \begin{pmatrix} V_1^{(n)} & V_2 \\ V_3 & V_4 \end{pmatrix}$ in $GL_{2n}(\mathbb{Z})$ such that $U(CD)V^{-1} = (G0)$ with (n, n) integral non-singular G. Hence $(G^{-1}UCG^{-1}UD) = (V_1 V_2)$; evidently (V_1, V_2) is a symmetric pair, which being primitive is coprime as well. The lemma follows on taking $P = V_2$, $Q = -V_1$. If $0 < r = \operatorname{rank} C < n$, there exist U_1, U_2 in $GL_n(\mathbb{Z})$ with $U_1 C U_2 = \begin{pmatrix} C_1 & 0 \\ 0 & 0 \end{pmatrix}$ and $\det C_1 \neq 0$. Now $U_1 C U_2$ and $U_1 D {}^t U_2^{-1} = \begin{pmatrix} D_1^{(r,r)} & D_2 \\ D_3 & D_4 \end{pmatrix}$ form a symmetric pair again implying that (C_1, D_1) is a symmetric pair; further $C_1 {}^t D_3 = 0$ and so $D_3 = 0$. By the earlier case, there an r-rowed coprime symmetric pair (P_1, Q_1) with $C_1 {}^t P_1 + D_1 {}^t Q_1 = 0$. The lemma is now immediate, on taking $P = \begin{pmatrix} P_1 & 0 \\ 0 & E_{n-r} \end{pmatrix} {}^t U_2$, $Q = \begin{pmatrix} Q_1 & 0 \\ 0 & 0 \end{pmatrix} U_2^{-1}$. The next lemma is quite vital for the sequel. ◻

Lemma 1.6.14. *For any M in Γ_n with $\operatorname{rank}(\lambda_{n-r}(C_M)) = n - r$, there exists N in $\Delta_{n,r} M$ such that $\det C_N \neq 0$ and further $(A_N C_N^{-1})^*$ is integral.*

Proof. First, there exist U_4 in $GL_{n-r}(\mathbb{Z})$ and V in $GL_n(\mathbb{Z})$ such that **139**
$U_4 \lambda_{n-r}(C_M) {}^t V = (0 \;\; C_4^{(n-r,n-r)})$; necessarily then, $\det C_4 \neq 0$. Then for

$$U := \begin{pmatrix} E_r & 0 \\ 0 & U_4 \end{pmatrix}, K := \begin{pmatrix} {}^t U^{-1} & 0 \\ 0 & U \end{pmatrix} M \begin{pmatrix} {}^t V & 0 \\ 0 & V^{-1} \end{pmatrix} \text{ is in } \Delta_{n,r} M \begin{pmatrix} {}^t V & 0 \\ 0 & V^{-1} \end{pmatrix}$$

and moreover, $C_K = \begin{pmatrix} C_1 & C_2 \\ 0 & C_4 \end{pmatrix}$. Correspondingly, if $A_K = \begin{pmatrix} A_1 & A_2 \\ A_3 & A_4 \end{pmatrix}$, then, from the relation ${}^t C_K A_K = {}^t A_K C_K$, we get ${}^t C_1 A_1 = {}^t A_1 C_1$. Applying Lemma 1.6.13 to the r-rowed symmetric pair $({}^t C_1, {}^t A_1)$, there exists an r-rowed coprime symmetric pair (R_1, S_1)-and consequently, some $\begin{pmatrix} Q_1 & P_1 \\ S_1 & R_1 \end{pmatrix}$ in Γ_r-such that ${}^t C_1 {}^t R_1 + {}^t A_1 {}^t S_1 = 0$ i.e. $R_1 C_1 + S_1 A_1 = 0$. ◻

Now $L : \begin{pmatrix} Q_1 & 0 & P_1 & 0 \\ 0 & {}^t U_4^{-1} & 0 & 0 \\ S_1 & 0 & R_1 & 0 \\ 0 & 0 & 0 & U_4 \end{pmatrix}$ is in $\Delta_{n,r}$ and further, clearly, for $H :=$ $LM \begin{pmatrix} {}^t V & 0 \\ 0 & V^{-1} \end{pmatrix}$, we have $A_H = \begin{pmatrix} A_1' & A_2' \\ A_3 & A_4 \end{pmatrix}$ and $C_H = \begin{pmatrix} 0 & C_2' \\ 0 & C_4 \end{pmatrix}$.

From ${}^t C_H A_H = {}^t A_H C_H$, we obtain ${}^t A_1' C_2' + {}^t A_3 C_4 = 0$ i.e. $A_3 = -{}^t C_4^{-1} {}^t C_2' A_1'$. Since the rank of the matrix formed by the first r columns

of H is r, the last relation implies that A_1' has necessarily rank r i.e. $\det A_1' \neq 0$. Now $N := \begin{pmatrix} E_n & & 0 \\ E_r & 0 & E_n \\ 0 & 0 & \end{pmatrix} H \begin{pmatrix} {}^tV^{-1} & 0 \\ 0 & V \end{pmatrix}$ is evidently in $\Delta_{n,r}M$ and
140 moreover, $C_N = \begin{pmatrix} A_1' & A_2'+C_2' \\ 0 & C_4 \end{pmatrix} {}^tV^{-1}$ is indeed non-singular. Since $A_N = \begin{pmatrix} A_1' & A_2' \\ A_3 & A_4 \end{pmatrix} {}^tV^{-1}$, $(A_N C_N^{-1})^* = E_r$, which proves the lemma.

Let (C_4, D_4) be an $(n-r)$-rowed integral symmetric pair with $\det C_4 \neq 0$ and D_3 an $(n-r, r)$ integral matrix such that $F := (C_4 D_3 D_4)$ is primitive. To F, we associate a unique right coset of Γ_n modulo $\Delta_{n,r}$ as follows (and denote it by $\Delta_{n,r}M\{C_4, D_3, D_4\}$. Indeed, there exists V in $GL_{2(n-r)}(\mathbb{Z})$ such that $(C_4 D_4)V^{-1} = (0\ G)$ for an integral $(n-r, n-r)$ nonsingular matrix G. Now $(G^{-1}C_4, G^{-1}D_4) = (0, E_{n-r})V$ is an integral symmetric pair which (being primitive) is a coprime pair as well. Further, since $(D_3 C_4 D_4) = (D_3(0G)V)$ is primitive, so are $(D_3 0 G)$ and $(D_3 G)$. Thus there exists U in $GL_n(\mathbb{Z})$ with $\lambda_{n-r}(U) = (D_3 G)$. Now it is clear that $C := U \begin{pmatrix} 0 & 0 \\ 0 & G^{-1}C_4 \end{pmatrix}$, $D := U \begin{pmatrix} E^{(r)} & 0 \\ 0 & G^{-1}D_4 \end{pmatrix}$ form a coprime symmetric pair and $\lambda_{n-r}(C) = (0C_4)$, $\lambda_{n-r}(D) = (D_3 D_4)$. Choose any M in Γ_n with $\lambda_n(M) = (CD)$; then, clearly $\lambda_{n-r}(M) = (0 C_4 D_3 D_4)$. By Lemma 1.6.14, there exists N in $\Delta_{n,r}M$ such that $\det C_N \neq 0$ and $(A_N C_N^{-1})^*$ is integral. Now there exists W_4 is $GL_{n-r}(\mathbb{Z})$ such that $W_4 \lambda_{n-r}(N) = \lambda_{n-r}(M)$ and we take, for $M\{C_4, D_3, D_4\}$, the matrix $P = \begin{pmatrix} {}^tW^{-1} & 0 \\ 0 & W \end{pmatrix} N$ where $W := \begin{pmatrix} E_r & 0 \\ 0 & W_4 \end{pmatrix}$. Clearly $\lambda_{n-r}(P) = W_4 \lambda_{n-r}(N) = \lambda_{n-r}(M) = (0 C_4 D_3 D_4)$, $\det C_p \neq 0$ and $(A_P C_p^{-1})^*$ is integral. Any such P is denoted as $M\{C_4, D_3, D_4\}$; by Lemma 1.6.10, $\Delta_{n,r}M\{C_4, D_3, D_4\}$ is uniquely determined by $(C_4 D_3 D_4)$ from which we started above.

141 Denote by $\mathscr{C}_{n,r}$ the set of $F = (C_4 D_3 D_4)$ as described at the beginning of the last paragraph and define two such matrices F, F' to be equivalent (in symbols, $F \sim F'$) if $F = WF'$ for some W in $GL_{n-r}(\mathbb{Z})$. Let $P(n, r; \mathbb{Z}) = \{U = \begin{pmatrix} U_1^{(r,r)} & U_2 \\ 0 & U_4 \end{pmatrix} \in GL_n(\mathbb{Z})\}$. In $\mathscr{C}_{n,r}$, introduce also another equivalence relation $F = (C_4 D_3 D_4) = (C_4' D_3' D_4') = F'$ by the condition $WF' = (C_4 D_3 + C_4 S_3 D_4 + C_4 S_4)$ for some W in $GL_{n-r}(\mathbb{Z})$, integral $(n-r)$-rowed symmetric S_4 and $(n-r, r)$ integral S_3. It is easily verified $F - F'$ if and only if

$$\Delta_{n,r}M\{C_4', D_3', D_4'\} = \Delta_{n,r}M\{C_4, D_3, D_4\}P \ \text{ for}$$

$$P = \begin{pmatrix} E^{(n)} & 0^{(r,r)} & {}^tS_3 \\ 0 & S_3 & S_4 \\ 0 & E^{(n)} & \end{pmatrix} \text{ in } \Gamma_n.$$

We now prove the following crucial

Lemma 1.6.15. (i)

$$\coprod_{\substack{M\in\Gamma_n \\ \text{rank}(\lambda_{n-r}(C_M))=n-r}} \Delta_{n,r}M = \coprod \Delta_{n,r}M\{C_4, D_3, D_4\} \left(\begin{smallmatrix} {}^tU & 0 \\ 0 & U^{-1} \end{smallmatrix}\right)$$

where, on the right hand side, $(C_4D_3D_4)$ *runs over a complete set* $\tilde{\mathscr{C}}$ *of representatives of the - equivalence classes in* $\mathscr{C}_{n,r}$ *and* ${}^tU$ *runs over a complete set* $\mathscr{U}$ *of representatives of the right cosets* $P(n, r; \mathbb{Z})\backslash GL_n(\mathbb{Z})$

(ii) $$\coprod_{\substack{M\in\Gamma_n \\ \text{rank}(\lambda_{n-r}(C_M))=n-r}} \Delta_{n,r}M = \coprod \Delta_{n,r}M\{C_4, D_3D_4\} \left(\begin{smallmatrix} E_n & S \\ 0 & E_n \end{smallmatrix}\right)\left(\begin{smallmatrix} {}^tU & 0 \\ 0 & U^{-1} \end{smallmatrix}\right)$$

where, on the right hand side, $(C_4D_3D_4)$ *runs over a complete set* $\tilde{\tilde{\mathscr{C}}}$ *of representatives of the* $\approx$ *-equivalence classes in* $\mathscr{C}_{n,r}$, ${}^tU$ *runs over* $\mathscr{U}$ *as in* (i) *and* S *runs over all* (n, n) *integral symmetric* 142
matrices of the form $\left(\begin{smallmatrix} 0^{(r,r)} & * \\ * & * \end{smallmatrix}\right)$.

Proof. Given M in Γ_n with rank $(\lambda_{n-r}(C_M)) = n - r$, we can find, as in the proof of Lemma 1.6.4, H in Γ_n with $\lambda_{n-r}(H) = (0C_4D_3D_4)$ for some $(C_4D_3D_4)$ in $\mathscr{C}_{n,r}$ and W in $GL_n(\mathbb{Z})$ such that $\Delta_{n,r}M = \Delta_{n,r}H\left(\begin{smallmatrix} {}^tW & 0 \\ 0 & W^{-1} \end{smallmatrix}\right) = \Delta_{n,r}M\{C_4, D_3, D_4\}\left(\begin{smallmatrix} {}^tW & 0 \\ 0 & W^{-1} \end{smallmatrix}\right)$. To get the chosen representatives in $\tilde{\mathscr{C}}$ and $\mathscr{U}$, we need only to take $\left(\begin{smallmatrix} * & & 0 \\ & E_r & 0 \\ 0 & 0 & U_4' \end{smallmatrix}\right) M\{C_4, D_3, D_4\}\left(\begin{smallmatrix} {}^tW'{}^tW & 0 \\ 0 & (W')^{-1}W^{-1} \end{smallmatrix}\right)$ for suitable U_4' in $GL_{n-r}(\mathbb{Z})$ and W' in $P(n, r; \mathbb{Z})$. To prove (i), we have therefore only to prove that the cosets on the right hand side are all disjoint. Let, if possible,

$$\Delta_{n,r}M\{C_4, D_3, D_4\}\begin{pmatrix} {}^tU & 0 \\ 0 & U^{-1} \end{pmatrix} = \Delta_{n,r}M\{C_4', D_3', D_4'\}\begin{pmatrix} {}^tU' & 0 \\ 0 & (U')^{-1} \end{pmatrix}$$

for the chosen representatives from $\mathscr{C}$ and $\mathscr{U}$. Writing M, M' instead of $M\{C_4, D_3, D_4\}$, $M\{C_4', D_3', D_4'\}$ for the moment, we know that $A_M =$

$\left(\begin{smallmatrix} A_1 & A_2 \\ A_3 & A_4 \end{smallmatrix}\right)$, $C_M = \left(\begin{smallmatrix} C_1 & C_2 \\ 0 & C_4 \end{smallmatrix}\right)$ and $C_{M'} = \left(\begin{smallmatrix} C_1' & C_2' \\ 0 & C_4' \end{smallmatrix}\right)$. Taking $V = 1$ in the proof of Lemma 1.6.14, we may find a suitable L' in $\Delta_{n,r}$ so that for $H' := L'M$, the first r columns of $C_{H'}$ are 0. Since the coset $\Delta_{n,r}M$ is unchanged in the process, we may suppose already that the first r columns of C_M and likewise of $C_{M'}$ are 0. Now, for some K in $\Delta_{n,r}$, we have $KM = M'\left(\begin{smallmatrix} {}^tV & 0 \\ 0 & V^{-1} \end{smallmatrix}\right)$ with $V = U^{-1}U' = \left(\begin{smallmatrix} V_1^{(r,r)} & V_2 \\ V_3 & V_4 \end{smallmatrix}\right)$.

143 Also

$$C_M = \begin{pmatrix} 0 & C_2 \\ 0 & C_4 \end{pmatrix}, C_{M'} = \begin{pmatrix} 0 & C_2' \\ 0 & C_4' \end{pmatrix}, A_M = \begin{pmatrix} A_1 & A_2 \\ A_3 & A_4 \end{pmatrix}, C_K = \begin{pmatrix} C_1^* & 0 \\ 0 & 0, \end{pmatrix}$$

$D_K = \left(\begin{smallmatrix} D_1^* & D_2^* \\ 0 & D_4^* \end{smallmatrix}\right)$ with $\det C_4$. $C_4' \neq 0$. Further, $C_{KM} = C_{M'}{}^tV$ gives $C_4'{}^tV_2 = 0$, so that $V_2 = 0$, ${}^tU' \in P(n,r;\mathbb{Z})^tU$ and so $U' = U$. Hence $KM = M'$, $D_4^*(C_4D_3D_4) = (C_4'D_3'D_4')$ with D_4^* in $GL_{n-r}(\mathbb{Z})$ and so $(C_4D_3D_4) = (D_4'D_3'D_4')$. This proves assertion (i). We omit the proof of (ii), since it is similar to that of (i). □

As an immediate generalization of the well-known formula $\int_{\mathbb{R}} \exp(-ax^2 + 2bx)dx = \sqrt{\pi/a}\exp(b^2/a)$ for $\operatorname{Re}(a) > 0$, with $\sqrt{\pi/a} > 0$ for $a \in \mathbb{R}$, we know that for (m,m) complex $A = {}^tA$ with $\operatorname{Re} A > 0$ and any m-rowed column b, $\int_{\mathbb{R}^m} \exp(-{}^txAx + 2{}^tbx)dx = (\det \pi A^{-1})^{1/2} \exp({}^tbA^{-1}b)$ with $(\det \pi A^{-1})^{1/2} > 0$ for $A > 0$. As a further generalization, we have

Lemma 1.6.16. *Let $W^{(r,r)} = W = {}^tW > 0$, A an $(n-r, n-r)$ complex symmetric matrix with $\operatorname{Re} A > 0$ and Q a complex $(n-r, r)$ matrix. Then*

$$\int_{X^{(r,n-r)}} \exp(-2\pi \operatorname{tr}(WXA^tX) + 2\pi \operatorname{tr}(XQ))dX$$
$$= (\det W)^{(r-n)/2} 2^{r(r-n)/2} (\det A^{-1})^{r/2} \exp(\pi \operatorname{tr}({}^tQA^{-1}QW^{-1})/2)$$

where the integration with respect to $X = (x_{ij})$ is over the space of $(r, n-r)$ real matrices, $dX = \prod_{i,j} dx_{ij}$ and $(\det A^{-1})^{r/2} > 0$ for real $A = {}^tA > 0$.

144 *Proof.* Writing ${}^tX = ({}^tx_1, \ldots, {}^tx_r)$ where $x_1, \ldots, x_r$ are the r rows of X with $n-r$ entries each, we have $\mathrm{tr}(XA^tX) = {}^txBx$ with ${}^tx := (x_1 \ldots x_r)$ and $B = \begin{pmatrix} A & 0 & 0 \\ \cdot & \cdot & \cdot \\ 0 & \cdot & A \end{pmatrix}$ being the $((n-r)r, (n-r)r)$ matrix whose r blocks of size $(n-r, n-r)$ on the diagonal are all equal to A and other $(n-r, n-r)$ matrix blocks are 0. If W_0 is the positive square root of W and $QW_0^{-1} = (y_1 \ldots y_r)$ with columns y_i, we have $\mathrm{tr}(XQW_0^{-1}) = ({}^ty_1 \ldots {}^ty_r)x$. Thus the integral on the left hand side becomes

$$(\det W_0)^{r-n} \int_X \exp(-2\pi\,\mathrm{tr}(XA^tX) + 2\pi\,\mathrm{tr}(XQW_0^{-1}))dX$$
$$= (\det W)^{(r-n)/2} \int_{\mathbb{R}^{(n-r)r}} \exp(-2\pi{}^txBx + 2\pi({}^ty_1 \ldots {}^ty_r)x)dx$$
$$= (\det W)^{(r-n)/2} 2^{r(r-n)/2} (\det A^{-1})^{r/2} \exp(\pi\,\mathrm{tr}({}^tW_0^{-1t}QA^{-1}QW_0^{-1})/2)$$

on using the formula preceding this lemma. □

Lemma 1.6.17. *For Z in $\mathscr{G}_n$, N in Γ_n with $\det C_N \neq 0$ and $(A_NC_N^{-1})^*$ integral, $\begin{pmatrix} W_1^{(r,r)} & W_2 \\ {}^tW_2 & W_3 \end{pmatrix} = W := (C_NZ + D_N)^tC_N$ and cusp form f in $\{r, k, s\}$, we have*

$$f((N < Z >)^*)(\det(C_NZ + D_N))^{-k} = (\det C_N)^k(\det W_3)^{-k} \sum_{1 \le j \le m} \alpha_j f_j(W_4)$$

where $\{f_1, \ldots, f_m\}$ is a basis for the space of cusp forms in $\{r, k, s\}$, $\alpha_1, \ldots, \alpha_m$ are (bounded) constants depending on f, $(A_NC_N^{-1})^*$ and $W_4 = W_1 - W_2W_3^{-1t}W_2$.

Proof. Dropping the suffix N from A_N, B_N, C_N, D_N, we note that $N < Z >= AC^{-1} - {}^tC^{-1}(CZ + D)^{-1} = AC^{-1} - W^{-1}$, in view of the relations $B - AC^{-1}D = B - A^tD^tC^{-1} = (B^tC - A^tD)^tC^{-1} = -{}^tC^{-1}$. From the 145
Babylonian identity

$$W = \begin{pmatrix} E_r & W_2W_3^{-1} \\ 0 & E_{n-r} \end{pmatrix} \begin{pmatrix} W_4 & 0 \\ 0 & W_3 \end{pmatrix} \begin{pmatrix} E_r & 0 \\ W_3^{-1t}W_2 & E_{n-r} \end{pmatrix},$$

we have $(W^{-1})^* = W_4^{-1}$. On the other hand, there exist constants $\alpha_1, \dots, \alpha_m$ depending on f and the residue class of $(A_N C_N^{-1})^*$ modulo s such that

$$\begin{aligned}(f|\begin{pmatrix}(A_N C_N^{-1})^* - E_r & \\ E_r & 0\end{pmatrix})(Z_1) &= f((A_N C_N^{-1})^* - Z_1^{-1})(\det Z_1)^{-k}\\ &= \sum_{1\le j\le m} \alpha_j f_j(Z_1) \text{for} \quad Z_1 \in \mathscr{G}_r.\end{aligned}$$

Thus

$$\begin{aligned}(f||N)(Z) &= f((A_N C_N^{-1})^* - W_4^{-1})(\det W^t C^{-1})^{-k}\\ &= \sum_{1\le j\le m} \alpha_j f_j(W_4)(\det W_4)^k (\det W)^{-k} (\det C)^k\\ &= \sum_j \alpha_j f_j(W_1 - W_2 W_3^{-1t} W_2)(\det W_3)^{-k}(\det C)^k.\end{aligned}$$

Since the number of residue classes of (r,r) integral $S = {}^tS$ modulo s is finite, $|\alpha_j| \le \nu$ for $1 \le j \le m$ and a constant $\nu = \nu(f)$. □

Let us now *fix* N in Γ_n as in Lemma 1.6.17 with $\det C_N \neq 0$ $C_N = \begin{pmatrix} C_1^{(r,r)} & * \\ 0 & * \end{pmatrix}$, $(A_N C_N^{-1})^*$ integral and a natural number c_0 with $c_0 C_N^{-1}$ integral. We shall study more closely the subseries

$$\mathscr{S}(f;N) := \sum_S (f||N\begin{pmatrix} E_n & C^{-1} S\, {}^tC^{-1} \\ 0 & E_n \end{pmatrix})(Z)$$

146 where $S = \begin{pmatrix} 0^{(r,r)} & S_2 \\ {}^tS_2 & S_3 \end{pmatrix}$ runs over all matrices of this form in $a\Lambda_n := \{aT^{(n,n)} | T = {}^tT \text{ integral}\}$ and $a := sc_0^2$. Recall

$$\Lambda_n^* = \{T^{(n,n)} = (t_{ij}) | t_{ii}, 2t_{ij} = 2t_{ji} \in \mathbb{Z}\},$$

the lattice dual to Λ_n. Let us further write $eta_s(*)$ for $\exp(2\pi i * |s)$ and η for η_1. As usual, let ${}^tBAB$ be abbreviated as $A[B]$. In view of Lemma 1.6.17,

$$\mathscr{S}(f;N) = \sum_j \alpha_j \sum_{S_2,S_3} (\det C_N)^k (\det(W_3 + S_3))^{-k} f_j$$

$$(W_1 - (W_3 + S_3)^{-1}[{}^t(W_2 + S_2)])$$

where S_2, S_3 have entries divisible by a. As a first step, we note that, for $T_0 > 0$ in Λ_r^*,

$$\sum_{S_2^{(r,n-r)} \equiv 0 (\text{mod } 1)} n_s(-\operatorname{tr}(T_0 W_3^{-1}[{}^t(w_2 + aS_2)])$$
$$= \sum_{S_2^{(r,n-r)}} \int_{X^{(r,n-r)}} \eta_s(-\operatorname{tr}(T_0 W_3^{-1}[{}^t(W_2 + aX)])\eta(\operatorname{tr}(S_2{}^t X))dX$$

(Poisson formula)

$$= \eta_s(-\operatorname{tr}(T_0 W_3^{-1}[{}^t W_2])) \sum_{S_2} \int_X \eta(-\operatorname{tr}((a^2|s)T_0 W_3^{-1}[{}^t X]))$$
$$(-\operatorname{tr}\left(\frac{2a}{s} X W_3^{-1 t} W_2 T_0\right) + \operatorname{tr}(X^t S_2))dX$$
$$= \eta_s(-\operatorname{tr}(T_0 W_3^{-1}[{}^t W_2])) \sum_{S_2} \left(\det\left(\frac{2a^2}{s} T_0\right)\right)^{(r-n)/2}$$
$$(\det(-iW_3))^{r/2} \eta\left(-\frac{s}{4a^2} \operatorname{tr}\left({}^t Q W_3 Q T_0^{-1}\right)\right)$$

where $Q := -\dfrac{2ia}{s} W_3^{-1t} W_2 T_0 + i^t S_2$. Now

$$\operatorname{tr}({}^t Q W_3 Q T_0^{-1}) = -\frac{4a^2}{s^2} \operatorname{tr}(T_0 W_3^{-1}[{}^t W_2]) + \frac{4a}{s} \operatorname{tr}(S_2{}^t W_2) - \operatorname{tr}(W_3[{}^t S_2] T_0^{-1})$$

and so

$$\sum_{S_2^{(r,n-r)} \equiv 0 (\text{mod a})} \eta_s(-\operatorname{tr}(T_0 W_3^{-1}[{}^t(W_2 + S_2)]) = \left(\frac{2a^2}{s}\right)^{r(r-n)/2}$$
$$(\det T_0)^{(r-n)/2} (\det(-iW_3))^{r/2}$$
$$\sum_{S_2^{(r,n-r)} \text{ integral}} \eta\left(-\frac{1}{a} \operatorname{tr}(S_2{}^t W_2) + \frac{s}{4a^2} \operatorname{tr}(W_3[{}^t S_2] T_0^{-1})\right)$$

For the Fourier coefficients $b_j(T_0)$ of the cusp form **147**

$$f_j(Z^*) = \sum_{0<T_0\in\Lambda_r^*} b_j(T_0)\eta_n(T_0Z^*),$$

we know from an analogue [19] of Theorem 1.1.1 (Hecke) that $b_j(T_0) = O((\det T_0)^{k/2})$. Using this Fourier expansion, we prove

Lemma 1.6.18. *For a cusp form f in $\{r, k, s\}$ and Z in $\mathscr{G}_n$, we have, with the same notation as in Lemma 1.6.17,*

$$\sum_{S=\begin{pmatrix} 0^{(r)} & S_2 \\ {}^tS_2 & 0\end{pmatrix}\in a\Lambda_n} (f\|N\begin{pmatrix} E_n & C_N^{-1}S & {}^tC_N \\ 0 & E_n & \end{pmatrix})(Z) = (\det C_N)^k \left(\frac{2a^2}{s}\right)^{r(r-n)/2}$$
$$(\det W_3)^{-k}(\det(-iW_3))^{r/2}\times$$
$$\times \sum_j \alpha_j \sum_{\substack{0<T_0\in\Lambda_r^* \\ S_2^{(r,n-r)} \text{ integral}}} (\det T_0)^{(r-n)/2} b_j(T_0)\eta_s(\operatorname{tr}(T_0W_1))\eta$$
$$\left(-\frac{1}{a}\operatorname{tr}(W_2{}^tS_2) + \frac{s}{4a^2}\operatorname{tr}(W_3[{}^tS_2]T_0^{-1})\right)$$

the series over T_0 and S_2 being absolutely convergent.

Proof. In view of the arguments preceding this lemma, for its proof we need only to insert the Fourier expansion for each $f_j(1 \le j \le m)$ and show the resulting (double) series over T_0 and S_2 to be absolutely convergent. □

Let us observe that the matrix P defined, for real $X^{(r,n-r)}$, by

$$P = \operatorname{Im}(W_1 - W_3^{-1}[{}^t(W_2 + X)]) + (\operatorname{Im}(W_3^{-1}))$$
$$[{}^t(X + \operatorname{Re} W_2 + \operatorname{Im}(W_2)(\operatorname{Re}(W_3^{-1}))(\operatorname{Im}(W_3^{-1}))^{-1})]$$

is actually independent of X, since the terms involving X give

$$-(\operatorname{Re}(W_2) + X)(\operatorname{Im}(W_3^{-1}))({}^tX + \operatorname{Re}({}^tW_2))$$
$$-\operatorname{Im}(W_2)\operatorname{Re}(W_3^{-1})\cdot({}^tX + \operatorname{Re}({}^tW_2))$$

$$\begin{aligned}
&- (\operatorname{Re}(W_2) + X)\operatorname{Re} W_3^{-1} \cdot \operatorname{Im} {}^tW_2 \\
&+ (\operatorname{Re}(W_2) + X)(\operatorname{Im}(W_3^{-1}))({}^tX + \operatorname{Re}, ({}^tW_2)) \\
&+ \operatorname{Im}(W_2)\operatorname{Re}(W_3^{-1})({}^tX + \operatorname{Re}({}^tW_2)) + (\operatorname{Re} W_3^{-1} \cdot \operatorname{Im} {}^tW_2 = 0.
\end{aligned}$$

On the other hand, for any real $X^{(r,n-r)}$, clearly $W + \begin{pmatrix} 0^{(r)} & X \\ {}^tX & 0 \end{pmatrix} \in \mathscr{G}_n$ and **148**
hence the imaginary part of the leading (r, r) submatrix

$$(W_1 - W_3^{-1}[{}^t(W_2 + X)])^{-1} \text{ of } (W + \begin{pmatrix} 0^{(r)} & X \\ {}^tX & 0 \end{pmatrix})^{-1}$$

is negative definite. Thus $P = P(X_0) = \operatorname{Im}(W_1 - W_3^{-1}[{}^t(W_2 + X_0)]) > 0$ taking $X_0 = -\operatorname{Re}(W_2) - \operatorname{Im}(W_2) \cdot \operatorname{Re}(W_3^{-1})(\operatorname{Im}(W_3^{-1}))^{-1}$. Now

$$\begin{aligned}
&|\eta_s(\operatorname{tr}(T_0(W_1 - W_3^{-1}[{}^t(W_2 + S_2)])| \\
&\qquad = \exp(-\frac{2\pi}{s} \operatorname{tr}(T_0(P - (\operatorname{Im}(W_3^{-1}))[{}^t(S_2 - X_0)])) \\
&\qquad < \exp\left(-\frac{2\pi\rho}{s} \operatorname{tr}(T_0 + (S_2 - X_0)^t(S_2 - X_0))\right)
\end{aligned}$$

where $\rho > 0$ is such that $P - \sqrt{\rho}E^{(r)}$, $\operatorname{Im}(-W_3^{-1}) - \sqrt{\rho}E^{(r)}$ and $T_0 - \sqrt{\rho}E^{(r)}$ are all > 0. The series on the left hand side of the asserted identity

$$= O\left(\sum_{\substack{0<T_0\in\Lambda_r^* \\ S_2^{(r,n-r)}\equiv 0 (\text{mod a})}} (\det T_0)^{k/2} |\eta_s(\operatorname{tr}(T_0(W_1 - W_3^{-1}[{}^t(W_2 + S_2)])))\right)$$

and is now easily seen to be absolutely convergent.

To prove the absolute convergence of the double series on the right hand side, it suffices to prove that

$$\begin{aligned}
&\sum_{S_2^{(r,n-r)} \text{ integral}} |\eta_s(\operatorname{tr}(T_0W_1) - \frac{s}{a}\operatorname{tr}(W_2{}^tS_2) + \frac{s^2}{4a^2}\operatorname{tr}(W_3[{}^tS_2]T_0^{-1})) \\
&\quad = O((\det T_0)^{n-r} \exp(-2\pi\rho \operatorname{tr}(T_0)) \text{ for some } \rho > 0.
\end{aligned}$$

Now **149**

$$\begin{aligned}\operatorname{Im}(\operatorname{tr}(T_0 W_1) - \frac{s}{a}\operatorname{tr}(W_2{}^tS_2) + \frac{s^2}{4a^2}\operatorname{tr}(W_3[{}^tS_2]T_0^{-1})) &= \\ &= \operatorname{tr}(\operatorname{Im}(W)\begin{pmatrix} T_0 & -(s/2a)S_2 \\ -(s/2a){}^tS_2 & (s^2/4a^2)T_0^{-1}[S_2]\end{pmatrix}) \\ &= \operatorname{tr}((\operatorname{Im}(W))\begin{bmatrix} E_r & 0 \\ -\frac{s}{2a}{}^tS_2T_0^{-1} & E_{n-r}\end{bmatrix}\begin{pmatrix} T_0^{(r)} & 0 \\ 0 & 0\end{pmatrix})\end{aligned}$$

and further taking $\rho_1 > 0$ with $\operatorname{Im}(W) > \rho_1 E_n$, we see that the above series over S_2 is

$$O\left(\sum_{S_2} \exp_{\text{integral}}\left(-\frac{2\pi\rho_1}{s}\operatorname{tr}\left(T_0 + \frac{s^2}{4a^2}S_2{}^tS_2T_0^{-1}\right)\right)\right).$$

To complete the proof of the lemma, we have only to show that for $\rho' = 2\pi s\rho_1/(4a^2)$ and for every $T_0 > 0$ in Λ_r^*,

$$\sum_{S_2^{(r,n-r)}} \exp_{\text{integral}}(-\rho' \operatorname{tr}(S_2{}^tS_2T_0^{-1})) = O((\det T_0)^{n-r}).$$

For this purpose, we may assume, without loss of generality that T_0^{-1} is M-reduced, so that $T_0^{-1} = \begin{pmatrix} t_1 & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & t_r\end{pmatrix}\begin{bmatrix} 1 & & * \\ & \ddots & \\ 0 & \ldots & 1\end{bmatrix}$ and for $\rho_2 = \rho_2(r) > 0$, $\rho_3 = \rho_3(r) > 0$,

$$\rho_2 T_0' := \rho_2\begin{pmatrix} t_1 & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & t_r\end{pmatrix} < T_0^{-1} < \rho_3\begin{pmatrix} t_1 & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & t_r\end{pmatrix},$$

$$(\Lambda_r^* \ni) T_0 < \rho_2^{-1}\begin{pmatrix} t_1^{-1} & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & t_r^{-1}\end{pmatrix}$$

and hence $t_i < \rho_2^{-1} (1 \leq i \leq r)$. Thus, as a majorant for the last mentioned
150 series over S_2, we have

$$\sum_{S_2^{(r,n-r)}} \exp_{\text{integral}}(-\rho'\rho_2 \operatorname{tr}(S_2{}^tS_2T_0'))$$

$$
\begin{aligned}
&= \prod_{1\le i\le r}\left(\sum_{\ell\in\mathbb{Z}}\exp(-\rho'\rho_2 t_i\ell^2)\right)^{n-r}\\
&\le \prod_{1\le i\le r}\left(1+\frac{2\exp(-\rho'\rho_2 t_i)}{1-\exp(-\rho'\rho_2 t_i)}\right)^{n-r}\\
&< \prod_i\left(1+\frac{2}{\rho'\rho_2 t_i}\right)^{n-r} = \prod_i\left(\frac{2+\rho'\rho_2 t_i}{\rho'\rho_2 t_i}\right)^{n-r}\\
&< \prod(\rho'+2)/\rho'\rho_2)^{n-r}(\det T_0)^{n-r}
\end{aligned}
$$

which proves our claim above and the lemma as well.

Lemma 1.6.19. *For $0 < T_0$ in Λ_r^*, we have*

$$
\begin{aligned}
&\sum_{S_3\in a\Lambda_{n-r}}(\det(W_3+S_3))^{-k}(\det(-i(W_3+S_3))^{r/2}\eta((s/4a^2)\operatorname{tr}((W_3+S_3)\\
&T_0^{-1}[S_2]) = i^{(r-n)k}(2\pi)^{(n-r)(k-r/2)}2^{(r-n)(n-r-1)/2}a^{(r-n)(n-r+1)/2}\\
&(4a^2t_0)^{(r-n)(2k-n-1)/2}(1/\Gamma_{n-r}(k-r/2))\eta((s/a^2)\operatorname{tr}(W_3T_0^{-1}[S_2])\\
&\sum_T(\det T)^{k(n+1)/2}\eta((1/4a^2t_0)\operatorname{tr}(TW_3))
\end{aligned}
$$

where t_0 is a fixed natural number with $t_0T_0^{-1}$ integral, $S_2^{(r,n-r)}$ is integral, $\Gamma_m(\ell) := \pi^{m(m-1)/4}\prod_{0\le\nu\le m-1}\Gamma(\ell-\nu/2)$ and T runs over $\{T\in\Lambda_{n-r}^*|T > 0, \frac{1}{4a}(sT_0^{-1}[S_2]+t_0^{-1}T)\in\Lambda_{n-r}^*\}$.

Proof. The left hand side is just 151

$$
\begin{aligned}
&i^{k(r-n)}\eta((s/4a^2)\operatorname{tr}(W_3T_0^{-1}[S_2]))\\
&\qquad\sum_{S_3\in\Lambda_{n-r}}\det(-i(W_3+aS_3))^{r/2-k}\eta((s/4a)\operatorname{tr}(S_3T_0^{-1}[S_2]))\\
&= i^{k(r-n)}\eta((s/4a^2)\operatorname{tr}(W_3T_0^{-1}[S_2]))\sum_{\Lambda_{n-r}\ni S_3'\bmod 4at_0}\eta(s/4a)\operatorname{tr}(S_3'T_0^{-1}[S_2]))\\
&\qquad\sum_{S_3\in\Lambda_{n-r}}\det(-i(W_3+aS_3'-4a^2t_0S_3))^{r/2-k}
\end{aligned}
$$

$$= i^{k(r-n)}\eta((s/4a^2)\operatorname{tr}(W_3T_0^{-1}[S_2]))$$
$$\sum_{S_3'\bmod 4at_0}\eta((s/4a)\operatorname{tr}(S_3'T_0^{-1}[S_2]))\left(\frac{\pi}{2a^2t_0}\right)^{(n-r)(k-r/2)}$$
$$\times 2^{(r-n)(n-r-1)/2}(1/\Gamma_{n-r}(k-r/2))$$
$$\sum_{0<T\in\Lambda_{n-r}^*}(\det T)^{k-(n+1)/2}\eta((1/4a^2t_0)\operatorname{tr}(T(W_3+aS_3'))),$$

on using the well-known formula (for $\operatorname{Re}Y_1>0$ and $\rho>m+1$)

$$2^{m(m-1)/2}\Gamma_m(\rho)\sum_{F\in\Lambda_m}(\det(Y_1+2\pi iF))^{-\rho}$$
$$=\sum_{0<T\in\Lambda_m^*}(\det T)^{\rho-(m+1)/2}\exp(-\operatorname{tr}(TY_1)).$$

The lemma now follows from

$$\sum_{\Lambda_{n-r}\geq S_3'\bmod 4at_0}\eta((s/4a)\operatorname{tr}(S_3'T_0^{-1}[S_2])+(1/4at_0)\operatorname{tr}(TS_3'))$$
$$=\begin{cases}(4at_0)^{(n-r)(n-r+1)/2} & \text{if } sT_0^{-1}[S_2]+\\ & +t_0^{-1}T\in 4a\Lambda_{n-r}^*\\ 0 & \text{otherwise}\end{cases}$$

$\square$

Going back to $\mathscr{S}(f;N)$, we have, in view of Lemma 1.6.18 and 1.6.19,

$$\mathscr{S}(f;N)=\sum_j\alpha_j\sum_{S_3\in a\Lambda_{n-r}}(\det C_N)^k\left(\frac{2a^2}{s}\right)^{r(r-n)/2}$$
$$\sum_{\substack{0<T_0\in\Lambda_r^*\\ S_2^{(r,n-r)}\text{ integral}}}(\det T_0)^{(r-n)/2}b_j(T_0)n_s(\operatorname{tr}(T_0W_1)-\frac{s}{a}\operatorname{tr}(W_2^tS_2))\times$$
$$\times(\det(W_3+S_3))^{-k}(\det(-i(W_3+S_3))^{r/2}\eta\left(\frac{s}{4a^2}\operatorname{tr}((W_3+S_3)T_0^{-1}[S_2])\right)$$

$$= (\det C_N)^k \frac{2^{(r-n)(n-1)/2} i^{(r-n)k} (2\pi)^{(n-r)(k-r/2)} a^{(r-n)(r+n+1)/2}}{s^{r(r-n)/2} \Gamma_{n-r}(k-r/2)} \times$$
$$\times \sum_{1\leq j\leq m} \alpha_j \sum_{T_0, S_2, T} (\det T_0)^{(r-n)/2} (4a^2 t_0)^{(r-n)(2k-n-1)/2} b_j(T_0) (\det T)^{k-\frac{n+1}{2}} \times$$
$$\times \eta_s (\operatorname{tr}(T_0 W_1) - \frac{s}{a} \operatorname{tr}(W_2 {}^t S_2) + \frac{s}{4a^2 t_0} \operatorname{tr}(T W_3) + \frac{s^2}{4a^2} \operatorname{tr}(W_3 T_0^{-1}[S_2]))$$

where $0 < T_0 \in \Lambda_r^*$, $S_2^{(r,n-r)}$ is integral, $0 < T \in \Lambda_{n-r}^*$, $sT_0^{-1}[S_2] + t_0^{-1} T \in$ **152**
$4a\Lambda_{n-r}^*$. Let

$$P := \begin{pmatrix} T_0 & -\frac{s}{2a} S_2 \\ -\frac{s}{2a} {}^t S_2 & \frac{s}{4a^2}(t_0^{-1} T + s T_0^{-1}[S_2]) \end{pmatrix} = \begin{pmatrix} P_1^{(r)} & P_2 \\ {}^t P_2 & P_3^{(n-r)} \end{pmatrix}, \text{ say.}$$

Then from
$$P = \begin{pmatrix} T_0 & 0 \\ 0 & \frac{s}{4a^2 t_0} T \end{pmatrix} \begin{bmatrix} E_r & -\frac{s}{2a} T_0^{-1} S_2 \\ 0 & E_{n-r} \end{bmatrix},$$
we see that $P > 0$ and further $\det P = \left(\frac{s}{4a^2 t_0}\right) \det T_0 \cdot \det T$.

Out assumptions above on T_0, S_2 and T mean precisely that $P_1 \in \Lambda_r^*$, $\frac{2a}{s} P_2$ is integral, $\frac{a}{s} P_3 \in \Lambda_{n-r}^*$ and $\frac{4a^2}{s} t_0 P_3 - s t_0 T_0^{-1}[S_2]$ is in Λ_{n-r}^* (the last condition being superfluous). Now $\{T_0, S_2, T\}$ is in bijective correspondence with P as above and

$$\operatorname{tr}(WP) = \operatorname{tr}(W_1 T_0) - \frac{s}{a} \operatorname{tr}(W_2 {}^t S_2) + \frac{s}{4a^2} (\operatorname{tr}(t_0^{-1} W_3 T) + \operatorname{tr}(s W_3 T_0^{-1}[S_2])).$$

We have thus proved **153**

Lemma 1.6.20. *For a cusp form f in $\{r, k, s\}$ and N in Γ_n as in Lemma 1.6.17,*

$$\mathscr{S}(f; N) = \frac{(\det C_N)^k 2^{(r-n)(n-1)/2} i^{(r-n)k} (2\pi)^{(n-r)(k-r/2)}}{a^{(n-1)(n+r+1)/2} s^{(n-r)(k-(n+r+1)/2)} \Gamma_{n-r}(k-r/2)} \times$$
$$\times \sum_j \alpha_j \sum_{0<P} b_j(P_1) (\det P_1)^{\frac{r+1-2k}{2}} (\det P)^{\frac{2k-n-1}{2}} \eta_s(\operatorname{tr}(PW))$$

where $P_1 \in \Lambda_r^*$, $2c_0^2 p_2^{(r,n-r)}$ is integral and $c_0^2 P_3 \in \Lambda_{n-r}^*$.

We recall that for N in Γ_n fixed above, $C = C_N = \begin{pmatrix} C_1^{(r)} & C_2 \\ 0 & C_4 \end{pmatrix}$ and $c_0 C^{-1} = c_0 \begin{pmatrix} C_1^{-1} & -C_1^{-1} C_2 C_4^{-1} \\ 0 & C_4^{-1} \end{pmatrix}$ is integral. Let us define G, G' by

$$G = \{\lambda_{n-r}(S\,{}^tC^{-1}) | S = \begin{pmatrix} 0^{(r)} & S_2 \\ {}^tS_2 & S_3 \end{pmatrix} \in a\Lambda_n\},$$
$$G' = \{\lambda_{n-r}(CS) | S = \begin{pmatrix} 0^{(r)} & S_2 \\ {}^tS_2 & S_3 \end{pmatrix} \in s\Lambda_n\}.$$

Clearly $G' = \{(C_4\,{}^tS_2, C_4 S_3) | \frac{1}{s} S_2^{(r,n-r)}$ integral, $S_3 \in s\Lambda_{n-r}\}$ is a subgroup of index $\mathrm{abs}(\det C_4)^r$ in the (additive) group $G_0 = \{({}^tS'_2, C_4 S_3) | \frac{1}{s} S'_2$ integral and of size $(n-r, r)$, $S_3 \in s\Lambda_{n-r}\}$. Moreover, $G = \{({}^tS_2\,{}^tC_1^{-1} - S_3^t(C_1^{-1} C_2 C_4^{-1}), S_3\,{}^tC_4^{-1}) | \frac{1}{a} S_2^{(r,n-r)}$ integral, $S_3 \in a\Lambda_{n-r}\} \subset G'$. As representatives of G_0/G, we can take representatives of $\{C_4 S_3 | S_3 \in s\Lambda_{n-r}\} / \{S_3\,{}^tC_4^{-1} | S_3 \in a\Lambda_{n-r}\}$ together with representatives of $\{{}^tS'_2 | S'_2$ of size $(r, n-r)$ and with entries in $s\mathbb{Z}\} / \{{}^tS_2\,{}^tC_1^{-1} | S_2$ of size $(r, n-r)$ and with entries in $a\mathbb{Z}\}$. Hence

$$\begin{aligned}[G_0 : G] &= [s\Lambda_{n-r} : aC_4^{-1}\Lambda_{n-r}\,{}^tC_4^{-1}]\,\mathrm{abs}(\det(a/s)\,{}^tC_1^{-1})^{n-r} \\ &= \mathrm{abs}(\det c_0 c_4^{-1})^{n-r+1}\,\mathrm{abs}(\det c_0^2 C_1^{-1})^{n-r}\end{aligned}$$

154 and so

$$[G' : G] = c_0^{(n-r)(n+r+1)}\,\mathrm{abs}((\det C_1)^{r-n}/(\det C_4)^{n+1}) = \nu_0(C_N), \quad \text{say.}$$

Let

$$S'_j = \begin{pmatrix} 0 & S_{j,2} \\ {}^tS_{j,2} & S_{i,3} \end{pmatrix} \in s\Lambda_n \text{ for } 1 \leq j \leq \nu_0(C_N)$$

be chosen such that $\lambda_{n-r}(C_N S'_j)$ are representatives for G'/G. We now claim that for ${}^tS = S \equiv 0(\mathrm{mod}\ s)$ and $M = N\begin{pmatrix} E_n & S \\ 0 & E_n \end{pmatrix}$, $(f||M)(Z)$ is determined already by $\lambda_{n-r}(M)$. Indeed, let

$$M' = N\begin{pmatrix} E_n & S' \\ 0 & E_n \end{pmatrix}, M'' = N\begin{pmatrix} E_n & S'' \\ 0 & E_n \end{pmatrix}$$

with integral symmetric S', $S'' \equiv O(\bmod\ s)$ and let $\lambda_{n-r}(M') = \lambda_{n-r}(M'')$. Then, by Lemma 1.6.10, $M' = KM''$ for some K in $\Delta_{n,r}$ and the hypothesis on S', S'' forces K to be in $\Delta_{n,r}(s)$ and the associated K^* in Γ_r to lie in $\Gamma_r(s)$; hence we have $(f\|M')(Z) = (f\|KM'')(Z) = ((f\|K^*)\|M'')(Z) = (f\|M'')(Z)$. Writing therefore $(f\|(\lambda_{n-r}(C_M), \lambda_{n-r}(D_M))(Z)$ for $M = N\begin{pmatrix} E_n & S \\ 0 & E_n\end{pmatrix}$ in Γ_n as above, we have

$$\begin{aligned}
\mathscr{T}(f,N) :&= \sum_{S=\begin{pmatrix} 0^{(r)} & S_2 \\ {}^tS_2 & S_3\end{pmatrix}\in s\Lambda_n} (f\|N\begin{pmatrix} E_n & S \\ 0 & E_n\end{pmatrix})(Z)\\
&= \sum_{H\in G'} (f\|(\lambda_{n-r}(C_N), \lambda_{n-r}(D_N)+H))(Z)\\
&= \sum_i \sum_{H\in G} (f\|\lambda_{n-r}(C_N), \lambda_{n-r}(D+CS'_i))+H))(Z)\\
&= \sum_i \sum_{S=\begin{pmatrix} 0^{(r)} & S_2 \\ {}^tS_2 & S_3\end{pmatrix}\in a\Lambda_n} \left(f\|N\begin{pmatrix} E_n & S'_i \\ 0 & E_n\end{pmatrix}\begin{pmatrix} E_n & C_N^{-1}S\,{}^tC_N^{-1} \\ 0 & E_n\end{pmatrix}\right)(Z).
\end{aligned}$$

For $M = N\begin{pmatrix} E^{(n)} & S'_i \\ 0 & E^{(n)}\end{pmatrix}$, we have, however, $C_M = C_N = \begin{pmatrix} C_1^{(r)} & C_2 \\ 0 & C_4\end{pmatrix}$, $D_M = CS'_i + D_N$, $(A_M\ \ C_M^{-1})^*$ is integral and $C_M Z^t C_M + D_M{}^tC_M = W + C_M S'_1{}^tC_M$. In view of Lemma 1.6.20, we have **155**

$$\begin{aligned}
&\mathscr{T}(f,N) = \beta(\det C_N)^k a^{(r-n)(n+r+1)/2}\\
&\sum_{j,i}\alpha_j \sum_{0<P} b_j(P_1)(\det P_1)^{(r+1-2k)/2}(\det P)^{k-(n+1)/2}\times\\
&\times \eta_s(\operatorname{tr}(P(W+S'_i[{}^tC_N])))
\end{aligned}$$

where $P = \begin{pmatrix} P_1^{(r)} & P_2 \\ {}^tP_2 & P_3^{(n-r)}\end{pmatrix} > 0$ runs over all such matrices with $P_1 \in \Lambda_r^*$, $2c_0^2P_2$ integral, $c_0^2P_3 \in \Lambda_{n-r}^*$ and

$$\begin{aligned}
\beta :&= i^{(r-n)k}2^{(r-n)(n-1)/2}(2\pi)^{(n-r)(k-r/2)}\times\\
&\quad s^{(r-n)(k-(n+r-1)/2)}/\Gamma_{n-r}(k-r/2).
\end{aligned}$$

For any such P and any $H = (H_1^{(n-r,r)}, H_2^{(n-r,n-r)})$ in G', let $\chi(H) := \eta_s(2\operatorname{tr}(H_1{}^tC_1P_2) + 2tr(H_2{}^tC_2P_2) + \operatorname{tr}(H_2{}^tC_4P_3))$. Then it is not hard to prove that $\chi(H) = 1$ for all H in G and $\eta_s(\mathrm{tr}(PS[{}^tC_N]) = \chi((C_4{}^tS_2, C_4S_4)) = \chi(\lambda_{n-r}(CS))$ for $S = \begin{pmatrix} 0 & S_2 \\ {}^tS_2 & S_3 \end{pmatrix} \in s\Lambda_n$. Therefore, in view of our choice of S_i', we have $\sum_i \eta_s(\mathrm{tr}(PS_i'[{}^tC])) = \sum_{H\in G'/G}\chi(H) = \nu_0(N)$ or 0 according as χ is trivial or not. Now, χ is clearly trivial if and only if $2{}^tC_1P_2C_4 \equiv O(\mathrm{mod}\ 1)$ and ${}^tC_2P_2C_4 + {}^tC_4{}^tP_2C_2 + P_3[C_4] \in \Lambda^*_{n-r}$.

Lemma 1.6.21. *For P as above and $T := P[C_N] = \begin{pmatrix} T_1^{(r)} & T_2 \\ {}^tT_2 & T_3 \end{pmatrix}$, we have*

$$\left.\begin{array}{l} P_1 \in \Lambda^*_r, 2c_0^2P_2 \equiv 0(\mathrm{mod}\ 1), \mathrm{c}_0^2\mathrm{P}_3 \in \Lambda^*_{\mathrm{n-r}} \\ 2{}^tC_1P_2C_4 \equiv 0(\mathrm{mod}\ 1), \\ {}^tC_2P_2C_4 + {}^tC_4{}^tP_2C_2 + P_3[C_4] \in \Lambda^*_{n-r} \end{array}\right\} \Longleftrightarrow \begin{cases} T \in \Lambda^*_n \\ T_1[C_1^{-1}] = (T[C_N^{-1}])^* \in \Lambda^*_r \end{cases}$$

156 *Proof.* $T = P[C_N]$ is equivalent to the conditions

$$\begin{aligned} &T_1 = P_1[C_1], T_2 = {}^tC_1P_1C_2 + {}^tC_1P_2C_4, \\ &T_3 = P_1[C_2] + {}^tC_4{}^tP_2C_2 + {}^tC_2P_2C_4 + P_3[C_4]. \end{aligned}$$

From the assumptions on P, we see that $T_1 = P_1[C_1] \in \Lambda^*_r$, $2T_2 = 2{}^tC_1P_1C_2 + 2{}^tC_1P_2C_4 \equiv 0(\mathrm{mod}\ 1)$ and $T_3 \in \Lambda^*_{n-r}$, proving the implication $\Longrightarrow$. We uphold next the reverse implication. From $T \in \Lambda^*_n$ and $T_1[C_1^{-1}]$. $(T[C_N^{-1}])^* \in \Lambda^*_r$, we have

$$P_1 = T_1[C_1^{-1}] \in \Lambda^*_r, {}^tC_2P_2C_4 + {}^tC_4{}^tP_2C_2 + P_3[C_4] = T_3 - P_1[C_2] \in \Lambda^*_{n-r}.$$

Further

$$\begin{aligned} &2{}^tC_1P_2C_4 = 2T_2 - 2{}^tC_1P_1C_2 \equiv 0(\mathrm{mod}\ 1), \\ &2c_0^2P_2 = 2c_0{}^tC_1^{-1}(2{}^tC_1P_2C_4)c_0C_4^{-1} \equiv 0(\mathrm{mod}\ 1), \\ &P_3 = T_3[C_4^{-1}] - P_1[C_2C_4^{-1}] - {}^tC_4^{-1}({}^tT_2 - {}^tC_2P_1C_1)C_1^{-1}C_2C_4^{-1} \\ &\qquad - {}^t(C_1^{-1}C_2C_4^{-1})(T_2 - {}^tC_1P_1C_2)C_4^{-1} \end{aligned}$$

and so $c_0^2P_3 \in \Lambda^*_{n-r}$, in view of $c_0C^{-1} = c_0\begin{pmatrix} C_1^{-1} & -C_1^{-1}C_2C_4^{-1} \\ 0 & C_4^{-1} \end{pmatrix}$ being integral. ◻

Putting together the results above, we have, for f and N as above,

$$\begin{aligned}\mathscr{T}(f,N) = \beta\frac{(\det C_1)^k/(\det C_4)^k}{s^{(n-r)(n+r+1)/2}}\sum_j \alpha_j \\ \sum_{0<T\in\Lambda_n^*} b_j([T[C_N^{-1}])^*)(\det T^*)^{(r+1)/2-k}(\det T)^{k-(n+1)/2} \\ \times\,\eta_s(\mathrm{tr}(TC_N^{-1}D_N))\eta_s(\mathrm{tr}(TZ))\end{aligned}$$

Lemma 1.6.22. *The number of* (D_3, D_4) *such that* $F = (C_4D_3D_4)$ *runs over a set of representatives of* $\approx$ *-equivalence classes in* $\mathscr{C}_{n,r}$ *for fixed* C_4 *with* $\det C_4 \neq 0$ *is at most* $\mathrm{abs}(\det C_4)^r\delta_1^{n-r}\ldots\delta_{n-r}$ *where* $\delta_1|\ldots|\delta_{n-r}$ *are elementary divisors of* C_4*.*

Proof. For fixed C_4, the number of $\approx$ -inequivalent F is at most the index of $\{C_4H|H = H^{(n-r,r)}$ integral$\}$ in $\{H|H^{(n-r,r)}$ integral$\}$ multiplied by the index of $\{C_4L|L \in \Lambda_{n-r}\}$ in $\{D_4^{(n-r,n-r)}$ integral $|C_4^{-1}D_4$ is symmetric$\}$ and hence at most equal to $\mathrm{abs}(\det C_4)^r \cdot \sigma_{n-r}(C_4)$ where $\sigma_{n-r}(C_4)$ is the index of Λ_{n-r} in $\{{}^tS = S^{(n-r,n-r)}$ with entries in $\mathbb{Q}|C_4S$ integral$\}$. **157**
Now there exist U_1, U_2 in $GL_{n-r}(\mathbb{Z})$ such that $U_1C_4U_2 = \delta$ is a diagonal matrix with diagonal entries $\delta_1,\ldots,\delta_{n-r}$ for which $\delta_1|\ldots|\delta_{n-r}$. For calculating $\sigma_{n-r}(C_4)$, there is no loss of generality in taking C_4 to be already equal to δ and so $\sigma_{n-r}(C_4) = \delta_1^{n-r}\ldots\delta_r$, proving the lemma. □

We are finally in a position to state

Theorem 1.6.23 ([10], [20])**.** *Let* f *be a cusp form of degree* r*, (even) weight* $k \geq n + r + 1$ *and stufe* s*, for* $1 \leq r \leq n - 1$*. Then for* $T^{(n,n)} = \begin{pmatrix} T^{*(r,r)} & * \\ * & * \end{pmatrix} > 0$ *in* Λ_n^**, the Fourier coefficients* $a(T, f; M)$ *of the transform* $E_{n,r}^k(Z, f)|M$ *of the Eisenstein series, for* M *in* Γ_n*, we have the estimate*

$$a(T, f; M) = O((\det T)^{k-(n+1)/2}/(\det T^*)^{k-(r+1)/2})$$

the O-constants depending on f*,* n*,* s *and* k *and being uniform as long as* T *lies in a fixed Siegel domain.*

Proof. Now $E_{n,r}^k(Z, f)|M := \sum_{N\in\Delta_{n,r}(s)\backslash\Gamma_n(s)M}(f||N)(Z)$ and in view of Proposition 1.6.12, contributions to $a(T, f; M)$ arise only from terms for which rank $(\lambda_{n-r}(C_N)) = n - r$. By Lemma 1.6.15, we have

$$\Gamma_n(s)M = \coprod_{(C_4D_3D_4)\in\overset{\approx}{\mathscr{C}}_{n,r}} \Delta_{n,r}(s)KM\{C_4, D_3, D_4\}$$

$$\begin{pmatrix} E_n & S' \\ 0 & E_n \end{pmatrix}\begin{pmatrix} E_n & sS \\ 0 & E_n \end{pmatrix}\begin{pmatrix} {}^tU & 0 \\ 0 & U^{-1} \end{pmatrix}$$

$$\begin{pmatrix} 0^{(r,r)} & * \\ * & * \end{pmatrix} = S' = {}^tS' \bmod s, {}^t\mathrm{S} = \mathrm{S} = \begin{pmatrix} 0^{(r,r)} & * \\ * & * \end{pmatrix} \text{ integral}$$

$$K \in \Delta_{n,r}(s)\backslash\Delta_{n,r}, {}^tU \in P(n,r,\mathbb{Z})\backslash GL_n(\mathbb{Z})$$

158 where the accent on $\coprod$ indicates that only the $(C_4D_3D_4)$, $K = K(S', U)$ and ${}^tU$ relevant for the decomposition of the left hand side appear. (Indeed $(KM(C_4, D_3, D_4)\left(\begin{smallmatrix} E_n & S' \\ 0 & E_n \end{smallmatrix}\right))^{-1}M\left(\begin{smallmatrix} {}^tU^{-1} & 0 \\ 0 & U \end{smallmatrix}\right)$ must be in $\Gamma_n(s)$, this condition clearly being independent of the matrices sS). Applying the formula for $\mathscr{T}(f, N)$, stated just prior to Lemma 1.6.22, to $f|K^*$ instead of f, $Z + S'$ instead of Z (since $\left(\begin{smallmatrix} E_n & S' \\ 0 & E_n \end{smallmatrix}\right)$ commutes with $\left(\begin{smallmatrix} E_n & sS \\ 0 & E_n \end{smallmatrix}\right)$ and $N = M\{C_4, D_3, D_4\}$ we get, for the Fourier coefficient $a(T, f; M)$ corresponding to $T > 0$ in Λ_n^* an expression of the form

$$\gamma \sum_j \alpha'_j {\sum}'_{\substack{(C_4D_3D_4)\in\overset{\approx}{\mathscr{C}}_{n,r}\\ K,S',{}^tU}} ((\det C_1)^k/(\det C_4)^k) b_j((T[{}^tU^{-1}C_N^{-1}])^*)$$
$$(\det(T[{}^tU^{-1}])^*)^{\frac{r+1}{2}-k}(\det T)^{k-\frac{n+1}{2}}\times$$
$$\times\, \eta_s(\mathrm{tr}(TS'))\eta_s(\mathrm{tr}(T[{}^tU^{-1}]C^{-1}D))$$

with a similar connotation for the account on $\sum$ as for $\coprod'$ earlier and further $\gamma = \beta/s^{(n-r)(n+r+1)/2}$ and bounded constants $\alpha'_j (1 \le j \le m)$. By Lemma 1.6.22, we know that the number of (D_3, D_4) such that $(C_3D_3D_4)$ runs over $\overset{\approx}{\mathscr{C}}_{n,r}$, for fixed (non-singular) C_4 with $\delta_1, \ldots, \delta_{n-r}$ as elementary divisors is at most $(\mathrm{abs}\det C_4)^r\delta_1^{n-r}\ldots\delta_{n-r}$. Under the equivalence $\approx$, C_4 and VC_4 for V in $GL_{n-r}(\mathbb{Z})$ have to be identified and hence, in order to estimate the number of integral invertible C_4 with $\delta_1, \ldots, \delta_{n-r}$ as elementary divisors, we may assume $C_4 = \begin{pmatrix} c_1 & \ldots & \vdots \\ \vdots & \ddots & c_{ij} \\ 0 & \ldots & c_{n-r} \end{pmatrix}$ in triangular form with $c_1, \ldots, c_{n-r} > 0$ and $0 \le c_{ij} < c_i$ for $j \ge i$. Since

$\delta_1^{n-r} \ldots \delta_1 = \delta_1(\delta_1\delta_2)\ldots(\delta_1\ldots\delta_{n-r}) \leq c_1(c_1c_2)\ldots(c_1\ldots c_{n-r})$ and the number of such C_4 for fixed $c_1,\ldots,c_{n-r}$ is evidently $\leq c_2\ldots c_{n-r}^{n-r-1}$, we may now conclude, in view also of the estimate for Fourier coefficients of cusp derived earlier, the finiteness of the number of K, S' and the boundedness of α'_j, that 159

$$\begin{aligned}
a(T,f;M) = O(&\sum_{\substack{(C_4 D_3 D_4)\in\stackrel{\approx}{\mathscr{C}}_{n,r}\\ {}^tU\in P(n,r;\mathbb{Z})\backslash GL_n(\mathbb{Z})}} (\det C_1/\det C_4)^k (\det(T[{}^tU^{-1}])^*/\\
&\det C_1^2)^{k/2}(\det(T[{}^tU^{-1}])^*)^{\frac{r+1}{2}-k} \times (\det T)^{k-(n+1)/2}\\
= O((&\sum_{1\leq c_1,\ldots,c_{n-r}<\infty} (c_1\ldots c_{n-r})^{-k+r} c_1^{n-r}\ldots c_{n-r}c_2\ldots c_{n-r}^{n-r-1})\\
(&\sum_{{}^tU\in P(n,r;\mathbb{Z})\backslash GL_n(\mathbb{Z})} (\det(T[{}^tU^{-1}])^*)^{\frac{r+1-k}{2}}(\det T)^{k-\frac{n+1}{2}})\\
= \zeta&(k-n)^{n-r} O((\det T^*)^{(r+1-k)/2}(\det T)^{k-(n+1)/2})
\end{aligned}$$

since, for the sum over ${}^tU$ which is a Selberg zeta function, we have the above O-estimate involving $\det T^*$ and $\det T$, as long as T stays in a fixed Siegel domain (see page 143 and the Theorem on page 144, [17]). This completes the proof of Theorem 1.6.23. □

Remarks. 1) The case of half-integral $k \geq n+r+1$ can also be dealt with similarly.

2) Let $f(Z) = \sum_T a(T)\eta_s(\mathrm{tr}(TZ) \in \{n,k,s\}$ for even $k \geq 2n+2$, such that the constant term of the Fourier expansions at all the cusps vanish. Then, for $T > 0$, and $\min(T) \geq \mathscr{X} > 0$, we have $a(T) = O((\det T)^{k-(n+1)/2}/(\min(T))^{k/2-1})$. (This is just Theorem D stated on page 7 and it follows from the reformulation of Theorem 1.6.9 given immediately thereafter and Theorem 1.6.23, on noting that $(\det T^*)^{(r+1-k)/2} \ll ((\min(T^*))^{-r(k-r-1)/2} \leq (\min(T))^{-r(k-r-1)/2} < (\min T))^{1-k/2}$, since $r(k-r-1)/2 \geq k/2-1$ for $1 \leq r \leq n \leq (k/2)-1$.

3) Applying the theorem above to the theta series

$$\vartheta_n(Z,S) := \sum_{G^{(m,n)}} \exp(2\pi i\,\mathrm{tr}(S[G]Z))$$

associated with an integral (m,m) positive-definite matrix S, we get, for the number $r(S,T)$ of integral representations of $T =$
160 $T^{(n,n)} > 0$ by S, an 'asymptotic formula' for $m \geq 4n+4$:

$$r(S,T) = 2^{n(m-n+1)/2} \prod_{j=0}^{n-1} \frac{\pi(m-j)/2}{\Gamma((m-j)/2)} (\det T)^{\frac{m-n-1}{2}} \prod_p \alpha_p(S,T) +$$
$$+O((\det T)^{(m-n-1)/2}/(\min T)^{\frac{m}{4}-1})$$

as $\min(T)$ tends to infinity.

1.7 Primitive Representations

161

We fix a natural number n. For $G_P = GL_n(Q_P) \cap \mathscr{M}_n(\mathbb{Z}_P)$ and $U_P = GL_n(\mathbb{Z}_P)$, $L(U_P, G_P)$ stands for a vector space over $\mathbb{Q}$ spanned by left cosets $U_P g$, $g \in G_P$. U_P acts canonically from the right on $L(U_P, G_P)$ and we denote by $H(U_P, G_P)$ the set of all invariant elements of $L(U_P, G_P)$ under this action. The abbreviation $U_P g U_P (g \in G_P)$ denotes an element $\sum U_P g_i$ of $H(U_P, G_P)$ where $U_P g U_P = \coprod U_P g_i$ is a left coset decomposition. It is easy to see that the set $\{U_P g U_P | g \in G_P\}$ is a basis of $H(U_P, G_P)$. If we introduce a product in $H(U_P, G_P)$ by $(\sum a_i U_p g_i)) \cdot (\sum b_j U_p h_j)$:

$$= \sum a_i b_j U_p g_i h_j (a_i, b_j \in \mathbb{Q}, g_i, h_j \in G_p),$$

it is well defined. Let

$$\pi_p(i) := U_p[\underbrace{p, \ldots, p}_{i}, 1, \ldots 1]U_p \ (i = 0, 1, \ldots n),$$

$$T_p(k) := \sum_{\substack{r_1+\cdots+r_n=k \\ r_1 \geq \ldots \geq r_n \geq 0}} U_p[p^{r_1}, \ldots, p^{r_n}]U_p \ \text{ if } \ k \geq 0, \ \text{ and}$$

$T_p(k) := 0$ if $k < 0$. Then the following is a fundamental result of Tamagawa [ ]:

Lemma 1.7.1. *$H(U_p, G_p)$ is a commutative ring and*

$$\sum_{h=0}^{n} (-1)^h p^{h(h-1)/2} T_p(k-h)\pi_p(h) = 0 \ \text{for} \ k \geq 1.$$

Let V be a vector space over $\mathbb{Q}$ with $\dim V = n$. By a *lattice* in V we mean a finitely generated $\mathbb{Z}$-submodule L of V with rank $L = n$. Let $\tilde{V}$ be the vector space over $\mathbb{Q}$ whose basis is the set of all lattices on V. Then any element of $\tilde{V}$ is a formal sum of lattices on V with rational coefficients. If we consider a lattice L on V as an element of $\tilde{V}$, then we **162**
denote it by $[L]$. Now $\tilde{V}$ becomes a $H(U_P, G_P)$ module as follows: Let L be a lattice in V and $g \in G_P$. For a fixed basis $\{u_i\}$ of $\mathbb{Z}_p \otimes L$, let L'_p be lattice in $\mathbb{Q}_p \otimes V$ spanned by $(u_1, \ldots, u_n)g^{-1}$. Then we define $gL = V \cap (\bigcap\limits_{q \neq p} \mathbb{Z}_q \otimes L \cap L'_p)$. For a left coset decomposition $U_p g U_p = \coprod U_p g_i$, $\sum_i [g_i L]$ is independent of the choice of the basis $\{u_i\}$ and determined uniquely by $U_p g U_p$, and L. Hence we can set $U_p g U_p[L] = \sum\limits_i [g_i L]$ where $U_p g U_p = \coprod U_p g_i$.

If $\{p^{e_1}, \ldots, p^{e_n}\}$ are elementary divisors of $g \in G_p$, then $U_p g U_p[L]$ is a sum in $\tilde{V}$ of lattices M in V such that $M/L \simeq \mathbb{Z}/(p^{e_1}) \oplus \ldots \oplus \mathbb{Z}/(p^{e_n})$. If $U_p g U_p = \coprod U_p G_i$, $U_p h U_p = \coprod U_p h_j$, then $U_p h U_p(U_p g U_p[L]) = U_p h U_p(\sum [g_i L]) = \sum_{ij}[h_j g_i L] = ((U_p h U_p)(U_p g U_p))[L]$.

Thus V becomes a $H(U_p, G_p)$-module.

Theorem 1.7.2. *Let V be a regular quadratic space over $\mathbb{Q}$ with $\dim V = n$, and $B(,)$ the bilinear form on V. Let P be a linear mapping from $\tilde{V}$ to $\mathbb{C}$ such that $P([L]) = 0$ unless $d(L) := \det B(x_i, x_j) \in \mathbb{Z}$ where $\{x_i\}$ is a basis of L.*

Putting

$$R(L) := \sum_{M \supset L} P(M), \quad \text{we have}$$

$$P(L) = \sum_{M \supset L} \pi(M, L) R(M) \ \text{where}$$

$\pi(M, L)$ is defined as follows: Suppose $\mathbb{Z}_p M / \mathbb{Z}_p L = \underbrace{\mathbb{Z}/(p) \oplus \ldots \oplus \mathbb{Z}/(p)}_{h_p}$ **163**

for every prime p; then $\pi(M, L) = \prod_p (-1)^{h_p} p^{h_p(h_p-1)/2}$ and otherwise, $\pi(M, L) = 0$.

Proof. If $M \supset L$, then clearly $d(L) = [M : L]^2 d(M)$ and so $R(L)$ is a finite sum of nonzero $P(M)$.

By Lemma 1.7.1, we have

$$\begin{aligned} P([L]) &= P(\sum_{k=0}^{\infty}\sum_{h=0}^{n}(-1)^h p^{h(h-1)/2} T_p(k-h)\pi_p(h)[L]) \\ &= \sum_{h=0}^{n}(-1)^h p^{h(h-1)/2} P(\sum_{k=0}^{\infty} T_p(k-h)\pi_p(h)[L]) \\ &= \sum_{k=0}^{n}(-1)^h p^{h(h-1)/2} P(\sum_{k=0}^{\infty} T_p(k)\pi_p(h)[L]) \\ &= \sum_{0\le h_1\ldots,h_t\le n}\sum_{i=1}^{t}(-1)^{h_i} p^{h_i(h_i-1)/2} P(\sum_{k_1,\ldots,k_t\ge 0} T_{p_1}(k_1)\ldots \\ &\qquad \ldots T_{p_t}(k_t)\pi_{p_1}(h_1)\ldots\pi_{p_t}(h_t)[L]) \\ &= \sum_{0\le h_1,\ldots,h_t\le n}\prod_{i=1}^{t}(-1)^{h_i} p^{h_i(h_i-1)/2} R(\pi_{p_1}(h_1)\ldots\pi_{p_t}(h_t)[L]), \end{aligned}$$

where $p_1, \ldots, p_t$ are prime divisors of $d(L)$, since $R(L) = p(\prod_p \sum_k T_p(k)$
164 $[L])$. Since $\pi_{p_1}(h_1)\ldots\pi_{p_t}(h_t)[L]$ is a sum in $\tilde{V}$ of lattices M such that $\mathbb{Z}_{p_i}M/\mathbb{Z}_{p_i}L = \underbrace{\mathbb{Z}/(p_i)\oplus\ldots\oplus\mathbb{Z}(P_i)}_{h_i}$, the proof is complete. □

In the following, we fix a positive definite quadratic space W over $\mathbb{Q}$ $\dim W = m \ge n$ and a lattice S on W such that $B(x, y) \in \mathbb{Z}$, $B(x, x) \in 2\mathbb{Z}$ for every $x, y \in S$ where B is a bilinear form on W. For a lattice L on a positive definite quadratic space on V with $\dim V = n$, we denote by $R(L)$ and $P(L)$ the number of isometries from L to S and the number isometries σ from L to S such that $S/\sigma(L)$ is torsion-free. An isometry σ from L to S induces canonically an isometry from V to W and we denote the extension by the same letter σ. Considering $\sigma \mapsto a$ pair

$(\sigma|M, M)$ where $M = \sigma^{-1}(\sigma(V) \cap S)$, we obtain $R(L) = \sum_{M \supset L} P(M)$. Hence we have $P(L) = \sum_{M \supset L} \pi(M, L)R(M)$.

Let $\{S_i\}$ be a complete system of representatives of the (finitely many) classes in the genus of S and $E(S_i)$ the order of the group of isometries of S_i. Denote by $SW(L)$ (= Siegel's weighted sum)

$$(\sum_i E(S_i)^{-1} \sum_i \frac{R(L; S_i)}{E(S_i)}$$

where $R(L; S_i)$ is the number of isometries from L to S_i, and put $A(L) = R(L) - SW(L)$. If T is an (n, n) matrix corresponding to L, then $A(L)$ is the Fourier coefficient of $e(\mathrm{tr}(TZ))$ for a Siegel modular form of degree n, weight $m/2$ and some level whose constant term vanishes at every cusp. Put $SW_P(L) = \sum_{M \supset L} \pi(M, L)SW(M)$ and $A_p(L) = \sum_{M \supset L} \pi(M, L)$ $A(M)$; then $P(L) = SW_p(L) + A_p(L)$. It is known that

$$SW_p(L) = (\text{some constant depending on } n, S) \times d(L)^{(m-n-1)/2} \prod_p d_p(L, S),$$

where $d_p(L, S)$ is a so-called primitive density and for a fixed prime **165**
p the number of possible values of $d_p(L, S)$ is finite when L runs over regular lattices with rank $L = n$. Moreover if $m \geq 2n + 3$ and $SW_p(L) \neq 0$, then $SW_p(L) \gg d(L)^{(m-n-1)/2}$, and if $m = 2n + 2$, $SW_p(L) \neq 0$, then $SW_p(L) \gg \underline{n}(L)^{-\varepsilon} d(L)^{(m-n-1)/2}$ for any $\varepsilon > 0$, where $\underline{n}(L)$ is a natural number defined by $\underline{n}(L)\mathbb{Z} = \mathbb{Z}\{Q(x) | x \in L\}$.

Theorem 1.7.3. *Suppose that, for every Siegel modular form* $f(z) = \sum a(T)e(\mathrm{tr}(Tz))$ *of degree* n*, weight* $m/2$ *and some level, whose constant term vanishes at each cusp, the estimate* $a(T) = O(\min(T)^{-\varepsilon}$ $(\det T)^{(m-n-1)/2})$ *holds for* $\min T \geq \mathscr{X}$ *(= an absolute constant independent of* f*). If* $m \geq 2n + 2$ *and* ε *is a sufficiently small positive number, then* $A_p(L) = O((\min(L))^{-\varepsilon}(d(L)^{(m-n-1)/2})$.

Proof. Let $a \geq \mathscr{X} (a \in \mathbb{Z})$, and without loss of generality we may suppose $B(x, y) \equiv 0 \bmod a$ for any $x, y \in S$. If, then $\min(L) < \mathscr{X}$, $SW(L) = R(L) = A(L) = 0$. Hence we may suppose that the estimate for $a(T)$ holds without the restriction "$\min(T) \geq \mathscr{X}$". For a positive definite matrix T and integral non-singular matrix G, $\min(T[G^{-1}) = \min(\det G^{-2}.T[\det G \cdot G^{-1}] > \det G^{-2}\min(T)$. Hence, for $M \supset L$, we have $\min(M) \geq [M : L]^{-2}\min(L)$. From this, we have

$$\begin{aligned}
A_p(L) &= \sum_{M\supset L} \pi(M,L)A(M)\\
&= \sum_{\substack{M\supset L\\ d(M)\in\mathbb{Z}}} |\pi(M,L)|O((\min(M))^{-\varepsilon}(d(M))^{(m-n-1)/2}\\
&= \sum_{\substack{M\supset L\\ d(M)\in\mathbb{Z}}} |\pi(M,L)|O([M:L]^{2\varepsilon}(\min(L))^{-\varepsilon}\times\\
&\qquad \times([M:L]^{-2}d(L))^{(m-n-1)/2})\\
&\ll (\min(L))^{-\varepsilon}(d(L))^{(m-n-1)/2} \sum_{\substack{M\supset L\\ d(M)\in\mathbb{Z}}} |\pi(M,L)|[M:L]^{-(m-n-1)+2\varepsilon},
\end{aligned}$$

166 where the last sum is bounded by

$$\begin{aligned}
&\prod_{p|d(L)} (1 + \sum_{1\leq h\leq n} p^{h(h-1)/2-h(m-n-1)+2h\varepsilon+h(n-h)+\alpha})\\
&\qquad \text{for any } \alpha > 0 \quad \text{by Lemma 1.4.7.}\\
&\leq \prod_P (1 + \sum_{1\leq h\leq n} p^{h(-h/2-3/2+2\varepsilon)+\alpha})(m \geq 2n+2)\\
&\leq \prod_P (1 + np^{-1.5}) \ll 1.
\end{aligned}$$

If $n = 1$ and $m \geq 4$, then the supposition in Theorem 1.7.3 is valid and leads us to an asymptotic formula for $A_p(L)$; we can thus conclude that if a natural number t is primitively represented by S at every prime, then t is primitively represented globally by S if t is sufficiently large. A similar assertion is also true for $n = 2$, $m \geq 7$. Let $n = 2$, $m = 6$. The error term is $O((\min(L))^{-\varepsilon}\log\dfrac{\sqrt{d(L)}}{\min(L)}(d(L))^{3/2})$ by Theorem 1.5.13 under the Assumption $(*)$. Since $\dfrac{\sqrt{d(M)}}{\min(M)} \leq \dfrac{\sqrt{d(L)}}{\min(L)}[M : L]$ for $M \supset L$, $\log\dfrac{\sqrt{d(M)}}{\min(M)} \leq \log\dfrac{\sqrt{d(L)}}{\min(L)} + O([M : L]^{\alpha})$ for any $\alpha > 0$. Similarly, we get $A_p(L) = O((\min(L))^{-\varepsilon} \log \frac{\sqrt{d(L)}}{\min(L)} (d(L))^{3/2})$.

$\square$

Chapter 2

Arithmetic of Quadratic Forms

IN THIS CHAPTER, we exhibit several theorems on representations of quadratic forms obtained by an arithmetical approach. The only basic reference on quadratic forms here is 167

[S] J. -P. Serre, A Course in Arithmetic, Springer-Verlag, New York-Heidelberg- Berlin, 1973.

2.0 Notation and Terminology

Let k be a field with characteristic $\neq 2$, and $\underline{o}(\ni 1)$ a ring contained in k (with k as quotient field).

Let M be an $\underline{o}$-module and Q a mapping from M to k such that

(1) $Q(ax) = a^2 Q(x)$ for $a \in \underline{o}$ and $x \in M$

(2) $Q(x+y) - Q(x) - Q(y) = 2B(x,y)$ is a symmetric bilinear form. Then we call the triple (M, Q, B) or simply M a *quadratic module over* $\underline{o}$, and Q (resp. B) the *quadratic form* (resp. the *bilinear form* associated with M.

Hereafter, we consider only modules which are finitely generated and torsion-free.

2.0.0

Let M be a quadratic module over $\underline{o}$ and suppose that M has a basis $\{v_i\}$ over $\underline{o}$. Then we write $M =< (B(v_i, v_j)) >$; $\det(B(v_i, v_j))$ is determined up to multiplication by an element of $\underline{o}^{x^2} = \{x^2 | x \in \underline{o}^x\}$. Now $\det(B(v_i, v_j))\underline{o}^{x^2}$ is called the *discriminant* of M and denoted by $d(M)$ (= disc (Q) in [S]). If $d(M) \neq 0$, then we say that M is *regular* (=
168 non-degenerate in [S]]. We write $d(M) = (\det(B(v_i, v_j))$ if there is no ambiguity.

2.0.0

Let M, M' be quadratic modules over $\underline{o}$. If f is an injective linear mapping form M to M' which satisfies

$$Q(f(x)) = Q(x) \text{ for } x \in M,$$

then f is called an *isometry* from M to M' (= injective metric morphism in [S]), and we say that M is represented by M'. If, moreover, f is surjective, then M and M' are called isometric (= isomorphic in [S]) and we write $f : M \cong M'$ (or $M \cong M'$). The group of all isometries from M onto M is denoted by $O(M)$; $0^+(M)$ stands for $\{x \in 0(M) | \det x = 1\}$.

2.0.1.1

Let M be a quadratic module over $\underline{o}$ and suppose that M is the direct sum of submodules $M_1, \ldots, M_n$. If, for any different indices i, j,

$$B(x, y) = 0 \text{ for } x \in M_i \text{ and } y \in M_j,$$

then we write

$$M = M_1 \perp \ldots \perp M_n.$$

($\hat{\oplus}$ is used in [S] instead of $\perp$).

2.0.2.2

Let M be a quadratic module over $\underline{o}$ and N a subset of M. We denote by $N^{\perp}$ (= N^0 in [S]) the orthogonal complement of N, i.e.,

$$N^{\perp} = \{x \in M | B(x, N) = 0\}.$$

2.0.3.3

Let V be a quadratic module over k and M an $\underline{o}$-module on V. We call M a ($\underline{o}-$) *lattice* if $kM = V$.

2.0.4.4

Let M be a quadratic module over $\underline{o}$ and suppose that M contains a non-zero *isotropic vector* x, that is, $M \ni x \neq 0$, $Q(x) = 0$. Then M is called an *isotropic* quadratic module. (This definition is different from [S].) If M contains no (non-zero) isotropic element, M is said to be *anisotropic*. **169**

2.0.5.5

Let $K \supset k$ be fields and $K \supset \underline{\widetilde{o}}$, $k \supset \underline{o}$ rings and suppose that $\underline{\widetilde{o}} \supset \underline{o}$. For a quadratic module M over $\underline{o}$, $\underline{\widetilde{o}}M$ denotes a canonically induced quadratic module $\underline{\widetilde{o}} \otimes_{\underline{o}} M$ over $\underline{\widetilde{o}}$. Let M (resp. V) be a quadratic module over $\mathbb{Z}$ (resp. $\mathbb{Q}$). For a prime number p, we denote by M_p, V_p quadratic modules $\mathbb{Z}_p M$, $\mathbb{Q}_p V$ respectively. For $p = \infty$, we write $\mathbb{R}M$, $\mathbb{R}V$ for M_∞, V_∞.

2.1 Quadratic Modules Over $\mathbb{Q}_p$

In this paragraph, p is a prime number and we denote by $\underline{o} = \mathbb{Z}_p$, $k = \mathbb{Q}_p$ the ring of p-adic integers and the field of p-adic numbers.

2.1.0

Let V be a regular quadratic module over k. Suppose

$$V =< a_1 >\perp \ldots \perp< a_n > (a_i \in k^x),$$

that is, there is a basis $\{v_i\}$ such that $Q(v_i) = a_i$, $B(v_i, v_j) = 0$ for $i \neq j$. Then $S(V) = \prod_{i \leq j}(a_i, a_j)(= \varepsilon(V)(dV, -1)$ in the sense of $[S]$) where (,) - the Hilbert symbol of k-is an invariant of V and we quote the following theorem from ([S], p.39).

Theorem 2.1.1. *Regular quadratic modules over k are classified by $d(V)$, $S(V)$, $\dim V$.*

170 **Corollary.** *Let V, W be regular quadratic modules over k. If $\dim V + 3 \leq \dim W$, then V is represented by W.*

Proof. Without loss of generality, we may assume $\dim V + 3 = \dim W$. Let a, b, c be non-zero elements of k which satisfy

$$\begin{cases} ck^{x^2} = d(V) \cdot d(W), \\ -ac \notin k^{x^2}, \\ S(W) = (c, d(V))(a, c)(ab, ac)(bc, -1)S(V). \end{cases}$$

and put $W' =< a >\perp< ab >\perp< bc >\perp V$.

After simple manipulations, we get

$$d(W) = d(W'), S(W) = S(W'), \dim W = \dim W'.$$

The theorem implies that $W \cong W'$. $\square$

2.1.0 Modular and Maximal Lattices

Let M be a regular quadratic module over $\underline{o}$.

By the *scale* $s(M)$ (resp. the norm $\underline{n}(M)$) of M we mean an $\underline{o}$-module in k generated by

$$B(x, y) \quad \text{for} \quad x, y \in M (\text{resp. } Q(x) \quad \text{for} \quad x \in M).$$

$2s(M) \subset \underline{n}(M) \subset s(M)$ follows from $Q(x + y) - Q(x) - Qy) = 2B(x, y)$ and $Q(x) = B(x, x)$. Hence $\underline{n}(M)$ is $s(M)$ or $2s(M)$.

If there exist $a \in k^x$ and a symmetric matrix $A \in \mathscr{M}_n(\underline{o})$ with $\det A \in \underline{o}^x$ such that

$$M =< aA >,$$

171 then we call M ((a)-) *modular*. When $a \in \underline{o}^x$, M is said to be *unimodular.*

If M is (a)-modular, then $s(M)$ is equal to (a). We call M ((a)-) maximal ($a \in k^x$) if $n(M) \subset (a)$ and M is the only lattice N which satisfies $M \subset N \subset kM$ and $\underline{n}(N) \subset (a)$.

The fundamental fact on maximal lattices is the following

Theorem 2.1.2. *Let V be a regular quadratic module over k and $a \in k^x$. If M, N are (a)-maximal lattices on V, then M, N are isometric.*

To prove this, we need several lemmas.

Lemma 2.1.1. *Let V be a regular quadratic module over k with* $\dim V = n$ *and M a lattice on V. If $\underline{n}(M) \subset (a)(a \in k^x)$ and $(2^n a^{-n} d(M)) = \underline{o}$ or (p), then M is (a)-maximal.*

Proof. Suppose that a lattice N on V contains M and $\underline{n}(N) \subset (a)$. Then $d(M) = [N : M]^2 d(N)$, as is obvious. Since $(d(N)) \subset s(N)^n \subset (2^{-1} \underline{n}(N))^n \subset (a/2)^n$, we have $(2^n a^{-n} d(N)) \subset \underline{o}$. Then it implies

$$\underline{o} \quad \text{or} \quad (p) = (2^n a^{-n} d(M)) = [N : M]^2 (2^n a^{-n} d(N)) \subset [N : M]^2 \underline{o}.$$

From this it follows that $[N : M] = 1$ and M is maximal. □

Corollary . *If M is a unimodular lattice with $\underline{n}(M) \subset (2)$, then M is (2)-maximal.*

Proof. Since $\underline{n}(M) = (2)$ follows, Lemma 2.1.1 yields immediately the corollary. □

Lemma 2.1.2. *Let $V = < \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} >$ be a hyperbolic plane over k and M a lattice on V. The following assertions are equivalent:*

(1) *M is $(2a)$-maximal $(a \in k^x)$,*

(2) *M is (a)-modular with $\underline{n}(M) \subset (2a)(= 2s(M))$,*

(3) $M = < \begin{pmatrix} 0 & a \\ a & 0 \end{pmatrix} >$. 172

Proof. (3) $\Rightarrow$ (2) is trivial.

(2) $\Rightarrow$ (1) : $n(M) = (2a)$, $(dM) = (a^2)$ and Lemma 1 complete this step.

(1) $\Rightarrow$ (3) : Since any isotropic primitive vector of M is extended to a basis of M, there exists a basis $\{e_i\}$ of M such that $(B(e_i, e_j)) = \begin{pmatrix} 0 & b \\ b & c \end{pmatrix}$, $b, c \in k$. $Q(e_2) = c$, $Q(e_1 + e_2) = 2b + c \in n(M) \subset (2a)$ imply $c \in (2a)$, $b \in (a)$. Suppose $bp^{-1} \in (a)$. Since $Q(a_1 p^{-1} e_1 + a_2 e_2) = 2a_1 a_2 p^{-1} b + a_2^2 c \in (2a)$ for $a_1, a_2 \in \underline{o}$, $M \subsetneqq L = \underline{o}[p^{-1} e_1, e_2]$ and $n[L] \subset (2a)$. This is a contradiction. Therefore we have $a = bu (u \in \underline{o}^x)$ and $M = \underline{o}[ue_1, e_2 - \dfrac{c}{2b} e_1] =< \begin{pmatrix} 0 & a \\ a & 0 \end{pmatrix} >$. □

Lemma 2.1.3. *Let V be a regular quadratic module over k and M a lattice on V. Suppose that L is a modular $\underline{o}$-module in M. $B(L, M) \subset s(L)$ if and only if $M = L \perp K$ for some module K.*

Proof. Let $s(L) = (a)$. Suppose that $M = L \perp K$. Then $B(L, M) = B(L, L) = s(L)$. Conversely, suppose $B(L, M) \subset (a)$. We define a submodule L by $L^\perp = \{x \in M | B(L, x) = 0\}$. Then $L \perp L^\perp \subset M$ and $kL \perp kL^\perp = kM$. Take any element $x \in M$ and decompose x as $x = y + z (y \in kL, z \in kL^\perp)$. Then $B(L, y) = B(L, x) \subset B(L, M) \subset (a)$. Let $\{v_j\}$ be a basis of L, then $(B(v_i, v_j)) = a(a_{ij})$, $\det(a_{ij}) \in \underline{o}^x$ for $a_{ij} \in \underline{o}$. Put $y = \sum c_j v_j (c_j \in k)$ and $B(v_i, y) = aa_i (a_i \in \underline{o})$. These imply $(c_1, \ldots, c_n) a(a_{ij}) = a(a_1, \ldots, a_n)$ and then $c_i \in \underline{o}$. Hence we have $y \in L$, and $z \in L^\perp$ with $L \subset M$. Thus $L \perp L^\perp = M$ follows. □

173 **Lemma 2.1.4.** *Let V be a regular quadratic module over k and M an (a)-maximal lattice on V. For an isotropic primitive element x of M, there is an isotropic element y of M such that $M = \underline{o}[x, y] \perp *$, $\underline{o}[x, y] =< \begin{pmatrix} 0 & a/2 \\ a/2 & 0 \end{pmatrix} >$.*

Proof. By definition, $B(x, M) \subset s(M) \subset \dfrac{1}{2}\underline{n}(M) \subset \dfrac{1}{2}(a)$ holds. Suppose $B(x, M) \subset \dfrac{1}{2}(pa)$. Then, for every $w \in M$, we have $Q(w + p^{-1}x) = Q(w) + 2p^{-1}B(w, x) \in (a)$. Hence $\underline{n}(M + p^{-1}\underline{o}x) \subset (a)$ follows. This contradicts M being (a)-maximal since $M + p^{-1}\underline{o}x \supsetneqq M$. Taking an element $z \in M$ such that $B(x, z) = \dfrac{1}{2}a$, we put $y = z - a^{-1}Q(z)x \in M$;

$\underline{o}[x,y] =< \frac{a}{2}\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right) >\subset M$ is $(a/2)$-modular and $B(\underline{o}[x,y], M) \subset s(M) \subset \left(\frac{a}{2}\right)$. We may now apply Lemma 2.1.3 to complete the proof. □

Lemma 2.1.5. *Let V be an anisotropic quadratic module over k and M an (a)-maximal lattice. Then we have*

$$M = \{x \in V | Q(x) \in (a)\}.$$

Proof. We have only to prove $Q(x+y) \in (a)$ if $Q(x)$, $Q(y) \in (a)$. Suppose that $2B(x,y) \notin (a)$ for some x, $y \in V$ with $Q(x)$, $Q(y) \in (a)$. Then $(2B(x,y)p^n) = (a)$ for some $n \geq 1$. This implies

$$d(x,y) = Q(x)Q(y) - B(x,y)^2 = -B(x,y)^2(1 - Q(x)Q(y)/B(x,y)^2),$$

and $(Q(x)Q(y)B(x,y)^{-2}) = (Q(x)Q(y)a^{-2}4p^{2n}) \subset (4p^{2n})$. Hence $-d(x,y) \in k^{x^2}$ follows and then $k[x,y]$ is a hyperbolic plane and V is isotropic. This is a contradiction. Thus $2B(x,y) \in (a)$ and $Q(x+y) \in (a)$. □

Lemma 2.1.6. *Let V be a regular quadratic module over k and M an (a)-maximal lattice on V. Then there are hyperbolic planes H_i, and an anisotropic submodule V_0 of V such that* 174

$$\begin{aligned}
&V =\perp H_i \perp V_0,\\
&M =\perp (M \cap H_i) \perp (M \cap V_0),\\
&M \cap H_i =< \begin{pmatrix} 0 & a/2 \\ a/2 & 0 \end{pmatrix} >,\\
&M \cap V_0 = \{x \in V_0 | Q(x) \in (a)\}.
\end{aligned}$$

Proof. This follows inductively from Lemmas 2.1.4 and 2.1.5. □

In Lemma 2.1.6, the number of hyperbolic planes and V_0 up to isometry are uniquely determined by Witt's theorem. This proves the theorem.

Lemma 2.1.7. *Let V be a regular quadratic module over k and L an $\underline{o}$-submodule in V with $\underline{n}(L) \subset (a)(a \in k^x)$. Then there exists an (a)-maximal lattice on V containing L.*

Proof. Suppose that $\{v_1, \ldots, v_n\}$ is a basis of L over $\underline{o}$, and $\{v_1, \ldots, v_n, \ldots, v_m\}$ is a basis of V over k. Put $M = \{v_1, \ldots, v_n, p^t v_{n+1}, \ldots, p^t v_m\}$. It is easy to see $\underline{n}(M) \subset (a)$ for a sufficiently large integer t. Here we note the following two facts. (i) For lattice $K \subsetneqq N$ on V, $d(K)/d(N) \equiv 0 \mod p^2$. (ii) For a lattice K on V with $n(K) \subset (a)$, $d(K) \subset s(K)^m \subset (\frac{1}{2}\underline{n}(K))^m \subset (a/2)^m$. If M is not (a)-maximal, then there is a lattice M_1 on V with $M \subset M_1$. If M_1 is not (a)-maximal, repeat the preceding step and continue in this way. However, this process must terminate at a finite stage, and the last lattice is (a)-maximal. □

Proposition 2.1.10. *Let V, W be regular quadratic modules over k with* $\dim V + 3 \leq \dim W$, *and M a maximal lattice on W. Then every lattice*
175 *L on V is represented by M if $\underline{n}(L) \subset \underline{n}(M)$.*

Proof. From the Corollary to Theorem 2.1.1, V is represented by W. Theorem 2.1.2 and Lemma 2.1.7 imply the proposition. □

2.1.0 Jordan Splittings

Let L be a regular quadratic module over $\underline{o}$. We claim that L is an orthogonal sum of modular modules of rank 1 or 2. Suppose that there is an element $x \in L$ with $(Q(x)) = s(L)$. Then, since $\underline{o}x$ is $(Q(x))$-modular, Lemma 2.1.3 implies $L = \underline{o}x \perp *$. Next, suppose that $(Q(x)) \neq s(L)$ for every $x \in L$. Since $Q(x) = B(x, x) \in s(L)$ for $x \in L$, we have $Q(x) \in ps(L)$ for $x \in L$. Hence, for $x, y \in L$ with $(B(x, y)) = s(L)$, it is obvious that $\underline{o}[x, y]$ is $s(L)$-modular. Again by the same lemma, L is split by $\underline{o}[x, y]$. Grouping modular components of the above splitting, we have a Jordan splitting

$$(\sharp) \quad L = L_1 \perp \ldots \perp L_t.$$

where every L_i is modular and $s(L_1) \supsetneqq \ldots \supsetneqq s(L_t)$.

For a quadratic module M we put $M(a) = \{x \in M | B(x, M) \subset (a)\}(a \in k)$. Suppose that M is (b)-modular. Then it is easy to see $M(a) = M$ or $ab^{-1}M$ according as $(b) \subset (a)$ or $(b) \supsetneqq (a)$ respectively. Hence $s(M(a)) \subset (a)$; further $s(M(a)) = (a)$ if and only if $(a) = (b)$. On the

other hand, we have $L(a) = L_1(a) \perp \ldots \perp L_t(a)$ for ($\sharp$). The above argument implies $s(L(a)) = (a)$ if and only if $(a) = s(L_i)$ for some i. Thus the number t and $s(L_i)$ in the decomposition ($\sharp$) are uniquely determined. Fix any i and take $a \in k^x$ with $(a) = s(L_i)$. Then $B(L_j(a), L_j(a)) \subset (pa)$ for $j \neq i$; further $L_i(a) = L_i$ is (a)-modular. Set $V = L(a)/pL(a)$ and $B'(x,y) = a^{-1}B(x,y) \in \mathbb{Z}/(p)$ for $x, y \in V$. Then V is a vector space over $\mathbb{Z}/(p)$ and B' is a symmetric bilinear form. B' is identically zero on the images of $L_j(a)(j \neq i)$ on V and gives a regular matrix on the image of 176
$L_i(a)$ on V. Hence we get $\dim\{x \in V | B'(x,V) = 0\} = \sum_{j \neq i} \operatorname{rank} L_j$. Thus $\operatorname{rank} L_i$ is also uniquely determined by L. If $\underline{n}(L_i) \neq s(L_i)$, then $p = 2$ and $2s(L_i) = \underline{n}(L_i)$, and it is the case if and only if $B'(x,x)$ is identically zero for $x \in V$. This condition being satisfied or not is determined by L and $s(L_i)$. Thus we have proved

Proposition 2.1.11. *Let L be a regular quadratic module over $\underline{o}$. Then there is a decomposition*

$$L = L_1 \perp \ldots \perp L_t,$$

where every L_i is modular and $s(L_1) \supsetneqq \ldots \supsetneqq s(L_t)$. Moreover the number t, $s(L_i)$, $\operatorname{rank} L_i$ and the equality of $\underline{n}(L_i)$ and $s(L_i)$ or otherwise are uniquely determined by L.

Proposition 2.1.12. *Suppose $p \neq 2$. Let L be a unimodular quadratic module over $\underline{o}$. Then $L =< 1 >\perp \ldots \perp< 1 >\perp< d(L) >$. If rank $L \geqq 3$, $Q(L) = \underline{o}$.*

Proof. For a unimodular module M, suppose $(Q(x)) \neq \underline{o}(= s(M))$ for every $x \in M$. Then we have $\underline{o} = s(M) \subset \frac{1}{2}\underline{n}(M) \subset (p/2)$. This is a contradiction. Thus the proof of the previous propositions shows $L =< u_1 >\perp L_1 (u_1 \in \underline{o}^x)$. Since L is unimodular L_1 is also unimodular. Repeating this argument, we have $L =< u_1 >\perp \ldots \perp< u_n > (u_i \in \underline{o}^x)$. Since the Hasse invariant of kL is 1, $< u_1 >\perp \ldots \perp< u_n >$ and $< 1 >\perp \ldots \perp< 1 >\perp< d(L) >$ are isometric over k after the extension of coefficient ring from $\underline{o}$ to k, and they are $\underline{o}$-maximal by Corollary to Lemma 2.1.1. Hence they are isometric, by Theorem 2.1.2. If rank $L \geqq 3$, then $L \cong < \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} > \perp *$ holds. Therefore it follows that $Q(L) = \underline{o}$. $\square$

177 **Proposition 2.1.13.** *Suppose $p = 2$. Let L be a unimodular quadratic module over $\underline{o}$. L has an orthogonal basis if and only if $\underline{n}(L) = s(L)$. Otherwise L is an orthogonal sum of $< \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} >, < \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} >, < \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} > \perp < \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} >$ is isometric to $< \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} > \perp < \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} >$.*

Proof. As in the proof of Proposition 2.1.13, we have a decomposition

$$L = L_1 \perp L_2,$$

where $L_1 =< u_1 > \perp \ldots \perp < u_t > (u_i \in \underline{o}^x)$, L_2 is an orthogonal sum of $< \begin{pmatrix} 2a_i & b_i \\ b_i & 2c_i \end{pmatrix} > (a_i, c_i \in \underline{o}, b_i, \in \underline{o}^x)$. Moreover, $n(L) = s(L)$ if and only if rank $L_1 \geqq 1$. Suppose $M = \underline{o}x_1 \perp \underline{o}[x_2, x_3]$ and $Q(x_1) \in \underline{o}^x$, $(B(x_i, x_j))_{i,j=2,3} = \begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix}$, $a, b, c \in \underline{o}$, $b \in \underline{o}^x$. Then $N = \underline{o}[x_1 + x_2, x_3]$ is unimodular and $Q(x_1 + x_2) \in \underline{o}^x$. The proof of Proposition 2.1.11 shows that N has an orthogonal basis and M is isometric to $N \perp *$ by Lemma 2.1.3. Thus M has an orthogonal basis. This proves the first assertion. Let $K = \underline{o}[v_1, v_2]$, $(B(v_i, v_j)) = \begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix} (a, b, c \in \underline{o}, b \in \underline{o}^x)$. Then kK is isometric to $< 2a > \perp < 2ad >$, $d = 4ac - b^2 \equiv -1 \mod 4$. After easy manipulations, the Hasse invariant $S(kK)$ is 1 (resp. -1) according as $d \equiv 3$ (resp. 7) $\mod 8$. Hence by virtue of Theorem 2.1.1, kK is isometric to $< \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} >$ (resp. $< \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} >$) if $d \equiv 3$ (resp. 7) mod 8. Since they are (2)-maximal by Lemma 2.1.1, they are isometric by Theorem 2.1.2. By Theorem 2.1.1 again, it is easy to see $< \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} > \perp < \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} > \perp < \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} >$ over k. Over $\underline{o}$, they are (2)-maximal by Lemma 2.1.1 and then they are isometric. $\square$

2.1.0 Extension Theorems

178

Let V, W be quadratic modules over k and M a $(\underline{o})$-lattice on V. Suppose that

$$u : M \to W$$

is a linear mapping over $\underline{o}$. Then, putting, for $w \in W$,

$$B_u(w)(x) = B(u(x), w) \quad \text{for} \quad x \in M$$

we obtain $B_u(w) \in \mathrm{Hom}(M, k)$. The following theorem is fundamental.

Theorem 2.1.14. *Suppose that there is an o-submodule G in W such that, for $k \in \mathbb{Z}$, the conditions*

$$(\sharp)_k \begin{cases} \mathrm{Hom}(M, \underline{o}) = \{B_u(w) | w \in G\} + \mathrm{Hom}(M, po), \\ p^{k-1} n(G) \subset 2\underline{o}, \\ Q(u(x)) \equiv Q(x) \mod 2p^k \underline{o} \quad \textit{for} \quad x \in M \end{cases}$$

are satisfied. Then there is an element $u' \in \mathrm{Hom}(M, W)$ satisfying

$$u'(x) \equiv u(x) \mod p^k G \quad \textit{for} \quad x \in M \quad \textit{and} \quad (\sharp)_{k+1}.$$

If, moreover, V is regular, there is an isometry u_0 from M to W satisfying

$$u_0(x) \equiv u(x) \mod p^k G \quad \textit{for} \quad x \in M.$$

Proof. Let $\{v_1, \ldots, v_m\}$ be a basis of M. Put

$$\begin{aligned} a\left(\sum x_i v_i, \sum y_i v_i\right) = \frac{1}{2} p^{-k} \sum_i (Q(u(v_i)) - Q(v_i)) x_i y_i + p^{-k} \\ \sum_{i<j} (B(u(v_i), u(v_j)) - B(v_i, v_j)) x_i y_j. \end{aligned}$$

Since $Q(\sum w_i) = Q(w_i) + 2 \sum\limits_{i<j} B(w_i, w_j)$, we have **179**

$$2p^k a(x, x) = Q(u(x)) - Q(x) \quad \text{for} \quad x \in M.$$

It is obvious that

$$\begin{aligned} \frac{1}{2} p^{-k} (Q(u(v_i)) - Q(v_i)) \in \underline{o} \quad \text{and} \\ p^{-k} \{B(u(v_i), u(v_j)) - B(v_i, v_j)\} = \frac{1}{2} p^{-k} \{Q(u(v_i + v_j)) - Q(u(v_i)) \\ - Q(u(v_j)) - Q(v_i + v_j) + Q(v_i) \\ + Q(v_j)\} \in \underline{o}. \end{aligned}$$

Thus $a(x,y)$ is an $\underline{o}$-valued bilinear form on M. Therefore, for each i, there exist $g_i \in G$ and $m_i \in \mathrm{Hom}(M, p\underline{o})$ such that

$$a(x, v_i) = B(u(x), g_i) + m_i(x) \quad \text{for} \quad x \in M.$$

Making use of g_i, we define $v \in \mathrm{Hom}(M, G)$ by

$$v(\sum x_i v_i) = -\sum x_i g_i \ (x_i \in \underline{o}).$$

We put $u'(x) = u(x) + p^k v(x)$. Then $u'(x) \equiv u(x) \mod p^k G$ is obvious for $x \in M$. We must verify the property $(\sharp)_{k+1}$ for u'. For $x \in M$, $w \in G$, we have

$$\begin{aligned} B_{u'}(w)(x) &= B(u'(x), w) = B(u(x), w) + p^k B(v(x), w) \\ &= B_u(w)(x) + p^k B(v(x), w). \end{aligned}$$

Here the linear mapping $x \to p^k B(v(x), w)$ is in $\mathrm{Hom}(M, po)$ since $p^k B(v(x), w) \in p^k s(G) \in \dfrac{1}{2} p^k \underline{n}(G) \subset p\underline{o}$. Hence the first equation is valid for u'.

For $x = \sum x_i v_i \in M$, we have

$$\begin{aligned} Q(u'(x)) &= Q(u(x)) + p^{2k} Q(v(x)) + 2p^k B(u(x), v(x)) \\ &= Q(u(x)) + p^{2k} Q(v(x)) + 2p^k(-\sum x_i B(u(x), g_i)) \\ &= Q(u(x)) + p^{2k} Q(v(x)) - 2p^k(a(x,x) - \sum x_i m_i(x)) \\ &= Q(x) + p^{2k} Q(v(x)) + 2p^k \sum x_i m_i(x). \end{aligned}$$

180 Here $p^{2k} Q(v(x)) \in p^{2k} \underline{n}(G) \subset 2p^{k+1}\underline{o}$, $2p^k \sum x_i m_i(x) \in 2p^{k+1}\underline{o}$ hold. Thus the third property of $(\sharp)_{k+1}$ holds for u', and the former part of Theorem 2.1.14 is proved. Repeating this argument inductively, there is an element $u_\ell \in \mathrm{Hom}(M, W)(\ell \geq 1)$ satisfying

$$\begin{aligned} Q(u_\ell(x)) &\equiv Q(x) \mod 2p^{k+\ell}\underline{o} \quad \text{for} \quad x \in M, \\ u_\ell(x) &\equiv u(x) \mod p^k G \quad \text{for} \quad x \in M. \end{aligned}$$

Hence there is an element $u_0 \in \mathrm{Hom}(M, W)$ such that

$$Q(u_0(x)) = Q(x) \quad \text{and} \quad u_0(x) \equiv u(x) \mod p^k G \quad \text{for} \quad x \in M.$$

Suppose $u_0(y) = 0$ for $y \in M$. Then we have

$$B(y, M) = B(u_0(y), u_0(M)) = 0.$$

If V is regular, then $y = 0$ follows. Hence u_0 is injective and indeed an isometry. This completes the proof of Theorem 2.1.14. $\square$

Definition. *Let V be a quadratic module over k and M a lattice on V. Then we denote by $M^\sharp$*

$$\{x \in V | B(x, M) \subset \underline{o}\}.$$

Corollary 1. *Let V, W be regular quadratic modules over k and M, N lattices on V, M respectively. Let h be an integer such that* **181**

$$p^h \underline{n}(M^\sharp) \subset 2\underline{o}.$$

If $u \in \mathrm{Hom}(M, N)$ satisfies

$$Q(x) \equiv Q(u(x)) \mod 2p^{h+1}\underline{o} \quad \textit{for} \quad x \in M,$$

then there exists an isometry u' from M to N such that

$$\begin{aligned} &u'(M) = u(M) \\ &u'(x) \equiv u(x) \mod p^{h+1}u(M^\sharp) \quad \textit{for} \quad x \in M. \end{aligned}$$

In particular, we have $u' : M \cong u(M)$.

Proof. We claim that u is injective. Suppose that $u(x) = 0$ for $0 \neq x \in M$. Without loss of generality, we may assume that x is primitive in M. Hence there exists $x' \in M^\sharp$ satisfying $B(x, x') = 1$. $2s(M^\sharp) \subset \underline{n}(M^\sharp) \subset 2p^{-h}\underline{o}$ implies $B(p^h M^\sharp, M^\sharp) \subset \underline{o}$ and then $p^h M^\sharp \subset (M^\sharp)^\sharp = M$. Thus $p^h x'$ is in M. From

$$\begin{aligned} Q(x + p^h x') &\equiv Q(u(p^h x')) \mod 2p^{h+1}\underline{o} \\ &\equiv Q(p^h x') \mod 2p^{h+1}\underline{o} \end{aligned}$$

we have $0 \equiv Q(x) + 2p^h \equiv Q(u(x)) + 2p^h \equiv 2p^h \mod 2p^{h+1}\underline{o}$. This is a contradiction. Thus u is injective. Let φ be an element of $\mathrm{Hom}(M, \underline{o})$.

Then $\varphi(x) = B(x, z)$ for some $z \in M^\sharp$. We show that $(\sharp)_{h+1}$ holds for $G = u(M^\sharp)$. For $x \in M$, we have

$$p^h\varphi(x) = B(x, p^h z) \equiv (B(u(x), p^h u(z)) \mod p^{h+1}\underline{o}$$

and then $\varphi(x) \equiv B(u(x), u(z)) \mod p\underline{o}$. Thus the first condition holds. **182**
For $x \in M^\sharp$, we have

$$\begin{aligned} & Q(p^h x) \equiv Q(p^h u(x)) \quad \text{and} \quad 2p^{h+1}\underline{o} \\ \text{and} \qquad & p^{h+1}Q(x) \equiv p^{h+1}Q(u(x)) \mod 2p^2\underline{o}. \end{aligned}$$

From the assumption $p^h\underline{n}(M^\sharp) \subset 2\underline{o}$, it follows that

$$p^{h+1}Q(x) \equiv 0 \mod 2p\underline{o} \quad \text{and then} \quad p^{h+1}Q(u(x)) \equiv 0 \mod 2p\underline{o}.$$

Thus $p^h\underline{n}(G) \subset 2\underline{o}$. By Theorem 2.1.14, there exists an isometry u' from M to W such that

$$u'(x) \equiv u(x) \mod p^{h+1}u(M^\sharp) \quad \text{for} \quad x \in M.$$

Since $p^h M^\sharp \subset M$, $u'(x) \equiv u(x) \mod pu(M)$ for $x \in M$. This implies $u'(M) = u(M)$. □

Corollary 2. *Let V be a regular quadratic module over k and M a lattice on V. Let h be an integer such that*

$$p^h\underline{n}(M^\sharp) \subset 2\underline{o},$$

and let N be a submodule of M which is a direct summand of M as a module, and suppose that u_0 is an isometry from N to M satisfying

$$u_0(x) \equiv x \mod p^{h+1}M^\sharp \quad \textit{for} \quad x \in N.$$

Then u_0 extends to an isometry $u_1 \in o(M)$ such that

$$u_1(x) \equiv x \mod p^{h+1}M^\sharp \quad \textit{for} \quad x \in M.$$

183

Proof. We take a submodule N' such that $M = N \oplus N'$. We define an endomorphism u of M by

$$u(x + x') = u_0(x) + x' \quad \text{for} \quad x \in N, x' \in N'.$$

Put $G = M^\sharp$. By assumption, $p^h \underline{n}(G) \in 2\underline{o}$. For $\varphi \in \mathrm{Hom}(M, \underline{o})$ there exists $z \in M^\sharp$ such that

$$\varphi(x) = B(x, z) \quad \text{for} \quad x \in M.$$

Then we have, for $x \in M$,

$$\begin{aligned}
&\varphi(x) - B(u(x), z) \\
&= B(x - u(x), z) \in B(p^{h+1}M^\sharp, M^\sharp) \subset B(pM, M^\sharp) \\
&\subset p\underline{o},
\end{aligned}$$

since $p^n M^\sharp \subset M$ as in the proof of Corollary 1 to Theorem 2.1.14. Thus $\mathrm{Hom}(M, \underline{o}) = B_u(G) + \mathrm{Hom}(M, p\underline{o})$. For $x \in N$, $x' \in N'$, we have

$$\begin{aligned}
&Q(u(x + x')) - Q(x + x') = Q(u_0(x) + x') - Q(x + x') \\
&= Q(u_0 x)) - Q(x) + 2B(u_0(x) - x, x'), \ \text{ putting } \ u_0(x) - x = p^{h+1}y, \\
&= 2B(p^{h+1}y, x) + p^{2(h+1)}Q(y) + 2B(p^{h+1}y, x') \in 2p^{h+1}\underline{o} \ \text{ holds.}
\end{aligned}$$

Thus the condition $(\sharp)_{h+1}$ in Theorem 2.1.14 is satisfied for $V = W$ and a linear mapping u satisfying $u = u_0$ on N. In the proof of this theorem, we assume that $\{v_1, \ldots, v_n\}$ (respectively $\{v_{n+1}, \ldots, v_m\}$) is a basis of N (respectively N'). Then $Q(u(v_i)) = Q(v_i)$ for $1 \leqq i \leqq n$, and hence $a(x, y) = 0$ holds for $x \in M$, $y \in N$. Thus we can take $g_i = u$, $m_i = 0$ for **184**
$i \leqq n$. This implies $v(N) = 0$. Hence u' constructed in Theorem 2.1.14 satisfies the condition $u' = u = u_0$ on N. Repeating this argument, we obtain an isometry u_1 from M to V such that

$$\begin{aligned}
&u_1(x) \equiv u(x) \equiv x \mod p^{h+1}M^\sharp \quad \text{for} \quad x \in M, \\
&u_1(x) = u_0(x) \quad \text{for} \quad x \in N.
\end{aligned}$$

Now $p^h M^\sharp \subset M$ implies that $u_1(M) \subset M$ and then $u_1(M) = M$, on comparing the discriminants. $\square$

Corollary 3. *Let V be a regular quadratic module over k, M a lattice on V, and $\{u_1, \ldots, u_n\}$ a set of linearly independent elements of V. Then there is an integer h such that for a set $\{v_1, \ldots, v_n\}$ of linearly independent elements satisfying $B(u_i, u_j) = B(v_i, v_j)$ and $u_i - v_i \in p^h M$ for $1 \leq i \leq j \leq n$, there is an isometry $u \in o(M)$ such that $u(u_i) = v_i$ for $1 \leq i \leq n$.*

Proof. Without loss of generality, we may assume that $u_i \in M$ for $1 \leq in \leq n$, taking $p^r M$ instead of M. Put $N = k[u_1, \ldots, u_n] \cap M$ and let $\{w_1, \ldots, w_n\}$ be a basis of N and

$$(u_1, \ldots, u_n) = (w_1, \ldots, w_n)A \quad \text{for} \quad A \in M_n(\underline{o}).$$

We define an isometry u_0 from N to M by $u_0(u_i) = v_i$. Then we have

$$\begin{aligned}(\ldots, u_0(w_i) - w_i, \ldots) &= (\ldots, u_0(u_i) - u_i, \ldots)A^{-1} \\ &= (\ldots, v_i - u_i, \ldots)A^{-1}.\end{aligned}$$

If h is sufficiently large, then $u_0(x) \equiv x \mod p^{h'+1} M^\sharp$ for $x \in N$ and a sufficiently large h'. From the previous corollary our assertion follows. $\square$

185 **Corollary 4.** *Let L be a regular quadratic module over $\underline{o}$ and $x_1, \ldots, x_n \in L$ a set of elements of L satisfying* $\det(B(x_i, x_j)) \neq 0$. *Then there exists an integer h such that for any $y_1, \ldots, y_n \in L$ with $y_i \equiv x_i \mod p^h L$, there is an isometry $\sigma \in 0(L)$ for which*

$$\sigma(\underline{o}[x_1, \ldots, x_n]) = \underline{o}[y_1, \ldots, y_n]$$

holds.

Proof. Put $M = \underline{o}[x_1, \ldots, x_n]$, $N = \underline{o}[y_1, \ldots, y_n]$. We take a sufficiently large h; then $\det(B(y_i, y_j))/\det(B(x_i, x_j)) \in \underline{o}^{x^2}$. Applying Corollary 1 to Theorem 2.1.14 to $M, N, u : x_i \to y_i$, we see that there are $z_1, \ldots, z_n \in N$ such that $B(z_i, z_j) = B(x_i, x_j)$ and $z_i \equiv y_i \mod p^{h'} L$ for a sufficiently large h'. From the previous corollary follows the existence of an isometry $\sigma \in \underline{o}(L)$ such that $\sigma(M) = \underline{o}[z_1, \ldots, z_n] = N$. $\square$

2.2 The Spinor Norm

Let k be a field with characteristic $\neq 2$ and V a regular quadratic module over k.

Let $T(V) = \underset{n\geq 0}{\oplus} \overset{n}{\otimes} V (\overset{0}{\otimes} V = k, \overset{1}{\otimes} V = V)$ be the tensor algebra of V and let I be the two-sided ideal of $T(V)$ generated by elements of the form $x \otimes x - Q(x) \in T(V)$. Then $C(V) = T(V)/I$ is called the *Clifford algebra* of V. It is easy to see that $C(V)$ is the direct sum of the images of $T_0 = \oplus(\overset{n}{\otimes} V)$ (n : even) and $T_1 = \oplus(\overset{n}{\otimes} V)(n$: odd) since $I = (I \cap T_0) \oplus (I \cap T_1)$.

Lemma 2.2.15. *Let $\{v_1, \ldots, v_n\}$ be an orthogonal basis of V. Then the centre of $C(V)$ is contained in $k+kv_1 \ldots v_n$ (where $v_1 \ldots v_n$ is the product of $v_1, \ldots, v_n$ in $C(V)$).*

Proof. For $x, y \in V$, we have

$$Q(x + y) = (x + y)(x + y) = Q(x) + Q(y) + xy + yx \quad \text{in} \quad C(V),$$

and then $xy + yx = 2B(x, y)$. For a subset S of $\{1, \ldots, n\}$, we identify S **186**
with $v_{i_1} \ldots v_{i_j} (S = \{i_1 < \ldots < i_j\})$. If $S = \phi$, then we take the identity in $C(V)$. Then $x \in C(V)$ is written as

$$x = \sum_S a(S)S \quad (a(S) \in k),$$

where S runs over all subsets of $\{1, \ldots, n\}$. Although it is known that the expression is unique, i.e., $\dim C(V) = 2^n$, we do not need to prove the lemma. Set $e(S) = 1$ (resp. -1) if the cardinality of S is even (resp. odd). Since $v_i v_j = -v_j v_i$ for $i \neq j$, we have, for $S \subset \{1, \ldots, n\}$,

$$S v_i = \begin{cases} e(S)v_i S & \text{if} \quad i \notin S, \\ -e(S)v_i S & \text{if} \quad i \in S. \end{cases}$$

Hence it is easy to see that 1 and $v_1 \ldots v_n$ with n odd are in the centre of $C(V)$; moreover, 1 and $v_1 \ldots v_n$ for odd n are linearly independent, since $1 \in T_0$ and $v_1 \ldots v_n \in T_1$. Let $\mathfrak{S}$ consist of all subsets of $\{1, \ldots, n\}$, giving a basis of $C(V)$; we may assume that $\mathfrak{S} \ni \phi$ and $\{1, \ldots, n\}$ if n is odd. Suppose that x is an element of the centre of $C(V)$ and let

$$x = \sum_{S \in \mathfrak{S}} a(S)\, S\, (a(S) \in k).$$

Then $xv_i = v_i x$ implies

$$\begin{aligned} xv_i \sum a(S) S v_i \\ &= \sum_{i \notin S \in \mathfrak{S}} a(S) e(S) v_i S - \sum_{i \in S \in \mathfrak{S}} a(S) e(S) v_i S \\ &= \sum_{S \in \mathfrak{S}} a(S) v_i S. \end{aligned}$$

187 Multiplying v_i from the left, we have

$$\sum_{\substack{i \notin S \in \mathfrak{S} \\ e(S) = -1}} a(S) S + \sum_{\substack{i \in S \in \mathfrak{S} \\ e(S) = 1}} a(S) S = 0.$$

Since $\mathfrak{S}$ gives a basis of $C(V)$, we have

$$a(S) = 0,$$

if $\phi \neq S \subsetneq \{1, \ldots, n\}$, or $S = \{1, \ldots, n\}$ with n even. This completes the proof of Lemma 2.2.15. ◻

For any anisotropic vector $v \in V$ (i.e. with $Q(v) \neq 0$), we define an isometry τ_v of V by

$$\tau_v x = x - \frac{2B(x, v)}{Q(v)} v.$$

It is called a *symmetry* (with respect to v)

Lemma 2.2.16. *Suppose* $\tau_{u_1} \ldots \tau_{u_m} = 1$. *Then* $Q(u_1) \ldots Q(u_m) \in k^{x^2}$.

Proof. First, we note that m is even, since $\det \tau_u = -1$. For an anisotropic $u \in V$ and all $x \in V$ we have

$$\tau_u x = x - \frac{2B(u, x)}{Q(u)} u$$

$$\begin{aligned} &= x - Q(u)^{-1}(xu + ux)u \quad \text{in} \quad C(V) \\ &= -uxu^{-1}\ (u^{-1} = Q(u)^{-1}u \quad \text{in} \quad C(V)). \end{aligned}$$

Hence $\tau_{u_1} \ldots \tau_{u_m} = 1$, implying that

$$u_1 \ldots u_m x = x u_1 \ldots u_m \quad \text{for all} \quad x \in V.$$

By the previous lemma, we have **188**

$$u_1 \ldots u_m = a + b v_1 \ldots v_n,$$

where $a, b \in k$ and $\{v_1, \ldots, v_n\}$ is an orthogonal basis for V and $b = 0$ if n is even. If n is odd, then $bv_1 \ldots v_n$ is in the images of T_0 and T_1, since $u_1 \ldots u_m - a \in T_0$.

Hence $bv_1 \ldots v_n$ is 0 and $u_1 \ldots u_m = a \in k$. Since $x_1 \otimes \ldots \otimes x_t \to x_t \otimes \ldots \otimes x_1$ induces an anti isomorphism f of $C(V)$. Hence we have

$$\begin{aligned} Q(u_1) \ldots Q(u_m) &= u_1 \ldots u_m u_m \ldots u_1 \\ &= u_1 \ldots u_m f(u_m) \ldots f(u_1) \\ &= u_1 \ldots u_m f(u_1 \ldots u_m) \\ &= a^2. \end{aligned}$$ Q.E.D.

□

The following theorem is implicitly proved in [S].

Theorem 2.2.17. *The group $O(V)$ is generated by symmetries.*

Hence we can express $\sigma \in O(V)$ as a product of symmetries,

$$\sigma = \tau_{u_1} \ldots \tau_{u_m}$$

and denote by $\theta(\sigma)$ the element $Q(u_1) \ldots Q(u_m) \in k^x / k^{x^2}$. By Lemma 2.2.16, this mapping is well-defined and then it is obvious that θ is a group homomorphism from $O(V)$ to $k^x / k^{x^2} \cdot \theta(\sigma)$ is called the *spinor norm* of σ.

Definition. $O'(V) = \{\sigma \in O^+(V) | \theta(\sigma) \in (k^x)^2\}$.

Proposition 2.2.18. *Let L be a modular or maximal regular quadratic module over $\mathbb{Z}_p$ with* rank $L \geq 2$. *Suppose* rank $L \geq 3$ *unless L is modular with $p \neq 2$. Then $\theta(O^+(L)) \supset \mathbb{Z}_p^x$.*

Proof. Suppose that L is (a)-modular. Let, first $p \neq 2$. Proposition 189
2.1.12 implies

$$< a_1 >\perp \ldots \perp< a_n >\cong< b_1 >\perp \ldots \perp< b_n >$$

if $a_i, b_i \in \mathbb{Z}_p^x$ and $\Pi a_i = \Pi b_i$.

Hence, for each $b \in \mathbb{Z}_p^x$, there exists a decomposition

$$L = \mathbb{Z}_p v \perp *, Q(v) = ab.$$

Then τ_v induces an isometry of L and $\theta(\tau_v) = ab\mathbb{Q}_p^{x^2}$. Therefore $\theta(O^+(L)) \supset \mathbb{Z}_p^x$. Suppose $p = 2$. Let $M = \mathbb{Z}_2[v_1, v_2]$ and $(B(v_i, v_j)) = a\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. For $u \in \mathbb{Z}_2^x$, it is clear that $\tau_{v_1+uv_2} \in O(M)$ and $\theta(\tau_{v_1+uv_2}) = 2au$. Hence $\theta(O^+(M)) \supset \mathbb{Z}_2^x\mathbb{Q}_2^{x^2}$. Next suppose that $M = \mathbb{Z}_2[v_1, v_2]$ and $(B(v_1, v_j)) = a\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$. Then $\mathbb{Q}_2 M$ is anisotropic and M is $(2a)$-maximal, since $< \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} >$ is (2)-maximal by Lemma 2.1.1. Hence $M = \{x \in \mathbb{Q}_2 M | Q(x) \in (2a)\}$ and $O^+(M) = O^+(\mathbb{Q}_2 M) \cdot Q(v_1 + bv_2) = 2a$, $2a.3$, $2a.7$ and $2a.13$ according as $b = 0, 1, 2$ and 3 respectively. Hence we have $\theta(O^+(M)) \supset \mathbb{Z}_2^x\mathbb{Q}_2^{x^2}$. Thus, to prove our assertion, we have only to show $L =< a\begin{pmatrix} 2c & 1 \\ 1 & 2c \end{pmatrix} >\perp *(c = 0$ or $1)$. From Proposition 2.1.13, it follows that L has an orthogonal basis $\{v_i\}$ with $Q(v_i) = au_i$, $u_i \in \mathbb{Z}_2^x$. Put $M = \mathbb{Z}_2[v_1 + v_2, v_2 + v_3] =< a\begin{pmatrix} u_1+u_2 & u_2 \\ u_2 & u_2+u_3 \end{pmatrix} >$. Then M is (a)-modular, $M \subset L$ and hence $L = M \perp *$. Proposition 2.1.13 now implies $< \begin{pmatrix} u_1+u_2 & u_2 \\ u_2 & u_2+u_3 \end{pmatrix} >\cong< \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} >$ or $< \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} >$, and the previous assertion gives $\theta(O^+(L)) \supset \theta(O^+(M)) \supset \mathbb{Z}_2^x\mathbb{Q}_2^{x^2}$. □

190 Suppose that L is maximal. By virtue of Lemma 2.1.6 and the previous results, we may assume that $\mathbb{Q}_p L$ is anisotropic. By the same lemma, L is fixed as a set for every isometry of $\mathbb{Q}_p L$. Suppose rank $L \geq 4$; then the corollary on page 37 in [S] implies $Q(\mathbb{Q}_p L) = \mathbb{Q}_p$. Hence $\theta(O^+(L)) = \theta(O^+(\mathbb{Q}_p L)) = \mathbb{Q}_p^x \supset \mathbb{Z}_p^x$. Suppose rank $L = 3$. From the same corollary, it follows that $u \in Q(\mathbb{Q}_p L)$ if $-u \notin d(\mathbb{Q}_p L)$. Since

every non-zero element in $\mathbb{Q}_p$ is a product of two elements u, v with u, $v \in -d(\mathbb{Q}_p L)$, we have $\theta(O^+(L)) = \theta(O^+(\mathbb{Q}_p L)) = \mathbb{Q}_p^x$ again.

Proposition 2.2.19. *Let V be a regular quadratic module over $\mathbb{Q}$ with* $\dim V \notin 3$. *Then we have*

$$\theta(O^+(V)) = \{a \in \mathbb{Q}^x | a > 0 \quad \textit{if} \quad \mathbb{R}V \ \textit{is anisotropic}\}.$$

Proof. Suppose that $\mathbb{R}V$ is anisotropic. Then $\mathbb{R}V$ is definite and $Q(V) \subset \{a \in \mathbb{Q} | a \geqq 0\}$ or $\{a \in \mathbb{Q} | a \leq 0\}$. Hence the spinor norm is positive. Put $\delta = -1$ if $\mathbb{R}V$ is positive definite, $\delta = 1$ otherwise, and let a be a rational number such that $a > 0$ if $\mathbb{R}V$ is anisotropic. By Theorem 6 on page 36 in [S]. $\mathbb{Q}_p V$ is isotropic except at a finite number of primes. Hence we can choose $b \in \mathbb{Q}^x$ such that $b > 0$, and $\delta.a.b.d(V) \not\subset \mathbb{Q}_p^{x^2}$, $\delta.b.d(V) \not\subset \mathbb{Q}_p^{x^2}$ for a prime p if $\mathbb{Q}_p V$ is anisotropic. Then $V \perp < \delta b >$, $V \perp < \delta.a.b >$ are isotropic at every prime spot by the same theorem and hence they are isotropic by the Hasse-Minkowski theorem on page 41 in [S]. By Corollary 1 on page 33 in [S], $-\delta b$ and $-\delta ab$ are in $Q(V)$. Therefore $a\mathbb{Q}^{x^2} = (-\delta b)(-\delta ab)\mathbb{Q}^{x^2} \subset \theta(O^+(V))$. ◻

Proposition 2.2.20. *Let V be a regular quadratic module over $\mathbb{Q}_p$ with* $\dim V \geqq 3$. *Then $\theta(O^+(V)) = \mathbb{Q}_p^x$.*

Proof. If $Q(V) = \mathbb{Q}_p$, the assertion is obvious. Otherwise, it follows that $\dim V = 3$ and if $-a.d(V)(a \in \mathbb{Q}_p^x)$ is not a square, then V represents **191**
a. Hence $\theta(O^+(V)) = \mathbb{Q}_p^x$, as it is easy to see. ◻

Proposition 2.2.21. *Let V be a regular isotropic quadratic module over a field k with* characteristic $\neq 2$. *Then $O'(V)$ is generated by $\tau_x \tau_y (x, y \in V, Q(x) = Q(y) \neq 0)$.*

Proof. Let Ω be the subgroup of $O(V)$ which is generated by $\tau_x \tau_y (x, y \in V, Q(x) = Q(y) \neq 0)$. Then clearly $\Omega \subset O'(V)$, and from $\sigma \tau_x \tau_y \sigma^{-1} = \tau_{\sigma(x)} \tau_{\sigma(y)} (\sigma \in 0(V))$, it follows that Ω is a normal subgroup of $O'(V)$. Let $V = H \perp W$ where $H = k[e_1, e_2]$, $Q(e_1) = Q(e_2) = 0$, $B(e_1, e_2) = 1$. Let $\sigma = \tau_{x_1} \ldots \tau_{x_n} \in O'(V)$; then take $y_i \in H$ so that $Q(y_i) = Q(x_i)$. Since $\tau_{x_i} \tau_{y_i} \in \Omega$, $\sigma = \tau_{y_1} \ldots \tau_{y_n}$ in $O'(V)/\Omega$. Set $\eta = \tau_{y_1} \ldots \tau_{y_n}$; then η is identity on W, and hence $\eta|_H \in O'(H)$. Since $\eta|_H \in O'(H)$, there exist

$z_1, z_2 \in H$ such that $\eta|_H = \tau_{z_1} \cdot \tau_{z_2}$ and $Q(z_1)Q(z_2) = 1$. Then $\eta = \tau_{z_1}\tau_{z_2}$ on V. Thus we have $\sigma = \eta = 1$ in $O'(V)/\Omega$ and so $O'(V) \subset \Omega$. □

2.3 Hasse-Minkowski Theorem

This section is a complement to § 3 of Chapter IV in [S].

Theorem 2.3.22. *V, W be regular quadratic modules over $\mathbb{Q}$. If V_p, V_∞ are represented by W_p, W_∞ for every prime p, then V is represented by W.*

Proof. When $\dim V = 1$, this is nothing but Corollary 1 on page 43 in [S]. We prove the theorem by induction on $\dim V$. Decompose V as $V =< a >\perp V_0$, $a \in \mathbb{Q}^x$. The inductive hypothesis shows that V_0 is represented by W and hence there is a submodule W_0 in W which
192 is isometric to V_0. Since V is locally represented by W, $< a >$ is locally represented by $W_0^\perp := \{x \in W | B(x, W) = 0\}$, using Witt's theorem (Corollary on page 32 in [S]). Hence $< a >$ is represented by $W_0^\perp$. Thus V is represented by W. □

Corollary. *Let V, W be regular quadratic modules over $\mathbb{Q}$ with $\dim V + 3 \leq \dim W$. If $\mathbb{R}V$ is represented by $\mathbb{R}W$, then V is represented by W.*

Proof. Corollary to Theorem 2.1.1 and the above theorem yield the assertion. □

2.4 Integral Theory of Quadratic Forms

For a finite set $S = \{p_1, \ldots p_n\}$ of prime numbers, we define a ring $\mathbb{Z}[S]$ by

$$\mathbb{Z}[S] = \mathbb{Z}[p_1^{-1}, \ldots, p_n^{-1}].$$

If $S = \phi$, then $\mathbb{Z}[S]$ means the ring $\mathbb{Z}$ of rational integers. We define the class, the spinor genus, and the genus of quadratic modules.

Let V be a quadratic module over $\mathbb{Q}$, S a finite set of primes, and L a $\mathbb{Z}[S]$-lattice on V. Now we put

$$\operatorname{cls} L = \left\{ K \;\middle|\; \begin{array}{l} \mathbb{Z}[S] - \text{lattice on } V \text{ such that } K = \sigma(L) \\ \text{for some } \sigma \in O(V) \end{array} \right\},$$

$$\operatorname{spn} L = \left\{ K \;\middle|\; \begin{array}{l} \mathbb{Z}[S] - \text{lattice on } V \text{ such that there exists} \\ \text{isometries } \sigma \in O(V), \text{ and } \sigma_p \in O'(V_p) \\ \text{satisfying } \sigma(K_p) = \sigma_p(L_p) \text{ for every } p \notin S \end{array} \right\},$$

$$\operatorname{gen} L = \left\{ K \;\middle|\; \begin{array}{l} \mathbb{Z}[S] - \text{lattice on } V \text{ such that for every } p \notin S \text{ there} \\ \text{is an isometry } \sigma_p \text{ satisfying } K_p = \sigma_p(L_p) \end{array} \right\}.$$

It is obvious that $\operatorname{gen} L \supset \operatorname{spn} L \supset \operatorname{cls} L$. When $K \in \operatorname{cls} L$, $\operatorname{spn} L$, $\operatorname{gen} L$ **193**
respectively, we say that K and L belong to the same class, spinor genus, genus, respectively.

Here we recall the fundamental relations between global lattices and their localizations.

Theorem 2.4.1. *Let V be a finite dimensional vector space over $\mathbb{Q}$, S a finite set of prime numbers, and K a $\mathbb{Z}[S]$-lattice on V. Suppose that a collection $\{L_P\}$ of a $\mathbb{Z}_p$-lattice on $V_p (p \notin S)$ is given and that L_p is equal to $K_p = \mathbb{Z}_p K$ for almost all (= all but a finite number of) prime numbers. Then $M = \bigcap_{p\notin S} (V \cap L_p)$ is a $\mathbb{Z}[S]$-lattice on V satisfying $M_p = \mathbb{Z}_p M = L_p$ for every $p \notin S$.*

2.4.0

The most fundamental result is the following

Theorem 2.4.2. *Let V be a regular quadratic module over $\mathbb{Q}$, S a finite set of prime numbers. For any $\mathbb{Z}[S]$-lattice L on V, $\operatorname{gen} L$ contains only a finite number of distinct classes.*

Proof. Suppose that the assertion is proved for $S = \phi$. For $p \in S$, we take and fix a $\mathbb{Z}_p$-lattice M_p on V_p, and for $K \in \operatorname{gen} L$ we put $K_0 = \bigcap_{p\notin S} (V \cap K_p) \bigcap_{p\in S} (V \cap M_p)$. Then K_0 is a $\mathbb{Z}$-lattice on V and $K_0 \in \operatorname{gen} L_0$

as is obvious. By assumption, $\operatorname{gen} L_0$ contains only a finite number of distinct classes $\operatorname{cls} K_i (i = 1, \ldots, n)$. Hence there is an isometry $\sigma \in O(V)$ such that $\sigma(K_0) = K_i$ for some $i = 1, 2, \ldots, n$, and then $\sigma(K) = \sigma(\mathbb{Z}[S]K_0) = \mathbb{Z}[S]K_i \in \operatorname{gen} L$. Thus $\operatorname{cls} \mathbb{Z}[S]K_i (i = 1, 2, \ldots, n)$ are the only classes contained in $\operatorname{gen} L$. $\square$

Thus we have only to prove our assertion in case $S = \phi$. In the rest of the proof, we assume $S = \phi$. For an integer $a \neq 0$, it is obvious
194 that if $\operatorname{gen} L = \{\operatorname{cls} K_i\}$ the $\operatorname{gen} aL = \{\operatorname{cls} aK_i\}$. Thus we may assume $s(L) = \{\sum B(x_i, y_i) | x_i, y_i \in L\} \subset \mathbb{Z}$. If $K \in \operatorname{gen} L$, then $d(L) = d(K)$ and $s(L) = s(K)$ since $s(L)\mathbb{Z}_p = s(L_p)$. Thus we have only to prove

Proposition 2.4.25. *Let V be a regular quadratic module over $\mathbb{Q}$ and $d \neq 0$ an integer. Then there is only a finite number of* $\operatorname{cls} L$ *such that $s(L) \subset \mathbb{Z}$ and $d(L) = d$.*

Lemma 2.4.26. *Let V be a regular quadratic module over $\mathbb{Q}$ and M a $\mathbb{Z}$-lattice with $s(M) \subset \mathbb{Z}$ on V. Suppose that N is a regular quadratic submodule of M. Put $K = N^{\perp} = \{x \in M | B(x, N) = 0\}$. Then we have*

$$N \perp K \subset M \subset M^{\sharp} \subset N^{\sharp} \perp K^{\sharp} \quad \textit{and} \quad |d(K)| \,\Big|\, |d(M)| \cdot |d(N)|,$$

where, for a quadratic module L over $\mathbb{Z}$, we denote $\{x \in \mathbb{Q}L | B(x, L) \subset \mathbb{Z}\}$ by $L^{\sharp}$.

Proof. The relations on inclusions are trivial, since $L_1 \subset L_2$ implies $L_1^{\sharp} \supset L_2^{\sharp}$. Let x be an element of M. Then there is an element $y \in N^{\sharp}$ such that $B(x, z) = B(y, z)$ for all $z \in N$. This correspondence φ is linear and we claim that $\varphi^{-1}(N) = N \perp K$. Suppose that $\varphi(x) \in N$; then $B(x - \varphi(x), z) = 0$ for $z \in N$ and so $x - \varphi(x) \in K$. If, conversely, $x = x_1 + x_2$, $x_1 \in N$, $x_2 \in K$, then $B(x - \varphi(x), z) = B(x_1 - \varphi(x), z) = 0$ for $z \in N$ and $\varphi(x) = x_1 \in N$. Thus we have $[M : N \perp K] = [\varphi(M) : N] | [N^{\sharp} : N] = d(N)$, and $|d(N) \cdot d(K)| = |d(M)| \cdot [M : N \perp K]^2 | |d(M)| \cdot |d(N)|^2$. $\square$

Lemma 2.4.27. *For a regular quadratic module L over $\mathbb{Z}$,* $\min(L) := \min\{|Q(x)| \ \ |x \in L, x \neq 0\} \leq (4/3)^{(n-1)/2} |d(L)|^{1/n}$ *where $n = \operatorname{rank} L$.*

Proof. We use induction on rank L. In case rank $L = 1$, the assertion is trivial. For rank $L > 1$, we take $v_1 \in L$ such that $|Q(v_1)| = m(L)$, $v_1 \neq 0$.
195 If $\min(L) = 0$, then we have nothing to prove. Suppose $Q(v_1) \neq 0$, and $\{v_1, \ldots, v_n\}$ is a basis for L. Define a linear mapping p by $p(v_1) = v_1$, $p(v_i) = v_i - Q(v_1)^{-1}B(v_i, v_1)v_i (i \geqq 2)$. Then the determinant of p is one, and hence

$$\begin{aligned}|d(L)| &= |\det(B(v_i, v_j))| = |\det(B(pv_i, pv_j))| \\ &= \min(L)|\det(B(pv_i, pv_j))_{i,j\geq 2}|,\end{aligned}$$

since $B(v_1, pv_i) = 0$ for $i \geqq 2$. Put $M = \mathbb{Z}[p(v_2), \ldots, p(v_n)]$. By the inductive assumption, we have

$$\min(M) \leqq (4/3)^{(n-2)/2}|d(M)|^{1/n-1}.$$

Take $y \in M$ and a rational number r such that

$$|Q(y)| = \min(M), y + rv_1 = x(\text{say}) \in L, |r| \leqq 1/2.$$

Then we obtain $\min(L) \leqq |Q(x)| = |Q(y) + r^2 Q(v_1)| \leqq \min(M) + \dfrac{1}{4}\min(L)$. Hence

$$\begin{aligned}\min(L) &\leqq \frac{4}{3}\min(M) \\ &\leqq (4/3)^{n/2}|d(M)|^{1/n-1} \\ &= (4/3)^{n/2}|d(L)/\min(L)|^{1/n-1}\end{aligned}$$

implying that

$$\min(L) \leqq (4/3)^{(n-1)/2}|d(L)|^{1/n}.$$

□

We prove the proposition by induction on $\dim V$. In the case of $\dim V = 1$, it is obvious.

Suppose that M is a lattice on V such that $s(M) \subset \mathbb{Z}$ and $d(M) = d$. If $\min(M) \neq 0$, then for $v \in M$ with $|Q(v)| = \min(M)$, we put $N = \mathbb{Z}v$. If $\min(M) = 0$, then there is a primitive isotropic vector $v_1 \in M$. We can

take a basis $\{v_1, v_2, \ldots\}$ of M such that $B(v_1, M) = B(v_1, v_2)\mathbb{Z}$, $B(v_1, v_i) = 0$ for $i \geqq 3$. Hence $a = |B(v_1, v_2)|$ divides d. Since $Q(v_2 + bv_1) = Q(v_2) \pm 2ba$, we may assume $|Q(v_2)| \leqq a$. In this case, we put $N = \mathbb{Z}[v_1, v_2]$.
196 If $\dim V = 2$, then $M = N$ and the number of possible corresponding matrices is finite. Hence, for a binary isotropic quadratic module V, the assertion is proved. Otherwise, we have constructed a sub-module N of M such that $|d(N)|$ is bounded by a constant depending only on $d(M)$ and $\dim V$. Put $K = N^{\perp}$. Then $rank K = rank M - 1$ or $rank M - 2$, and $|d(K)| \leqq |d(M)||d(N)|$ which is less than a constant depending only on $d(M)$ and $\dim V$. By the inductive assumption, the number of possible K is finite and then the number of possible K is finite and then the number of possible M for which $N \perp K \subset M \subset N^{\sharp} \perp K^{\sharp}$ is also finite. This completes the proof.

Theorem 2.2.28. *Let W, V be regular quadratic modules over $\mathbb{Q}$, S a finite set of prime numbers, and $M, L\mathbb{Z}[S]$-lattices on W, V respectively, and suppose that M_p is represented by L_p for $p \notin S$ and W_p, W_∞ are represented by V_p, V_∞ for $p \in S$. Then there is a lattice $K \in \operatorname{gen} L$ such that M is represented by K.*

Proof. By the Hasse-Minkowski theorem, we may assume that W is a submodule of V. Then there is an isometry $\sigma_p \in 0(V_p)$ such that $\sigma_p(M_p) \subset L_p$, and for almost all p, $M_p \subset L_p$. Hence q $\mathbb{Z}[S]$-lattice $K = \bigcap_{M_1 \not\subset L_p} (V \cap \sigma_p^{-1}(L_p)) \bigcap_{M_p \subset L_p} (V \cap L_p)$ contains M and obviously, $K \in \operatorname{gen} L$
. $\square$

2.2.0

In this paragraph, we give two different kinds of approximation theorems which are necessary latter. Before stating the results, we first describe the topology. Let V be a vector space over $\mathbb{Q}_p$ with $\dim V = n < \infty$. Fixing a basis of V over $\mathbb{Q}_p, V$ (resp. End V) is isomorphic to $\mathbb{Q}_p^n (resp. \mathfrak{M}_n(\mathbb{Q}_p))$. Using this isomorphism, we can introduce a topology on V or End V which is independent of the choice of bases. Take two bases $\{u_i\}$, $\{v_i\}$ of V. If u and $v \in V$ or End V) are sufficiently close
197 with respect to the topology introduced by $\{u_i\}$, then they are also suffi-

ciently close with respect to $\{v_i\}$. Hence we can use "sufficiently close" without ambiguity, when a finite number of fixed bases are involved.

The first theorem is an approximation theorem for $0'(V)$.

Theorem 2.2.29. *Let V be a regular quadratic modular over $\mathbb{Q}$ with* $\dim V \geqq 3$ *and suppose that $V_v = \mathbb{Q}_v V$ is isotropic for some spot v. (v may be finite or infinite). Let L be a $\mathbb{Z}$-lattice on V and S a finite set of prime numbers with $S \not\ni v$. For a given $\sigma_p \in 0'(V_p)$ for $p \in S$, there is an isometry $\sigma \in 0'(V)$ such that*

$\sigma(L_p) = L_p$ *for* $p \notin S \cup \{v\}$ *and*
σ *and* σ_p *are sufficiently close in* $EndV_p$ *for* $p \in S$.

To prove the theorem, we need some preparatory lemmas.

Lemma 2.2.30. *Let V be a regular quadratic module over $\mathbb{Q}$ and S a finite set of spots including ∞. For given $\sigma_v \in 0^+(V_v)$ for $v \in S$, there are vectors $x_1, \ldots, x_{2n} \in V$ such that σ_v and $\tau_{x_1} \cdots \tau_{x_{2n}}$ are sufficiently close for $v \in S$.*

Proof. Put $\sigma_v = \tau_{x_1(v)} \cdots \tau_{x_{2n}(v)} (x_i(v), \in V_v)$. Since the order of any symmetry is 2, we may suppose that n is independent of $v \in S$. We have only to choose $x_i \in V$ so that x_i and $x_i(v)$ are sufficiently close in V_v for $v \in S$. □

Lemma 2.2.31. *Let W be a regular quadratic module of* $\dim W \geqq 3$, *over $\mathbb{Q}$, S a finite set of sports, and v a spot $\notin S$. For a $\mathbb{Z}$-lattice K on W there is an integer μ such that*

(i) $\mu \in \mathbb{Z}_p^x$ *if* $p \in S$. **198**

(ii) *if a rational number a is represented by W, and*

$a \in Q(K_p) \cap \mu\mathbb{Z}_p$ *for* $p \neq v$, $W \ni y$ *with* $Q(y) = a$ *and* $y \in K_p$ *for* $p \neq v$.

Proof. Extending S, we may assume that if $p \notin S$, $p \neq v$, then K_p is unimodular and $p \neq 2$. Let $K_1, \ldots, K_h$ be a complete set of representatives of classes in gen K. We show that K_i can be chosen so that $(K_i)_p = K_p$ for $p \in S$. First, we note that every regular quadratic module M over $\mathbb{Z}_p$

has a symmetry, since, for $m \in M$ satisfying $(Q(m)) = \underline{n}(M)$, τ_m gives a symmetry of M . Hence by the definition of the genus, there is an isometry $\sigma_{i,p} \in 0^+(W_p)$ such that $\sigma_{i,p}((K_i)_p) = K_p$, and then by Lemma 2.2.30 there is an isometry σ_i such that σ_i and $\sigma_{i,p}$ are sufficiently close for $p \in S$. As representatives we have only to take $\sigma_i(K_i)$. Thus we may assume $(K_i)_p = K_p$ for $p \in S$. Now we choose an integer λ so that $\lambda K_i \subset K$ for all i and $\lambda \in \mathbb{Z}_p^x$ for $p \in S$, and put $\mu = \lambda^2$. The condition (i) is satisfied. Suppose that a is a rational number as in (ii). If $p \in S$, then $a/\mu \in Q(K_p)$. If $p \notin S$, $p \neq v$, then $p \neq 2$, and K_p is unimodular, and then $K_p \cong < \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} > \perp *$. Since $a/\mu \in \mathbb{Z}_p$, a/μ is represented by $< \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} > \subset K_p$. If v is a finite spot associated with a prime number q, then $a/\mu \cdot q^{2t} \in Q(K_q)$ for a sufficiently large integer t. Thus a/μ or $a/\mu \cdot q^{2t}$ is locally represented by K according as $v = \infty$ or q. By Theorem 2.2.28, there is a vector x in some K_i such that $Q(x) = a/\mu$ or $a/\mu \cdot q^{2t}$ according as $v = \infty$ or q. Then $y = \lambda x$ or $\lambda q^{-t} x$ is what we want. ◻

Lemma 2.2.32. *Let V be a regular quadratic module over $\mathbb{Q}$ of* $\dim v \geqq 4$ *which is isotropic at a spot v, L a $\mathbb{Z}$-lattice on V, and T a finite set of prime numbers with $T \not\ni v$.*

199 *Suppose that a non-zero rational number a and $z_p \in V_p (p \neq v)$ satisfy*

(i) $Q(z_p) = a \in Q(V)$ *for every $p \neq v$, and*

(ii) $z_p \in L_p$ *if $p \notin T$.*

Then there is a vector $z \in V$ satisfying

(i) *z and z_p are sufficiently close if $p \in T$,*

(ii) *$z \in L_p$ if $p \notin T \cup \{v\}$,*

(iii) *$Q(z) = a$.*

Proof. Multiplying the quadratic form by a^{-1}, we may assume $a = 1$ without loss of generality. Extending T, we may assume that if $p \notin T \cup \{v\}$, then L_p is unimodular and $p \neq 2$. If V_∞ is isotropic, then we have only to consider the case of $v = \infty$. Thus we may assume that $a = 1$, and V_∞ is anisotropic in case $v \neq \infty$. Since we can take $(\prod_{p\in T} p)^{-r}L$ instead of $L (r \geqq 0)$, we may assume that $z_p \in L_p$ if $p \neq v$. Take and fix any vector x such that $Q(x) = 1$. Take $\varphi_p \in 0^+(V_p)$ so that $\varphi_p(x) = z_p$ for $p \in T$. From Lemma 2.2.30, follows the existence of an isometry $\varphi \in 0^+(V)$ such that φ and φ_p are sufficiently close for $p \in T$, and $y \in L_p$ if $p \in T$. Choose an integer λ so that λ and 1 are sufficiently close in $\mathbb{Z}_p$ if $p \in T$, and $\lambda y \in L_p$ if $p \notin T \cup \{v\}$, and set $u = \lambda y$; then $u \in L_p$ if $p \neq v$ and $Q(u) = \lambda^2$. Set $W = u^\perp = \{w \in V | B(u, w) = 0\}$, and we determine a lattice K on W under the following conditions:

$$K_p = (L \cap W)_p = L_p \cup W_p \text{ if } p \notin T,$$

$K_p \subset p^r L_p$ for sufficiently large r if $p \in T$. $K \subset L$, as is obvious. Set $T_\lambda = \{p | \lambda \notin \mathbb{Z}_p^x, p \neq v\}$; then $T \cap T_\lambda = \phi$ since $\lambda \in \mathbb{Z}_p^x$ if $p \in T$. Let μ be an integer in Lemma 2.2.31 for $v \notin S = T \cup T_\lambda$ and M. Set $T_\mu = \{p | \mu \notin \mathbb{Z}_p^x, p \neq v\}$; then $T_\mu \cap (T \cup T_\lambda \cup \{v\}) = \phi$. We claim that (♯) there is a rational number β so that **200**

$$1 - \lambda^2\beta^2 \in \mu\mathbb{Z}_p \cap Q(K_p) \text{ and } \beta \in \mathbb{Z}_p \text{ if } p \neq v,$$

β and 1 are sufficiently close if $p \in T$,

$$1 - \lambda^2\beta^2 \in Q(W_v) \text{ and } 1 - \lambda^2\beta^2 \in Q(W_\infty).$$

We return to the proof of this latter and first complete with its help the proof of Lemma 2.2.32. By the Hasse-Minkowski Theorem, $1 - \lambda^2\beta^2 \in Q(W)$. Applying the property (ii) in Lemma 2.2.31 to $a = 1 - \lambda^2\beta^2$, there is a vector $w \in W$ such that $Q(w) = 1 - \lambda^2\beta^2$ and $w \in K_p$ for $p \neq v$. We show that $z = \beta u + w$ is what we want. Suppose $P \in T$; then β and 1 are sufficiently close in $\mathbb{Z}_p$ and $w \in K_p \subset p^r L_p$. Thus z and u are sufficiently close in V_p. On the other hand, z_p and y, u and y are sufficiently close respectively. Hence z and z_p are sufficiently close for $p \in T$. If $p \notin T \cup \{v\}$, then $z = \beta\lambda y + w \in \beta L_p + K_p \subset L_p$. Lastly $Q(z) = \beta^2\lambda^2 + Q(w) = 1$. Thus the assertions (i), (ii)., (iii) are satisfied. It remains for us to prove the existence of a rational number β. First, we construct $\beta_p \in \mathbb{Q}_p$ which satisfies the condition (♯) locally with $1-\lambda^2\beta_p^2 \neq 0$ for $p \in T \cup T_\lambda \cup T_\mu$. Then we approximate β_p by β, noting that $Q(K_p)\backslash\{0\}$, $Q(W_v)\backslash\{0\}$, $Q(W_\infty)\backslash\{0\}$ are open sets.

Let $p \in T$; take a non-zero number $\alpha_p \in Q(K_p)$ which is sufficiently close to 0 and set $\beta_p = \lambda^{-1}(1-\alpha_p/2)$. Since λ and 1 are sufficiently close,
201 β_p and 1 are also sufficiently close. Clearly, $1-\lambda^2\beta_p^2 = 1-(1-\alpha_p/2)^2 = \alpha_p(1-\alpha_p/4) \in \alpha_p\mathbb{Z}_p^{x^2} \subset Q(K_p)$. Since $T \cap T_\mu = \phi$, we have $\mu \in \mathbb{Z}_p^x$ and then $1-\lambda^2\beta_p^2 \in \mu\mathbb{Z}_p$. Thus the condition ($\sharp$) is satisfied for β_p with $q-\lambda^2\beta_p^2 \neq 0$.

Let $p \in T_\mu$; take $\beta_p \in \mathbb{Q}_p$ so that β_p and λ^{-1} are sufficiently close but $\beta_p \neq \lambda^{-1}$. Since $\lambda \in \mathbb{Z}_p^x, \beta_p \in \mathbb{Z}_p^x$. Obviously $0 \neq 1-\lambda^2\beta_p^2 \in \mu\mathbb{Z}_p$. Since $p \notin T$ and $Q(u) = \lambda^2 \in \mathbb{Z}_p^x$, $K_p = u^\perp$ in L_p is unimodular, by virtue of Lemma 2.1.3. From Proposition 2.1.12, it follows that $Q(K_p) = \mathbb{Z}_p$. Thus the condition ($\sharp$) is satisfied for β_p with $1-\lambda^2\beta_p^2 \neq 0$.

Let $p \in T_\lambda$; first, we claim that K_p contains a unimodular submodule of *rank* $\geqq 2$. Let $\{v_i\}$ be a basis of L_p over $\mathbb{Z}_p$ and assume $v_1 = by$, $b \in \mathbb{Q}_p$. Since $T \cap T_\lambda = \phi$, L_p is unimodular and then $Q(v_1) = b^2 \in \mathbb{Z}_p$. Suppose $b \in \mathbb{Z}_p^x$; then $L_p = \mathbb{Z}_p v_1 \perp (v_1^\perp \text{ in } L_p) = \mathbb{Z}_p v_1 \perp K_p$ by virtue of Lemma 2.1.3 and the definition of K. Hence K_p itself is unimodular. Suppose $b \in p\mathbb{Z}_p$; since $\mathbb{L}_p$ is unimodular, $B(v_1, L_p) = \mathbb{Z}_p$ and in view of $Q(v_1) \in p\mathbb{Z}_p$, we may assume $B(v_1, v_2) = 1$, without loss of generality. Then $\mathbb{Z}_p[v_1, v_2]$ is unimodular and so is $\mathbb{Z}_p[v_1, v_2]^\perp$ in $L_p(\subset K_p)$ by Lemma 2.1.3. Thus our claim above has been proved, and then Proposition 2.1.12 implies that $Q(K_p) \ni 1$. For $\beta_p = 0$, the condition ($\sharp$) is satisfied with $1-\lambda^2\beta_p^2 \neq 0$ since $\mu\mathbb{Z}_p = \mathbb{Z}_p$.

Suppose $v = \infty$; then we choose a large number $\beta \in \mathbb{Q}$ such that β and β_p are sufficiently close for $p \in T \cup T_\lambda \cup T_\mu$, and $\beta \in \mathbb{Z}_p$ otherwise. If $p \notin T \cup T_\lambda \cup T_\mu$, then $\mu \in \mathbb{Z}_p^x$ and K_p is unimodular since L_p is unimodular
202 and $Q(u) \in \mathbb{Z}_p^x$. Hence $\mu\mathbb{Z}_p = Q(K_p) = \mathbb{Z}_p$, and the condition ($\sharp$) is satisfied for each prime number. By assumption $Q(W_\infty) \supset \{a \in \mathbb{R} | a < 0\}$, and then it is also satisfied for $v = \infty$.

Suppose $v = q < \infty$. Set $\beta_q = q^{-r}$ for a sufficiently large r; then $1-\lambda^2\beta_q^2 = -\lambda^2\beta_q^2(1-\lambda^{-2}q^{2r}) \in Q(W_v)$, since $V_q =< \lambda^2 >\perp W_q$ is isotropic and $1-\lambda^{-2}q^{2r}$ is a square. We take a rational number β' so that β' and β_p are sufficiently close for $p \in T \cup T_\lambda \cup T_\mu \cup \{q\}$ and $\beta' \in \mathbb{Z}_p$ otherwise. Next we take a sufficiently large integer m such that q^m and

1 are sufficiently close for $p \in T \cup T_\lambda \cup T_\mu$, and set $\beta = \beta' q^{-m}$. In the process, V_∞ is positive definite, and $1 - \lambda^2\beta^2$ is sufficiently close to 1 in $\mathbb{R}$. It is easy to see that β is the rational number required in ($\sharp$). $\square$

PROOF of Theorem 2.2.29 when dim $V \geqq 4$.

Let V, v, S, σ_p be as in Theorem 2.2.29.

(i) Suppose that $\sigma_p = \tau_{x_p}\tau_{y_p}$, $Q(x_p) = Q(y_p)$ $(x_p, y_p \in V_p)$ for any $p \in S$.

Take a vector $x \in V$ so that x and x_p are sufficiently close for $p \in S$, and $x \in L_p$ otherwise, and take $\eta_p \in 0(V_p)$ so that $y_p = \eta_p x_p$. Choose a finite set S' of prime numbers so that $S' \cap (S \cup \{v\}) = \phi$ and if $p \notin S'$, then $\tau_x L_p = L_p$, $Q(x) \in \mathbb{Z}_p^x$, $p \neq 2$, and L_p is unimodular. Set $z_p = \eta_p x$ for $p \in S$, $z_p = x$ for $p \in S'$. If $p \notin S \cup S' \cup \{v\}$, then there exists $z_p \in L_p$ such that $Q(z_p) = Q(x)$ since L_p is unimodular ($p \neq 2$) and $Q(x) \in \mathbb{Z}_p^x$. Applying Lemma 2.2.32 to $z_p, T = S \cup S'$, $0 \neq a = Q(x) \in Q(V)$, there is a vector $z \in V$ with $Q(z) = Q(x)$ such that z and z_p are sufficiently close for $p \in S \cup S'$, $z \in L_p$ for $p \notin S \cup S' \cup \{v\}$. If $p \in S$, then $\tau_x\tau_z$ **203**
and $\tau_{x_p}\tau_{y_p} = \sigma_p$ are sufficiently close. If $p \in S'$, then $\tau_x\tau_z$ and $\tau_x\tau_x = id$ are sufficiently close and hence $\tau_x\tau_z L_p = L_p$. Suppose $p \notin S \cup S' \cup \{v\}$; then $\tau_x L_p = L_p$ by the definition of S', and further $\tau_z L_p = L_p$ since $Q(z) = Q(x) \in \mathbb{Z}_p^x$ and $z \in L_p$. Thus $\sigma = \tau_x\tau_z$ is what we want.

(ii) Suppose that $\sigma_p = \tau_{x_{1,p}}\tau_{y_{1,p}} \cdots \tau_{x_{r,p}}\tau_{y_{r,p}}$, $Q(x_{i,p}) = Q(y_{i,p})$ for each $p \in S$.

In this case, we may assume that r is independent of each $p \in S$, since the order of any symmetry is 2. Applying (i) to $\tau_{x_i}\tau_{y_i}$, we complete the proof.

(iii) **General Case.**

Set $\sigma_p = \tau_{x_{1,p}} \cdots \tau_{x_{2r,p}}$ with $\Pi Q(x_{i,p}) = 1$ and assume r is independent of each $p \in S$ as in (ii). Extending S, we may assume that V_p is isotropic if $p \notin S$, by virtue of Theorem 6 on page 36 in [S]. On this occasion, we set σ_p = the identity mapping

for p which belongs not to the originale S but to the extended S. Take $x_1, \ldots, x_{2r-1} \in V$ so that x_i and $x_{i,p}$ are sufficiently close for $p \in S, 1 \leqq i \leqq 2r-1$ and so are $\prod_{1 \leqq i \leqq 2r-1} Q(x_i)$ and $\prod_{q \leqq i \leqq 2r-1} Q(x_{i,p}) (\neq 0)$ for $p \in S$. Hence there is a unit $\varepsilon_p \in \mathbb{Z}_p^x$ such that $Q(x_{2r,p})^{-1} = \prod_{1 \leqq i \leqq 2r-1} Q(x_{i,p}) = \epsilon_p^2 \prod_{1 \leqq i \leqq 2r-1} Q(x_i)$, and ϵ_p is sufficiently close to 1. We claim that there is a vector $x_{2r} \in V$ so that $Q(x_{2r}) = \prod_{1 \leqq i \leqq 2r-1} Q(x_i)^{-1}$, and x_{2r} and $x_{2r,p}$ are sufficiently close for $p \in S$. Set $a = \prod_{1 \leqq i \leqq 2r-1} Q(x_i)^{-1}$; then $a = Q(\epsilon_p \; x_{2r,p})$ for $p \in S$, and since V_p is isotropic for $p \notin S$, a is represented
204 by V_p for every prime number p. If V_∞ is isotropic, then a is also represented by V_∞. If V_∞ is anisotropic, then the sign of a is equal to $Q(x_{2r-1})$, and hence a is also represented by V_∞. By virtue of Hasse-Minkowski Theorem, a is represented by V. Take a vector $w \in V$ with $Q(w) = a$, and $\eta_p \in 0^+(V_p)$ with $\eta_p w = \epsilon_p \; x_{2r,p}$ for $p \in S$, and approximate η_p by $\eta \in 0^+(V)$ by Lemma 2.2.30. We can take $\eta(w)$ as x_{2r}. Then $\prod_{1 \leqq i \leqq 2r} Q(x_i) = 1$ and $\tau_{x_1} \cdots \tau_{x_{2r}}$ and $\tau_{x_{1,p}} \cdots \tau_{x_{2r,p}}$ are sufficiently close for $p \in S$. Set $S' = \{p \notin S \cup \{v\} | \tau_{x_1} \cdots \tau_{x_{2r}} L_p \neq L_p\}$. Since V_p is isotropic for $p \in S'$, it follows that $\tau_{x_1} \cdots \tau_{x_{2r}}$ is a product of $\tau_x \tau_y (x, y \in V_p, Q(x) = Q(y))$ for $p \in S'$. From (ii), follows the existence of $\sigma_1 \in 0'(V)$ such that σ_1 and 1 (resp. $\tau_{x_1} \cdots \tau_{x_{2r}}$) are sufficiently close for $p \in S$ (resp. $p \in S'$) and $\sigma_1(L_p) = L_p$ for $p \notin S \cup S' \cup \{v\}$. Then $\sigma = \sigma_1^{-1} \tau_{x_1} \cdots \tau_{x_{2r}}$ is what we want. Thus we have completed the proof of Theorem 2.2.28 when $\dim V \geqq 4$.

Suppose now that $\dim V = 3$. Multiplying the quadratic form by a constant, we may assume $d(V) = 1$, that is, $V = < a_1 > \perp < a_2 > \perp < a_1 a_2 >, a_i \in \mathbb{Q}^x$. Now we define a quaternion algebra $C = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k$ by $i^2 = -a_1$, $j^2 = -a_2$, $k^2 = -a_1 a_2$ and $-ji = k$. The conjugate $\overline{x}$ of $x = a + bi + cj + dk (a, b, c, d \in \mathbb{Q})$ is defined by $a - bi - cj - dk$. Then the norm $N(x)$ of x is, by definition, $x\overline{x} = a^2 + b^2 a_1 + c^2 a_2 + d^2 a_1 a_2$, and so it is a quadratic form and the corresponding bilinear form $B(x, y)$

is $\frac{1}{2}(x\overline{y}+y\overline{x})$. Thus V is isometric to the subspace $\mathbb{Q}i+\mathbb{Q}j+\mathbb{Q}k$ and we identify them. We note that V and $\mathbb{Q}\subset\mathbb{C}$ are orthogonal. For $x\in V$ with $N(x)\neq 0$, we have

$$\begin{aligned}\tau_x y &= y-\frac{(x\overline{y}+y\overline{x})}{N(x)}\\ &= -N(x)^{-1}x\overline{y}x = -xyx^{-1} \text{ for } y\in V.\end{aligned}$$

Therefore $\varphi\in 0^{+}(V)$ is written, for some $z\in C$, as **205**

$$\varphi(y)=zyz^{-1} \text{ for } y\in V,$$

and then the spinor norm $0(\varphi)$ is $N(z)\mathbb{Q}^{x^2}$. Set $\widetilde{L}=\mathbb{Z}\perp L$ and extend the given $\sigma_p\in 0'(V_p)$ to $\widetilde{\sigma}_p\in 0'(C_p)$ where $\widetilde{\sigma}_p(1)=1(\in C)$. Similarly to the foregoing, there is a vector $z_p\in C_p$ so that $\widetilde{\sigma}_p(y)=z_pyz_p^{-1}(p\in S)$. Since $\widetilde{\sigma}_p(\in 0'(V_p), Nz_p=a_p^2, a_p\in\mathbb{Q}_p^x$. Taking $a_p^{-1}z_p$ instead of z_p, we may assume $Nz_p=1$. If $p\notin S$, then set $z_p=1$. Let $T(\not\ni v)$ be a finite set of prime numbers such that $T\supset S$ and if $p\notin T$, then $\widetilde{L}_p$ is unimodular and a subring. Applying Lemma 2.2.32, there is a vector $z\in C$ so that $N(z)=1, z$ and z_p are sufficiently close if $p\in T$ and $z\in\widetilde{L}_p$ if $p\notin T\cup\{v\}$. We define an isometry $\widetilde{\sigma}0'(C)$ by $\widetilde{\sigma}(y)=zyz^{-1}$. Since $\widetilde{\sigma}(1)=1$, $\widetilde{\sigma}(V)=V$ follows, and set $\sigma=\widetilde{\sigma}|V$. If $p\in S$, then z and z_p are sufficiently close, and then $\widetilde{\sigma}$ and $\widetilde{\sigma}_p$ are sufficiently close, and hence so are σ and σ_p since $\widetilde{\sigma}(1)=\widetilde{\sigma}_p(1)=1$. If $p\in T\backslash S$, then $\widetilde{\sigma}$ and id are sufficiently close, and then $\widetilde{\sigma}(\widetilde{L}_p)$, and hence $\sigma(L_p)=L_p$. Suppose $p\notin T$; then $z\in\widetilde{L}_p$, and $\widetilde{L}_p$ is unimodular. Hence $\tau_z(\widetilde{L}_p)=\widetilde{L}_p$, since $N(z)=1$. From $\widetilde{L}_p=\tau_z\widetilde{L}_p=z\widetilde{L}_pz=z\widetilde{L}_pz^2z^{-1}\subset z\widetilde{L}_pz^{-1}=\widetilde{\sigma}\widetilde{L}_p$, it follows that $\widetilde{\sigma}$ preserves $\widetilde{L}_p$, and then $\sigma(L_p)=L_p$. Thus σ is what we wanted, and the proof of Theorem 2.2.29 is complete.

Theorem 2.2.33. *Let V be a regular quadratic module over $\mathbb{Q}$ with* $\dim V=m\geqq 2$ *and suppose that V is not a hyperbolic plane, i.e., either* $\dim V=2$ *and* $d(V)\neq -1$ *or* $\dim V\geqq 3$, *and that* $V_\infty=\mathbb{R}V\cong(\underset{r}{\perp}<1>)\perp(\underset{s}{\perp}<-1>)$. *Suppose that the following are given:* **206**

(a) *a $\mathbb{Z}$-lattice M on V,*

(b) *a finite set S of prime numbers p such that $S \ni 2$ and M_p is unimodular for $p \notin S$,*

(c) *integers r', s' with $0 \leqq r' \leqq r$, $0 \leqq s' \leqq s$,*

(d) *$x_{1,p}, \ldots, x_{n,p} \in M_p (r' + s' = \eta < m)$ for $p \in S$.*

Then there are vectors $x_1, \ldots, x_n$ in M satisfying

(i) *x_i and $x_{i,p}$ are sufficiently close in V_p for $p \in S$, $1 \leqq i \leqq n$,*

(ii) *for $p \notin S$, $\det(B(x_i, x_j)) \in \mathbb{Z}_p^x$ with precisely one exception $p = q$, where*
$\det(B(x_i, x_j)) \in q\mathbb{Z}_p^x$,

(iii) *a subspace spanned by $\{x_i\}$ in $\mathbb{R}V$ is isometric to $(\underset{r'}{\perp} < 1 >) \perp (\underset{s'}{\perp} < -1 >)$.*

Proof. We use induction on $n = r' + s'$. First suppose $n = 1$, $m = 2$. This case is fundamental. Let $V^a (a \in \mathbb{Q}^x)$ denote the vector space provided with a new quadratic form $aQ(x)$. We shall use L^a to denote the lattice L when it is regarded as a lattice in V^a. First, we show that if the theorem is true for V^a, then it holds for V. Suppose that the theorem holds for $V^a (a \in \mathbb{Q}^x)$ and that $M, S, r', s', x_{1,p}$ in $(a), \ldots, (d)$ are given. Put $S(a) = S \cup \{p | a \notin \mathbb{Z}_p^x\}$. Then for a lattice M^a and $S(a)$, the condition (b) is satisfied. For a prime number $p \in S(a) \backslash S$, we can choose $x_{1,p} \in M_p$ with $Q(x_{1,p}) \in \mathbb{Z}_p^x$ since p is odd and M_p is unimodular. If a is positive, then we put $r'' = r'$, $s'' = s'$. Otherwise, put $r'' = s'$, $s'' = r'$. From the assumption, it follows that there exists $x \in M^a$ for which

(i′) x and $x_{1,p}$ are sufficiently close in V_p for $p \in S(a)$,

(ii′) for $p \notin S(a)$, $aQ(x) \in \mathbb{Z}_p^x$ with precisely one exception $p = q$, where $aQ(x) \in q\mathbb{Z}_q^x$, and

207 (iii′) $aQ(x)$ is positive (resp. negative) if $r'' = 1$, $s'' = 0$ (resp. $r'' = 0$, $s'' = 1$).

(i′) (resp. (iii′)) implies (i) (resp. (iii)). If $p \notin S(a)$, $p \neq q$, then we have $aQ(x) \in \mathbb{Z}x_p$ and $a \in \mathbb{Z}_p^x$ and therefore $Q(x) \in \mathbb{Z}_p^x$. For $p = q$, $Q(x) \in q\mathbb{Z}_q^x$ since $q \notin S(a)$. For $p \in S(a)\backslash S$, (i′) implies that $Q(x)$ and $Q(x_{1,p}) \in \mathbb{Z}_p^x$ are sufficiently close. Hence $Q(x) \in \mathbb{Z}_p^x$. Thus we get the assertions (i), (ii), (iii). Therefore, we may assume that V is a quadratic field k over $\mathbb{Q}$ and the quadratic form Q is equal to the norm N from k to $\mathbb{Q}$. We take a finite set $S' \supset S$ of prime numbers so that for $p \notin S'$, M_p is equal to the localization of the maximal order of k. We choose $x_{1,p} \in M_p$ is equal to the localization of the maximal order of k. We choose $x_{1,p} \in M_p$ for $p \in S'\backslash S$ such that $Nx_{1,p} \in \mathbb{Z}_p^x$. By the approximation theorem, there exists $y \in k$ such that Ny is positive (resp. negative) for $r' = 1$, $s' = 0$ (resp. $r' = 0$, $s' = 1$) and y and $x_{1,p}$ are sufficiently close for $p \in S'$. Decompose the principal ideal (y) as $(y) = \widetilde{m}\widetilde{n}$ where $\widetilde{m}, \widetilde{n}$ are ideals of k and the prime divisor $\widetilde{p}$ appears in $\widetilde{m}$ if and only if $\widetilde{p}$ divides some prime number p in S'. Thus it is known that there exists a number $z \in k$ for which z and 1 are sufficiently close for $p \in S'$, Nz is positive, and $\widetilde{q} = \widetilde{n}z$ is a prime divisor with $N\widetilde{q} = q$ prime. □

Put $x = yz$. Then the conditions (i), (iii) are obviously satisfied. For $p \in S'\backslash S, y, x_{1,p}$ and $z, 1$ are sufficiently close respectively and $Nx_{1,p} \in \mathbb{Z}_p^x$. Hence $Q(x) \in \mathbb{Z}_p^x$, for $p \in S'\backslash S$. Since $(x) = (yz) = \tilde{m}\tilde{q}$, we have $Q(x) = \pm N(\widetilde{m})q$. By the assumption on $\widetilde{m}$, the condition (ii) is satisfied. By the construction, it is easy to see that x is contained in every **208**
localization of M and hence in M. Thus we have completed the proof for the case $n = 1$, $m = 2$. Suppose now that $n = 1$ and $m = \dim V \geqq 3$. Take any prime $h \notin S$. Then there exists a basis $\{v_i\}$ of M_h such that $(B(v_i, v_j))_{i=1,2} = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, $Q(v_3) \in \mathbb{Z}_h^x$ and $M_h = \mathbb{Z}_h[v_1, v_2] \perp \mathbb{Z}_h v_3 \perp \cdots$ by Proposition 2.1.12. We take $x_1 \in M$ so that x_1 and $x_{1,p}$ are sufficiently close for $p \in S$, and x_1 and $v_1 + hv_2$ are sufficiently close for h. Put $T = \{p \notin S | Q(x_1) \notin \mathbb{Z}_p^x\} \ni h$. There exists $x_2 \in V$ such that $Q(x_2) > 0$ (resp. < 0) for $r' = 1$, $s' = 0$ (resp. $r' = 0$, $s' = 1$), for $p \in T$, $x_2 \in M_p$ and $Q(x_2) \in \mathbb{Z}_p^x$ and moreover, x_2 and v_3 are sufficiently close for $p = h$. Then we have a natural number a such that $ax_2 \in M$ and $p \nmid a$ for $p \in T$. The discriminant of $M' = \mathbb{Z}[x_1, ax_2]$ is divisible exactly by h. Hence $W = \mathbb{Q}[x_1, ax_2]$ is not a hyperbolic plane. Put

$U = \{p \notin S \cup T | d(M') \notin \mathbb{Z}_p^\times\}$ and $x'_{1,p} = x_1$ if $p \in S \cup U$, $x'_{1,p} = x_2$ if $p \in T$, and $S' = S \cup T \cup U$. Then M'_p is unimodular for $p \notin S'$, since $d(M'_p)$ is a unit and $M' \subset M$. Applying the previous result to this, we have an element $x \in M'$ such that

(i) x and $x'_{1,p}$ are sufficiently close for $p \in S'$

(ii) for $p \notin S'$, $Q(x) \in \mathbb{Z}_p^\times$ with precisely one exception $p = q$, where $Q(x) \in q\mathbb{Z}_p^\times$,

(iii) $Q(x) > 0$ (resp. < 0) if $r' = 1$ (resp. $r' = 0$).

It is easy to see that this x is what we wanted. Now suppose $1 < n < m$. Applying the inductive assumption to $x_{1,p}, \dots, x_{n-1,p}, S$ and M, there exist $x_1, \dots, x_{n-1} \in M$ such that x_i and $x_{i,p}$ are sufficiently close
209 for $1 \leqq i \leqq n-1$, $p \in S$, $\det(B(x_i, x_j))_{i,j<n} \in \mathbb{Z}_p^\times$ for $p \notin S \cup \{q_1\}$ for some prime $q_1 \notin S$, $\det(B(x_i, x_j))_{i,j<n} \in q_1\mathbb{Z}_{q_1}^\times$, and over $\mathbb{R}$

$$(< B(x_i, x_j))_{i,j<n} > \perp < \delta > \cong (\underset{r'}{\perp} < 1 >) \perp (\underset{s'}{\perp} < -1 >) \text{ for } \delta = \pm 1.$$

Put $U = \sum_{i=1}^{n-1} \mathbb{Q}x_i$, $W = \{x \in V | B(x, U) = 0\}$. Then $V = U \perp W$. Put $A = \mathbb{Z}[x_1, \dots, x_{n-1}]$; then $d(A_{q_1}) \in q_1\mathbb{Z}_{q_1}^\times$. From the local version of Lemma 2.4.26, it follows that $d(A_{q_1}^\perp \text{ in } M_{q_1}) \in \mathbb{Z}_{q_1}^\times$. On the other hand, $d(M_{q_1}) \in \mathbb{Z}_{q_1}^\times$ implies $d(A_{q_1}) \cdot d(A_{q_1}^\perp) \in \mathbb{Z}_{q_1}^\times \mathbb{Q}_{q_1}^{\times 2} / \mathbb{Q}_{q_1}^{\times 2}$. Thus $d(A_{q_1}^\perp$ in $M_{q_1}) \in q_1\mathbb{Z}_{q_1}^\times$. Let $A_{q_1} = L_1 \perp L_2$, $A_{q_1}^\perp = L_3 \perp L_4$ be Jordan splittings so that L_1, L_3 are unimodular and rank $L_2 =$ rank $L_4 = 1$. Since M_{q_1} is unimodular, $L_2 \perp L_4$ is contained in the unimodular module $(L_1 \perp L_3)^\perp$ in M_{q_1}, and then $A_{q_1} \subset L_1 \perp (L_1 \perp L_3)^\perp$. From $d(A_{q_1}) \in q_1\mathbb{Z}_{q_1}^\times$, it follows that A_{q_1} is a direct summand in $L_1 \perp (L_1 \perp L_3)^\perp$, and hence there is an element $x_{n,q_1} \in M_{q_1}$ such that $A_{q_1} + \mathbb{Z}_q x_{n,q_1}$ is a unimodular module $L_1 \perp (L_1 \perp L_3)^\perp$. Decompose $x_{n,p}$ as $x_{n,p} = y_{n,p} + z_{n,p}(y_{n,p} \in U_p, z_{n,p} \in W_p)$ for $p \in S \cup \{q_1\}$. We can take $y_n \in U$ so that y_n and $y_{n,p}$ are sufficiently close for $p \in S \cup \{q_1\}$ and $y_n \in A_p$ for $p \notin S \cup \{q_1\}$. We claim that

($\sharp$) there exist an element z_n in the projection M' of M to W and a prime $q \notin S \cup \{q_1\}$ such that

$$z_n \text{ and } z_{n,p} \text{ are sufficiently close for } p \in S \cup \{q_1\},$$

$Q(z_n) \in \mathbb{Z}_p^\times$ for $p \notin S \cup \{q, q_1\}$ and $Q(z_n) \in q\mathbb{Z}_q^\times$,
$Q(x_n)\delta > 0$.

We come to the proof of this later and first complete the proof of the **210**
theorem with its help. put $x_n = y_n + z_n$. Then x_n and $x_{n,p} = y_{n,p} + z_{n,p}$ are sufficiently close for $p \in S \cup \{q_1\}$. Hence the condition (i) is satisfied, and $x_n \in M_p$, for $p \in S \cup \{q_1\}$. For $p \notin S \cup \{q_1\}$, M_p, A_p are unimodular and hence $M_p = A_p \perp (*)$. Since M' is the projection of M to W, we have $M_p = A_p \perp M'_p$. Hence we have $x_n = y_n + z_n \in A_p + M'_p = M_p$ for $p \notin S \cup \{q_1\}$. Thus $x_n \in M$. We check the condition (ii). $d(\mathbb{Z}_p[x_1, \ldots, x_n])$ and $d(\mathbb{Z}_p[x_{1,p}, \ldots, x_{n,p}])$ are sufficiently close for $p = q_1$, and the latter is a unit by the definition of x_{n,q_1}. Hence $d(\mathbb{Z}_p[x_1, \ldots, x_n]) \in \mathbb{Z}_p^\times$, for $p = q_1$. For $p \notin S \cup \{q_1\}$, $d(\mathbb{Z}_p[x_1, \ldots, x_n]) = d(\mathbb{Z}_p[x_1, \ldots, x_{n-1}, y_n + z_n]) = d(\mathbb{Z}_p[x_1, \ldots, x_{n-1}, z_n])$ $(y_n \in A_p) = d(A_p) \cdot Q(z_n) \in Q(z_n)\mathbb{Z}_p^\times$. Thus from the property of z_n in ($\sharp$) condition (ii) follows. Condition (iii) follows from

$$\begin{aligned}\mathbb{Q}[x_1, \ldots, x_n] &= \mathbb{Q}[x_1, \ldots x_{n-1}] \perp \mathbb{Q}z_n \\ &=< (B(x_i, x_j))_{i,j<n} >\perp< \delta > \text{ over } \mathbb{R}.\end{aligned}$$

It remains to show ($\sharp$). For $\dim W \geqq 2$, this is clear. Since $d(W_{q_1}) = d(A_{q_1}^\perp) \in q_1\mathbb{Z}_{q_1}^\times$, W is not the hyperbolic plane. As we have seen, $M_p = A_p \perp M'_p$ for $p \notin S \cup \{q_1\}$ and then M'_p is unimodular for $p \notin S \cup \{q_1\}$. Also, $z_{n,p} \in M'_p$, from the definitions of $z_{n,p}$ and M'. Obviously, $W \cong< \delta >\perp (*)$ over $\mathbb{R}$, by the definition of δ. Applying the theorem for the case $n = 1$, we obtain the existence of z_n.

2.2.0

In this paragraph, we give sufficient conditions under which $\operatorname{gen} L = spnL$ or $spnL = clsL$, and also a result on representation of indefinite **211**
quadratic forms.

Theorem 2.2.34. *Let V be a regular quadratic module over $\mathbb{Q}$ with $\dim V \geqq 3$, S a finite set of prime numbers and L a $\mathbb{Z}[S]$-lattice on V.*

If $\theta(0^+(L_p)) \supset \mathbb{Z}_p^x$ *for every prime number* $p \notin S$, *then we have* $\operatorname{gen} L = spnL$.

Proof. Suppose $K \in \operatorname{gen} L$. Then from the definition, we have an isometry $\sigma_p \in 0(V_p)$ such that $\sigma_p(K_p) = L_p$. For $v \in K_p$ satisfying $Q(v)\mathbb{Z}_p = \underline{n}(K_p)$, the symmetry $\tau_v(x) = x - \dfrac{2B(x,v)}{Q(v)}v$ belongs to $0(K_p)$. Hence we may assume $\sigma_p \in 0^+(V_p)$, after multiplying it by τ_v, if necessary. Moreover, we assume $\sigma_p = id$, if $K_p = L_p$. We can take a positive number a so that $a\theta(\sigma_p)$ contains a unit for $p \notin S$. By Proposition 2.2.19, there is an isometry $\sigma \in 0^+(V)$ such that $\theta(\sigma) = a\mathbb{Q}^{x^2}$. For $M = \sigma^{-1}(K)$, we have $\sigma_p\sigma(M_p) = L_p$ for every p, and $\theta(\sigma_p\sigma) \subset \mathbb{Z}_p^x\mathbb{Q}_p^{x^2}$ for $p \notin S$.

By assumption, there is an isometry $\eta_p \in 0^+(L_p)$ such that $\theta(\eta_n\sigma_p\sigma) = \mathbb{Q}_p^{x^2}$. Thus we have

$$\sigma^{-1}(K_p) = (\eta_p\sigma_p\sigma)^{-1}L_p, \quad \eta_p\sigma_p\sigma \in 0'(V_p) \text{ for } p \notin S.$$

This means $K \in spnL$. □

Remark. Let $L_p = L_1 \perp \cdots \perp L_t$ be a Jordan splitting. If either rank $L_i \geq 2$ (resp. 3) for some i for $p \neq 2$ (resp. $p = 2$), or L_p is maximal and rank $L_p \geqq 3$, then the condition $\theta(0^+(L_p)) \supset \mathbb{Z}_p^x$ is satisfied by Proposition 1 in previous section.

212 **Theorem 2.2.35.** *Let* V *be a regular quadratic module over* $\mathbb{Q}$ *with* $\dim V \geqq 3$, S *a finite set of prime numbers, and* L *a* $\mathbb{Z}[S]$*-lattice on* V. *If* $V_\infty = \mathbb{R}V$ *is isotropic or* V_{p_o} *is isotropic for some* $p_0 \in S$, *then* $spnL = clsL$.

Proof. Suppose $K \in spnL$. Then there exist isometries $\mu \in 0(V)$, $\sigma_p \in 0'(V_p)$ for $p \notin S$ such that

$$\mu(K_p) = \sigma_p(L_p).$$

Put $T = \{p \notin S | \mu(K_p) \neq L_p\}$ (a finite set). Then by Theorem 2.2.29, there is an isometry $\sigma \in 0'(V)$ such that $\sigma(L_p) = L_p$ if $p \neq T$ or $T \cup \{p_0\}$ according to the hypothesis, σ and σ_p are sufficiently close if $p \in T$.

Hence for $p \in T$, $\sigma(L_p) = \sigma_p(L_p)$ and then $\mu(K_p) = \sigma(L_p)$ for $p \notin S$. This leads to $K = \mu^{-1}\sigma(L)$. □

Corollary 1. *Let V be a regular quadratic module over $\mathbb{Q}$ with* $\dim V \geqq 3$, *and suppose that V_∞ is isotropic. If L is a $\mathbb{Z}$-lattice on V that $s(L) \subset \mathbb{Z}$, $d(L)$ is odd and square-free,* $\operatorname{gen} L = clsL$.

Proof. By assumption, L_2 is modular and L_p is maximal for $p \neq 2$. Hence Theorems 2.2.34, 2.2.35 and the Remark for $S = \phi$ imply the corollary. □

Corollary 2. *Let V, W be regular quadratic modules over $\mathbb{Q}$ with* $\dim V + 3 \geqq \dim W$, *and $L(resp. .M)$ a $\mathbb{Z}$-lattice on $V(resp. W)$. Suppose that*

$$L_p \text{ is represented by } M_p \text{ for all } p,$$
$$V_\infty \text{ is represented by } W_\infty, \text{ and}$$
$$W_\infty \text{ is isotropic}.$$

Then L is represented by M. **213**

Proof. From the Corollary to Theorem 2.1.1, it follows that V_p is represented by W_p, and then the Hasse-Minkowski theorem implies that V is represented by W. We may assume $V \subset W$. By assumption, there is an isometry σ_p from L_p to M_p. By Witt's theorem, we may assume $\sigma_p \in 0(W_p)$. Multiplying a symmetry of $V_p^\perp$ from the right, we may assume $\sigma_p \in 0^+(W_p)$. From Proposition 2.2.20 follows the existence of $\eta_p \in 0^+(V_p^\perp)$ and that $\theta(\sigma_p)\theta(\eta_p) = 1$. Multiplying σ_p by η_p on the right, we may assume $\theta(\sigma_p) = 1$. Then there exists an isometry $\sigma \in 0'(W)$ such that

$$\sigma(M_p) = M_p \text{ if } L_p \subset M_p.$$
$$\sigma \text{ is sufficiently close to } \sigma_p \text{ if } L_p \not\subset M_p.$$

Hence $\sigma(L_p) \subset M_p$ for every p and so $\sigma(L) \subset M$.

2.2.0

The aim of this paragraph is to prove the fundamental theorem on representations of positive definite quadratic forms. We mean by a positive lattice a quadratic module $M = \mathbb{Z}[v_1, \ldots, v_m]$ over $\mathbb{Z}$ with basis $\{v_i\}$ such that $(B(v_i, v_j))$ is positive definite. By definition, every $B(v_i, v_j)$ is rational. $\square$

Theorem 2.2.36 ([8]). *Let M be a positive lattice of $\operatorname{rank} M \geqq 2n + 3$. There is a constant $c(M)$ such that any positive lattice N of $\operatorname{rank} N = n$ is represented by M provided that*

$$\min(N) := \min_{0 \neq x \in N} Q(x) \geqq c(M), \text{ and}$$

N_p is represented by M_p for every prime p.

The proof is based on several lemmas.

214 Let $\mathbb{N}$ be the set of non-negative integers and we introduce a partial ordering in $\mathbb{N}^k$ defined by $(x_1, \cdots, x_k) \leqq (y_1, \ldots, y_k)$ if $x_i \leqq y_i (1 \leqq i \leqq k)$. Then our first lemma is the following.

Lemma 2.2.37. *Every subset X of $\mathbb{N}^k$ contains only finitely many minimal elements.*

Proof. We use induction on k. The assertion is trivial for $k = 1$. Write $x = (x', x_k)$ with $x' = (x_1, \ldots, x_{k-1}) \in \mathbb{N}^{k-1}$, and put $X'_n = \{x' \in \mathbb{N}^{k-1} | (x', n) \in X\}$. Let Y_n, Y' be the sets of minimal elements of $X'_n, \bigcup_{n=0}^{\infty} X'_n$ respectively. By the inductive assumption, Y_n, Y' are finite sets. For $y' \in Y'$ we choose and fix an element $y \in X$ satisfying $y = (y', y_k)$, and denote by Y the set of such y. Y is also a finite set and put $m = \max\{y_k | y \in Y\}$. Suppose that $x \in X$ is minimal. Then $x' \in X'_{x_k}$ from the definition and then there exist $y \in Y$ such that $y' \leqq x'$. If $x_k \geqq y_k$, then $x \geqq y$ and then $x = y \in Y$ in view of the minimality of x. Suppose $x_k < y_k (\leqq m)$. Since x is minimal in X_{x_k}, x is minimal in X'_{x_k}. Hence $x \in (Y_{x_k}, x_k) \subset \cup_{n=0}^{m} (Y_n, n)$. Thus every minimal element x is in a finite set $Y \cup \cup_{n=0}^{m} (Y_n, n)$. $\square$

Lemma 2.2.38. *Let M_p be a regular quadratic module over $\mathbb{Z}_p$ of rank $M_p = m \geqq n$. Then there are only finitely many regular submodules $N_p(j)$ of $\operatorname{rank} N_p(j) = n$ such that each regular regular submodule N_p of $\operatorname{rank} N_p = n$ of M_p is represented by some $N_p(j)$.*

Proof. If is obvious that the assertion holds if it is true for $p^\tau M_p$ instead of M_p. Hence we may assume that $s(M_p) \subset \mathbb{Z}_p$. Let N_p be a regular quadratic module of rank n and $N_p = \mathop{\perp}\limits_{i=1}^{t} L_i$ a Jordan splitting. Since L_i is modular, $p^{-b_i} L_i = K_i$ is unimodular or (p)-modular for some $b_i \in \mathbb{N}$. By 215
virtue of Propositions 2.1.12 and 2.1.13, there are only finitely many isometric modules over $\mathbb{Z}_p$ of unimodular or (p)-modular quadratic modules of fixed rank. Thus there are only finitely many possibilities for the whole collection $(rank L_i, K_i)$. Fix one of these and consider the corresponding $(b_1, \ldots, b_t)$. By Lemma 2.2.37, there exist only finitely many minimal ones. It is clear that if

$$\begin{aligned}
&N_p = \mathop{\perp}\limits_{i=1}^{t} L_i, \quad N'_p = \mathop{\perp}\limits_{i=1}^{t} L'_i, \\
&rank L_i = rank L'_i, \quad p^{-b_i} L_i \cong p^{-b'_i} L'_i, \\
&b_i \leqq b'_i \quad \text{for} \quad 1 \leqq i \leqq t,
\end{aligned}$$

then N'_p is represented by N_p. Hence N_p, ranging over all possible collections $(rank L_i, K_i)$ and minimal families (b_i), constitute a finite family with the required property. □

Lemma 2.2.39. *Let L be a positive lattice of rank $L \geqq 3$ and suppose that L_p is maximal for all p, and let q be a prime such that $(\mathbb{Q}L)_p$ is isotropic. Then there is a natural number s such that L represents every positive lattice N for which $q^s L_p$ represents N_p for every prime p.*

Proof. Let $\{L_i\}$ be a complete set of representatives of classes in $\operatorname{gen} L$. From Theorem 2.2.35, it follows that $spn \mathbb{Z}\{q^{-1}\} L = cls \mathbb{Z}[q^{-1}] L$. On the other hand, our assumption implies $\operatorname{gen} L = spn L$ and then $\operatorname{gen} \mathbb{Z}[g^{-1}]$ $L = spn \mathbb{Z}[g^{-1}] L$ by virtue of Proposition 2.2.18 and Theorem 2.2.34. Thus we have $\operatorname{gen} \mathbb{Z}[q^{-1}] L = cls \mathbb{Z}[g^{-1}] L$. Hence there is an isometry $\sigma_i \in 0(\mathbb{Q}L)$ such that $\mathbb{Z}[q^{-1}] L = \mathbb{Z}[g^{-1}] \sigma_i(L_i)$. We determine s by

$$q^s \sigma_i(L_i) \subset L \text{ for every } i.$$

The lemma follows immediately from Theorem 2.2.28. □

Lemma 2.2.40. *Let L, q, s be as in Lemma 2.2.39, rank$L \geqq n+3$, K a positive lattice. Then there is a constant c such that $K \perp L$ represents a positive lattice $N = \mathbb{Z}[v_1, \ldots, v_n]$ of rankn for which N_p is represented by $K_p \perp q^s L_p$ for every p, and $(B(v_i, v_j)) > cE_n$.* 216

Proof. Let S be a finite set of prime numbers such that $S \ni 2, q$ and for $p \notin S K_p, L_p$ are unimodular, and fix a natural number r such that $p^r s(K_p) \subset \underline{n}(q^s L_p)$ for $p \in S$. Choose vectors $v_i^h \in K (i = 1, 2, \ldots, n, h = 1, \ldots, t)$ so that for given $x_{1,p}, \ldots, x_{n,p} \in K_p$, we have

$$v_i^h \equiv x_{i.p} \mod p^r K_p \cdots (*)$$

for some $h (q \leqq h \leqq t)$ and every $i = 1, 2, \ldots, n$ and all $p \in S$. We choose a positive number c so that

$$cE_n - (B(v_i^h, v_j^h)) > 0 \text{ for } h = 1, \ldots, t.$$

Let $N = \mathbb{Z}[v_1, \ldots, v_n]$ be a lattice which satisfies the conditions in the lemma. By the first condition, there exist $x_{i,p} \in K_p, y_{i,p} \in q^s L_p$ such that

$$B(v_i, v_j) = B(x_{i,p}, x_{j,p}) + B(y_{i,p}, y_{j,p}) \text{ for all } p.$$

For some h satisfying $(*)$ for these $x_{i,p}$, we put

$$A = (B(v_i, v_j)) - (B(v_i^h, v_j^h)).$$

We have only to prove that A is represented by L. All the entries of A are rational and A is positive definite, since $A = ((B(v_i, v_j)) - cE_n +$
217 $(cE_n - (B(v_i^h, v_j^h)) > 0$. Let $H = \mathbb{Z}[u_1, \ldots, u_n]$ be a positive lattice such that $(B(u_i, u_j)) = A$. Put $x_{i,p} = v_i^h + p^r z_{i,p} (z_{i,p} \in K_p)$. Then

$$\begin{aligned} A &= (B(x_{i,p}, x_{j,p})) + (B(y_{i,p}, y_{j,p})) - (B(v_i^h, v_j^h)) \\ &= (B(v_j^h, v_j^h) + p^r B(v_i^h, z_{j,p}) + p^r B(z_{i,p}, v_j^h) + p^{2r} B(z_{i,p}, z_{j,p})) + \\ &\quad + (B(y_{i,p}, y_{j,p}) - (B(v_i^h, v_j^h)) \end{aligned}$$

holds.

By the choice of r, the (i, j)th entry of A is congruent to $B(y_{i,p}, y_{j,p})$ modulo $\underline{n}(q^s L_p)$ for $p \in S$. It follows from $y_{i,p} \in q^s L_p$ that $\underline{n}(H_p) \subset$

$\underline{n}(q^s L_p)$ for $p \in S$. Since $v_i \in N$, $v_i^h \in K$ and $\underline{n}(N_p) \subset \underline{n}(K_p \perp q^s L_p) \subset \mathbb{Z}_p$ for $p \notin S$, we have $\underline{n}(H_p) \subset \mathbb{Z}_p = \underline{n}(q^s L_p)$ for $p \notin S$. Thus we have proved $\underline{n}(H_p) \subset \underline{n}(q^s L_p)$ for every p. Proposition 2.1.10 implies that H_p is represented by $q^s L_p$ for all p. From Lemma 2.2.39, it follows that H is represented by L and the proof is complete. ◻

Proof of Theorem 2.2.36. Let M be a positive lattice of $rankM \geqq 2n+3$. Let S be a finite set of prime numbers such that $S \ni 2$ and M_p is unimodular for $p \notin S$ and M_q is unimodular for some $q(\neq 2) \in S$. We construct a set of submodules $K(J)$, $L(J)$ of M as in Lemma 2.2.40 and show that N satisfies the condition in Lemma 2.2.40 for some J. For each $p \in S$, we choose finitely many submodules $N_p(j_p)$ of rank $ninM_p$ according to Lemma 2.2.38 and to each collection $J = (j_p)_{p \in S}$ we take a submodule $K(J)$ or rank $n \in M$ satisfying the conditions $K(J)_p \cong N_p(j_p)$ and $d(K(J)) \in \mathbb{Z}_p^x$ or $p\mathbb{Z}_p^x$ for $p \notin S$ by Theorem 2.2.33 and Corollary 4 to Theorem 2.1.14. We construct a submodule $L(J)$ of **218**
$rankL(J) = rankM - n \geqq n + 3$ in $\{x \in M | B(x, K(J)) = 0\}$ as follows: For $p \notin S$, $L(J)_p = K(J)_p^{\perp} = \{x \in M_p | B(x, K(J_p)) = 0\}$. In this case, $L(J)_p$ is ($\mathbb{Z}_p$−) maximal, since $s(L(J)_p) \subset \mathbb{Z}_p$ and $d(L(J)_p) \in \mathbb{Z}_p^x \cup p\mathbb{Z}_p^x$ by the local version of Lemma 2.4.26. For $p \in S$, we take any maximal module in $\{x \in M_p | B(x, K(J)_p) = 0\}$. From Proposition 2.2.18 and Theorem 2.2.34, it follows that $\operatorname{gen} L = spnL$. We show that $L(J)_q$ is isotropic. If $rankL(J)_q \geqq 5$, then $L(J)_q$ is isotropic. Otherwise, we have $rankL(J)_q = 4$, $n = 1$, $rankM_q = S$. By the assumption $q(\neq 2) \in S$, M_q is unimodular. Hence $M_q = < \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} > \perp < \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} > \perp < * >$. Unless $L(J)_q$ is isotropic, $\mathbb{Q}_q M$ does not contain two copies of hyperbolic planes. Thus $L(J)_q$ is isotropic. Let N be a positive lattice of $rank\ n$ such that N_p is represented by M_p for every p. Suppose $p \notin S$; then M_p is unimodular. Hence $\underline{n}(N_p) \subset \mathbb{Z}_p$. Since $L(J)_p$ is $\mathbb{Z}_p$-maximal and $rankL(J)_p \geqq n+3$, N_p is represented by $L(J)_p = q^s L(J)_p$ by Proposition 2.1.10 for every J. For $p \in S$, N_p is represented by $K(J)_p$ for some J. By Lemma 2.2.40, there is a constant $c(J)$ so that N is represented by $K(J) \perp L(J) \subset M$ if $(B(v_i, v_j)) > c(J)$ for some basis $\{v_i\}$ of N. Put

$c' = \max\limits_J c(J)$. By reduction theory, there is a basis $\{v_i\}$ of N such that

$$(B(v_i, v_j)) \in S_{4/3,1/2}, \text{ and then } (B(v_i, v_j)) \gg \begin{pmatrix} Q(v_1) & & \\ & \ddots & \\ & & Q(v_n) \end{pmatrix}.$$

If $\min\limits_{0 \neq v \in N} Q(v)$ is sufficiently large, then we have $(B(v_i, v_j)) > c' E_n$.

This completes the proof.

Remark. By the analytic considerations in §1.7 of Chapter 1, the following assertion holds for $n = 1$, $m \geq 4$ or $n = 2$, $m \geq 7$.

219 Let M be a positive lattice with $M = m$. There is a constant $c(M)$ such that any positive lattice N with rank $N = n$ is primitively represented by M provided that

$$\min(N) = \min_{0 \neq x \in N} Q(x) \geqq c(M) \text{ and}$$

N_p is primitively represented by M_p for every prime p.

2.2.0

In this last subsection, we show that there is a submodule of codim 1 which characterizes a given module.

Let $L = L_1 \perp \cdots \perp L_k$ be a Jordan splitting of a regular quadratic module L over $\mathbb{Z}_p$, that is, every L_i is modular and $s(L_1) \underset{\neq}{\supset} \cdots \underset{\neq}{\supset} s(L_k)$. Then we put

$$t_p(L) = (\underbrace{a_1, \ldots, a_1}_{\text{rank } L_1}, \ldots, \underbrace{a_k, \ldots, a_k}_{\text{rank } L_k})$$

where a_i is defined by $p^{a_i}\mathbb{Z}_p = s(L_i)$ and then $a_1 < a_2 < \ldots < a_k$. For two ordered sets $a = (a_1, \ldots, a_n), b = (b_1, \ldots, b_n)$, we define the ordering $a \leqq b$ by either $a_i = b_i$ for $i < k$ and $a_k < b_k$ for some $k \leqq n$ or $a_i = b_i$ for all i. For brevity, we denote $t_p(L_p)$ by $t_p(L)$ for a regular quadratic module over $\mathbb{Z}$.

Lemma 2.2.41. *Let L be a $\mathbb{Z}_p$-lattice on a regular quadratic module U over $\mathbb{Q}_p$. Then L contains a $\mathbb{Z}_p$-submodule M satisfying the following conditions 1), 2):*

1) *$d(M) \neq 0$, rank M = rank $L - 1$ and M is a direct summand of L as a module.*

2) *Let L' be a $\mathbb{Z}_p$-lattice on U containing M. If $d(L') = d(L)$ and $t_p(L') \geqq t_p(L)$, then $L' = L$.*

Proof. First, we assume that L is modular. Multiplying the quadratic 220
form by some constant, we may suppose that L is unimodular, without loss of generality. Let L' be a lattice as in 2). Then $t_p(L') \geqq t_p(L) = (0, \ldots, 0)$ implies $s(L') \subset \mathbb{Z}_p$, and $d(L') = d(L)$ implies that L' is unimodular. Suppose that L has an orthogonal basis, that is, $L = \mathop{\perp}\limits_{i=1}^{n} \mathbb{Z}_p v_i$. Then we put $M = \mathop{\perp}\limits_{i=1}^{n-1} \mathbb{Z}_p v_i$. The condition 1) is trivially satisfied. L' is split by M, in view of Lemma 2.1.3. Thus $L' = M \perp a\mathbb{Z}_p v_n (a \in \mathbb{Q}_p^{x})$. Further, $d(L') = d(L)$ implies $a \in \mathbb{Z}_p^{x}$ and $L' = L$. Suppose that L does not have any orthogonal basis. Then, from Propositions 2.1.12 and 2.1.13, it follows that $p = 2$ and

$$L = \mathop{\perp}\limits_{i=1}^{n} \mathbb{Z}_2[u_i, v_i],$$

$$\mathbb{Z}_2[u_i, v_i] =< \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} > \text{ for } i < k,$$

$$\mathbb{Z}_2[u_k, v_k] =< \begin{bmatrix} 2c & 1 \\ 1 & 2c \end{bmatrix} >$$

$c = 0$ or 1. Let $Q(u_k) = Q(v_k) = 2c$, $B(u_k, v_k) = 1$ and put $M = \mathop{\perp}\limits_{i=1}^{k-1} \mathbb{Z}_2[u_i, v_i] \perp\perp \mathbb{Z}_2[u_k + v_k]$. Then condition 1) is satisfied. From Lemma 2.1.3, it now follows that $L' = \mathop{\perp}\limits_{i=1}^{k-1} \mathbb{Z}_2[u_i, v_i] \perp L''$. Moreover, L'' is unimodular and $L'' \ni u_k + v_k$. Since $Q(u_k + v_k) = 2(2c+1)$, $u_k + v_k$ is primitive in L''. Hence $L'' = \mathbb{Z}_2[u + v, au + bv](u = u_k, v = v_k)$, for some $a, b \in \mathbb{Q}_2^{x}$. Since L'' is unimodular, and $Q(u + v) = 2(2c + 1)$, we have $B(u+v, au+bv) \in \mathbb{Z}_2^{x}$ and $Q(au+bv) \in \mathbb{Z}_2$. Thus $B(u+v, au+bv) = (a+b)(2c+1) \in \mathbb{Z}_2^{x}$ and $Q(au+bv) = 2(2c-1)a^2 - 2(2c-1)ax + 2cx^2 \in \mathbb{Z}_2 (x = a + b)$. Hence $x \in \mathbb{Z}_2^{x}$ and $2a(a - x) \in \mathbb{Z}_2$. This implies $a \in \mathbb{Z}_2$ and $b = x - a \in \mathbb{Z}_2$. Thus we have $L'' = \mathbb{Z}_2[u, v]$ and $L' = L$. Returning to the general case, let $L = \mathop{\perp}\limits_{i=1}^{k} L_i$, where L_i is $p^{a_i}\mathbb{Z}_p$-modular

and $a_1 < \cdots < a_k$. Denote by M_k a submodule of L_k which satisfies 1), 2) for L_k, and put $M = \perp_{i=1}^{k-1} L_i \perp M_k$. Then condition 1) is obviously
221 satisfied. For a lattice L' as in 2), L' contains a modular module L_1 and $t_p(L') \geqq t_p(L)$ implies $s(L') \subset s(L_1)$. By Lemma 2.1.3, $L' = L_1 \perp L''$, and $t_p(L'') \geqq t_p(\underset{1\geqq 2}{\perp} L_i)$ and clearly $L'' \supset \overset{k-1}{\underset{1=2}{\perp}} L_i \perp M_k$. Repeating this argument, we get $L' = \underset{i<k}{\perp} L_i \perp \tilde{L}$, $t_p(\tilde{L}) \geqq t_p(L_k)$, $\tilde{L} \supset M_k$, $d(\tilde{L}) = d(L_k)$. Thus we have $L' = L$.

We call a submodule M in Lemma 2.2.41 a *characteristic submodule* of L. Obviously the images of a characteristic submodule by $0(L)$ are also characteristic. □

Theorem 2.2.42. *Let L be a $\mathbb{Z}$-lattice on regular quadratic module U over $\mathbb{Q}$; then L contains a $\mathbb{Z}$-submodule M satisfying the following conditions 1), 2):*

1) $d(M) \neq 0$, *rank$M$ = rank$L - 1$, and M is a direct summand of L as a module.*

2) *Let L' be a $\mathbb{Z}$-lattice on a regular quadratic module U' over $\mathbb{Q}$ satisfying $d(L') = d(L)$, rank L' = rank L, $t_p(L') \geqq t_p(L)$ for every prime p. If there is an isometry u from M to L', then L' is isometric to L.*

Proof. We separate the case when U is a hyperbolic plane.

Suppose that U is a hyperbolic plane and further, let $L = \mathbb{Z}[u_1, u_2]$, $(B(u_i, u_j)) = \begin{pmatrix} 0 & b' \\ b' & c' \end{pmatrix}$. Multiplying the quadratic form on U some constant, we may assume $2|c'$, and $(b', c'/2) = 1$ without loss of generality. Since $Q(xu_1 + u_2) = 2(xb' + c'/2)$, there is an integer x such that $\dfrac{1}{2}Q(xu_1 + u_2)$ is a prime number q with $(q, 2dL) = 1$. Hence to L corresponds the matrix $\begin{pmatrix} 2q & b \\ b & c \end{pmatrix}$ with $0 < b < q$. It is easy to see that b, c are uniquely determined by q and $d(L)$. We put $M = \mathbb{Z}[xu_1 + u_2]$, and let L' be a lattice in 2). From the hypothesis, it follows that $s(L'_p) \subset \mathbb{Z}_p$ for every p and hence to L' corresponds the matrix $\begin{pmatrix} 2q & b'' \\ b'' & c'' \end{pmatrix}$ with $0 < b'' < q$.
222 Hence $b'' = b$, $c'' = c$. As a result, $L' \cong L$. From now on, we suppose that U is not a hyperbolic plane. Let S be a set of prime numbers such

that $S \ni 2$, and L_p is unimodular for $p \notin S$, and $\tilde{M}_p$ a characteristic submodule of L_p for $p \in S$. Suppose $\mathbb{Z}_p x_p = \tilde{M}_p^{\perp} = \{x \in L_p | B(x, \tilde{M}_p) = 0\}$. Then $x_p^{\perp} = \tilde{M}_p$, since $\tilde{M}_p$ is a direct summand of L_p. By Theorem 2.2.33, there exists an element $x \in L$ such that x and x_p are sufficiently close for $p \in S$ and $Q(x) \in \mathbb{Z}_p^x$ for $p \notin S$ with precisely one exception $p = q$, where $Q(x) \in q\mathbb{Z}_p^x$. We put $M = x^{\perp}$. Then M satisfies the condition 1). From Corollary 4 to Theorem 2.1.14, it follows that $\mathbb{Z}_p x$ and $\mathbb{Z}_p x_p$ are transformed by $0(L_p)$ for $p \in S$. Thus $\tilde{M}_p, M_p$ are also transformed by $0(L_p)$. Hence M_p is a characteristic submodule of L_p. If $p \notin S$, $p \neq q$, then M_p is unimodular and then M_p is a characteristic submodule of L_p. Let L' be a lattice as in 2). Then $\mathbb{Q}L' = \mathbb{Q}u(M) \perp < d(L')d(M) > \cong \mathbb{Q}L$. Hence we may suppose that L' is a lattice on U and L' contains M. Since M_p of Lemma 2.4.26, we have $d(M_q) \in q\mathbb{Z}_p^x$. Hence there is a basis $\{w_i\}$ of M_q such that $\underset{i \leqq n-2}{\perp} \mathbb{Z}_q w_i$ is unimodular and $Q(w_{n-1}) \in q\mathbb{Z}_q^x$. Since $\underset{i \leqq n-2}{\perp} \mathbb{Z}_q w_i$ splits L_q, and M_q is a direct summand of L_q, there is $w_n \in L_p$ such that $\{w_1, \ldots, w_n\}$ is a basis of L_q. Since $N = \mathbb{Z}_q[w_{n-1}, w_n]$ is unimodular, $d(N) = Q(w_{n-1})Q(w_n) - B(w_{n-1}, w_n)^2$ is a unit. From $Q(w_{n-1}) \in q\mathbb{Z}_q^x$, it follows that $B(w_{n-1}, w_n) \in \mathbb{Z}_q^x$ and $\mathbb{Q}_q N$ is hyperbolic. By Lemma 2.1.2, there is a basis $\{e_1, e_2\}$ of N such that $Q(e_i) = 0 (i = 1, 2) B(e_1, e_2) = 1$. Put $w_{n-1} = a_1 e_1 + a_2 e_2 (a_i \in \mathbb{Z}_q)$; then $2a_1 a_2 \in q\mathbb{Z}_q^x$. Multiplying e_i by a unit and renumbering, we may suppose $w_{n-1} = e_1 + vqe_2 (v \in \mathbb{Z}_q^x)$. Since L'_q is unimodular and L'_q contains M_q, there is a unimodular submodule K_q such that $L'_q = \underset{i \leqq n-2}{\perp} \mathbb{Z}_q w_i \perp K_q, K_q \ni w_{n-1}$. Let $\{w_{n-1}, ce_1 + de_2\}$ **223**
be a basis of K_q. Since K_q is unimodular, we have $d + vqc \in \mathbb{Z}_q^x$ and $cd \in \mathbb{Z}_q$. Then $c \in q^{-1}\mathbb{Z}_q^x, d \in q\mathbb{Z}_q$ or $c \in \mathbb{Z}_q, d \in \mathbb{Z}_q^x$. Thus we have $K_q = \mathbb{Z}_q[q^{-1}e_1, qe_2]$ or $\mathbb{Z}_q[e_1, e_2]$. Since $B(x, M) = 0$ and $B(e_1 - vqe_2, M_q) = 0$, $\tau_x = \tau_{e_1 - vqe_2}$. It is easy to see that $\tau_{e_1 - vqe_2}\mathbb{Z}_q[e_1, e_2] = \mathbb{Z}_q[q^{-1}e_1, qe_2]$. Thus we have $L'_q = L_q$ or $\tau_x L_q$. Since $\tau_x M_p = M_p$ and M_p is a characteristic submodule of L_p for $p \neq q$, we have $L'_p = L_p = \tau_x L_p$. Thus we have $L' = L$ or $\tau_x L$. □

Remark. Let L be a regular quadratic module over $\mathbb{Z}$ and S a finite set of prime numbers such that $2 \in S$ and L_p is unimodular for $p \notin S$, and let M be a submodule of L, of rank $= rankL - 1$, such that M_p is characteristic for $p \in S$ and for $p \notin S$, $d(M_p) \in \mathbb{Z}_p^x$ with precisely one exception $p = q$ and $d(M_q) \in q\mathbb{Z}_q^x$. Let u be an isometry from M to L. Extend u to an isometry of $\mathbb{Q}L$. Another extension is $u\tau_x(x \in M^\perp)$. The proof shows that $u^{-1}(L) = L$ or $\tau_x L$. Hence u is uniquely extended to an isometry of L. In particular, if L is positive definite, then we have

$$r(M, L) = \sharp\{\text{isometries } : M \to L\} = \sharp 0(L).$$

Corollary 1. *Let $\{L_i\}_{i=1}^m$ be a set of regular quadratic modules over $\mathbb{Z}$ such that rank$L_i = n, d(L_i) = d(1 \leqq i \leqq m)$, and $L_i \neq L_j$ if $i \neq j$. Then there is a regular quadratic module M over $\mathbb{Z}$ such that rank$M = n - 1$ and there is precisely one $i(1 \leqq i \leqq m)$ for which M is represented by L_i.*

Proof. Let S be a finite set of prime numbers such that $2 \in S$ and $(L_i)_p$ is unimodular for $1 \leq i \leq m$, $p \notin S$. Put $S = \{p_1, \cdots, p_r\}$ and define $A_1, \ldots, A_r$ as follows:

$$A_1 = \{L_i; t_{p_1}(L_i) \text{ is minimal in } \{t_{p_1}(L_j); 1 \leqq j \leqq m\}\}, \ldots,$$
$$A_{k+1} = \{L_i; t_{p_{k+1}}(L_i) \text{ is minimal in } \{t_{p_{k+1}}(L_j); L_j \in A_k\}\}.$$

224 Suppose $L_i \in A_r$, and M is a submodule of L_i which is constructed in the proof of Theorem 2.2.42. Assume M is represented by L_j. Since $L_i \in A_r \subset A_1, t_{p_1}(L_i) \leqq t_{p_1}(L_j)$. Further, M_{p_1} is a characteristic submodule of L_i. Hence $(L_i)_p \cong (L_j)_p$ and then $t_{p_1}(L_i) = t_{p_1}(L_j)$. Thus L_j belongs to A_1. Repeating this argument, we have $L_j \in A_r$. Thus $t_p(L_i) = t_p(L_j)$ for every p. From Theorem 2.2.42, it follows that L_j is isometric to L_j. This completes the proof. □

Corollary 2 ([9])**.** *Let $\{S_i\}_{i=1}^m$ be a set of positive definite rational symmetric matrices such that rank $S_i = n$, $|S_i| = d(1 \leqq i \leqq m)$ and there is no element $T \in GL_n(\mathbb{Z})$ which satisfies $S_i[T] = S_j$ if $i \neq j$. Then $\theta(Z, S_i) = \sum e(\sigma(S_i[G]Z))$ are linearly independent where G runs over $\mathfrak{M}_{n,n-1}(\mathbb{Z})$ and*

$$Z \in H_{n-1} = \{Z \in \mathfrak{M}_{n-1}(\mathbb{C}) | Z = {}^tZ, ImZ > 0\}.$$

Proof. This follows immediately from the previous corollary. □

Bibliography

[1] A.N. Andrianov: Spherical functions for GL_n over local fields and 225
summation of Hecke series, Math. Sbornik 12 (1970), 429-452.

[2] A.N. Andrianov and G.N. Maloletkin: Behaviour of theta-series of degree n under modular substituions, Math. USSR Izv. 9(1975), 227-241.

[3] H. Braun: Darstellung hermitischer Modulformen durch Poincaresche Reihen, Abhand. Math. Sem. Hamburg 22 (1958), 9-37.

[4] J.W.S. Cassels: Rational Quadratic Forms, Academic Press, 1978.

[5] R. Carlsson and W. Johanssen: Der Multiplikator von Thetareihen höheren Grades *zu* quadratischen Formen ungerader Ordnung, Math, Zeit 177 (1981), 439-449.

[6] U. Christian: Uber Hilbert-Siegelsche Modulformen und Poincaresche Reihen, Math. Annalen 148 (1962), 257-307.

[7] E. Hecke: Theorie der Eisensteinscher Reihen und ihre Anwendung auf Funktionentheorie und Arithmetik, Abh Math. Sem. Hamburg 5 (1927), 199-224, Gesamm. Abhand. 461-486.

[8] J. C Hsia, Y. Kitaoka and M. Kneser: Representations of positive definite quadratic forms, Jour. reine angen. Math, 301 (1978), 132-141.

[9] Y. Kitaoka: Representations of quadratic forms and their application to Selberg's zeta functions, Nagoya Math. J. 63 (1976), 153-162.

[10] Y. Ditaoka: Modular forms of degree *n* and representation by quadratic forms I, II, III Nagoya Math. J. 74 (1979), 95-122, ibid. 87(1982). 127-146, Proc. Japan. Acad. 57 (1981). 373-377.

226 [11] Y. Kitaoka: Fourier coefficients of Siegel cusp forms of degree 2, Nagoya Math. J. 93 (1984), 149-171.

[12] Y. Kitaoka: Dirichlet series in the theory of Siegel modular forms, Nagoya Math. J. 95 (1984), 73-84.

[13] H. Klingen: Zum Darstellungssatz fur Siegelsche Modulformen, Math. Zeit. 102 (1967), 30-43.

[14] H.D. Kloosterman: Asymptotische Foremeln fur die Fourierkoeffizienten ganzer Modulformen, Math. Sem. Hamburg 5 (1927), 337-352.

[15] M. Kneser: Quadratische Formen, Vorlesungs-Ausarbeitung, Giottingen, 1973-'74.

[16] M. Koecher: Zur Theorie der Modulformen *n*-ten Grades I, II, Math. Zeit. 59 (1954), 399-416, ibid. 61 (1955), 455-466.

[17] H. Maass: Siegel's Modular Forms and Dirichlet Series, Lecture Notes in Math. 216, Springer-Verlag, 1971.

[18] O.T.O'Meara: Introduction to Quadratic Forms, Grundlehren Math. Wissen. 117, Springer-Verlag, 1973.

[19] S. Raghavan: Modular forms of degree *n* and representation by quadratic forms, Annals Math. 70 (1959), 449-477.

[20] S. Raghavan: Estimates of coefficients of modular forms and generalized modular relations, International Colloq. on Automorphic forms, Representation theory and Arithmetic, Bombay 1979.

[21] J.P. Serre: A Course in Arithmetic, Springer-Verlag, 1973.

[22] G. Shimura: On Eisenstein series, Duke Math. J. 35 (1984), 73-84.

[23] C.L. Siegel: Über die analytische Theorie der quadratischen Formen, Annals Math. 36 (1935), 527-607, Gesamm. Abhand.I, 326-405. 227

[24] C.L. Siegel: Einführung in der Theorie der Modulfunktionen, Math. Annalen 116 (1939), 617-657, Gesamm. Abhand. II, 97-137.

[25] C.L. Siegel: On the theory of indefinite quadratic forms, Annals Math. 45 (1944), 577-622, Gesamm. Abhand II, 421-466.

[26] T. Tamagawa: On the ς-functions of a division algebra, Annals Math. 77 (1963), 387-405.

[27] W.A. Tartakowsky: Die Gesamtheit der Zahlen, die durch eine positive quadratische Form $F(x_1, \ldots, x_s)(s \geq 4)$ darstellbar sind, Izv. Akad. Nauk SSSR u (1929), 111-122, 165-196.

[28] A. Weil: On some exponential sums, Proc. Nat. Acad. Sci. USA, 34 (1948), 204-207.