asymptotic formula (38), and the fact that k must be divisible by 4 also follows because if $k \equiv 2 \pmod 4$ then B_k is positive and therefore the right-hand side of (38) tends to $-\infty$ as $k \to \infty$, contradicting $R_Q(n) \geq 0$.

The first statement of Proposition 12 is purely algebraic, and purely algebraic proofs are known, but they are not as simple or as elegant as the modular proof just given. No non-modular proof of the asymptotic formula (38) is known.

Before continuing with the theory, we look at some examples, starting in rank 8. Define the lattice $\Lambda_8 \subset \mathbb{R}^8$ to be the set of vectors belonging to either $\mathbb{Z}^8$ or $(\mathbb{Z}+\frac{1}{2})^8$ for which the sum of the coordinates is even. This is unimodular because the lattice $\mathbb{Z}^8 \cup (\mathbb{Z}+\frac{1}{2})^8$ contains both it and $\mathbb{Z}^8$ with the same index 2, and is even because $x_i^2 \equiv x_i \pmod 2$ for $x_i \in \mathbb{Z}$ and $x_i^2 \equiv \frac{1}{4} \pmod 2$ for $x_i \in \mathbb{Z}+\frac{1}{2}$. The lattice Λ_8 is sometimes denoted E_8 because, if we choose the $\mathbb{Z}$-basis $u_i = e_i - e_{i+1}$ $(1 \leq i \leq 6)$, $u_7 = e_6 + e_7$, $u_8 = -\frac{1}{2}(e_1 + \cdots + e_8)$ of Λ_8, then every u_i has length 2 and (u_i, u_j) for $i \neq j$ equals -1 or 0 according whether the ith and jth vertices (in a standard numbering) of the "E_8" Dynkin diagram in the theory of Lie algebras are adjacent or not. The theta series of Λ_8 is a modular form of weight 4 on $\mathrm{SL}(2,\mathbb{Z})$ whose Fourier expansion begins with 1, so it is necessarily equal to $E_4(z)$, and we get "for free" the information that for every integer $n \geq 1$ there are exactly $240\,\sigma_3(n)$ vectors x in the E_8 lattice with $(x,x) = 2n$.

From the uniqueness of the modular form $E_4 \in M_4(\Gamma_1)$ we in fact get that $r_Q(n) = 240\sigma_3(n)$ for any even unimodular quadratic form or lattice of rank 8, but here this is not so interesting because the known classification in this rank says that Λ_8 is, in fact, the only such lattice up to isomorphism. However, in rank 16 one knows that there are two non-equivalent lattices: the direct sum $\Lambda_8 \oplus \Lambda_8$ and a second lattice Λ_{16} which is not decomposable. Since the theta series of both lattices are modular forms of weight 8 on the full modular group with Fourier expansions beginning with 1, they are both equal to the Eisenstein series $E_8(z)$, so we have $r_{\Lambda_8 \oplus \Lambda_8}(n) = r_{\Lambda_{16}}(n) = 480\,\sigma_7(n)$ for all $n \geq 1$, even though the two lattices in question are distinct. (Their distinctness, and a great deal of further information about the relative positions of vectors of various lengths in these or in any other lattices, can be obtained by using the theory of Jacobi forms which was mentioned briefly in §3.1 rather than just the theory of modular forms.)

In rank 24, things become more interesting, because now $\dim M_{12}(\Gamma_1) = 2$ and we no longer have uniqueness. The even unimodular lattices of this rank were classified completely by Niemeyer in 1973. There are exactly 24 of them up to isomorphism. Some of them have the same theta series and hence the same number of vectors of any given length (an obvious such pair of lattices being $\Lambda_8 \oplus \Lambda_8 \oplus \Lambda_8$ and $\Lambda_8 \oplus \Lambda_{16}$), but not all of them do. In particular, exactly one of the 24 lattices has the property that it has no vectors of length 2. This is the famous Leech lattice (famous among other reasons because it has a huge group of automorphisms, closely related to the monster group and other sporadic simple groups). Its theta series is the unique modular form of weight 12 on Γ_1 with Fourier expansion starting $1+0q+\cdots$, so it must equal $E_{12}(z)-\frac{21736}{691}\Delta(z)$, i.e., the number $r_{\mathrm{Leech}}(n)$ of vectors of length $2n$ in the Leech lattice equals $\frac{21736}{691}\big(\sigma_{11}(n)-\tau(n)\big)$ for every positive integer n. This gives another proof and an interpretation of Ramanujan's congruence (28).

In rank 32, things become even more interesting: here the complete classification is not known, and we know that we cannot expect it very soon, because there are more than 80 million isomorphism classes! This, too, is a consequence of the theory of modular forms, but of a much more sophisticated part than we are presenting here. Specifically, there is a fundamental theorem of Siegel saying that the average value of the theta series associated to the quadratic forms in a single genus (we omit the definition) is always an Eisenstein series. Specialized to the particular case of even unimodular forms of rank $m=2k\equiv 0 \pmod 8$, which form a single genus, this theorem says that there are only finitely many such forms up to equivalence for each k and that, if we number them $Q_1,\ldots,Q_I$, then we have the relation

$$\sum_{i=1}^{I}\frac{1}{w_i}\,\Theta_{Q_i}(z)\;=\;\mathsf{m}_k\,E_k(z)\,, \tag{39}$$

where w_i is the number of automorphisms of the form Q_i (i.e., the number of matrices $\gamma\in\mathrm{SL}(m,\mathbb{Z})$ such that $Q_i(\gamma x)=Q_i(x)$ for all $x\in\mathbb{Z}^m$) and m_k is the positive rational number given by the formula

$$\mathsf{m}_k\;=\;\frac{B_k}{2k}\,\frac{B_2}{4}\,\frac{B_4}{8}\cdots\frac{B_{2k-2}}{4k-4}\,,$$

where B_i denotes the ith Bernoulli number. In particular, by comparing the constant terms on the left- and right-hand sides of (39), we see that $\sum_{i=1}^{I}1/w_i=\mathsf{m}_k$, the *Minkowski-Siegel mass formula*. The numbers $\mathsf{m}_4\approx 1.44\times 10^{-9}$, $\mathsf{m}_8\approx 2.49\times 10^{-18}$ and $\mathsf{m}_{12}\approx 7,94\times 10^{-15}$ are small, but $\mathsf{m}_{16}\approx 4,03\times 10^{7}$ (the next two values are $\mathsf{m}_{20}\approx 4.39\times 10^{51}$ and $\mathsf{m}_{24}\approx 1.53\times 10^{121}$), and since $w_i\geq 2$ for every i (one has at the very least the automorphisms $\pm\,\mathrm{Id}_m$), this shows that $I>80000000$ for $m=32$ as asserted.

A further consequence of the fact that $\Theta_Q\in M_k(\Gamma_1)$ for Q even and unimodular of rank $m=2k$ is that the minimal value of $Q(x)$ for non-zero $x\in\Lambda$ is bounded by $r=\dim M_k(\Gamma_1)=[k/12]+1$. The lattice L is called *extremal* if this bound is attained. The three lattices of rank 8 and 16 are extremal for trivial reasons. (Here $r=1$.) For $m=24$ we have $r=2$ and the only extremal lattice is the Leech lattice. Extremal unimodular lattices are also known to exist for $m=32$, 40, 48, 56, 64 and 80, while the case $m=72$ is open. Surprisingly, however, there are no examples of large rank:

Theorem (Mallows–Odlyzko–Sloane). *There are only finitely many non-isomorphic extremal even unimodular lattices.*

We should not leave this section without mentioning at least briefly that there is an important generalization of the theta series (36) in which each term $q^{Q(x_1,\ldots,x_m)}$ is weighted by a polynomial $P(x_1,\ldots,x_m)$. If this polynomial is homogeneous of degree d and is *spherical with respect to* Q (this means that $\Delta P = 0$, where Δ is the Laplace operator with respect to a system of coordinates in which $Q(x_1,\ldots,x_m)$ is simply $x_1^2+\cdots+x_m^2$), then the theta series $\Theta_{Q,P}(z)=\sum_x P(x)q^{Q(x)}$ is a modular form of weight $m/2+d$ (on the same group and with respect to the same character as in the case $P=1$), and is a cusp form if d is strictly positive. The possibility of putting non-trivial weights into theta series in this way considerably enlarges their range of applications, both in coding theory and elsewhere.

4 Hecke Eigenforms and *L*-series

In this section we give a brief sketch of Hecke's fundamental discoveries that the space of modular forms is spanned by modular forms with multiplicative Fourier coefficients and that one can associate to these forms Dirichlet series which have Euler products and functional equations. These facts are at the basis of most of the higher developments of the theory: the relations of modular forms to arithmetic algebraic geometry and to the theory of motives, and the adelic theory of automorphic forms. The last two subsections describe some basic examples of these higher connections.

4.1 Hecke Theory

For each integer $m \ge 1$ there is a linear operator T_m, the mth *Hecke operator*, acting on modular forms of any given weight k. In terms of the description of modular forms as homogeneous functions on lattices which was given in §1.1, the definition of T_m is very simple: it sends a homogeneous function F of degree $-k$ on lattices $\Lambda\subset\mathbb{C}$ to the function T_mF defined (up to a suitable normalizing constant) by $T_mF(\Lambda)=\sum F(\Lambda')$, where the sum runs over all sublattices $\Lambda'\subset\Lambda$ of index m. The sum is finite and obviously still homogeneous in Λ of the same degree $-k$. Translating from the language of lattices to that of functions in the upper half-plane by the usual formula $f(z)=F(\Lambda_z)$, we find that the action of T_m is given by

$$T_mf(z) \;=\; m^{k-1}\sum_{\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)\in\Gamma_1\backslash\mathcal{M}_m}(cz+d)^{-k}\,f\left(\frac{az+b}{cz+d}\right)\qquad (z\in\mathfrak{H})\,, \quad (40)$$

where $\mathcal{M}_m$ denotes the set of 2×2 integral matrices of determinant m and where the normalizing constant m^{k-1} has been introduced for later convenience (T_m normalized in this way will send forms with integral Fourier coefficients to forms with integral Fourier coefficients). The sum makes sense because the transformation law (2) of f implies that the summand associated to a matrix $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathcal{M}_m$ is indeed unchanged if M is replaced by γM with $\gamma \in \Gamma_1$, and from (40) one also easily sees that $T_m f$ is holomorphic in $\mathfrak{H}$ and satisfies the same transformation law and growth properties as f, so T_m indeed maps $M_k(\Gamma_1)$ to $M_k(\Gamma_1)$. Finally, to calculate the effect of T_m on Fourier developments, we note that a set of representatives of $\Gamma_1 \backslash \mathcal{M}_m$ is given by the upper triangular matrices $\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$ with $ad = m$ and $0 \le b < d$ (this is an easy exercise), so

$$T_m f(z) \;=\; m^{k-1} \sum_{\substack{ad=m \\ a,\, d>0}} \frac{1}{d^k} \sum_{b \pmod{d}} f\left(\frac{az+b}{d}\right). \tag{41}$$

If $f(z)$ has the Fourier development (3), then a further calculation with (41), again left to the reader, shows that the function $T_m f(z)$ has the Fourier expansion

$$T_m f(z) \;=\; \sum_{\substack{d|m \\ d>0}} (m/d)^{k-1} \sum_{\substack{n \ge 0 \\ d|n}} a_n\, q^{mn/d^2} \;=\; \sum_{n\ge 0} \Biggl(\sum_{\substack{r|(m,n) \\ r>0}} r^{k-1}\, a_{mn/r^2} \Biggr) q^n \,. \tag{42}$$

An easy but important consequence of this formula is that the operators T_m ($m \in \mathbb{N}$) all commute.

Let us consider some examples. The expansion (42) begins $\sigma_{k-1}(m)a_0 + a_m q + \cdots$, so if f is a cusp form (i.e., $a_0 = 0$), then so is $T_m f$. In particular, since the space $S_{12}(\Gamma_1)$ of cusp forms of weight 12 is 1-dimensional, spanned by $\Delta(z)$, it follows that $T_m\Delta$ is a multiple of Δ for every $m \ge 1$. Since the Fourier expansion of Δ begins $q + \cdots$ and that of $T_m\Delta$ begins $\tau(m)q + \cdots$, the eigenvalue is necessarily $\tau(m)$, so $T_m\Delta = \tau(m)\Delta$ and (42) gives

$$\tau(m)\,\tau(n) \;=\; \sum_{r|(m,n)} r^{11}\,\tau\left(\frac{mn}{r^2}\right) \qquad \text{for all } m,\, n \ge 1\,,$$

proving Ramanujan's multiplicativity observations mentioned in §2.4. By the same argument, if $f \in M_k(\Gamma_1)$ is any simultaneous eigenfunction of all of the T_m, with eigenvalues λ_m, then $a_m = \lambda_m a_1$ for all m. We therefore have $a_1 \ne 0$ if f is not identically 0, and if we normalize f by $a_1 = 1$ (such an f is called a *normalized Hecke eigenform*, or *Hecke form* for short) then we have

$$T_m f \;=\; a_m\, f\,, \qquad a_m\, a_n \;=\; \sum_{r|(m,n)} r^{k-1}\, a_{mn/r^2} \qquad (m,\, n \ge 1)\,. \tag{43}$$

Examples of this besides $\Delta(z)$ are the unique normalized cusp forms $f(z) = \Delta(z)E_{k-12}(z)$ in the five further weights where $\dim S_k(\Gamma_1) = 1$ (viz. $k = 16$, 18, 20, 22 and 26) and the function $\mathbb{G}_k(z)$ for all $k \ge 4$, for which we have $T_m\mathbb{G}_k = \sigma_{k-1}(m)\mathbb{G}_k$, $\sigma_{k-1}(m)\sigma_{k-1}(n) = \sum_{r|(m,n)} r^{k-1}\sigma_{k-1}(mn/r^2)$. (This was the reason for the normalization of $\mathbb{G}_k$ chosen in §2.2.) In fact, a theorem of Hecke asserts that $M_k(\Gamma_1)$ has a basis of normalized simultaneous eigenforms for all k, and that this basis is unique. We omit the proof, though it is not difficult (one introduces a scalar product on the space of cusp forms of weight k, shows that the T_m are self-adjoint with respect to this scalar product, and appeals to a general result of linear algebra saying that commuting self-adjoint operators can always be simultaneously diagonalized), and content ourselves instead with one further example, also due to Hecke. Consider $k = 24$, the first weight where $\dim S_k(\Gamma_1)$ is greater than 1. Here S_k is 2-dimensional, spanned by $\Delta E_4^3 = q + 696q^2 + \cdots$ and $\Delta^2 = q^2 - 48q^3 + \ldots$. Computing the first two Fourier expansions of the images under T_2 of these two functions by (42), we find that $T_2(\Delta E_4^3) = 696\,\Delta E_4^3 + 20736000\,\Delta^2$ and $T_2(\Delta^2) = \Delta E_4^3 + 384\,\Delta^2$. The matrix $\left(\begin{smallmatrix} 696 & 20736000 \\ 1 & 384 \end{smallmatrix}\right)$ has distinct eigenvalues $\lambda_1 = 540 + 12\sqrt{144169}$ and $\lambda_2 = 540 - 12\sqrt{144169}$, so there are precisely two normalized eigenfunctions of T_2 in $S_{24}(\Gamma_1)$, namely the functions $f_1 = \Delta E_4^3 - (156 - 12\sqrt{144169})\Delta^2 = q + \lambda_1 q^2 + \cdots$ and $f_2 = \Delta E_4^3 - (156 + 12\sqrt{144169})\Delta^2 = q + \lambda_2 q^2 + \cdots$, with $T_2 f_i = \lambda_i f_i$ for $i = 1,\, 2$. The uniqueness of these eigenfunctions and the fact that T_m commutes with T_2 for all $m \geq 1$ then implies that $T_m f_i$ is a multiple of f_i for all $m \geq 1$, so $\mathbb{G}_{24}$, f_1 and f_2 give the desired unique basis of $M_{24}(\Gamma_1)$ consisting of normalized Hecke eigenforms.

Finally, we mention without giving any details that Hecke's theory generalizes to congruence groups of $\mathrm{SL}(2,\mathbb{Z})$ like the group $\Gamma_0(N)$ of matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1$ with $c \equiv 0 \pmod{N}$, the main differences being that the definition of T_m must be modified somewhat if m and N are not coprime and that the statement about the existence of a unique base of Hecke forms becomes more complicated: the space $M_k(\Gamma_0(N))$ is the direct sum of the space spanned by all functions $f(dz)$ where $f \in M_k(\Gamma_0(N'))$ for some proper divisor N' of N and d divides N/N' (the so-called "old forms") and a space of "new forms" which is again uniquely spanned by normalized eigenforms of all Hecke operators T_m with $(m, N) = 1$. The details can be found in any standard textbook.

4.2 *L*-series of Eigenforms

Let us return to the full modular group. We have seen that $M_k(\Gamma_1)$ contains, and is in fact spanned by, normalized Hecke eigenforms $f = \sum a_m q^m$ satisfying (43). Specializing this equation to the two cases when m and n are coprime and when $m = p^\nu$ and $n = p$ for some prime p gives the two equations (which together are equivalent to (43))

$$a_{mn} = a_m\, a_n \text{ if } (m,n) = 1\,, \quad a_{p^{\nu+1}} = a_p\, a_{p^\nu} - p^{k-1}\, a_{p^{\nu-1}} \;\; (p \text{ prime}, \nu \geq 1)\,.$$

The first says that the coefficients a_n are *multiplicative* and hence that the Dirichlet series $L(f,s) = \sum_{n=1}^{\infty} \dfrac{a_n}{n^s}$, called the *Hecke L-series* of f, has an Eu-

Durchläuft G_j jeweils ein Vertretersystem der Linksnebenklassen $G\mathrm{Aut}\,S_j$ mit $G \in \mathcal{D}(S, pS_j)$, so folgern wir

$$f(\tau) = \sum_{j=1}^{h} \sum_{G_j} \sum_{g \in \mathbb{Z}^n} e^{\pi i \tau S[G_j][g]/p} = \sum_{H\mathfrak{U}_n \in A_p(S)} \sum_{g \in \mathbb{Z}^n} e^{\pi i \tau S[Hg]/p} \,,$$

wobei wir im letzten Schritt Lemma 3b) verwenden. Man beachte hier

$$S[Hg] \equiv 0 \pmod{2p} \quad \text{für alle} \quad H\mathfrak{U}_n \in A_p(S) \quad \text{und} \quad g \in \mathbb{Z}^n.$$

Bezeichnen wir die FOURIER–Koeffizienten von f mit $\alpha_f(m)$, so gilt

$$\alpha_f(m) = \sharp\{(H\mathfrak{U}_n, g)\ ;\ g \in \mathcal{D}(S, 2mp)\,,\ H\mathfrak{U}_n \in A_p(S)\,,\ H^{-1}g \in \mathbb{Z}^n\}.$$

Es gibt genau $\sharp\,(S, 2m/p)$ Vektoren $g \in \mathcal{D}(S, 2mp)$ mit $g \equiv 0 \,(\mathrm{mod}\ p)$. Ein solches g erfüllt $H^{-1}g \in \mathbb{Z}^n$ für alle $H\mathfrak{U}_n \in A_p(S)$ aufgrund von Lemma 3a), so dass es dann nach Satz 3 genau $a(p,k)$ Möglichkeiten für $H\mathfrak{U}_n$ gibt.

Man hat genau $\sharp(S, 2mp) - \sharp\,(S, 2m/p)$ Vektoren $g \in \mathcal{D}(S, 2mp)$ mit der Eigenschaft $g \not\equiv 0 \,(\mathrm{mod}\ p)$. Ist ein solches g gegeben, so gibt es nach Satz 3b) genau $a(p, k-1)$ Linksnebenklassen $H\mathfrak{U}_n \in A_p(S)$ mit $H^{-1}g \in \mathbb{Z}^n$.

Mit dem Wert für $a(p,k)$ aus Satz 3 folgern wir

$$\begin{aligned} \alpha_f(m) &= \sharp\,(S, 2m/p) \cdot a(p,k) + (\sharp(S, 2mp) - \sharp\,(S, 2m/p)) \cdot a(p, k-1) \\ &= a(p, k-1) \cdot \big(\sharp(S, 2mp) + p^{k-1} \sharp\,(S, 2m/p)\big)\ . \end{aligned}$$

Mit Proposition 2.4 schließen wir aus Korollar IV.1.1, dass die FOURIER–Koeffizienten von $\frac{1}{a(p,k-1)} \cdot f$ und $T_p\Theta(\cdot; S)$ übereinstimmen. Aus der Eindeutigkeit der FOURIER–Entwicklung ergibt sich (1). □

Bemerkungen. a) Die Formel (1) gilt auch für $p = 2$. Der beweistechnische Aufwand ist allerdings höher. In den Aufgaben wird der Beweis angedeutet.
b) Die Formel (1) ist im Prinzip explizit. Für praktische Rechnungen ist sie jedoch kaum brauchbar, wenn man die Größe der Klassenzahl etwa in **2.5** beachtet. Die Linearkombination in (1) ist i. A. nicht eindeutig, da die Theta–Reihen i. A. linear abhängig sind.

5. Die EISENSTEIN–Reihe als Linearkombination der Theta–Reihen. In diesem Abschnitt beweisen wir einen Spezialfall der analytischen Version des SIEGEL*schen Hauptsatzes*. Die EISENSTEIN–Reihe ist das gewichtete Mittel der Theta–Reihen.

Satz. *Seien $S_1, \ldots, S_h$ Vertreter der Klassen der geraden, unimodularen, positiv definiten $n \times n$ Matrizen mit $n = 2k$. Dann gilt*

$$(1) \qquad \sum_{j=1}^{h} \frac{\frac{1}{\sharp(S_j,S_j)}}{\frac{1}{\sharp(S_1,S_1)} + \ldots + \frac{1}{\sharp(S_h,S_h)}} \cdot \Theta(\tau; S_j) = G_k^*(\tau)\ ,\ \tau \in \mathbb{H}.$$

Beweis. Wir schreiben $f(\tau) \in \mathbb{M}_k$ für die linke Seite von (1) und verwenden zur Abkürzung N für den im Nenner stehenden Ausdruck. Ist $p > 2$ eine Primzahl, so folgern wir aus Satz 4

$$\begin{aligned} T_p f &= \frac{1}{N} \cdot \sum_{j=1}^{h} \frac{1}{\sharp(S_j, S_j)} \cdot T_p \Theta(\cdot; S_j) \\ &= \frac{1}{N \cdot a(p, k-1)} \cdot \sum_{i=1}^{h} \frac{1}{\sharp(S_i, S_i)} \cdot \left(\sum_{j=1}^{h} \frac{\sharp(S_j, pS_i)}{\sharp(S_j, S_j)} \right) \cdot \Theta(\cdot; S_i) \, . \end{aligned}$$

Aus Korollar 3 und Satz 3 ergibt sich

$$T_p f = \frac{a(p,k)}{N \cdot a(p, k-1)} \cdot \sum_{i=1}^{h} \frac{1}{\sharp(S_i, S_i)} \cdot \Theta(\cdot; S_i) = (p^{k-1} + 1) \cdot f.$$

Wegen $\alpha_f(0) = 1$ folgt die Behauptung aus Satz IV.2.4. □

Vergleicht man die m–ten FOURIER–Koeffizienten auf beiden Seiten von (1), so bekommt man mit III.2.1(9) das

Korollar. *Für alle* $m \geq 1$ *gilt*

$$\sum_{j=1}^{h} \frac{\sharp(S_j, 2m)}{\sharp(S_j, S_j)} = -\frac{2k}{B_k} \left(\frac{1}{\sharp(S_1, S_1)} + \cdots + \frac{1}{\sharp(S_h, S_h)} \right) \cdot \sigma_{k-1}(m).$$

Bemerkungen. a) Eine wesentlich allgemeinere Version des Satzes wurde 1935 von C.L. SIEGEL (*Ges. Abh. I*, 326–405) bewiesen. Der im Satz betrachtete Spezialfall der geraden, unimodularen, positiv definiten Matrizen wurde 1941 für so genannte SIEGELsche Modulformen von E. WITT (Abh. Math. Semin. Hans. Univ. **14**, 323–337) aus dem allgemeinen Resultat herauspräpariert.
b) Die im Nenner von (1) auftretende Größe

$$M(n) := \frac{1}{\sharp(S_1, S_1)} + \cdots + \frac{1}{\sharp(S_h, S_h)}$$

heißt *Maß* des Geschlechtes der geraden, unimodularen, positiv definiten $n \times n$ Matrizen. Die MINKOWSKI–SIEGEL*sche Maßformel* gibt die Größe an:

$$M(n) = \frac{|B_k|}{2k} \cdot \prod_{j=1}^{k-1} \frac{|B_{2j}|}{4j} \; , \; n = 2k.$$

Numerisch erhält man für das Maß die folgenden Werte (vgl. J.H. CONWAY und

N.J.A. SLOANE [1999], Chap. 16.2):

n	Maß	
8	$\dfrac{1}{696729600}$	$\approx 1,4 \cdot 10^{-9}$
16	$\dfrac{691}{277667181515243520000}$	$\approx 2,5 \cdot 10^{-18}$
24	$\dfrac{1027637932586061520960267}{129477933340026851560636148613120000000}$	$\approx 7,9 \cdot 10^{-15}$
32	$\dfrac{4890529010450384254108570593011950899382291953107314413193123}{121325280941552041649762780685623131486814208000000000}$	$\approx 4,0 \cdot 10^{7}$

Wegen $h(8) = 1$ folgt aus dem Wert für $M(8)$

$$\sharp(S_8, S_8) = \sharp\mathrm{Aut}\,(S_8) = 696.729.600\,.$$

c) Im Fall $n > 8$ sind die im Satz auftretenden Theta–Reihen zwar linear abhängig, man kann jedoch (1) als eine „kanonische“ Darstellung der EISENSTEIN–Reihe ansehen.

d) Die FOURIER–Koeffizienten von G_{12}^* sind nicht ganzzahlig. Also folgt im Fall $n = 24$ die Existenz von 2 linear unabhängigen Theta–Reihen (und damit auch $h_{12} > 1$) aus dem Satz. Somit erhält man einen neuen Beweis von Korollar 2.7B ohne Rückgriff auf das LEECH–Gitter.

e) Der hier angegebene Beweis des Satzes folgt im wesentlichen einer Vorlesungsausarbeitung von H.–G. QUEBBEMANN (*Geometrie der Zahlen*, Münster 1987). In einer allgemeineren Situation geht R. SCHULZE–PILLOT (Invent. Math. **75**, 282–299 (1984)) analog vor. Für Gitter über Ordnungen in Quaternionenschiefkörpern stammt ein entsprechendes Resultat von H.–G. QUEBBEMANN (Mathematika **31**, 12–16 (1984)). Ein wesentlich allgemeineres Ergebnis wurde 1965 von A. WEIL (Acta Math. **113**, 1–87) hergeleitet.

Aufgaben. 1) Seien $S \in \mathrm{Sym}\,(n;\mathbb{Z})$ und $\ell \geq 1$. Dann gibt es ein $U \in GL(n;\mathbb{Z})$ sowie $\alpha_1, \ldots, \alpha_r \in \mathbb{Z}$ und Matrizen $A_1, \ldots, A_s \in \mathrm{Mat}(2;\mathbb{Z})$ mit der Eigenschaft

$$S[U] \equiv [\alpha_1, \ldots, \alpha_r, A_1, \ldots, A_s] \;(\mathrm{mod}\; 2^\ell)\;, \quad r + 2s = n.$$

2) Es gibt genau dann eine gerade Matrix $S \in \mathrm{Sym}\,(n;\mathbb{Z})$ mit $\det S = 1$, wenn $n \equiv 0\,(\mathrm{mod}\; 4)$.
3) Sei $S \in \mathrm{Sym}\,(n;\mathbb{Z})$ gerade mit ungerader Determinante. Dann ist $n = 2k$ gerade und es gibt ein $U \in GL(n;\mathbb{Z})$ mit der Eigenschaft

$$S[U] \equiv [D_1, \ldots, D_k] \;\;(\mathrm{mod}\; 4)\;, \quad D_j = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\;,\; \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}\;, \quad j = 1, \ldots, k.$$

4) Sei $S \in \mathrm{Sym}\,(n;\mathbb{Z})\,,\ n = 2k$, gerade mit ungerader Determinante. Dann gibt es $2^{2k-1} + 2^{k-1}$ Vektoren $g \in \mathbb{Z}^n\,(\mathrm{mod}\; 2)$ mit $S[g] \equiv 0\,(\mathrm{mod}\; 4)$ und $2^{2k-1} - 2^{k-1}$ Vektoren $g \in \mathbb{Z}^n\,(\mathrm{mod}\; 2)$ mit $S[g] \equiv 2\,(\mathrm{mod}\; 4)$.
5) Sei $S \in \mathrm{Sym}\,(n;\mathbb{Z})\,,\ n = 2k$, gerade mit ungerader Determinante. $a_2(S)$ bezeichne die Anzahl der Linksnebenklassen $H\mathcal{U}_n$ mit $|\det H| = 2^k$, so dass $\frac{1}{2}S[H]$ gerade ist.
a) Es gilt

$$a_2(S) = a(2,k) = \prod_{j=0}^{k-1} (2^j + 1).$$