REDUCTION MODULO 2 AND 3 OF EUCLIDEAN LATTICES

by Jacques Martinet

Abstract. Let Λ be a Euclidean lattice, We study upper bounds for the norm of shortest representatives of Λ modulo $d\Lambda$, $d = 2$ or 3, as well as the structure of the sets of such vectors with the same norm and the same image modulo d. Root systems appear in connection with this last problem.

Résumé. Soit Λ un réseau euclidien. Nous étudions des majorations de la norme des représentants les plus courts des classes de Λ modulo $d\Lambda$, $d = 2$ ou 3, ainsi que la structure des ensembles de tels vecteurs qui ont même norme et même image modulo d. Les systèmes de racines interviennent en liaison avec ce dernier problème. Titre français : **Réduction modulo 2 et 3 des réseaux euclidiens**.

In this paper, we prove some results which are useful for the determination of the classes $\Lambda/d\Lambda$ where Λ is a *lattice in some real vector space* E and $d \geq 2$ an integer. For any $\lambda > 0$, we denote by $S_\lambda = S_\lambda(\Lambda)$ (resp. $S'_\lambda = S'_\lambda(\Lambda)$) the set of vectors (resp. of primitive vectors) of norm λ in Λ and we set $s_\lambda = \frac{1}{2}|S_\lambda|$ and $s'_\lambda = \frac{1}{2}|S'_\lambda|$. We write simply S and s when λ is the *norm* (or *minimum*) $N(\Lambda)$ of Λ. We denote by m this norm and by m' the norm of the second layer of Λ.

Our aim is to study congruences modulo d among vectors of Λ and deduce from this a system of representatives of $\Lambda/d\Lambda \setminus \{0\}$ up to the sign. We wish to find vectors which are as short as possible. To this end, we may choose in each class modulo $d\Lambda$ one of the shortest possible vectors. The results to be proved below assert in particular that for $d = 2$ (resp. for $d = 3$), one must consider vectors of norm up to the greatest number $r \leq 2m$ (resp. $r \leq 2m + m'$) such that the layer $S_r(\Lambda)$ is not empty. We also give conditions under which two vectors of norm $N \leq 2m$ (resp. $N \leq 2m + m'$) may be congruent modulo 2 (resp. modulo 3). Once more, root systems play an important rôle.

We develop some general results in section 1, then turn to results modulo 2 in section 2 and modulo 3 in section 3. Section 4 is devoted to the study of the Leech lattice modulo 3. We describe briefly some applications (mainly to $\mathbb{E}_8$ and Λ_{24}) in section 5.

I thank Christine Bachoc, Heinz-Georg Quebbemann, and Nils Skoruppa for various comments on this paper.

Key words and phrases. Lattices, short vectors, reduction modulo 2 and 3.

Laboratoire associé au C.N.R.S. (UMR 5465) – Université Bordeaux 1

§ **1. Basic results.** We shall only consider non-zero vectors x, y such that $y \neq \pm x$. Moreover, we shall enumerate classes of $\Lambda \mod d\Lambda$ in pairs $c, -c$. They reduce to a single element if and only if $d = 2$ (or if $c = \{0\}$).

1.1. Proposition. *Let x and $y \neq \pm x$ be two non-zero vectors of Λ, such that $y - x = dz$ for some $z \in \Lambda$. Then, the following three identities hold:*

(1) $N(y) + (d-1)N(x) = d\big((d-1)N(z) + N(x+z)\big)$.
(1') $N(x) + (d-1)N(y) = d\big((d-1)N(z) + N(y-z)\big)$.
(2) $N(y) + N(x) = 2(d-1)N(z) + N(x+z) + N(y-z)$.

Moreover, if Λ is integral, we have $N(y) \equiv N(x) \mod d$, and even $N(y) \equiv N(x) \mod 4$ if $d = 2$.

Proof. We have

$$N(y) = N(x) + 2d\, x \cdot z + d^2 N(z) = N(x) + d(d-1)\, N(z) + d\big(N(x+z) - N(x)\big)\,,$$

which proves (1). We then derive (1') from (1) by using the double exchange $y \leftrightarrow x$ and $z \leftrightarrow -z$ and finally prove (2) by adding (1) and (1') and dividing out both sides by d. The last two assertions are consequences of the formula displayed above. □

1.2. Proposition. *We keep the hypotheses of Proposition 1.1. Let $a = N(z)$, $b = N(x+z)$ and $c = N(y-z)$.*

(1) *If $d = 2$, then $c = b$.*
(2) *If $d > 2$, then*

$$N(x) = (d-1)a + b + \frac{b-c}{d-2} \quad \text{and} \quad N(y) = (d-1)a + c - \frac{b-c}{d-2}\,;$$

Moreover, $2\, x \cdot z = -da - \dfrac{b-c}{d-2}$, $N(y) - N(x) = \dfrac{d(c-b)}{d-2}$ and $2\, x \cdot y = -(d^2 - 2d + 2)a + b + c$.

Proof. We have $y - z = x + (d-1)\, z$, hence $y - z = x + z$ if $d = 2$. If $d > 2$, the calculation of the norms of $x + z$ and of $x + (d-1)z$ yields $N(x) + 2\, x \cdot z = b - a$ and $N(x) + 2(d-2)\, x \cdot z = -(d-1)^2 a + c$, which gives us first the values of $N(x)$ and $x \cdot z$, then that of $N(y)$ by Proposition 1.1, and finally the other values we need. □

1.3. Theorem. *Let $x, y \in \Lambda$ such that $y = x + dz$ for some $z \in \Lambda$ and that none of the vectors $x, y, y \pm x$ is zero. If $d = 3$, suppose moreover that none of the equalities $x = -2y$ and $y = -2x$ hold. Then, we have $N(y) + N(x) \geq 2dm$, and equality holds if and only if $d = 2$ or $d = 3$ and if moreover:*

(1) *When $d = 2$, x and y are of the form $x = e - f$ and $y = e + f$ where e and f are orthogonal minimal vectors.*
(2) *When $d = 3$, x and y are of the form $x = e - f$ and $y = e + 2f$ where e, f and $e + f$ are minimal vectors.*

If $d = 2$, x and y, of norm $2m$, are orthogonal, and $\{\pm x, \pm y\}$ is the second layer of the square lattice generated by e and f. If $d = 3$, $\pm x$, $\pm y$ and $\pm(x + y)$, of norm $3m$, constitute the second layer of the hexagonal lattice of minimum m whose minimal vectors are $\pm e$, $\pm f$ and $\pm(e + f)$.

Proof. By Proposition 1.1, (2), since $z \neq 0$, we have $N(x) + N(y) \geq 2(d-1)m + N(x+z) + N(y-z)$. If $x + z = 0$, then $y = 2z = -2x$, $y - z = x + 2z = -x$ and $N(x) + N(y) = 5m$ whereas $2(d-1)N(z) + N(y-z) = (2d-1)m$. By Proposition 1.1, we must have $d = 3$. Similarly, $y - z = 0$ implies $x = -2y$ and again $d = 3$. Consequently, $x+z$ and $y-z$ are non-zero, which implies the required inequality.

Suppose now that equality holds, i.e. that $N(x) + N(y) = 2d\,m$. Then, z, $x + z$ and $y-z = x+2z$ are minimal. Now, $x+z$ and z are not proportional, for $x+z = z$ implies $x = 0$ and $x + z = -z$ implies $y - z = 0$. We thus have $|(x + z) \cdot z| \leq \frac{m}{2}$, whence

$$N(x) \leq N(x + z) + N(z) + 2|z \cdot (x + z)| \leq 3m$$

and similarly $N(y) \leq 3m$. Since $N(x) + N(y) \geq 2d\,m$, we have $d \leq 3$.

Set $e = x + z$ and $f = z$.

If $d = 2$, we have $e-f = x$, $e+f = x+2z = y$. This implies $x \cdot y = N(e)-N(f) = 0$ and also $e \cdot f = 0$ since $N(e + f) = 2m = N(e) + N(f)$.

If $d = 3$, we again have $e - f = x$, but now $y = x+3z = e+2f$, and $e+f = y-z$ is minimal. This last property implies $e \cdot f = -\frac{m}{2}$, hence $N(x) = N(e) + N(f) - 2e \cdot f = 3m$, $N(y) = N(e) + 4N(f) + 4e \cdot f = m + 4m - 2m = 3m$ and similarly $N(x + y) = N(2e + f) = 3m$.

Conversely, if x and y have the form given in the theorem above, it is easily seen that the equality $N(x) + N(y) = 2d\,m$ holds in both the cases $d = 2$ and $d = 3$. □

1.4. Remark. If Λ is integral, more restrictions can be derived from the proof of Theorem 1.3. For instance, if $d = 3$ and if $N(x) + N(y) = 6m$, then the norm m of Λ must be even, since $-2e \cdot f = m$.

Since vectors which are independent modulo $d\Lambda$ are a fortiori independent in Λ, a sequence $e_1, \ldots, e_n$ of representatives of the successive minima $m_1 = m \leq m_2 \leq \cdots \leq m_n$ of Λ must occur among a set of short representatives of L/dL.

For the applications to the classification up to isometry of sublattices with cyclic quotients of order d, it suffices to consider the classes of Λ^* mod $d\Lambda^*$ up to an automorphism of Λ. Exchanging Λ and Λ^*, we go back to Λ itself. Let us say that two orbits o and o' in Λ are *d-equivalent* (denoted $o \sim_d o'$) if there exist $x \in o$ and $x' \in o'$ such that $x' \equiv x \mod d\Lambda$. We denote by T a set of representatives of the non-zero orbits modulo d-equivalence. (We represent the null class by $\{0\}$.) To an orbit o, we attach its *(d-)weight* $wt(o)$, which is the number of elements within a class modulo d of o. Of course, we have the relation $\dfrac{1}{wt(o)}\,|o| = \dfrac{1}{wt(o')}\,|o'|$

whenever $o' \sim_d o$. (Even if we choose the orbits so as to minimize the norm, we cannot exclude the possibility that two orbits of vectors having the same norm be d-equivalent.)

Now, a description of $\Lambda/d\Lambda$ corresponds to a weighted formula

$$\sum_{o\in T} \frac{1}{wt(o)}\,|o| = d^n - 1\,. \tag{1.5}$$

Examples for $d = 2$ and $d = 3$ will be given in the forthcoming sections.

§ 2. Reduction modulo 2. It results from Theorem 1.3 that vectors of norm $N \leq 2m$ represent distinct classes in $\Lambda/d\Lambda$ except for pairs $(x, -x)$ and possibly for orthogonal vectors x, y of norm $2m$. For $x \in S_{2m}$, assuming $S_{2m} \neq \emptyset$, let $\ell_2(x) = \ell(x)$ be the number of lines containing a vector $y \in S_{2m}$ with $y \equiv x \mod 2\Lambda$ (or $y \equiv x \mod 2S_m$, this amounts to the same). Note that $\ell(x)$ in an invariant of the class $\mathcal{C}$ of x in $\Lambda/2\Lambda$, which allows us to define $\ell(\mathcal{C})$ for any class $\mathcal{C} \mod 2\Lambda$ which contains elements of S_{2m}. We have for ℓ the obvious bounds $1 \leq \ell(x) \leq n$. The following statement is now clear:

2.1. Theorem. *Any complete set of representatives of $\Lambda/2\Lambda$ whose elements are vectors whose norms are minimal in their class modulo 2Λ contains elements of all the spheres S_k with $k \leq 2m$. Moreover, we have*

$$\sum_{0<k<2m} s_k \;+\; \sum_{x\in S_{2m} \bmod 2\Lambda} \frac{1}{\ell(x)} \leq 2^n - 1\,,$$

and equality holds if and only if all classes modulo 2Λ possess representatives of norm at most $2m$. □

When $\ell(x)$ is constant on S_{2m}, for instance when $\mathrm{Aut}(\Lambda)$ acts transitively on S_{2m}, the formula of Theorem 2.1 can be written in the simplified form

$$\sum_{0<k<2m} s_k \;+\; \frac{1}{\ell}\, s_{2k} \leq 2^n - 1\,. \tag{2.2}$$

Taking into account the upper bound $\ell(x) \leq n$, we immediately obtain:

2.3. Theorem. *We have*

$$\sum_{0<k<2m} s_k \;+\; \frac{1}{n}\, s_{2m} \leq 2^n - 1\,.$$

If equality holds, vectors of norm $2m$ in Λ appear in systems of $2n$ vectors lying on n pairwise orthogonal lines, and one obtains a system of representatives of $\Lambda/d\Lambda \setminus \{0\}$

by taking one vector out of each such system and one vector in each pair $\pm x$ of non-zero vectors of norm $N < 2m$. □

The formula above plays a crucial rôle in Conway's characterization of the Leech lattice, see [C-S], chapter 12. Computing s_4, s_6, s_8 by means of Theta series, Conway obtains the formula

$$s_4 + s_6 + \frac{1}{24}\, s_8 = 98280 + 8386560 + \frac{199017000}{24} = 16777215 = 2^{24} - 1\,,$$

valid a priori for any even 24-dimensional unimodular lattice without roots.

Suppose that there exists an orthogonal frame of n vectors of norm $2m$, and let L be the lattice they generate. Then, the ratio $\dfrac{(2m)^n}{\det(\Lambda)}$ is the square of an integer, namely of the index $[\Lambda : L]$; in particular, if Λ is integral and if n is even, $\det(\Lambda)$ must be a square. When this condition is not satisfied, there may be at most $n-1$ directions of pairwise orthogonal vectors defining the same class modulo 2. Thus:

2.4. Theorem. *Suppose that there does not exist in Λ any orthogonal frame of vectors of norm $2m$. We then have*

$$\sum_{0<k<2m} s_k \;+\; \frac{1}{n-1}\, s_{2m} \le 2^n - 1\,.$$

If equality holds, vectors of norm $2m$ in Λ appear in systems of $2(n-1)$ vectors lying on $n-1$ pairwise orthogonal lines, and one obtains a system of representatives of $\Lambda/d\Lambda \smallsetminus \{0\}$ by taking one vector out of each such system and one vector in each pair $\pm x$ of non-zero vectors of norm $N < 2m$. □

As was pointed out to me by Quebbemann on the example of K_{12}, it is interesting to consider examples with constant $\ell(x) \le n-2$. Indeed, some examples can be easily handled via Theorem 2.1, by first proving sharper bounds for ℓ other that $\ell(x) \le n$ or $\ell(x) \le n-1$. The following proposition can be used to derive such bounds. We denote by $\boldsymbol{A}_n$ $(n \ge 1)$, $\boldsymbol{D}_n$ $(n \ge 2)$, $\boldsymbol{E}_n$ $(n = 6, 7, 8)$ the irreducible root systems whose vectors all have norm 2 and by $\mathbb{A}_n$, $\mathbb{D}_n$, $\mathbb{E}_n$ the corresponding root lattices. Recall that $\boldsymbol{D}_2 \simeq \boldsymbol{A}_1 \perp \boldsymbol{A}_1$ and $\boldsymbol{A}_3 \simeq \boldsymbol{D}_3$.

2.5. Theorem. *A set $\mathcal{T}_r = \{\pm x_1, \ldots, \pm x_r\}$ of $r \ge 2$ vectors of S_{2m} is contained in a single class modulo 2Λ if and only if the set $\{\frac{\pm x_i \pm x_j}{2}\}$ is a (rescaled) root system $\mathcal{R}$ of type $\boldsymbol{D}_r$ contained in S_m, and the map $\mathcal{T}_r \to \mathcal{R}$ is one-to-one if $r \ne 4$, and three-to-one if $r = 4$.*

Proof. Given pairwise non-proportional vectors $x_1, \ldots, x_r \in S_{2m}$, set

$$\varepsilon_i = \frac{x_i}{2},\ (i = 1, \ldots, r) \quad \text{and} \quad e^+_{i,j} = \frac{x_i + x_j}{2},\ e^-_{i,j} = \frac{x_i - x_j}{2}\ (1 \le i < j \le r)\,.$$

If $x_1, \dots, x_r$ represent the same class modulo 2, they are pairwise orthogonal. Then, the system of vectors $\pm\varepsilon_i$, all of norm $\frac{m}{2}$, is an orthogonal frame in some r-dimensional subspace of E, and the vectors $e^+_{i,j}$ and $e^-_{i,j}$ belong to Λ if and only if $x_1 \equiv \cdots \equiv x_r \mod 2\Lambda$. If it is the case, they lie in S_m, and the set $\{\pm e^+_{i,j}, \pm e^-_{i,j}\}$ is a root system of type $\boldsymbol{D}_r$, since $e^\pm_{i,j} = \varepsilon_i \pm \varepsilon_j$. The converse is clear, since $e^+_{i,j}$ belongs to Λ if and only if $x_i \equiv x_j \mod \Lambda$.

The map $\mathcal{T}_r \to \mathcal{R}$ is clearly onto by the proof of the first assertion. Now, consider the lattice $\mathbb{D}_r$ scaled to its natural norm 2; it is the even sublattice of $\mathbb{Z}^r$, whose canonical basis we denote by $(\varepsilon_1, \dots, \varepsilon_r)$. If another orthogonal frame $(\pm\varepsilon'_1, \dots, \pm\varepsilon'_r)$ generates a lattice L isometric to $\mathbb{Z}^r$ containing $\mathbb{D}_r$, we have $\mathbb{D}_r \subset L \subset \mathbb{D}^*_r$. The quotient $\mathbb{D}_r/\mathbb{D}^*_r$ is cyclic if r is odd and of type $(2,2)$ if r is even, and in this last case, the other two lattices are $\mathbb{D}^\pm_r = \mathbb{D}_r \cup \frac{1}{2}(\pm\varepsilon_1 + \varepsilon_2 + \cdots + \varepsilon_r)$, of norm $\min(2, \frac{r}{4})$. Hence, $\mathcal{T}_r \to \mathcal{R}$ is injective if $r \neq 4$. If $r = 4$, both lattices $\mathbb{D}^+_r$ and $\mathbb{D}^-_r$ are isometric to $\mathbb{Z}^4$, so that there are two more systems $\mathcal{T}'_r = \{\pm x'_1, \dots, \pm x'_r\}$ and $\mathcal{T}''_r = \{\pm x''_1, \dots, \pm x''_r\}$ which define the same class modulo 2, namely the sets $\{\frac{1}{2}(x_1 \pm x_2 \pm x_3 \pm x_4)\}$ with an even and and odd number of minus signs respectively. It is easily verified that they define distinct elements of $\Lambda/2\Lambda$: for instance, if $\{\frac{1}{2}(x_1 \pm x_2 \pm x_3 \pm x_4)\} - x_1 = 2z$, then $N(z) = \frac{m}{2}$, so that z cannot belong to Λ. □

2.6. Corollary. *If Λ is an integral lattice of odd norm, one has $\ell(x) \leq 2$ for all $x \in S_{2m}$, and even $\ell(x) = 1$ if no two minimal vectors of Λ are orthogonal.*

Proof. The lattice $\mathbb{D}_r$ scaled to norm m contains minimal vectors with scalar product $\frac{m}{2}$ for all $r \geq 3$ and orthogonal minimal vectors for all $r \geq 2$. □

2.7. Remark. Given a root system $\mathcal{R}$ of type $\boldsymbol{D}_r$, $r \geq 2$ inside $S(\Lambda)$, we recover the orthogonal frame(s) $\mathcal{T}_r \subset S_{2m}(\Lambda)$ in the following way: let $r \in \mathcal{R}$; let $\mathcal{R}' = \mathcal{R} \cap r^\perp$; one selects an $r' \in \mathcal{R}'$ such that $cR'' = \langle r, r'\rangle^\perp \cap \mathcal{R}$ is a root system of type $\boldsymbol{D}_{r-2}$ (it could be of type $2\boldsymbol{A}_1 + \boldsymbol{D}_{r-4}$; this amounts to the same only if $r = 4$); then, $\mathcal{T}_r$ is the union of the set $\mathcal{T}_{r-2}$ attached to $\mathcal{R}''$ with $\{\pm r, \pm r'\}$. We reduce ourselves in this way to the easy cases of dimensions 2 and 3.

We shall come back later on properties of classes of Λ modulo 2Λ related to root systems contained in Λ. For the while, we give an application of Theorem 2.5:

2.8. Theorem. *Suppose that Λ is integral. Let p be a prime number and let t be the number of elementary divisors of (Λ^*, Λ) which are divisible by p. Let $x \in S_{2m}$.*

(1) *If p is odd and does not divide m, we have $\ell(x) \leq \max(2, n - t)$.*
(2) *If $p = 2$ and if $m \equiv 2 \mod 4$, we have $\ell(x) \leq \max(2, n + 2 - t)$.*

Proof. Let $x \in S_{2m}$ with $\ell(x) \geq 3$ and let $r = \ell(x)$. By Theorem 2.5 and Corollary 2.6, the norm m of Λ is even and there exists inside $S(\Lambda)$ a root system $\mathcal{R}$ of type $\boldsymbol{D}_r$. Let $L \sim \mathbb{D}_r$ be the lattice generated by $\mathcal{R}$ and let F be the subspace of E spanned by $\mathcal{R}$. Then, $F^\perp \cap \Lambda^*$ is an $(n - r)$-dimensional lattice contained in Λ^*.

Since Λ is integral, $L' = F \cap \Lambda$ is an $(n-r)$-dimensional lattice contained in Λ. We have the inclusions

$$L \perp L' \subset \Lambda \subset \Lambda^* \subset L^* \perp L'^*$$

which induce an injective homomorphism $\Lambda^*/\Lambda \to L^*/L \bigoplus L'^*/L'$.

Let u and u' be the number of elementary divisors divisible by p in L and in L' respectively. One has $t \leq u + u'$. Since L is isometric to $\sqrt{\frac{m}{2}}\,\mathbb{D}_r$ and p does not divide $\frac{m}{2}$, the value of u is 0 if p is odd, 1 if $p = 2$ and r is odd, and 2 if $p = 2$ and r is even. Using the trivial upper bound $u' \leq n - r$, we see that r is bounded above by $n + u - t$.

If p is odd, this is precisely the bound of the proposition.

If p is even, we have $u = 2$ if r is even and $u = 1$ if r is odd, whence the bound $r \leq n + 2 - t$. □

For some small values of n (certainly for all $n \leq 6$, see below, table 2.10), it may happen that representatives of norm $N \leq 2m$ exist on an open set in the set of n-dimensional lattices. Examples are easily obtained using the following proposition:

2.9. Proposition. *Suppose that there exists for some n an n-dimensional lattice Λ such that all classes in $\Lambda/2\Lambda$ possess representatives of norm $N < 2m$ (strict inequality). Then, there exists a neighbourhood of Λ on which all lattices satisfy this condition.*

Sketch of proof. Let

$$m_1(\Lambda) = \min_{x \in \Lambda \smallsetminus \{0\}} N(x) \quad \text{and} \quad m_2(\Lambda) = \max_{x \in \Lambda,\, N(x) \leq 2m_1} N(x)\,,$$

and let $\varepsilon > 0$. Since the set T of vectors in Λ of norm $N \leq 2m$ is finite, we can find a neighbourhood $\mathcal{N}_\varepsilon$ of the identity in $\mathrm{GL}(E)$ such that

$$\forall\, u \in \mathcal{N}_\varepsilon \text{ and } \forall\, x \in u(T),\ m_1 - \varepsilon < N(u(x)) < m_2 + \varepsilon\,,$$

and moreover that all vectors x with $N(x) < m_2 + \varepsilon$ belong to $u(T)$. (Compare [M], Chapter III, proof of Lemma 4.2.) Since u is injective, $u(T)$ and T have the same cardinality, indeed $2^n - 1$. Choosing $\varepsilon < 2m_1 - m_2$, we obtain $2^n - 1$ vectors in $u(\Lambda)$ of norm $N < 2\,N(\Lambda)$. The proposition to be proved is now a consequence of Theorem 2.1. □

We now give some examples, beginning with irreducible root lattices.

We define as usual $\mathbb{A}_n$ and $\mathbb{D}_n$, $n \geq 4$ using orthogonal bases $(\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_n)$ and $(\varepsilon_1, \ldots, \varepsilon_n)$ of $\mathbb{Z}^n$, by the respective conditions $\sum_{0 \leq i \leq n} x_i = 0$ and $\sum_{1 \leq i \leq n} x_i \equiv 0 \mod 2$. For $L = \mathbb{A}_n$ (resp. $L = \mathbb{D}_n$, $n \geq 5$), we then consider for every k with $0 \leq k \leq \frac{n+1}{2}$ (resp. with $0 \leq k \leq \frac{n}{2}$) the orbit o_{2k} of sums of $2k$ distinct vectors $\pm\varepsilon_i$, and moreover in case $L = \mathbb{D}_n$ the orbit $o'_4 = \{\pm 2\varepsilon_i\}$. (For $\mathbb{D}_4$, there is a single orbit of vectors of norm 4.) Then, shortest representatives of $L/2L$ need the

consideration of all orbits o_{2k} if $L = \mathbb{A}_n$ and of moreover o_4' if $L = \mathbb{D}_n$, $n \geq 5$. In particular, $L/2L$ possesses representatives of norm $N \leq 2m = 4$ if and only if L is one of the lattices $\mathbb{A}_n$, $n \leq 4$, $\mathbb{D}_n$, $n \leq 5$, $\mathbb{E}_6$ or $\mathbb{E}_8$.

The cases of $\mathbb{E}_6$ and $\mathbb{E}_8$ are easily dealt with, using Theorems 2.4 and 2.3 respectively. For $\mathbb{E}_7$, vectors of norm $N \leq 4$ represent all classes but one, which is represented by any vector of one among two orbits of norm 6 vectors.

As for the duals of irreducible root lattices which are not similar to a root lattice, it can be verified that all classes modulo 2 possess representatives of norm $N \leq 2m$ exactly for the lattices $\mathbb{A}_n^*$ $(3 \leq n \leq 6)$, $\mathbb{D}_5^*$, and $\mathbb{E}_6^*$. (For $\mathbb{E}_7^*$ scaled to norm 3, one must make use of vectors of norm $3, 4, 7$.)

The following three tables contain some classical lattices. We do not define them here, referring to [C-S], Chapter 6 for the laminated lattices Λ_n, to [M], chapter VIII, for Barnes's series L_n^r (section 4) and for both the series K_n, K_n' contained in the Leech lattice Λ_{24} (sections 5 and 7; in particular, Proposition 7.9), and to [C-S], Chapter 8, section 6 or [M], Chapter V, section 4 for the Craig lattices $\mathbb{A}_n^{(r)}$. The lattices which are displayed are rescaled to the smallest norm which makes them integral. Indeed, $\mathbb{A}_n^*$ stands for $\sqrt{n+1}\,\mathbb{A}_n^*$ and $\mathbb{D}_5^*$ for $2\,\mathbb{D}_5^*$.

Table 2.10. Some lattices with representatives of norm $N < 2m$.

$n = 1$	$\mathbb{Z}$	$s_1 = 1$		
$n = 2$	$\mathbb{A}_2$	$s_2 = 3$		
$n = 3$	$\mathbb{A}_3^*$	$s_3 = 4$	$s_4 = 3$	
$n = 3$	K_3'	$s_4 = 5$	$s_6 = 2$	
$n = 4$	$\mathbb{A}_4^*$	$s_4 = 5$	$s_6 = 10$	
$n = 4$	K_4'	$s_4 = 9$	$s_6 = 6$	
$n = 5$	$\mathbb{A}_5^*$	$s_5 = 6$	$s_8 = 15$	$s_9 = 10$
$n = 6$	K_6'	$s_4 = 27$	$s_6 = 36$	

[K_3' is *the* 3-dimensional eutactic lattice with $s = 5$; one has $K_4' \simeq \mathbb{A}_2 \bigotimes \mathbb{A}_2$ and $K_6' \sim \mathbb{E}_6^*$.]

I do not know of any lattice of dimension $n \geq 7$ possessing representatives of norm $N < 2m$.

In the following table, we consider lattices possessing representatives of norm $N \leq 2m$ for which the equality $N = 2m$ is needed, and for which the function $\ell(x)$ (defined at the beginning of this section) is constant. The value of ℓ is always an easy consequence of one of the statements 2.3, 2.4, 2.6, or 2.8.

Table 2.11. Some lattices with representatives of norm $N \leq 2m$ and constant ℓ.

$n = 2$	$\ell = 2$	$\mathbb{Z}^2$	$s_1 = 2$	$s_2 = 2$
$n = 3$	$\ell = 3$	$\mathbb{A}_3$	$s_2 = 6$	$s_4 = 3$

$n=4$	$\ell=4$	$\mathbb{D}_4$	$s_2=12$	$s_4=12$		
$n=4$	$\ell=3$	$\mathbb{A}_4$	$s_2=10$	$s_4=15$		
$n=4$	$\ell=2$	$\mathbb{A}_2^{\perp 2}$	$s_2=6$	$s_4=18$		
$n=5$	$\ell=2$	$\mathbb{D}_5^*$	$s_4=5$	$s_5=16$	$s_8=20$	
$n=6$	$\ell=5$	$\mathbb{E}_6$	$s_2=36$	$s_4=135$		
$n=6$	$\ell=3$	$\mathbb{A}_6^{(2)}$	$s_4=21$	$s_6=28$	$s_8=42$	
$n=6$	$\ell=1$	$\mathbb{A}_6^*$	$s_6=7$	$s_{10}=21$	$s_{12}=35$	
$n=8$	$\ell=8$	$\mathbb{E}_8$	$s_2=120$	$s_4=1080$		
$n=8$	$\ell=3$	L_8^4	$s_4=54$	$s_6=120$	$s_8=243$	
$n=10$	$\ell=4$	${K'_{10}}^*$	$s_6=120$	$s_8=135$	$s_{10}=648$	$s_{12}=480$
$n=12$	$\ell=6$	K_{12}	$s_4=378$	$s_6=2016$	$s_8=10206$	
$n=24$	$\ell=24$	Λ_{24}	$s_4=98280$	$s_6=8386560$	$s_8=199017000$	

When $\mathrm{Aut}(\Lambda)$ does not act transitively on S_{2m}, the function $\ell(x)$ need not be constant. For instance, the orbits named above o_4 and o'_4 of norm 4 vectors in $\mathbb{D}_n$, $n \geq 5$, contain $s_{4,1} = 8\binom{n}{4}$ and $s_{4,2} = n$ pairs of vectors, with $\ell = 4$ and $\ell = n$ respectively. The left hand side of the weighted formula of Theorem 2.1 for $\mathbb{D}_n$ is then of the form

$$s_2 + \frac{1}{4}\, s_{4,1} + \frac{1}{n}\, s_{4,2} = n(n-1) + \frac{n(n-1)(n-2)(n-3)}{12} + 1\,;$$

For $n = 5$, it is $20 + 10 + 1 = 2^5 - 1$; from $n = 6$ onwards, it is strictly smaller than $2^n - 1$.

Table 2.12. Some other lattices with representatives of norm $N \leq 2m$.

$n=5$	$\mathbb{D}_5$	$s_2=20$	$s_4=40$		
$n=7$	K_7	$s_4=46$	$s_6=32$	$s_8=218$	
$n=7$	$\mathbb{A}_7^{(2)}$	$s_4=36$	$s_6=48$	$s_8=142$	
$n=8$	K_8	$s_4=66$	$s_6=96$	$s_8=414$	
$n=9$	Λ_9	$s_4=136$	$s_6=128$	$s_8=1529$	
$n=10$	Λ_{10}	$s_4=168$	$s_6=384$	$s_8=2475$	

Exactly 12 lattices among the 48 perfect lattices of dimension $n \leq 7$ possess mod 2 representatives of norm $N \leq 2m$, that we list using Conway–Sloane's notation in [C-S1]; see also the tables in [M], chapitre VI: the 5 lattices with $n \leq 4$, 1 out of 3 for $n = 5$ ($P_5^1 \simeq \mathbb{D}_5$), 3 out of 7 for $n = 6$ ($P_6^1 \simeq \mathbb{E}_6$, $P_6^2 \sim \mathbb{E}_6^*$, and $P_6^5 \simeq \mathbb{A}_6^{(2)}$), and 3 out of 33 for $n = 7$ ($P_7^5 \simeq \mathbb{A}_7^{(2)}$, P_7^{20}, and P_7^{23}). Similarly, exactly 5 lattices among the 10916 known perfect lattices of dimension $n = 8$ possess mod 2 representatives of norm $N \leq 2m$. In the notation of [Bt-M], they are $lh(2) \simeq L_8^4$, $lh(179)$, $lh(1172) \simeq \mathbb{E}_8$, $np(160)$, and $bt(5)$. These "no-name lattices" are not displayed in the previous tables.

Lattices belonging to one of the series Λ_n, K_n, K'_n contained in the Leech lattice and their duals have been tested for $n \leq 12$. Only lattices which occur in one of the tables 2.10 to 2.12 do have mod 2 representatives of norm $N \leq 2m$.

§ **3. Reduction modulo 3.** We must first make more precise the statement in Theorem 1.3 about congruent vectors of norm $3m$.

3.1. Proposition. *Let $x \in \Lambda$ of norm $3m$. Then, the set of vectors of norm $3m$ which are congruent to x modulo 3Λ reduces to $\{x\}$ or is of the form $\{x, y, -x-y\}$.*

Proof. If there exists $y \equiv x \mod 3\Lambda$ with $N(y) = N(x) = 3m$, then we know by Theorem 1.3 that there exist e, f minimal in Λ such that $x = e - f$ and $y = e + 2f$ (and $-x - y = -(2e + f)$). If there exists $y' \neq x, y, -x - y$ also congruent to x mod 3Λ, there exist minimal vectors e', f' in Λ such that $x = e'-f'$ and $y' = e'+2f'$ and that $e' + f'$ is also minimal. We have $y' \equiv y \mod 3\Lambda$, hence $N(y - y') = 9m$, since $\frac{1}{3}(y-y')$ is minimal by Theorem 1.3. We also have $y-y' = (x+3f)-(x+3f') = 3(f - f')$, hence $N(f - f') = m$. But this is not possible, for the 3-dimensional lattice generated by e, f, e' would then contain the seven pairs of minimal vectors represented by $e, f, e + f, e', f', e' + f', f - f'$. □

In analogy with Theorem 2.3, we deduce from the proposition above the following inequality

$$\sum_{0<k<3m} s_k \; + \; \frac{1}{3}\, s_{3m} \leq \frac{1}{2}(3^n - 1)\,. \tag{**3.2**}$$

and the fact that representatives of $\Lambda/3\Lambda$ can be found among vectors of norm $N \leq 3m$ when equality holds. However, in practice, we must consider vectors of norm greater than $3m$ (e.g., $4m = 8$ for $\mathbb{E}_8$, giving the sum $N(x) + N(y)$ the value $8m = 16$).

We shall now use the notation m' for $m^{(2)}$ and m'' for $m^{(3)}$ (the norms of the second and third layers of Λ). Proposition 1.1 shows that if $N(x) + N(y) > 6m$, then $y \equiv x \mod 3\Lambda$ implies $N(x) + N(y) \geq 5m + m'$, with equality if and only if $N(z) = m$ and $(N(x + z), N(y - z)) = (m, m')$ or (m', m). (Note that the transformation $(x, z) \mapsto (y, -z)$ exchanges these two possibilities.)

The next possible value of $N(x) + N(y)$ is either $4m + 2m'$, with equality if and only if $N(z) = m$ and $N(x + z) = N(y - z) = m'$, or $5m + m''$ with equality if and only if $N(z) = m$ and $(N(x + z), N(y - z)) = (m, m'')$ or (m'', m). (As above, we can exchange (m, m'') and (m'', m).) We remark that

$$5m + m'' = 4m + 2m' \Longleftrightarrow m'' - m' = m' - m\,, \tag{**3.3**}$$

a possibility which often occurs, for instance if Λ is integral and if its first three layers have norm $m, m + h, m + 2h$ ($h = 1$ or 2 according to whether Λ is odd or even).

If the equality $N(x) + N(y) = 5m + m'$ holds for $y \equiv x \mod 3\Lambda$ with $N(z) = N(x + z) = m$, whence $N(y - z) = m'$, Proposition 1.2 shows that

$$N(x) = 4m - m' \quad \text{and} \quad N(y) = m + 2m'\,. \tag{**3.4**}$$

a congruence which does not occur among vectors of norm $N < 2m + m'$.

The next possible value of $N(x) + N(y)$ is $4m + 2m'$, attained for

$$N(x) = N(y) = 2m + m' , \tag{3.5}$$

or $5m + m''$, attained (assuming the inequality $N(y) \geq N(x)$) for

$$N(x) = 4m - m'' \quad \text{and} \quad N(y) = m + 2m'' \tag{3.6}$$

(or in both cases when relation 3.3 holds). Now, under conditions 3.5 (resp. 3.4, resp. 3.6), $\max(N(x), N(y))$ has value $2m + m'$ (resp. $m + 2m' > 2m + m'$, resp. $m + 2m'' > m + 2m'$). We have thus proved:

3.7. Proposition. *Primitive vectors $x, y \in \Lambda$ of norm $N \leq 2m + m'$ which are congruent modulo 3Λ have the same norm, equal to $3m$ or to $2m + m'$.* □

To go further, we must now study how many vectors of norm $2m + m'$ may represent the same class modulo 3Λ, as we previously did for vectors of norm $3m$.

3.8. Proposition. *Suppose that $m' < 7m$. Let $x \in S_{2m+m'}$, and let $y_0 = x, y_1, \ldots, y_r$ be distinct elements of $S_{2m+m'}$ which are congruent to x modulo 3Λ. Then, $S(\Lambda)$ contains a root system of type $\boldsymbol{A}_r$ and the lattice L generated by $y_0, \ldots, y_r$ has minimum $2m + m'$ and rank r or $r + 1$.*

Proof. For $i = 1, \ldots, r$, let z_i such that $y_i = x + 3z_i$. We know that the z_i are minimal vectors of Λ. Because of the congruence $y_j \equiv y_k \mod 3\Lambda$, the differences $z_j - z_k$, $j < k$ also belong to $S(\Lambda)$. Hence, the set $\mathcal{R} = \{\pm z_i, \pm(z_j - z_k)\}$ $(1 \leq i \leq r,$ $1 \leq j < k \leq r)$ is a root system of type $\boldsymbol{A}_r$ (scaled to norm m). We have of course $\operatorname{rk} L \leq r + 1$, and also $\operatorname{rk} L \geq r$ since L contains $\sqrt{3}\mathcal{R}$. Let $u = a_0 y_0 + \cdots + a_r y_r$ be a non-zero element of L and let $a = a_0 + \cdots + a_r \in \mathbb{Z}$. We have $u \equiv ax \mod 3\Lambda$. If $a \equiv \pm 1 \mod 3$, then $u \equiv \pm x \mod 3\Lambda$ has a norm $N \geq 2m + m'$ by Proposition 3.7. If $a \equiv 0 \mod 3$, then $u = 3v$ for some $v \in L \smallsetminus \{0\}$ and we have $N(u) = 9N(v) \geq 9m > 2m + m'$. □

From the obvious inequality $r \leq n$, we obtain:

3.9. Corollary. *Under the assumption $m' < 7m$, the number of elements of $S_{2m+m'}$ which are congruent to a given $x \in S_{2m+m'}$ modulo 3Λ is at most $n+1$.* □

This corollary suffices to obtain representatives of $\mathbb{E}_8$ modulo 3. We shall prove this later, and we now look more precisely at the lattice L in Proposition 3.8. Note that the condition $m' < 7m$ is scarcely a restriction: in practice, m' is much smaller than $7m$.

3.10. Proposition. *We keep the hypotheses and notation of Proposition 3.8. Then, L is of rank r if and only if one has*

$$m' < \frac{5m}{2} \quad \text{and} \quad r = \frac{4m + 2m'}{5m - 2m'} .$$

Under these conditions, one has moreover $r \equiv -1 \mod 3$ *and* L *is similar to* $\mathbb{A}_r^*$.

Proof. Without any hypothesis on the rank of L, we have $x \cdot z_i = -\frac{3m}{2}$ for $1 \le i \le r$ (a consequence of the equalities $N(y_i) = N(x)$), from which we easily deduce the relations $y_i \cdot z_i = +\frac{3m}{2}$ and $y_i \cdot z_j = 0$ $(1 \le i, j \le r,\ j \ne i)$ and also $y_i \cdot y_j = -\frac{5m-m'}{2}$ for $0 \le i < j \le r$.

Suppose now that $\operatorname{rk} L = r$. There is a relation $x = \sum_{j=1}^{r} \lambda_j z_j$. Taking the r scalar products of the two sides with z_i and setting $\lambda = \sum_j \lambda_j$, we obtain the r equations $\lambda_i + \lambda = -3$, whose sum reads $(r+1)\lambda = -3r$, whence $\lambda_i = -\frac{3}{r+1}$ for all $i \ge 1$ and finally

$$(*) \qquad x = -\frac{3}{r+1} \sum_{j=1}^{r} z_j \,.$$

This relation first shows that $(r+1)x \in 3\Lambda$; since x does not belong to 3Λ (because $N(x) = 2m + m' < 9m = N(3\Lambda)$), $r+1$ must be divisible by 3. Taking the norms of both sides, we obtain the equation

$$2m + m' = \frac{9}{(r+1)^2} \frac{r(r+1)}{2}$$

which is equivalent to $r(5m - 2m') = (4m + 2m')$. Using $(*)$, we see that $x = -(y_1 + \cdots + y_r)$, so that $(y_1, \ldots, y_r)$ is a basis of L whose Gram matrix is easily seen to be proportional to the matrix M whose entries are $m_{i,i} = r$ and $m_{i,j} = -1$ for $i \ne j$, which is itself proportional to a standard Gram matrix for $\mathbb{A}_n^*$.

Conversely, using the value above for r, we prove first that

$$x + \frac{3}{r+1}(z_1 + \cdots + z_r) = \frac{1}{r+1}(y_0 + \cdots + y_r)$$

and then that $N(y_0 + \cdots + y_r) = 0$ by making use of the known values of the scalar products $y_i \cdot y_j$, which implies that L is of rank at most r. $\square$

To study the case when L has rank $r+1$, we need the following lemma:

3.11. Lemma. *Let* $\alpha > 0$ *and* β *be real numbers and let* q *be the quadratic form*

$$q(x) = \alpha \sum_{i=1}^{r} x_i^2 + 2\beta \sum_{1 \le i < j \le r} x_i x_j \,.$$

Then, q *is positive definite with minimum* α *if and only if the two inequalities* $-\frac{\alpha}{r} \le \beta \le +\frac{\alpha}{2}$ *hold. When these inequalities are satisfied, the minimal vectors of* q *(up to the sign) are the* r *vectors of the canonical basis of* $\mathbb{Z}^r$*, except if* $\beta = -\frac{\alpha}{r}$ *or if* $\beta = \frac{\alpha}{2}$ *where extra minimal vectors exist: the vectors* $\pm(\varepsilon_1 + \cdots + \varepsilon_r)$ *in the first case (and*

q then corresponds to a scaled copy of $\mathbb{A}_r^*$) and the vectors $\pm(\varepsilon_i - \varepsilon_j)$, $1 \le i < j \le r$ in the second case (and q then corresponds to a scaled copy of $\mathbb{A}_r$).

Proof. See [M1], where one makes use of a Voronoi like interpretation involving the symmetric group S_r, or use according to the sign of β one of the identities

$$q(x) = (\alpha-\beta)\sum x_i^2 + \beta\left(\sum x_i\right)^2 = (\alpha+(r-1)\beta)\sum x_i^2 - \beta\sum_{i<j}(x_i-x_j)^2\,. \qquad \square$$

3.12. Proposition. *With the hypotheses and notation of Proposition 3.8, if L has rank r, then we have either $m' \ge \dfrac{5m}{2}$ or $m' < \dfrac{5m}{2}$ and $r < \dfrac{4m+2m'}{5m-2m'}$.*

Proof. Applying lemma 3.11 with $\alpha = 2m + m'$ and $\beta = m' - \frac{5m}{2}$, we obtain the double inequality

$$-\frac{2m+m'}{r} \le m' - \frac{5m}{2} \le m + \frac{m'}{2}\,.$$

The second inequality is always satisfied, and so is the first one if $m' \ge \frac{5m}{2}$. Otherwise, the first inequality is equivalent to $r \le \frac{4m+2m'}{5m-2m'}$, and Proposition 3.11 shows that this inequality must be strict. $\square$

I do not see how one could obtain more restrictive conditions without a detailed investigation of the root systems contained in $S(\Lambda)$. For particular lattices (e.g., for the Leech lattice), we can find the exact value of r, see below.

Recall that s'_λ is the number of primitive pairs of vectors of norm λ; obviously, one has $s'_\lambda = s_\lambda$ unless $\frac{\lambda}{m}$ is the square of an integer. Corollary 3.9 immediately yields the following weighted formula, that we only state when the number of vectors in $S_{2m+m''}$ congruent to a given one of the same layer attains its maximal possible value:

3.13. Theorem. *One has the inequality*

$$\sum_{0<k<3m} s'_k + \sum_{3m<k<2m+m'} s'_k \;+\; \frac{1}{3}\,s'_{3m} + \frac{1}{n+1}\,s'_{2m+m'} \le \frac{1}{2}\,(3^n-1)\,.$$

If equality holds, vectors of norm $3m$ (resp. $2m+m'$) appear in systems of 3 (resp. $n+1$) vectors with configuration $S(\mathbb{A}_2) \sim S(\mathbb{A}_2^*)$ (resp. $S(\mathbb{A}_n^*)$), and one obtains a system of representatives of $\Lambda/3\Lambda \setminus \{0\}$ by taking all vectors of norm $N < 2m+m'$, $N \ne 3m$, and one vector out of 3 (resp. out of $n+1$) in each system of 3 vectors of norm $3m$ (resp. of $n+1$ vectors of norm $2m+m'$). $\square$

For root lattices, one has $m = 2$ and $m' = 4$, and to apply Theorem 3.13, it suffices to consider $s_2 = s$, s_4, s_6 and $s'_8 = s_8 - s_2$. Theorem 3.13 applies with equality to $\mathbb{A}_2$ ($s_2 = s_6 = 3, s_4 = s'_8 = 0$), to $\mathbb{D}_4$ ($s_2 = s_4 = 12, s_6 = 48, s'_8 = 0$) and to $\mathbb{E}_8$. For $\mathbb{E}_8$ one can use the identification of $\Theta_{\mathbb{E}_8}$ with the Eisenstein series E_4,

which implies the formulae $s_t = 120\sum_{q|\frac{t}{2}} q^3$ for all even $t > 0$, whence $s_2 = 120$, $s_4 = 120\,(1^3+2^3) = 1080$, $s_6 = 120\,(1^3+3^3) = 3360$ and $s_8 = 120\,(1^3+2^3+4^3) = 8760$, thus $s'_8 = s_8 - s_2 = 8640$, and it is easy to check the equalities

$$120 + 1080 + \frac{1}{3}3360 + \frac{1}{9}8640 = 120 + 1080 + 1120 + 960 = 3280 = \frac{1}{2}(3^8 - 1)\,.$$

We can be more precise: in the three examples above, there is zero or one orbit of primitive vectors of norm $N \leq 8$. Only the case of $\mathbb{E}_8$ deserves a proof, which can be done along the following line: we first consider the Weyl group $W(\mathbb{D}_8)$, which stabilizes $\mathbb{E}_8$ and is easy to handle; one finds that the number of pairs of vectors in orbits of primitive vectors are

Norm 2 : $56 + 64 = 120$;
Norm 4 : $8 + 560 + 512 = 1080$;
Norm 6 : $672 + 896 + 1792 = 3360$;
Norm 8 : $4480 + 64 + 3584 + 512 = 8640$;

one moreover proves that the orbit of an element not in $2\mathbb{E}_8$ under $\mathrm{Aut}(\mathbb{E}_8) = W(\mathbb{E}_8)$ cuts both $\mathbb{D}_8$ and $\mathbb{E}_8 \smallsetminus \mathbb{D}_8$; consideration of reflections defined by minimal vectors $e \in \mathbb{E}_8 \smallsetminus \mathbb{D}_8$ quickly shows the required properties of transitivity.

A complete discussion of congruences modulo 3Λ between vectors of norm $N > 2m + m'$ involves the description of many possibilities. We shall nevertheless look closely at one of them, which on the one hand will be useful in the sequel, and on the other hand involves root systems of type $\boldsymbol{E}_8$.

We shall indeed consider congruences involving vectors x, $y \neq x$ and z such that $N(x) = N(y) = 2m + m''$, $y = x + 3z$ and $N(z) = m$. We thus have $N(x+z) = N(y-z) = m''$. We first state an identity, which properly belongs to the general theory of quadratic forms, and that we are going to use several times:

3.14. Lemma. *Let $x, z_1, \ldots, z_k$ ($k \geq 1$) be $r+1$ vectors of E. Then, the following identity holds:*

$$N(x+\sum_{i=1}^{k} z_i) = -(k-1)N(x)+\sum_{i=1}^{k} N(x+z_i)+(k-1)\sum_{i=1}^{k} N(z_i)-\sum_{1\leq i<j\leq k} N(z_i-z_j)\,.$$

Proof. Just develop both sides. □

3.15. Theorem. *Consider a system of $r+1$ vectors $y_0 = x, y_1, \ldots, y_r$ of norm $2m + m''$ such that $N(\frac{y_j - y_i}{3}) = m$ for all i, j with $0 \leq i < j \leq r$. Set $y_i = x + 3z_i$ for $i = 1, \ldots, r$. Then, one has $r \leq 8$, and equality holds if and only if $x + z_1 + z_2, z_1, \ldots, z_8$ generate a lattice isometric to $\sqrt{\frac{m}{2}}\,\mathbb{E}_8$. Moreover, we then have $m'' = 2m$, the 9 vectors $y_0, y_1, \ldots, y_8$ add to zero, and the set $\{\pm y_0, \ldots, \pm y_8\}$ is a configuration of type $\mathbb{A}_8^*$.*

Proof. One has $y_j - y_i = 3(z_j - z_i)$. Thus, the set $\{\pm z_i, \pm(z_i - z_j)\}$ is a system of type $\boldsymbol{A}_r$ (scaled to the norm m), whose corresponding Coxeter-Dynkin diagram may be obtained from the vectors $-z_1, z_2 - z_1, \ldots, z_{r-1} - z_r$.

By lemma 3.14, the vector $v = x + z_1 + z_2$ is of norm 4. Calculating the norm of $y_i - x$, we obtain successively equalities $x \cdot y_i = -\frac{5m}{2} + m''$ and $x \cdot z_i = -\frac{3m}{2}$, and then $v \cdot (-z_1) = 0$, $v \cdot (z_i - z_{i+1}) = 0$ if $i = 1$ or if $i \geq 3$ and $v \cdot (z_2 - z_3) = -\frac{m}{2}$ (because $z_i \cdot z_i = \frac{m}{2}$ for $i \neq j$). Thus, extending with v the previous diagram, we obtain a diagram of type $\boldsymbol{E}_{r+1}$. This is impossible if $r + 1 > 9$, for the corresponding quadratic form is then of signature $(r, 1)$, and may occur for $r + 1 = 9$ only if $v, z_1, \ldots, z_8$ are linearly dependent, for the quadratic form attached to E_9 is positive semi-definite of rank 8. When this is the case, the lattice generated by $v, z_1, \ldots, z_8$ is also generated by $v, z_1, \ldots, z_7$, whose Coxeter-Dynkin diagram is of type $\boldsymbol{E}_8$.

Consider now a linear relation $\lambda_1 z_1 + \cdots + \lambda_r z_r = \lambda x$. Taking the scalar products with $z_1, \ldots, z_r$ yields the linear system

$$2\lambda_i + \sum_{j \neq i} \lambda_j = -3\lambda$$

whose unique solution is $\lambda_1 = \cdots = \lambda_r = -\dfrac{3}{r+1}\lambda$. We thus must have $x = -\dfrac{3}{r+1}(z_1 + \cdots + z_r)$. Taking the norm of both sides, we first obtain the relation

$$2m + m'' = \frac{9r}{2(r+1)}\, m\,,$$

whence $m'' = 2m$ if $r = 8$, and then

$$y_0 + y_1 + \cdots + y_r = (r+1)x + 3(z_1 + \cdots + z_r) = 0\,.$$

Finally, we saw above that $y_0 \cdot y_i = x \cdot y_i = -\frac{5m}{2} + m''$, which implies the further equalities $y_i \cdot y_j = (x + 3z_i) \cdot (x + 3z_j) = -\frac{5m}{2} + m''$. The Gram matrix M of the system $(y_1, \ldots, y_r)$ has entries $2m + m''$ on the diagonal and $-\frac{5m - 2m''}{2}$ outside. When $m'' = 2m'$, M is proportional to the matrix with entries 8 on the diagonal and -1 outside, which is a standard Gram matrix for A_8^*. □

[Here is an alternative argument to the use of Coxeter-Dynkin diagrams. By lemma 3.14, the vectors $x + z_i + z_j$ and $x + z_i + z_j + z_k$ have norm m. Together with the z_i and $z_i - z_j$, we obtain $s_r = \binom{r}{3} + 2\binom{r}{2} + r = \frac{r(r+1)(r+2)}{6}$ vectors of norm m in the lattice generated by $x, z_1, \ldots, z_r$. But it is easily checked that s_r is strictly larger that $s(L)$ for any root lattice L of rank r if $r > 8$. We must thus have $r \leq 8$, and $L \sim \mathbb{E}_8$ when $r = 8$ since $s_8 = 120$.]

§ **4. Orbits and congruences in the Leech lattice.** We find in [ATLAS] a description of the orbits in the Leech lattice $\Lambda = \Lambda_{24}$ of all vectors of norm $N \leq 32$. (In the notation of [ATLAS], $\frac{N}{2}$ is the *type*.) We shall make use of it up to $N = 18$. Each orbit is written either as a $\mathbb{Z}$-linear combination $au_t + a'v_{t'}$ where the indices t, t' are the types of $u_t, v_{t'}$ and $u_t + v_{t'}$ is a vector $w_{t''}$ of type t'', or on the standard orthogonal frame made of vectors of norm 8. The first (resp. second) case occurs

for vectors which are congruent modulo 2 to a vector of norm 0, 4 or 6 (resp. to a vector of norm 8). In this last case, we shall provide a description in terms of short vectors. For instance, vectors of norm 8, since they constitute a single orbit, are the sums $e+f$ where e and f are orthogonal minimal vectors.

As we know, an exact system of representatives of non-zero classes modulo 2 is provided by one vector of norm 4 or 6 out of each pair $\pm x$ and one vector of norm 8 out of systems of 48 vectors lying on 24 pairwise orthogonal lines. Proposition 1.1 shows that vectors which are congruent modulo 2Λ have norms which are congruent modulo 4. Hence, a vector of $\Lambda \setminus 2\Lambda$ is congruent to a vector of norm 6 (resp. of norm 4 or 8) if its norm is congruent to 2 mod 4 (resp. to 0 mod 4).

We shall denote the orbits of vectors of norm m by a_m, b_m, etc., choosing the letter $a, b, \ldots$ in the order of the ATLAS. Thus, the first non-zero orbits are a_4, a_6, a_8, a_{10}, a_{12}, b_{12}, a_{14}, a_{16}, b_{16}, c_{16}, a_{18}, b_{18}, a_{20}, b_{20}, ... (The orbit a_{16} is the imprimitive orbit $2a_4$; for $m \geq 16$, there are at least two orbits of vectors of norm m.)

We are going to prove the following theorem:

4.1. Theorem. *Representatives of* $\Lambda/3\Lambda$ *may be found among vectors of norms up to* 18*, according to the weighted equality*

$$|a_4| + |a_6| + |a_8| + |a_{10}| + |a_{12}| + \frac{|b_{12}|}{3} + \frac{|a_{14}|}{2} + \frac{|b_{16}|}{9} + \frac{|b_{18}|}{36} = 3^{24} - 1\,.$$

The cardinality of any orbit in Λ is actually divisible by 65520 ([ATLAS], p. 181). One has $\dfrac{3^{24}-1}{65520} = \dfrac{38795266}{9}$. Dividing out by 65520 both sides of the formula in Theorem 4.1, we obtain the following explicit weighted formula:

$$3 + 256 + 6075 + 70656 + 518400 + \frac{6900}{3} + \frac{2861568}{2} + \frac{12295800}{9} + \frac{32972800}{36} = \frac{38795266}{9}\,; \tag{4.2}$$

the denominators 3, 9 and 36 in the left hand side correspond to configurations $\boldsymbol{A}_2 \sim \boldsymbol{A}_2^*$, $\boldsymbol{A}_8^*$ and $\boldsymbol{A}_2^{\perp 12} \sim \boldsymbol{A}_2^{*\perp 12}$ respectively, the second one being related to an $\boldsymbol{E}_8$ configuration contained in $S(\Lambda)$.

To prove Theorem 4.1, we shall examine which orbits are to be used to find representatives of $\Lambda/3\Lambda$ of minimal length, prove upper bounds for their weights, and verify that the left hand side of 4.2, which is a priori known not to be greater than the right hand side, is indeed equal to the right hand side.

No problem arises with vectors of norm 4, 6, 8, 10 which all represent distinct classes by Proposition 3.7. The first difficulty occurs for norm 12, where (Proposition 3.1) a vector may be congruent to 1 or 3 vectors having the same norm.

Now, by Theorem 1.3, a system (x, y, z) of vectors of norm 12 which are congruent modulo 3Λ is of the form $(e - f, e + 2f, -2e - f)$ where $e, f, e + f$ are minimal. Modulo 2Λ, these vectors are congruent to a vector of norm 4 (respectively, $e + f$, e, f). They thus belong to the orbit b_{12}. Conversely, given $x = u_2 + 2v_2 \in b_{12}$, $y = u_2 - v_2$ and $z = -2u_2 - v_2$ belong to b_{12} and are congruent to x modulo 3Λ.

Hence, the orbits a_{12} and b_{12} must be considered with the respective weights 1 and 3.

Let e, f, g be minimal vectors with $e \cdot f = e \cdot g = -1$ and $f \cdot g = 2$, e.g. $e_2, -e_1, e_9$ in the notation of 5.1 below. Set $x = e + f + g$, $y = e - f + g$ and $z = e + f - 2g$. We have $N(x) = 12$, $x \equiv y \mod 2\Lambda$, and $N(y) = 8$. Hence, x belongs to a_{12}. Moreover, we have $x \equiv z \mod 3\Lambda$ and $N(z) = 18$. Writing $z = u_3 + 2v_2$ with $u_3 = e + f$ and $v_2 = -g$, we see that z belongs to a_{18}. Otherwise stated, with the notation of section 1, we have $a_{18} \sim_3 a_{12}$. Hence, we need not consider a_{18}. (This shows that $|a_{12}|$ divides $|a_{18}|$; indeed, $\dfrac{|a_{18}|}{|a_{12}|} = 24$.)

Similarly, $u_3 + 2v_2 \in a_{10}$ is congruent to $u_3 - v_2$ of norm 16. Since $\dfrac{|c_{16}|}{|a_{10}|} = 2$ whereas $\dfrac{|b_{16}|}{|a_{10}|} = \dfrac{22275}{128}$ is not integral, we have $c_{16} \sim_3 a_{10}$ (and the two vectors of c_{16} which are congruent to $u_3 + 2v_2$ modulo 3Λ are $u_3 - v_2$ and $-2u_3 - v_2$).

Applying Propositions 3.10 and 3.12, we see that the number r of vectors $y \in S_{2m+m'} = S_{14}$ which are congruent modulo 3Λ to a given $x \in S_{14}$ cannot exceed $\left\lfloor \dfrac{2\,(2m + m')}{5m - 2m'} \right\rfloor = 3$. Any element of S_{14} may be written in the form $x = u_3 + 2v_2$. Now, this representation of x is unique:

$$u_3 + 2v_2 = u_3' + 2v_2' \Longrightarrow u_3' \equiv u_3 \mod 2\Lambda \Longleftrightarrow u_3' = \pm u_3\,;$$

then $u_3' = u_3 \Rightarrow (u_3', v_2') = (u_3, v_2)$ and $u_3' = -u_3 \Rightarrow v_2' = u_3 + v_2 \Rightarrow N(v_2') = 6$. We have $x = u_3 + 2v_2 \equiv y = u_3 - v_2 = (u_3 + v_2) + (-2v_2) \mod 3\Lambda$. The map $x \mapsto y$ defined by $(u_3, v_2) \mapsto (u_3 + v_2, -v_2)$ is an involution without fixed points of S_{14} which preserves congruences modulo 3Λ. Hence, r is even. Since r is at most 3, we have $r = 2$. Consequently, the orbit a_{14} must be considered with the weight 2.

4.3. Lemma. *The only vectors of norm $N \leq 18$ which are congruent modulo 3Λ to a shorter vector are those of the orbits a_{16}, c_{16}, a_{18}.*

Proof. We know by Proposition 3.7 that such a congruence may occur only for vectors of norm $N > 2m + m' = 14$, and we have previously proved equivalences $a_{16} \sim_3 0$, $c_{16} \sim_3 a_{14}$ and $a_{18} \sim_3 a_{12}$. We shall now prove that given y of norm $N = 16$ or $N = 18$, a congruence $y \equiv x \mod 3\Lambda$ with $N(x) < N(y)$ cannot hold unless y belongs to a_{16}, c_{16}, a_{18}.

By Proposition 1.1, we have $N(x) \equiv N(y) \mod 6$. Define δ by $N(y) - N(x) = 6\delta$. We have $N(z) \geq 4$, hence $\delta = 1$ or $\delta = 2$. By Proposition 1.1, for primitive y,

we have $N - 4\delta = 2N(x) + N(x+y) \geq 12$, hence $\delta \leq \dfrac{18-12}{4}$, i.e. $\delta = 1$, and we are left with the two possibilities:

(1) $N(y) = 16$, $N(x) = 10$, $N(z) = N(x+z) = 4$, $N(y-z) = 6$;
(2) $N(y) = 18$, $N(x) = 12$, $N(z) = 4$, $N(x+z) = 6$, $N(y-z) = 8$.

Now, if $N(y) = 16$ (resp. if $N(y) = 18$), $y = (x+z) + 2z$ is of the form $u_2 + 2v_2$ (resp. $u_3 + 2v_2$) with $u_2 = x + z$ (resp. $u_3 = x + z$) and $v_2 = z$, which proves that $y \in c_{16}$ (resp. that $y \in a_{18}$). $\square$

We are now faced with the problem of calculating the number of vectors in b_{16} and in b_{18} which are congruent modulo 3Λ to a vector of the same orbit. Evaluating the weighted sum of Theorem 4.1 on vectors of norm up to 14, we see that the complement to $3^{24} - 1$ is the sum $\frac{|b_{16}|}{9} + \frac{|b_{18}|}{36}$. It thus suffices now to prove the bounds $wt(b_{16}) \leq 9$ and $wt(b_{18}) \leq 36$.

For a pair (x, y) with $N(y) = N(x) = N \in \{16, 18\}$, we have by Proposition 1.1 $N(x+z) = N(y-z)$ and $2N(z) + N(x+z) = N$, which leaves a priori the four possibilities

(1) N=16, $N(z) = 6$, $N(x+z) = 4$;
(2) N=16, $N(z) = 4$, $N(x+z) = 8$;
(3) N=18, $N(z) = 6$, $N(x+z) = 6$;
(4) N=18, $N(z) = 4$, $N(x+z) = 10$;

the first one must be rejected, since we have $y \equiv x + z \mod 2\Lambda$ and the vectors of b_{16} are not congruent modulo 2Λ to a vector of norm 4.

Because of the congruence modulo 2 above, all the hypotheses of Theorem 3.15 are fulfiled. This proves the first upper bound $wt(b_{16}) \leq 9$, from which the structure of the sets of vectors which are congruent modulo 3Λ will follow once the equality $wt(b_{16}) = 9$ is proved.

The proofs of Theorem 4.1 and formula 4.2 now reduce to the inequality $wt(b_{18}) \leq 36$. We thus finally consider a vector $x \in b_{18}$ and look for systems of vectors $y_1, \ldots, y_r \equiv x \mod 3\Lambda$, writing as above $y_i = x + 3z_i$ and $y_0 = x$; we must prove that $r + 1$ is bounded above by 36.

We consider now more generally a lattice of dimension n whose first three non-zero norms are $m = 4$, $m' = 6$ and then some number $m'' > 7$, and a vector x of norm 18 in Λ such that any $y \equiv x \mod 3\Lambda$ is of norm $N \geq 18$, and we look for systems of vectors $y_1, \ldots, y_r \equiv x \mod 3\Lambda$ of norm 18, writing as previously $y_i = x + 3z_i$ and $y_0 = x$.

4.4. Theorem. *Under the hypotheses above, the set $T(x)$ of vectors of norm 18 which lie in the class of x in $\Lambda/3\Lambda$ contains at most $\lfloor \frac{3n}{2} \rfloor$ pairs $\pm x$, and if equality holds, $\pm T(x)$ contains a root system of type $\frac{n}{2}\boldsymbol{A}_2$ when n is even, and $\frac{n-1}{2}\boldsymbol{A}_2 + \boldsymbol{A}_1$ when n is odd. Moreover, $S_6(\Lambda)$ then contains a root system of the same type, and the set $\pm T(x)$ is the second layer of the lattice they generate.*

Proof. The result is obvious if $n \leq 2$. We shall prove the general statement by induction.

By Proposition 1.1, we have $N(x+z_i) = N(y-z_i)$ and $2N(z_i) + N(x+z_i) = N(x) = 18$ for all i. Given an index i, we are left with the following two possibilities:

(1) $N(z_i) = 4$, $N(x+z_i) = 10$, or
(2) $N(z_i) = N(x+z_i) = 6$,

for $N(z_i) \geq m''$ implies $N(x+z_i) \leq 18 - 2m'' \leq 2 < m$.

The transposition $x = y_0 \leftrightarrow y_i$ transforms z_i into $-z_i$ and z_j into $z_j - z_i$ for $j \neq i$. This proves that all vectors of the set $\mathcal{S} = \{\pm z_i, \pm(z_j - z_k)\}$ are of norm 4 or 6 and that $\mathcal{S}$ is invariant under the permutations of $y_0, y_1, \ldots, y_r$.

If all vectors of $\mathcal{S}$ are of norm 4, $\mathcal{S}$ is a root system of type $\boldsymbol{A}_r$, hence of rank r. There are thus at most $r+1 \leq n+1$ elements in the class of x modulo 3Λ, whence the result in this case, since $n+1 \leq \frac{3n}{2}$ for $n \geq 2$.

We now suppose that $\mathcal{S}$ contains at least one vector of norm 6. Under a convenient permutation of $y_0, \ldots, y_r$, this vector can be transformed into z_1. We have $y_1 = x + 3z_1$ and $N(y_1) = N(x)$, hence $x \cdot z_1 = -\frac{9}{6} N(z_1) = -9$, whence $x \cdot y_1 = x \cdot x + 3x \cdot z_1 = -9$. This shows that x, y_1 and $y' = -x - y_1$ are three minimal vectors with sum 0 in a hexagonal lattice of norm 18. But we have

$$y' = -2x - 3z_1 \equiv x \mod 3\Lambda\,,$$

which implies that y' is some y_i, say $y' = y_2$. We thus have $-2x - 3z_1 = x + 3z_2$, i.e. $x = -z_1 - z_2$, whence $z_1 \cdot z_2 = 3$, which shows that $\pm z_1, \pm z_2, \pm(z_1 - z_2)$ are the minimal vectors of a hexagonal lattice contained in $S_6(\Lambda)$ whose second layer is $\{\pm y_0, \pm y_1, \pm y_2\}$.

We now apply lemma 3.15 to a system (x, z_i, z_j) first with $N(z_i) = N(z_j) = 6$, and then with $N(z_i) = 6$, $N(z_j) = 4$. In the first case, we obtain $N(x + z_i + z_j) = 6 - N(z_i - z_j) \leq 2$, hence $N(x + z_i + z_j) = 0$, i.e. $x = -z_i - z_j$. This shows that there are at most two vectors z_ℓ of norm 6, for if $N(z_k) = 6$, we also have $x = -z_i - z_k$, i.e. $z_j = z_k$. Next, if $N(z_i) = 6$ and $N(z_4) = 4$, then$N(x + z_i + z_j) = 8 - N(z_i - z_j)$. We have $4 \leq N(z_i - z_j) \leq 6$, hence $2 \leq N(x + z_i + z_j) \leq 4$, and finally $N(x + z_i + z_j) = N(z_i - z_j) = 4$. We deduce successively from the last equality the following equalities $z_i \cdot z_j = 3$, $x \cdot z_j = -6$ (because $N(x+3z_j) = N(x)$), $x \cdot y_j = x \cdot x + 3x \cdot z_j = 0$ and $y_i \cdot y_j = x \cdot x + 3x \cdot z_i + 3x \cdot z_j + 9 z_i \cdot z_j = 0$.

The fact that the last two scalar products are zero shows that the hexagonal lattice generated by $y_0 = x, y_1, y_2 = x - y_1$ is orthogonal to $y_3, \ldots, y_r$. By the induction hypothesis, the number of elements in the class of x in $\Lambda/3\Lambda$ is at most $3 + \lfloor \frac{3(n-2)}{2} \rfloor = \lfloor \frac{3n}{2} \rfloor$. Moreover, when equality holds, we can factor out in the set $\{\pm y_0, \ldots, \pm y_r\}$ a direct sum of root systems $\boldsymbol{A}_2$ (scaled to norm 18) until we reach a system $\{z_i, z_j - z_k\}$ $(1 \leq i \leq t)$ without any vector of norm 6, for which the bound $\lfloor \frac{3n}{2} \rfloor$ is not attained unless $t \leq 1$. □

§ **5. Applications.** The set of sublattices L of a given lattice Λ such that Λ/L is cyclic of order d is in one-to-one correspondence with the set of elements of order

d in $\Lambda^*/d\Lambda^*$ modulo the operation of $(\mathbb{Z}/d\mathbb{Z})^*$, via the map

$$e \in \Lambda^* \mapsto L = \{x \in \Lambda \mid x \cdot e \equiv 0 \mod d\}.$$

For reasons of complexity, it is important to represent the classes of $\Lambda^* \mod d\Lambda^*$ by vectors which are as short as possible. (For the same reason, it is better to use Λ^* rather than Λ, even if an explicit isomorphism $\Lambda/d\Lambda \simeq \Lambda^*/d\Lambda^*$ is known.)

If we want to consider L only up to isometry, it is important to know the orbits of $\mathrm{Aut}(\Lambda)$ acting on $\Lambda/d\Lambda$, for it then suffices to consider one vector per orbit and to test the corresponding lattices for isometry.

For $\mathbb{E}_8$ (which is unimodular), there is exactly one primitive orbit for each norm $2, 4, 6, 8$. Using for $d = 2$ and $d = 3$ the description of $\Lambda/d\Lambda$ that we have found above, we see that $\mathbb{E}_8$ contains exactly 2 (resp. 4) isometry classes of lattices of index $d = 2$ (resp. $d = 3$). For $d = 2$, these lattices must be the root lattices $\mathbb{A}_1 \perp \mathbb{E}_7$ and $\mathbb{D}_8$; they are attached respectively to vectors of norm 2 (by definition of $\mathbb{E}_7$) and 4. For $d = 3$, there again correspond root lattices to vectors of norm 6 and 8, namely $\mathbb{A}_2 \perp \mathbb{E}_6$ and $\mathbb{A}_8$; lattices attached to vectors of norm 2 and 4 are not root lattices, as there root systems ($\boldsymbol{E}_7$ and $\boldsymbol{D}_7$ respectively) are only of rank 7.

We now turn to the case of the Leech lattice $\Lambda = \Lambda_{24}$. Explicit computations have been done on the *PARI* system, with the help of programs written by Batut and of its Gram matrix of a basis $(e_1, \ldots, e_{24})$ of Λ calculated from Eva Bayer's construction of Λ_{24} over the ring $\mathbb{Z}[\zeta_{35}]$. The entries $a_{i,j}$ of A solely depend on the differences $|j - i|$; thus, A is well defined by its first row, which is

(**5.1**) $\quad [4, 1, -1, 0, 0, 0, 1, -1, -2, -1, -1, -1, 1, 1, -1, -1, 1, 2, 2, 1, -1, -1, 1, 1].$

Representatives of all orbits up to the norm 18 can be chosen as follows: $a_4 : e_1$; $a_6 : e_1 - e_2$; $a_8 : e_1 + e_4$; $a_{10} : e_1 + e_2$; $a_{12} : e_1 + e_3 + e_8$; $b_{12} : e_1 - e_9$; $a_{14} : e_1 + e_2 + e_5$; $a_{16} : 2e_1$; $b_{16} : e_1 - 2e_2$; $c_{16} : e_1 + e_4 + 2e_9$; $a_{18} : e_1 - e_2 - 2e_7$; $b_{18} : e_1 + e_2 + 2e_{11}$.

The three sublattices of index 2 inside the Leech lattice $\Lambda = \Lambda_{24}$ were considered by Bachoc and Batut (see [M], Chapter V, Theorem 7.9). By Theorem 4.1, there are 9 sublattices of index 3. We give below the invariants $s = s(L)$ and $s^* = s(L^*)$ and the value $N^* = N(L')$ of the twelve lattices of index 2 or 3 in $\Lambda = \Lambda_{24}$ (given an integral lattice M, we denote by M' the lattice $\sqrt{a}\, M^*$ where a is the annihilator of M^*/M), which we characterize by their index p and the orbit o such that L is isometric to the orthogonal modulo p in Λ_{24} of a vector $e \in o$. One has $\det(L) = p^2$, and the Smith invariant of L (i.e., the system of elementary divisors of L^*/L) is (p, p) if $p \mid N(e)$ and (p^2) otherwise.

[Given an integral lattice Λ of norm m, a prime p which does not divide $\det(\Lambda)$ and a vector $e \in \Lambda \setminus p\Lambda$, let $\Lambda_{e,p} = \{x \in \Lambda \mid e \cdot x \equiv 0 \mod p\Lambda\}$; we have $\Lambda^*_{e,p} = \langle \Lambda^*, \frac{e}{p} \rangle$. Since Λ^*/Λ is of order prime to p, the p-component of $\Lambda^*_{e,p}/\Lambda_{e,p}$ is of order p^2 and is generated by

the class of $\frac{e}{p}$ and that of any element of $\Lambda \setminus \Lambda_{e,p}$. Clearly, $p\,\frac{e}{p} = e$ belongs to $\Lambda_{e,p}$ if and only if $e \cdot e \equiv 0 \mod p$. This proves that $\Lambda^*_{e,p}/\Lambda_{e,p}$ is non-cyclic if and only if $N(e) \equiv 0 \mod p$.]

Index 2.

a_4	$s = 51176$	$s^* = 1$	$N^* = 2$
a_6	$s = 49128$	$s^* = 1$	$N^* = 3$
a_8	$s = 49128$	$s^* = 24$	$N^* = 4$

Index 3.

a_4	$s = 46575$	$s^* = 1$	$N^* = 4$
a_6	$s = 38502$	$s^* = 1$	$N^* = 2$
a_8	$s = 34938$	$s^* = 1$	$N^* = 8$
a_{10}	$s = 33453$	$s^* = 1$	$N^* = 10$
a_{12a}	$s = 32913$	$s^* = 1$	$N^* = 4$
a_{12b}	$s = 33399$	$s^* = 3$	$N^* = 4$
a_{14}	$s = 32751$	$s^* = 2$	$N^* = 14$
a_{16b}	$s = 32724$	$s^* = 9$	$N^* = 16$
a_{18b}	$s = 32670$	$s^* = 36$	$N^* = 6$

The values of s^* and of N^* found above have the following interpretation: with the previous notation e, p, $\frac{e}{p}$ is a minimal vector of $\Lambda^*_{e,p}$, which implies that s^* is the weight of the orbit of e and that $N^* = \frac{N(e)}{p}$ if $p \mid N(e)$ and $N^* = N(e)$ otherwise.

5.2. Remark. The systems of 36 vectors of norm 18 with configuration $12\,\boldsymbol{A}_2$ plays for $p = 3$ the rôle that play the orthogonal frames of norm 8 for $p = 2$. This analogy could be made closer by considering the Leech lattice as a 12-dimensional module over the rings of Gaussian or Eisenstein integers.

5.3. Remark. By making use of Jacobi theta series to evaluate the repartition of the values of scalar products among vectors of norm $N \leq 18$ in the Leech lattice, C. Bachoc ([Ba]) was able to prove directly that one needs to consider exactly norms up to 18 to obtain the shortest representatives of the Leech lattice modulo 3. Putting the orbit structure in her machinery yields quickly 4.2 and 4.3. One cannot deduce directly from her method the structure of the sets of congruent vectors in each orbit (i.e., the occurrence of configurations $\boldsymbol{A}_2, \boldsymbol{E}_8, \boldsymbol{A}_8^*, 12\boldsymbol{A}_2$). However, these results might well follow from a more detailed study of the sets of scalar products.

APPENDIX : ON LATTICES OF MINIMUM 3

A.1. Theorem. *Let Λ be a well rounded lattice of norm 3. Then, the classes of $\Lambda/2\Lambda$ cannot be represented by vectors of norm $N \leq 2\,N(\Lambda) = 6$, except if Λ is one*

of the five lattices defined up to isometry by one of the following Gram matrices:

$$M_1 = (3)\,, \quad M_2 = \begin{pmatrix} 3 & 1 \\ 1 & 3 \end{pmatrix}\,, \quad M_2' = \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}\,,$$

$$M_3 = \begin{pmatrix} 3 & 1 & 1 \\ 1 & 3 & -1 \\ 1 & -1 & 3 \end{pmatrix}\,, \quad M_3' = \begin{pmatrix} 3 & 1 & 1 \\ 1 & 3 & 0 \\ 1 & 0 & 3 \end{pmatrix}\,, \quad \text{or} \quad M_4 = \begin{pmatrix} 3 & 0 & 1 & 1 \\ 0 & 3 & 1 & 1 \\ 1 & 1 & 3 & 0 \\ 1 & 1 & 0 & 3 \end{pmatrix}\,.$$

The lattice M_3 is similar to $\mathbb{A}_3^*$. The inclusions between the lattices above are $M_1 \subset M_2 \subset M_3$ and $M_1 \subset M_2' \subset M_3' \subset M_4$.

The proof is not really difficult, but needs somewhat tedious verifications of various details. For this reason, I do not give it, and refer the reader to my home page *http://math.u-bordeaux.fr/~martinet*.

REFERENCES

[ATLAS] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, R. A. Wilson, *ATLAS of Finite Groups*, Oxford Univ. Press, Oxford, 1985.

[Ba] C. Bachoc, *Private communication, 1999.*

[Bt-M] C. Batut, J. Martinet, *Tables of perfect lattices*, http://math.u-bordeaux.fr/~martinet.

[C-S] J. H. Conway, N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, Springer-Verlag, Grundlehren n°290, Heidelberg, 1988, (further editions: 1993, 1999).

[C-S1] J.H. Conway, N.J.A. Sloane, *Low-dimensional lattices. III. Perfect forms*, Proc. Royal Soc. London **A 418** (1988), 43–80.

[M] J. Martinet, *Les réseaux parfaits des espaces euclidiens*, Masson, Paris, 1996, (new editor: Dunod, Paris).

[M1] J. Martinet, *Une famille de réseaux dual-extrêmes*, J. Théor. Nombres Bordeaux **9** (1997), 169–181.

J. MARTINET
A2X, INSTITUT DE MATHÉMATIQUES
UNIVERSITÉ BORDEAUX 1
351, COURS DE LA LIBÉRATION
F–33405 TALENCE CEDEX

E-MAIL : MARTINET@MATH.U-BORDEAUX.FR