

Moreover, if one passes to other groups, then there are  $\sigma$  Eisenstein series of each type, where  $\sigma$  is the number of cusps, and, although they span the same vector space, they are not individually proportional. In fact, we will actually want to introduce a *third* normalization

$$\mathbb{G}_k(z) = \frac{(k-1)!}{(2\pi i)^k} G_k(z) \quad (12)$$

because, as we will see below, it has Fourier coefficients which are rational numbers (and even, with one exception, integers) and because it is a normalized eigenfunction for the Hecke operators discussed in §4.

As a first application, we can now determine the ring structure of  $M_*(\Gamma_1)$

**Proposition 4.** *The ring  $M_*(\Gamma_1)$  is freely generated by the modular forms  $E_4$  and  $E_6$ .*

**Corollary.** *The inequality (7) for the dimension of  $M_k(\Gamma_1)$  is an equality for all even  $k \geq 0$ .*

*Proof.* The essential point is to show that the modular forms  $E_4(z)$  and  $E_6(z)$  are algebraically independent. To see this, we first note that the forms  $E_4(z)^3$  and  $E_6(z)^2$  of weight 12 cannot be proportional. Indeed, if we had  $E_6(z)^2 = \lambda E_4(z)^3$  for some (necessarily non-zero) constant  $\lambda$ , then the meromorphic modular form  $f(z) = E_6(z)/E_4(z)$  of weight 2 would satisfy  $f^2 = \lambda E_4$  (and also  $f^3 = \lambda^{-1} E_6$ ) and would hence be holomorphic (a function whose square is holomorphic cannot have poles), contradicting the inequality  $\dim M_2(\Gamma_1) \leq 0$  of Corollary 1 of Proposition 2. But *any* two modular forms  $f_1$  and  $f_2$  of the same weight which are not proportional are necessarily algebraically independent. Indeed, if  $P(X, Y)$  is any polynomial in  $\mathbb{C}[X, Y]$  such that  $P(f_1(z), f_2(z)) \equiv 0$ , then by considering the weights we see that  $P_d(f_1, f_2)$  has to vanish identically for each homogeneous component  $P_d$  of  $P$ . But  $P_d(f_1, f_2)/f_2^d = p(f_1/f_2)$  for some polynomial  $p(t)$  in one variable, and since  $p$  has only finitely many roots we can only have  $P_d(f_1, f_2) \equiv 0$  if  $f_1/f_2$  is a constant. It follows that  $E_4^3$  and  $E_6^2$ , and hence also  $E_4$  and  $E_6$ , are algebraically independent. But then an easy calculation shows that the dimension of the weight  $k$  part of the subring of  $M_*(\Gamma_1)$  which they generate equals the right-hand side of the inequality (7), so that the proposition and corollary follow from this inequality.

## 2.2 Fourier Expansions of Eisenstein Series

Recall from (3) that any modular form on  $\Gamma_1$  has a Fourier expansion of the form  $\sum_{n=0}^{\infty} a_n q^n$ , where  $q = e^{2\pi iz}$ . The coefficients  $a_n$  often contain interesting arithmetic information, and it is this that makes modular forms important for classical number theory. For the Eisenstein series, normalized by (12), the coefficients are given by:

**Proposition 5.** *The Fourier expansion of the Eisenstein series  $\mathbb{G}_k(z)$  ( $k$  even,  $k > 2$ ) is*

$$\mathbb{G}_k(z) = -\frac{B_k}{2k} + \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n, \quad (13)$$

where  $B_k$  is the  $k$ th Bernoulli number and where  $\sigma_{k-1}(n)$  for  $n \in \mathbb{N}$  denotes the sum of the  $(k-1)$ st powers of the positive divisors of  $n$ .

We recall that the Bernoulli numbers are defined by the generating function  $\sum_{k=0}^{\infty} B_k x^k / k! = x / (e^x - 1)$  and that the first values of  $B_k$  ( $k > 0$  even) are given by  $B_2 = \frac{1}{6}$ ,  $B_4 = -\frac{1}{30}$ ,  $B_6 = \frac{1}{42}$ ,  $B_8 = -\frac{1}{30}$ ,  $B_{10} = \frac{5}{66}$ ,  $B_{12} = -\frac{691}{2730}$ , and  $B_{14} = \frac{7}{6}$ .

*Proof.* A well known and easily proved identity of Euler states that

$$\sum_{n \in \mathbb{Z}} \frac{1}{z+n} = \frac{\pi}{\tan \pi z} \quad (z \in \mathbb{C} \setminus \mathbb{Z}), \quad (14)$$

where the sum on the left, which is not absolutely convergent, is to be interpreted as a Cauchy principal value ( $= \lim \sum_{-M}^N$  where  $M, N$  tend to infinity with  $M - N$  bounded). The function on the right is periodic of period 1 and its Fourier expansion for  $z \in \mathfrak{H}$  is given by

$$\frac{\pi}{\tan \pi z} = \pi \frac{\cos \pi z}{\sin \pi z} = \pi i \frac{e^{\pi i z} + e^{-\pi i z}}{e^{\pi i z} - e^{-\pi i z}} = -\pi i \frac{1+q}{1-q} = -2\pi i \left( \frac{1}{2} + \sum_{r=1}^{\infty} q^r \right),$$

where  $q = e^{2\pi i z}$ . Substitute this into (14), differentiate  $k-1$  times and divide by  $(-1)^{k-1}(k-1)!$  to get

$$\sum_{n \in \mathbb{Z}} \frac{1}{(z+n)^k} = \frac{(-1)^{k-1}}{(k-1)!} \frac{d^{k-1}}{dz^{k-1}} \left( \frac{\pi}{\tan \pi z} \right) = \frac{(-2\pi i)^k}{(k-1)!} \sum_{r=1}^{\infty} r^{k-1} q^r$$

$(k \geq 2, z \in \mathfrak{H}),$

an identity known as Lipschitz's formula. Now the Fourier expansion of  $G_k$  ( $k > 2$  even) is obtained immediately by splitting up the sum in (10) into the terms with  $m = 0$  and those with  $m \neq 0$ :

$$\begin{aligned} G_k(z) &= \frac{1}{2} \sum_{\substack{n \in \mathbb{Z} \\ n \neq 0}} \frac{1}{n^k} + \frac{1}{2} \sum_{\substack{m, n \in \mathbb{Z} \\ m \neq 0}} \frac{1}{(mz+n)^k} = \sum_{n=1}^{\infty} \frac{1}{n^k} + \sum_{m=1}^{\infty} \sum_{n=-\infty}^{\infty} \frac{1}{(mz+n)^k} \\ &= \zeta(k) + \frac{(2\pi i)^k}{(k-1)!} \sum_{m=1}^{\infty} \sum_{r=1}^{\infty} r^{k-1} q^{mr} \\ &= \frac{(2\pi i)^k}{(k-1)!} \left( -\frac{B_k}{2k} + \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n \right), \end{aligned}$$

where in the last line we have used Euler's evaluation of  $\zeta(k)$  ( $k > 0$  even) in terms of Bernoulli numbers. The result follows.

to be immeasurably deeper than the assertion about multiplicativity and was only proved in 1974 by Deligne as a consequence of his proof of the famous Weil conjectures (and of his previous, also very deep, proof that these conjectures implied Ramanujan's). However, the weaker inequality  $|\tau(p)| \leq Cp^6$  with some effective constant  $C > 0$  is much easier and was proved in the 1930's by Hecke. We reproduce Hecke's proof, since it is simple. In fact, the proof applies to a much more general class of modular forms. Let us call a modular form on  $\Gamma_1$  a *cusp form* if the constant term  $a_0$  in the Fourier expansion (3) is zero. Since the constant term of the Eisenstein series  $\mathbb{G}_k(z)$  is non-zero, any modular form can be written uniquely as a linear combination of an Eisenstein series and a cusp form of the same weight. For the former the Fourier coefficients are given by (13) and grow like  $n^{k-1}$  (since  $n^{k-1} \leq \sigma_{k-1}(n) < \zeta(k-1)n^{k-1}$ ). For the latter, we have:

**Proposition 8.** *Let  $f(z)$  be a cusp form of weight  $k$  on  $\Gamma_1$  with Fourier expansion  $\sum_{n=1}^{\infty} a_n q^n$ . Then  $|a_n| \leq Cn^{k/2}$  for all  $n$ , for some constant  $C$  depending only on  $f$ .*

*Proof.* From equations (1) and (2) we see that the function  $z \mapsto y^{k/2}|f(z)|$  on  $\mathfrak{H}$  is  $\Gamma_1$ -invariant. This function tends rapidly to 0 as  $y = \Im(z) \rightarrow \infty$  (because  $f(z) = O(q)$  by assumption and  $|q| = e^{-2\pi y}$ ), so from the form of the fundamental domain of  $\Gamma_1$  as given in Proposition 1 it is clearly bounded. Thus we have the estimate

$$|f(z)| \leq c y^{-k/2} \quad (z = x + iy \in \mathfrak{H}) \tag{25}$$

for some  $c > 0$  depending only on  $f$ . Now the integral representation

$$a_n = e^{2\pi n y} \int_0^1 f(x + iy) e^{-2\pi i n x} dx$$

for  $a_n$ , valid for any  $y > 0$ , show that  $|a_n| \leq c y^{-k/2} e^{2\pi n y}$ . Taking  $y = 1/n$  (or, optimally,  $y = k/4\pi n$ ) gives the estimate of the proposition with  $C = c e^{2\pi}$  (or, optimally,  $C = c(4\pi e/k)^{k/2}$ ).

*Remark.* The definition of cusp forms given above is actually valid only for the full modular group  $\Gamma_1$  or for other groups having only one cusp. In general one must require the vanishing of the constant term of the Fourier expansion of  $f$ , suitably defined, at every cusp of the group  $\Gamma$ , in which case it again follows that  $f$  can be estimated as in (25). Actually, it is easier to simply *define* cusp forms of weight  $k$  as modular forms for which  $y^{k/2}f(x + iy)$  is bounded, a definition which is equivalent but does not require the explicit knowledge of the Fourier expansion of the form at every cusp.

♠ **Congruences for  $\tau(n)$**

As a mini-application of the calculations of this and the preceding sections we prove two simple congruences for the Ramanujan tau-function defined by

♠ **The Kac–Wakimoto Conjecture**

For any two natural numbers  $m$  and  $n$ , denote by  $\Delta_m(n)$  the number of representations of  $n$  as a sum of  $m$  triangular numbers (numbers of the form  $a(a-1)/2$  with  $a$  integral). Since  $8a(a-1)/2+1=(2a-1)^2$ , this can also be written as the number  $r_m^{\text{odd}}(8n+m)$  of representations of  $8n+m$  as a sum of  $m$  odd squares. As part of an investigation in the theory of affine superalgebras, Kac and Wakimoto were led to conjecture the formula

$$\Delta_{4s^2}(n) = \sum_{\substack{r_1, a_1, \dots, r_s, a_s \in \mathbb{N}_{\text{odd}} \\ r_1 a_1 + \dots + r_s a_s = 2n + s^2}} P_s(a_1, \dots, a_s) \tag{35}$$

for  $m$  of the form  $4s^2$  (and a similar formula for  $m$  of the form  $4s(s+1)$ ), where  $\mathbb{N}_{\text{odd}} = \{1, 3, 5, \dots\}$  and  $P_s$  is the polynomial

$$P_s(a_1, \dots, a_s) = \frac{\prod_i a_i \cdot \prod_{i < j} (a_i^2 - a_j^2)^2}{4^{s(s-1)} s! \prod_{j=1}^{2s-1} j!}.$$

Two proofs of this were subsequently given, one by S. Milne using elliptic functions and one by myself using modular forms. Milne’s proof is very ingenious, with a number of other interesting identities appearing along the way, but is quite involved. The modular proof is much simpler. One first notes that,  $P_s$  being a homogeneous polynomial of degree  $2s^2 - s$  and odd in each argument, the right-hand side of (35) is the coefficient of  $q^{2n+s^2}$  in a function  $F(z)$  which is a linear combination of products  $g_{h_1}(z) \cdots g_{h_s}(z)$  with  $h_1 + \dots + h_s = s^2$ , where  $g_h(z) = \sum_{r, a \in \mathbb{N}_{\text{odd}}} a^{2h-1} q^{ra}$  ( $h \geq 1$ ). Since  $g_h$  is a modular form (Eisenstein series) of weight  $2h$  on  $\Gamma_0(4)$ , this function  $F$  is a modular form of weight  $2s^2$  on the same group. Moreover, its Fourier expansion belongs to  $q^{s^2} \mathbb{Q}[[q^2]]$  (because  $P_s(a_1, \dots, a_s)$  vanishes if any two  $a_i$  are equal, and the smallest value of  $r_1 a_1 + \dots + r_s a_s$  with all  $r_i$  and  $a_i$  in  $\mathbb{N}_{\text{odd}}$  and all  $a_i$  distinct is  $1 + 3 + \dots + 2s - 1 = s^2$ ), and from the formula given in §1 for the number of zeros of a modular form we find that this property characterizes  $F(z)$  uniquely in  $M_{2s^2}(\Gamma_0(4))$  up to a scalar factor. But  $\theta_F(z) q^{4s^2}$  has the same property, so the two functions must be proportional. This proves (35) up to a scalar factor, easily determined by setting  $n = 0$ . ♡

**3.2 Theta Series in Many Variables**

We now consider quadratic forms in an arbitrary number  $m$  of variables. Let  $Q : \mathbb{Z}^m \rightarrow \mathbb{Z}$  be a positive definite quadratic form which takes integral values on  $\mathbb{Z}^m$ . We associate to  $Q$  the theta series

$$\Theta_Q(z) = \sum_{x_1, \dots, x_m \in \mathbb{Z}} q^{Q(x_1, \dots, x_m)} = \sum_{n=0}^{\infty} R_Q(n) q^n, \tag{36}$$

where of course  $q = e^{2\pi iz}$  as usual and  $R_Q(n) \in \mathbb{Z}_{\geq 0}$  denotes the number of representations of  $n$  by  $Q$ , i.e., the number of vectors  $x \in \mathbb{Z}^m$  with  $Q(x) = n$ . The basic statement is that  $\Theta_Q$  is always a modular form of weight  $m/2$ . In the case of even  $m$  we can be more precise about the modular transformation behavior, since then we are in the realm of modular forms of integral weight where we have given complete definitions of what modularity means. The quadratic form  $Q(x)$  is a linear combination of products  $x_i x_j$  with  $1 \leq i, j \leq m$ . Since  $x_i x_j = x_j x_i$ , we can write  $Q(x)$  uniquely as

$$Q(x) = \frac{1}{2} x^t A x = \frac{1}{2} \sum_{i,j=1}^m a_{ij} x_i x_j, \quad (37)$$

where  $A = (a_{ij})_{1 \leq i, j \leq m}$  is a symmetric  $m \times m$  matrix and the factor  $1/2$  has been inserted to avoid counting each term twice. The integrality of  $Q$  on  $\mathbb{Z}^m$  is then equivalent to the statement that the symmetric matrix  $A$  has integral elements and that its diagonal elements  $a_{ii}$  are even. Such an  $A$  is called an *even integral matrix*. Since we want  $Q(x) > 0$  for  $x \neq 0$ , the matrix  $A$  must be positive definite. This implies that  $\det A > 0$ . Hence  $A$  is non-singular and  $A^{-1}$  exists and belongs to  $M_m(\mathbb{Q})$ . The *level* of  $Q$  is then defined as the smallest positive integer  $N = N_Q$  such that  $NA^{-1}$  is again an even integral matrix. We also have the *discriminant*  $\Delta = \Delta_Q$  of  $A$ , defined as  $(-1)^m \det A$ . It is always congruent to 0 or 1 modulo 4, so there is an associated character (Kronecker symbol)  $\chi_\Delta$ , which is the unique Dirichlet character modulo  $N$  satisfying  $\chi_\Delta(p) = \left(\frac{\Delta}{p}\right)$  (Legendre symbol) for any odd prime  $p \nmid N$ . (The character  $\chi_\Delta$  in the special cases  $\Delta = -4, 12$  and  $8$  already occurred in §2.2 (eq. (15)) and §3.1.) The precise description of the modular behavior of  $\Theta_Q$  for  $m \in 2\mathbb{Z}$  is then:

**Theorem (Hecke, Schoenberg).** *Let  $Q : \mathbb{Z}^{2k} \rightarrow \mathbb{Z}$  be a positive definite integer-valued form in  $2k$  variables of level  $N$  and discriminant  $\Delta$ . Then  $\Theta_Q$  is a modular form on  $\Gamma_0(N)$  of weight  $k$  and character  $\chi_\Delta$ , i.e., we have  $\Theta_Q\left(\frac{az+b}{cz+d}\right) = \chi_\Delta(a)(cz+d)^k \Theta_Q(z)$  for all  $z \in \mathfrak{H}$  and  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$ .*

The proof, as in the unary case, relies essentially on the Poisson summation formula, which gives the identity  $\Theta_Q(-1/Nz) = N^{k/2}(z/i)^k \Theta_{Q^*}(z)$ , where  $Q^*(x)$  is the quadratic form associated to  $NA^{-1}$ , but finding the precise modular behavior requires quite a lot of work. One can also in principle reduce the higher rank case to the one-variable case by using the fact that every quadratic form is diagonalizable over  $\mathbb{Q}$ , so that the sum in (36) can be broken up into finitely many sub-sums over sublattices or translated sublattices of  $\mathbb{Z}^m$  on which  $Q(x_1, \dots, x_m)$  can be written as a linear combination of  $m$  squares.

There is another language for quadratic forms which is often more convenient, the language of lattices. From this point of view, a quadratic form is no longer a homogeneous quadratic polynomial in  $m$  variables, but a function  $Q$

from a free  $\mathbb{Z}$ -module  $\Lambda$  of rank  $m$  to  $\mathbb{Z}$  such that the associated scalar product  $(x, y) = Q(x + y) - Q(x) - Q(y)$  ( $x, y \in \Lambda$ ) is bilinear. Of course we can always choose a  $\mathbb{Z}$ -basis of  $\Lambda$ , in which case  $\Lambda$  is identified with  $\mathbb{Z}^m$  and  $Q$  is described in terms of a symmetric matrix  $A$  as in (37), the scalar product being given by  $(x, y) = x^t A y$ , but often the basis-free language is more convenient. In terms of the scalar product, we have a length function  $\|x\|^2 = (x, x)$  (actually this is the square of the length, but one often says simply “length” for convenience) and  $Q(x) = \frac{1}{2}\|x\|^2$ , so that the integer-valued case we are considering corresponds to lattices in which all vectors have even length. One often chooses the lattice  $\Lambda$  inside the euclidean space  $\mathbb{R}^m$  with its standard length function  $(x, x) = \|x\|^2 = x_1^2 + \dots + x_m^2$ ; in this case the square root of  $\det A$  is equal to the volume of the quotient  $\mathbb{R}^m/\Lambda$ , i.e., to the volume of a fundamental domain for the action by translation of the lattice  $\Lambda$  on  $\mathbb{R}^m$ . In the case when this volume is 1, i.e., when  $\Lambda \in \mathbb{R}^m$  has the same covolume as  $\mathbb{Z}^m$ , the lattice is called *unimodular*. Let us look at this case in more detail.

♠ **Invariants of Even Unimodular Lattices**

If the matrix  $A$  in (37) is even and unimodular, then the above theorem tells us that the theta series  $\Theta_Q$  associated to  $Q$  is a modular form on the full modular group. This has many consequences.

**Proposition 12.** *Let  $Q : \mathbb{Z}^m \rightarrow \mathbb{Z}$  be a positive definite even unimodular quadratic form in  $m$  variables. Then*

- (i) *the rank  $m$  is divisible by 8, and*
- (ii) *the number of representations of  $n \in \mathbb{N}$  by  $Q$  is given for large  $n$  by the formula*

$$R_Q(n) = -\frac{2k}{B_k} \sigma_{k-1}(n) + O(n^{k/2}) \quad (n \rightarrow \infty), \tag{38}$$

where  $m = 2k$  and  $B_k$  denotes the  $k$ th Bernoulli number.

*Proof.* For the first part it is enough to show that  $m$  cannot be an odd multiple of 4, since if  $m$  is either odd or twice an odd number then  $4m$  or  $2m$  is an odd multiple of 4 and we can apply this special case to the quadratic form  $Q \oplus Q \oplus Q \oplus Q$  or  $Q \oplus Q$ , respectively. So we can assume that  $m = 2k$  with  $k$  even and must show that  $k$  is divisible by 4 and that (38) holds. By the theorem above, the theta series  $\Theta_Q$  is a modular form of weight  $k$  on the full modular group  $\Gamma_1 = \text{SL}(2, \mathbb{Z})$  (necessarily with trivial character, since there are no non-trivial Dirichlet characters modulo 1). By the results of Section 2, this modular form is a linear combination of  $\mathbb{G}_k(z)$  and a cusp form of weight  $k$ , and from the Fourier expansion (13) we see that the coefficient of  $\mathbb{G}_k$  in this decomposition equals  $-2k/B_k$ , since the constant term  $R_Q(0)$  of  $\Theta_Q$  equals 1. (The only vector of length 0 is the zero vector.) Now Proposition 8 implies the

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  $k \rightarrow \infty$ , 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  $\Lambda_8$  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  $\Lambda_8$ , then every  $u_i$  has length 2 and  $(u_i, u_j)$  for  $i \neq j$  equals  $-1$  or  $0$  according whether the  $i$ th and  $j$ th 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  $\Lambda_8$  is a modular form of weight 4 on  $\text{SL}(2, \mathbb{Z})$  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  $\Lambda_8$  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  $\Lambda_{16}$  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 Niemeier 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