ON PARITY CLASSES

JACQUES MARTINET

Abstract. This paper deals with various problems in lattice theory related to the notion of parity.

Résumé. *Sur les classes de parité.* Nous considérons dans cet article divers problèmes de la théorie des réseaux liés à des questions de parité.

1. Introduction.

Recall that given an n-dimensional unimodular lattice Λ, a *parity* or *characteristic vector* is a vector e such that $\forall\, x \in \Lambda$, $e \cdot x \equiv x \cdot x \mod 2$. The set of parity vectors is a union of classes modulo 2Λ. Two theorems play a key rôle in the theory of unimodular lattices:

(1) $N(e) \equiv n \mod 8$;

(2) (Elkies) The smallest norm of a parity vector is at most n, and equality holds uniquely on the $\mathbb{Z}^n$ lattice.

Actually, we shall see that parity vectors may be defined for all integral lattices. More precisely, we shall define in Sections 2 and 3 **the** *parity class* in the dual lattice and *parity class***es** in the lattice itself. The aim of this paper is to prove various results on these vectors and their classes.

We recall various preliminary results in Section 2 and then consider in Section 3 parity vectors in Λ. Section 4 is devoted to various examples. In section 5, we explain how to construct from a given lattice a larger one having a smaller determinant. These technical results are then applied in Section 6 to study the norm modulo 8 of parity classes for lattices whose determinants are not divisible by 4. Finally, 2-modular lattices are considered in Section 7.

---

keywords: Integral quadratic forms, characteristic (parity) vectors

2000 Mathematics Subject Classification: 11H55, 11H56 .

Laboratoire A2X, UMR 5465 associée au C.N.R.S. & Université Bordeaux 1

A first draft of these notes was written after postdoctoral lectures delivered in Bordeaux during the winter semester 1999-2000. I thank Eva Bayer and the *EPFL (École Polytechnique Fédérale de Lausanne)* for their one-month invitation (May, 2003), which gave me the opportunity of considerably improving my previous notes.

As far as we only consider congruences, there is no need to restrict oneself to positive definite forms. Hence, unless otherwise stated, we shall use the word *lattice* in the more general sense we are going to define. Of course, for Euclidean lattices, to estimate the smallest possible norm on a given parity class (as in Elkies's theorem quoted above) is a very interesting problem, but that we shall not anymore consider in these notes; see [El1], [El2] and [N-V].

In the whole paper, we denote by V a finite-dimensional vector space over the field $\mathbb{Q}$ of rational numbers, equipped with a non-degenerate symmetric bilinear form $(x,y) \mapsto x \cdot y$, that we call the *scalar product on* V even when it is not positive definite. The *norm of* $x \in V$ is $N(x) = x \cdot x$. A *lattice in* V is then a finitely generated Z-module Λ of rank (or dimension) n in V. We say that Λ is *integral* if the scalar product takes only integral values on V, and *primitive* if it generates $\mathbb{Z}$. Given a basis $\mathcal{B} = (e_1, \dots, e_n)$ for Λ over $\mathbb{Z}$, the *Gram matrix of* $\mathcal{B}$ is $\mathrm{Gram}(\mathcal{B}) = \big(e_i \cdot e_j\big)$, and the *determinant of* Λ is $\det(\Lambda) = \det(\mathrm{Gram}(\mathcal{B}))$ where $\mathcal{B}$ is an arbitrary basis for Λ. We say that Λ is *unimodular* if it is integral of determinant ± 1.

We denote by (p,q) the signature of the quadratic form $x \mapsto N(x)$. It is the signature of the real quadratic space $E = \mathbb{R} \bigotimes_{\mathbb{Q}} V$. Of course, $p + q = n$, and if $q = 0$, E is a Euclidean vector space and the lattices naturally embed in E as classical Euclidean lattices. For any non-zero $\lambda \in \mathbb{Q}$, we denote by ${}^{\lambda}\Lambda$ the rescaled lattice Λ with scalar product $\lambda(x \cdot y)$. We write ${}^{-1}\Lambda = \Lambda^-$, and sometimes $\Lambda^+ = \Lambda$. The signature of ${}^{\lambda}\Lambda$ is (p,q) or (q,p), depending on the sign of λ.

2. Preliminaries.

We first recall the definition of elementary divisors (which does not make use of the scalar product). Given lattices Λ and $\Lambda' \supset \Lambda$ in V, the *elementary divisors of the pair* (Λ', Λ) are the positive integers $a_1, \dots, a_n$ uniquely defined by the two conditions:

(1) There exist bases $\mathcal{B}' = (e'_1, \dots, e'_n)$ for Λ' and $\mathcal{B} = (e_1, \dots, e_n)$ for Λ such that $e_i = a_i\, e'_i$ for $i = 1, \dots, n$ (we say that $\mathcal{B}$ is a *Smith basis for* (Λ', Λ));
(2) a_{i+1} divides a_i for $i = 1, \dots, n-1$.

We have $a_1 \cdots a_n = [\Lambda' : \Lambda]$, since Λ'/Λ is the direct sum of the cyclic groups $\mathbb{Z}/a_i\mathbb{Z}$.

Elementary divisors are indeed defined over any principal ideal domain (where one must considers the ideals (a_i) rather than the elements a_i), and in particular over localization of such rings, a very useful point of view (which yields in particular a quick definition over arbitrary Dedekind domains). In our situation, they are defined over $\mathbb{Z}_{(\ell)}$ for all primes ℓ, and are of the form $\ell^{m_i(\ell)}$, with $m_1(\ell) \geq \cdots \geq m_n(\ell)$. We have $m_i(\ell) = v_\ell(a_i)$. Disregarding the ordering of the exponents, the local invariants of direct sums are obtained by concatenation from those of the components.

The existence of a scalar product allows us to attach to any lattice Λ its *dual lattice*

$$\Lambda^* = \{x \in V \mid \forall\, y \in \Lambda,\, x \cdot y \in \mathbb{Z}\}\,.$$

The lattice Λ is integral if and only if it is contained in its dual and unimodular if and only if it is equal to its dual. Consequently, taking $\Lambda' = \Lambda^*$, we may attach to any integral lattice the set of elementary divisors of the pair (Λ^*, Λ):

Definition 2.1. The *Smith invariant* (also called the *group determinant*) *of an integral lattice* Λ, denoted by $\mathrm{Smith}(\Lambda)$, is the n-tuple $(a_1, \dots, a_n)$ of the elementary divisors of (Λ^*, Λ). The first term a_1 of $\mathrm{Smith}(\Lambda)$ (the annihilator of Λ^*/Λ) is called the *level of* Λ.
Warning. One sometimes consider for <u>even</u> lattices a more restrictive notion of a level, for which we require that the level N is such that $N\,\Lambda^*$ should be even. We then have $N = a_1$ or $N = 2a_1$.

Note that the last term a_n is the gcd of the $x \cdot y$, $x, y \in \Lambda$; it is equal to 1 if and only if Λ is primitive. Note also the formula $\mathrm{Smith}({}^\lambda\Lambda) = \lambda\, \mathrm{Smith}(\Lambda)$ which applies for all $\lambda \in \mathbb{Q}$ with $\lambda\, a_n \in \mathbb{Z}$, and the *reciprocity formula*

$$\mathrm{Smith}(a_1\Lambda^*) = \left(\frac{a_1}{a_n}, \dots, \frac{a_{n-1}}{a_n}, 1\right).$$

Lemma 2.2. *Let* Λ *be an integral lattice with Smith invariant* $(a_1, \dots, a_n)$*, and let* $\mathcal{B} = (e_1, \dots, e_n)$ *be a Smith basis for* (Λ^*, Λ)*, with dual basis* $\mathcal{B}^* = (e_1^*, \dots, e_n^*)$*. Then* $(a_1\, e_1^*, \dots, a_n\, e_n^*)$ *is a basis for* Λ*, namely the dual basis of the basis* $(e_1' = a_1^{-1} e_1, \dots, e_n' = a_n^{-1} e_n)$ *for* Λ^*.

Proof. By definition of a Smith basis, the vectors $e_i' = a_i^{-1} e_i$ constitute a basis for Λ^*, and we have $(a_i e_i^*) \cdot e_j' = \frac{a_i}{a_j}\, \delta_{i,j} = 1$. □

Next we say a few words about sublattices (of finite index).

Let $a \geq 2$ be an integer. We consider the set $\mathcal{E}_a$ of submodules M of Λ such that Λ/M is cyclic of order a. An isomorphism $\Lambda/M \to \mathbb{Z}/a\mathbb{Z}$ can be lifted first to a surjective homomorphism $\overline{\varphi} : \Lambda \to \mathbb{Z}/a\mathbb{Z}$ with kernel M, then to a homomorphism $\varphi : \Lambda \to \mathbb{Z}$, and two such homomorphisms φ, ψ define the same lattice M if and only if $\psi = b\varphi$ for some $b \in (\mathbb{Z}/a\mathbb{Z})^\times$. We have thus constructed a bijection

$$\mathcal{E}_a \to (\mathbb{Z}/a\mathbb{Z})^\times \backslash \operatorname{Hom}_{\text{onto}}(\Lambda, \mathbb{Z}/a\mathbb{Z})\,.$$

Now φ is of the form $x \mapsto e \cdot x$ for some $e \in \Lambda^* \smallsetminus \cup_{\ell | a} \ell\Lambda^*$ (ℓ prime). Finally, we obtain the following description of $\mathcal{E}_a$:

Proposition 2.3. *The map which to $e \in \Lambda^*$ attaches the kernel of $x \mapsto e \cdot x \mod a$ defines a one-to-one correspondence between the set of orbits of primitive elements in $\Lambda^*/a\Lambda^*$ under the action of $(\mathbb{Z}/a\mathbb{Z})^\times$ on the one hand, and the set $\mathcal{E}_a$ of submodules M of Λ such that Λ/M is cyclic of order a on the other hand. In particular, sublattices of index 2 in Λ are parametrized by $\Lambda^* \mod 2\Lambda^*$.* □

Let Λ be an integral lattice. Then the map

$$\Lambda \to \mathbb{Z}/2\mathbb{Z} \,:\, x \mapsto N(x) \mod 2$$

is clearly a homomorphism. Hence there exists $e \in \Lambda^*$, well-defined modulo $2\Lambda^*$, such that

$$\forall\, x \in \Lambda,\ N(x) \equiv e \cdot x \mod \Lambda\,.$$

Definition 2.4. A vector e as above is called a *dual-parity vector for* Λ and its class modulo 2 **the** *dual-parity class for* Λ.

Proposition 2.5. *Let $\mathcal{B} = (e_1, \dots, e_n)$ be a basis for Λ and let $\mathcal{B}^* = (e_1^*, \dots, e_n^*)$ be its dual basis. Then $e = \sum_j N(e_j)\, e_j^*$ is a dual-parity vector for Λ. Moreover, if $\mathcal{B}$ is a Smith basis for (Λ^*, Λ), then e belongs to Λ.*
[We could as well have chosen $e' = \sum_{i \le t_2} N(e_i)\, e_i^*$ instead of e.]

Proof. Let $x = \sum \lambda_j\, e_j \in \Lambda$. We have

$$N(x) = \sum_i \lambda_i^2\, N(e_i) + 2 \sum_{i<j} \lambda_i \lambda_j\, e_i \cdot e_j \equiv \sum_i \lambda_i\, N(e_i) \mod 2$$

on the one hand, and $e \cdot e_i = N(e_i)$, hence $e \cdot x = \sum_i \lambda_i\, N(e_i)$ on the other hand. This proves the first assertion.

If $\mathcal{B}$ is a Smith basis for (Λ^*, Λ), then $N(e_i) = e_i \cdot (a_i\, e_i') = a_i (e_i \cdot e_i')$ is divisible by a_i for all i. Hence $e = \sum_j \frac{N(e_j)}{a_j}\, (a_j\, e_j^*)$ belongs to Λ by Lemma 2.2. □

Corollary 2.6. *Dual-parity vectors for an orthogonal sum $\Lambda_1 \perp \Lambda_2$ are the sums $e_1 + e_2$ where e_i is a dual-parity vector for Λ_i.* □

If Λ is unimodular, the definition above is the usual one. More generally, if $\det(\Lambda)$ is odd, the inclusion $\Lambda \hookrightarrow \Lambda^*$ induces an isomorphism

$\Lambda/\Lambda^2 \simeq \Lambda^*/\Lambda^{*2}$, and we easily define a unique parity class in Λ. We shall consider in the next section lattices with an arbitrary determinant.

3. General parity classes.

In this section, Λ denotes an integral lattice.

Definition 3.1. For a prime ℓ, let $t_\ell = t_\ell(\Lambda)$ be the number of components of $\mathrm{Smith}(\Lambda)$ which are divisible by ℓ.

With the notation of Section 2, ℓ divides a_i for $i \le t_\ell$ but not for $i > t_\ell$, i.e. $e_i \in \ell\Lambda^* \iff i \le t_\ell$.

Proposition 3.2. (1) $t_\ell(\Lambda) = n - \dim_{\mathbb{F}_\ell}(\Lambda \cap \ell\Lambda^*)/\ell\Lambda$.

(2) *The difference $n - t_\ell(\Lambda)$ is also equal to the rank of the $\mathbb{F}_\ell$-bilinear form $(x, y) \mapsto x \cdot y \mod \ell$ on $\Lambda/\ell\Lambda$.*

Proof. With the notation of Section 2, ℓ divides a_i for $i \le t_\ell$ but not for $i > t_\ell$, i.e. $e_i \in \ell\Lambda^* \iff i \le t_\ell$. The first assertion follows, since $e_i \in \ell\Lambda^* \iff i \le t_\ell$. For $x \in \Lambda$, we have

$$\forall\, y \in \Lambda,\ x \cdot y \equiv 0 \mod \ell \iff \forall\, y \in \Lambda,\ (\frac{x}{\ell}) \cdot y \in \mathbb{Z} \iff \frac{x}{\ell} \in \Lambda^*,$$

hence $(\ell\Lambda^* \cap \Lambda)/\ell\Lambda$ is the kernel of the scalar product modulo ℓ. □

Definition 3.3. We say that Λ is *even* if all its vectors have even norms, and that it is *odd* otherwise. The kernel of the map $x \mapsto N(x) \mod 2$ is called the *even part of* Λ and denoted by Λ_{even}. We say that a vector $e \in \Lambda$ is a *parity* or *characteristic vector for* Λ if $\forall\, x \in \Lambda,\ N(x) \equiv e \cdot x \mod 2$. The class $\mod 2\Lambda$ of e is its *parity class*. [Clearly, if e is a parity vector, all the vectors in its class $\mod 2\Lambda$ also are parity vectors.]

The following proposition is well-known.

Proposition 3.4. *If Λ is even, $t_2 \equiv n \mod 2$.*

Proof. The bilinear form $(x, y) \mapsto x \cdot y \mod 2$ on $\Lambda/2\Lambda$ is alternating, hence has even rank, and we may apply Proposition 3.2. (More precisely, the form $x \cdot y$ mod 2 comes from the quadratic form $x \mapsto \frac{1}{2}\, N(x)$ mod 2.) □

Theorem 3.5. *The set of parity classes of Λ is an affine space of dimension $t_2(\Lambda)$ over $\mathbb{F}_2$. In particular, Λ contains $2^{t_2}(\Lambda)$ parity classes.*

Proof. First Proposition 2.5 shows that the set $\mathcal{P}$ of parity vectors is not empty. Let $e \in \mathcal{P}$. Then

$$f \in \mathcal{P} \iff \forall\, x \in \Lambda,\ (f - e) \cdot x \equiv 0 \mod 2 \iff f - e \in 2\Lambda^*\,.$$

This shows that the map

$$2\Lambda^* \cap \Lambda \to \mathcal{P}\ :\ x \mapsto e + x$$

induces on $\mathcal{P}$ mod 2 a structure of affine space over the $\mathbb{F}_2$-vector space $(\Lambda^* \cap \Lambda)/2\Lambda$, whose dimension is precisely $t_2(\Lambda)$. □

We now consider the norm of classes modulo a prime, and in particular those of parity classes.

Given a subset $\mathcal{E} \subset \Lambda$ and an integer q, we say that the norm of $\mathcal{E}$ is *defined modulo* q if for any two elements x, y of $\mathcal{E}$, we have $N(x) \equiv N(y) \mod q$.

Proposition 3.6. *Let ℓ be a prime, and let $\mathcal{C}$ be a class modulo ℓ.*

(1) *If ℓ is odd, the norm of $\mathcal{C}$ is defined modulo ℓ; it is defined modulo ℓ^2 if and only if $\mathcal{C} \subset \ell\Lambda^*$.*
(2) *If $\ell = 2$, the norm of $\mathcal{C}$ is defined modulo 4; it is defined modulo 8 if and only if $\mathcal{C}$ is a parity class.*

Proof. Let x, $y \in \mathcal{C}$, say, $y = x + \ell z$. Then

$$N(y) - N(x) = \ell\,(2\,(x \cdot z) + \ell\,N(z))\,.$$

This shows that the norm on $\mathcal{C}$ is well-defined modulo ℓ, and that if ℓ is odd, it is defined modulo ℓ^2 if and only if $x \cdot z \equiv 0 \mod \ell$ for all $z \in \Lambda$. This proves the first assertion.

If $\ell = 2$, the identity above can be written

$$N(y) - N(x) = 4(x \cdot z + N(z))\,,$$

which shows that the congruence $N(y) \equiv N(x) \mod 8$ holds if and only if $\forall\, z \in \Lambda$, $x \cdot z \equiv N(z) \mod 2$, which is the definition of x being a parity vector. □

The following lemma, which is needed to state Theorem 3.8 below, will be a consequence of the more precise statements of this theorem.

Lemma 3.7. *All parity vectors of Λ have the same norm modulo 2.*

Proof. Indeed, if e and e' are parity vectors, we have $N(e) \equiv e \cdot e' \mod 2$ and $N(e') \equiv e \cdot e' \mod 2$ as well. □

Theorem 3.8. *Set $\widetilde{\Lambda} = \Lambda_{even}$, $t = t_2(\Lambda)$ and $\tilde{t} = t_2(\widetilde{\Lambda})$.*

(1) *We have $\tilde{t} - t = 0$, 1 or 2.*
(2) *We have $\tilde{t} = t$ if Λ is even, $\tilde{t} = t + 1$ if both Λ and the norms of parity vectors are odd, and $\tilde{t} = t + 2$ if Λ is odd and parity vectors have even norms.*
(3) *Define $A(\Lambda) = A$ by $A = \{0\}$ if $\tilde{t} = t$, $A = \mathbb{Z}/4\mathbb{Z}$ if $\tilde{t} = t + 1$, and $A = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ if $\tilde{t} = t + 2$. Then $\widetilde{\Lambda}^*/\widetilde{\Lambda} \simeq (\Lambda^*/\Lambda) \bigoplus A$.*
(4) *The common norm modulo 2 of parity vectors is $N = n + t$.*

Proof. (1) If M and $L \supset M$ are integral lattices, we have $M \subset L \subset L^* \subset M^*$. Since the canonical maps $L^*/M \to L^*/L$ and $L^*/M \to M^*/M$ are respectively surjective and injective, we have between the 2-ranks r_2 of these groups the inequalities $r_2(L^*/L) \le r_2(L^*/M) \le r_2(M^*/M)$. Applied with $L = \Lambda$ and $M = \widetilde{\Lambda}$, this shows that $t \le \tilde{t}$. The bound $\tilde{t} \le t+2$ comes from the bound $\frac{\det(\widetilde{\Lambda})}{\det(\Lambda)} \le 4$.

(2) & (3) (a) If Λ is even, everything is evident.

(b) Otherwise, let e be a parity vector for Λ, and suppose first that $N(e)$ is odd. Then $\frac{e}{2} \in \widetilde{\Lambda} \smallsetminus \Lambda$, for $\frac{e}{2} \cdot x \in \mathbb{Z}$ on $\widetilde{\Lambda}$ but $\frac{e}{2} \cdot e \equiv \frac{1}{2} \mod \mathbb{Z}$. Hence $\widetilde{\Lambda}^* = \Lambda^* \cup ((\frac{e}{2}) + \Lambda)$. Writing any $x \in \Lambda^*$ as $x = y$ or $x = y + \frac{e}{2}$, the map $x \mapsto y$ induces a homomorphism modulo Λ, hence an exact sequence

$$0 \to \widetilde{\Lambda}^*/\Lambda^* \to \widetilde{\Lambda}^*/\Lambda \to \Lambda^*/\Lambda \to 0\,,$$

which is split by the canonical injection $\Lambda \hookrightarrow \Lambda^*$. Hence we have $\tilde{t} \ge t+1$, and indeed $\tilde{t} = t+1$ since $\frac{e}{2}$ has order 4 in $\widetilde{\Lambda}^*/\widetilde{\Lambda}$.

(c) Suppose finally that $N(e)$ is even, so that $e \in \widetilde{\Lambda}$, and let $f \in \Lambda \smallsetminus \widetilde{\Lambda}$. Then $\frac{e}{2}$, f and $\frac{e}{2} + f$ have order 2 in $\widetilde{\Lambda}^*/\widetilde{\Lambda}$, f is zero in Λ^*/Λ, and the other two do not belong to Λ^*. Hence $\widetilde{\Lambda}^*/\widetilde{\Lambda} \simeq \Lambda^*/\Lambda \bigoplus \mathbb{Z}/2\mathbb{Z} \bigoplus \mathbb{Z}/2\mathbb{Z}$, which completes the proof of both (2) and (3).

(4) By Proposition 3.4, we have $\tilde{t} \equiv n \mod 2$. Hence the last assertion in Theorem 3.8 amounts to the congruence $N(e) \equiv \tilde{t} - t \mod 2$, which is immediate from the proof of (2) and (3) above. □

The example of root lattices (see next section) shows that congruences modulo 4 cannot hold in general for *all* the parity classes of a given lattice.

4. Some Calculations of Parity Classes.

We still denote by Λ an integral lattice.

First, we consider the case of *irreducible root lattices*, i.e. Λ is one of the lattices $\mathbb{A}_n$, $n \ge 1$, $\mathbb{D}_n$, $n \ge 4$, or $\mathbb{E}_n$, $n = 6, 7, 8$, of determinants $n+1$, 4 and $9-n$ respectively. Since these lattices are even, 0 is a parity vector, and $\mathrm{cl}(0) = 2\Lambda$ is the only parity class if $\det(\Lambda)$ is odd, i.e. if $\Lambda = \mathbb{A}_n$ ($n \ge 2$ even), $\mathbb{E}_6$ or $\mathbb{E}_8$. We now consider the other irreducible root lattices, and display for every non-zero parity class a vector e having the smallest possible norm. Using the canonical bases $(\varepsilon_0, \varepsilon_1, \dots, \varepsilon_n)$ for $\mathbb{Z}^{n+1}$ and $(\varepsilon_1, \dots, \varepsilon_n)$ for $\mathbb{Z}^n$, we define $\mathbb{A}_n$ and $\mathbb{D}_n$ by

$$\mathbb{A}_n = \{x \in \mathbb{Z}^{n+1} \mid \sum x_i\,\varepsilon_i = 0\} \text{ and } \mathbb{D}_n = \{x \in \mathbb{Z}^n \mid \sum x_i\,\varepsilon_i \equiv 0 \mod 2\}\,.$$

Short parity vectors for root lattices

$t_2 = 1$:

$\mathbb{A}_n$, n odd	$: e = \sum_i (-1)^i \varepsilon_i\,,$	$N(e) = n+1\,;$
$\mathbb{D}_n$, n odd	$: e = 2\,\varepsilon_1\,.$	$N(e) = 4\,;$
$\mathbb{E}_7$	$: e \in 2S(\mathbb{E}_7^*)\,,$	$N(e) = 6\,.$

$t_2 = 2$ (besides $2\,\varepsilon_1$):

$\mathbb{D}_n$, n even	$: e = \varepsilon_1 + \cdots + \varepsilon_{n-1} \pm \varepsilon_n\,,$	$N(e) = n\,.$

For an even lattice, parity vectors are simply those of $2\Lambda^* \cap \Lambda$. However, the case where Λ is the even part of an odd lattice L deserves a remark: for every parity vector e in L, $2e$ is a parity vector for Λ whose class in $\Lambda/2\,\Lambda$ solely depends of L, which we recover as $L = \langle \Lambda, \frac{e'}{2} \rangle$ where e' is any representative for this class.

Next we consider Kneser-neighbours relative to the prime 2, which we define formally by the following construction: given $e \in \Lambda \smallsetminus 2\,\Lambda$, let

$$\Lambda_e = \{x \in \Lambda \mid x \cdot e \equiv 0 \mod 2\} \ \text{ and } \ \Lambda^e = \Lambda_e \cup (\Lambda_e + \frac{e}{2})\,;$$

Λ^e is the *Kneser-neighbour of* Λ *relative to* e. The lattice Λ_e solely depends on the class of e in $\Lambda/2\,\Lambda$, but Λ^e depends on e *modulo* $2\Lambda_e$, so that there are *two* neighbours corresponding to the class of $e \mod 2\,\Lambda$, namely Λ^e and $\Lambda^{e'}$ where $e' = e + 2f$ and f is any vector in $\Lambda \smallsetminus \Lambda_e$. Clearly, Λ^e is integral if and only if $N(e) \equiv 0 \mod 4$, and then both Λ^e and $\Lambda^{e'}$ are.

In the sequel, we restrict ourselves to integral neighbours. The neighbouring process may be considered as producing *cohorts* $\{\Lambda, \Lambda^e, \Lambda^{e'}\}$ of three lattices, every member of which is a neighbour of the others. Explicitly, with the notation above, we have

$$\Lambda_e = (\Lambda^e)_{2f} = (\Lambda^{e'})_{2f} \tag{1}$$

$$\Lambda = (\Lambda^e)^{2f} = (\Lambda^{e'})^{2f} \tag{2}$$

$$\Lambda^{e'} = (\Lambda^e)^{e'} \ \text{ and } \ \Lambda^e = (\Lambda^{e'})^e\,. \tag{3}$$

From the point of view of parity, there are four possibilities to consider:

(1) Λ is odd and e is not a parity vector. Then Λ^e and $\Lambda^{e'}$ are odd.
(2) Λ is odd, e is a parity vector, and $N(e) \equiv 4 \mod 8$. Then Λ^e and $\Lambda^{e'}$ are both odd.
(3) Λ is odd, e is a parity vector, and $N(e) \equiv 0 \mod 8$. Then Λ^e and $\Lambda^{e'}$ are both even.
(4) Λ is even. Then Λ^e and $\Lambda^{e'}$ have different parities. (We have $N(e') - N(e) \equiv 4 \mod 8$.)

[Cases (3) and (4) can be exchanged by a permutation of Λ, Λ^e and $\Lambda^{e'}$.]

Let as above $f \in \Lambda \smallsetminus \Lambda_e$. For $x \in \Lambda_e$, we have $x \cdot (2f) \equiv 0 \mod 2$ and $(x + \frac{e}{2}) \cdot (2f) = e \cdot f \equiv 1 \mod 2$. This shows that $2f$ is a parity vector of Λ^e whenever Λ^e is odd.

Our next example is devoted to hyperplane cross-sections. For the sake of simplicity, we only give partial results, which, however, suffice for our purpose.

Proposition 4.1. *Let $v \in \Lambda \smallsetminus 2\Lambda^*$ of norm not divisible by 4, and let Λ' be the orthogonal of v in Λ. Representatives for the parity classes of Λ' are given by the following formulae, where e runs through a system of representatives for the parity classes of Λ:*

1. *If $N(v) \equiv 1 \mod 2$, $e' = N(v)\,e - (e \cdot v)\,v$.*
2. *If $N(v) \equiv 2 \mod 4$, $e'_1 = \frac{N(v)}{2}\,e - \frac{(e \cdot v)}{2}\,v$ and $e'_2 = e'_1 + v'$ where $v' \in \Lambda'$ is any vector congruent to v modulo 2.*

Proof. Let p be the orthogonal projection onto $v^\perp$; it is given by the formula $p(y) = y = \frac{y \cdot v}{N(v)}\,v$. Then $e \cdot x = p(e) \cdot x$ for all $x \in \Lambda'$.

When $N(v) \equiv 1 \mod 2$, $N(v)\,p(e)$ is a parity vector for Λ'. Since there are $2^{t_2(\Lambda)}$ parity classes in Λ' (because $N(v)$ is odd), we have found all parity classes in Λ'.

When $N(v) \equiv 2 \mod 4$, the formula $e'_1 = \frac{N(v)}{2}\,e - \frac{(e \cdot v)}{2}\,v$ still produce 2^{t_2} parity classes (note that $e \cdot v \equiv n(v) \equiv 0 \mod 2$), but since $N(v)$ is even, there are 2^{t_2+1} such classes in Λ'. Now the equation $(v + 2w) \cdot v = 0$, which is equivalent to $v \cdot w = -\frac{N(v)}{2}$, is soluble in Λ. Then the sums $e'_1 + v'$ with $v' = v + 2w$ produces the 2^{t_2} missing classes. □

Our last example concerns cross-sections of twisted lattices $\mathbb{Z}^n$. Given p, $q \geq 0$, let $I_{p,q}$ be the orthogonal sum of p copies of $\mathbb{Z}^+ = \mathbb{Z}$ and q copies of $\mathbb{Z}^-$; this has dimension $n = p + q$, and is endowed with the canonical basis $(\varepsilon_1, \ldots, \varepsilon_n)$ of $\mathbb{Z}^n$ for which we choose $N(\varepsilon_i) = +1$ for $1 \leq i \leq p$ and $N(\varepsilon_i) = -1$ for $p + 1 \leq i \leq p + q = n$. We set $\eta_i = +1$ if $i \leq p$ and $\eta_i = -1$ if $i > p$. These lattices are important because of the following classification theorem, for a proof of which we refer to [M-H] or [Se]:

Theorem 4.2. *An indefinite, odd unimodular lattice of signature (p, q) is isometric to $I_{p,q}$.* □

The following well known theorem is an easy consequence of the theorem above:

Theorem 4.3. *The norm of the parity vectors of a unimodular lattice are congruent to $p - q$ modulo 8.*

Proof. For the sake of completeness, we give the short proof (in [M-H] and [Se], only the case of even lattices is considered). Let Λ be an odd indefinite unimodular lattice, of signature (p, q), and let e be a parity vector of Λ.

If $\Lambda = I_{p,q}$, e has odd components x_i, and we have $N(e) = \sum \eta_i x_i^2 \equiv \sum \eta_i = p - q \mod 8$. Now $L_1 = \Lambda \perp \mathbb{Z}^+$ and $L_2 = \Lambda \perp \mathbb{Z}^-$ are odd, and $(e, 1)$ is a parity vector for both. If $p = q = 0$, there is nothing to prove. If $q > 0$, L_1 is indefinite with signature $(p+1, q)$, hence we have $N(e) + 1 \equiv p + 1 - q \mod 8$. If $p > 0$, L_2 is indefinite with signature $(p, q+1)$, and we have $N(e) - 1 \equiv p - (q+1) \mod 8$. □

We now determine in full generality the parity classes of the hyperplane cross-sections of lattices of the form $I_{p,q}$. However, to be consistent with the previous notation, we consider the orthogonal Λ in $I_{p,q+1}$ of a *primitive* vector v, with components v_i. Let $d = \det(\Lambda)$. Thus $d = (-1)^{q+1} N(v)$ (because $\det(I_{p,q+1}) = (-1)^{q+1}$) and $N(v) = \sum \eta_i v_i^2$. Moreover, $\Lambda^*/\Lambda \simeq \mathbb{Z}/d\mathbb{Z}$.

Theorem 4.4. *If d is odd (resp. even), Λ possesses one parity class, denoted by $\mathcal{C}$ (resp. two parity classes, denoted by $\mathcal{C}$ and $\mathcal{C}'$). The vectors $e = (e_i)$ in these classes are characterized by the following two conditions:*

(1) $v_1 e_1 + \cdots + v_p e_p - v_{p+1} e_{p+1} - \cdots - v_{p+q+1} e_{p+q+1} = 0$.
(2) $\forall\, i$, $e_i \equiv v_i + 1$ *(resp. and* $e_i \equiv 1$*)* $\mod 2$.

Moreover, we have

$$N(\mathcal{C}) \equiv p - q - 1 + (-1)^q d \quad \textit{and} \quad N(\mathcal{C}') \equiv p - q - 1 \mod 8\,.$$

Proof. Condition (1) is simply the condition $v \cdot e = 0$, equivalent to $e \in \Lambda$. From now on, we assume it is satisfied by a parity vector e.

We next observe that each of the two forms of condition (2) characterizes a class modulo 2 in Λ. We must show that these classes are indeed parity classes. Let $x = \sum_i x_i \varepsilon_i \in \Lambda$. We have

$$N(x) - e \cdot x \equiv \sum_i (x_i^2 + e_i x_i) \mod 2\,.$$

If $e_i \equiv 1 \mod 2$, this is $\sum (x_i^2 + x_i) \equiv 0 \mod 2$. If $e_i \equiv v_i + 1 \mod 2$, we again find $N(x) - e \cdot x \equiv 0 \mod 2$ using the equality $\sum_i v_i e_i = 0$. (Of course, if $\forall\, i$, $e_i \equiv 1 \mod 2$, then $d \equiv e \cdot v \equiv 0 \bmod 2$.)

We must now evaluate modulo 8 the norms of $\mathcal{C}$ and $\mathcal{C}'$. The case of $\mathcal{C}'$ (if it exists) is easy: for $e' \in \mathcal{C}'$, we have ${e'_i}^2 \equiv 1 \mod 8$ for all i, hence $N(e') = \sum_i \eta_i \equiv p - q - 1 \mod 8$. Let now $e \in \mathcal{C}$. We have $e_i \equiv v_i + 1 \mod 2$, say, $e_i = v_i + 1 + 2\lambda_i$, hence

$$N(e_i) = v_i^2 + 1 + 2v_i + 4\lambda_i v_i + (4\lambda_i^2 + 4\lambda_i) \equiv v_i^2 + 1 + 2v_i + 4\lambda_i\,.$$

The condition $e \cdot v = 0$ reads $\sum_i \eta_i(v_i^2 + v_i + 2\lambda_i v_i) = 0$. Using this relation, we obtain $\sum_i \eta_i(2\lambda_i v_i) = -\sum_i \eta_i(v_i^2 + v_1)$, which implies

$$N(e) = \sum_i \eta_i(1 - v_i^2) = p - q - 1 - \sum_i \eta_i v_i^2 \,.$$

Since $\sum_i \eta_i v_i^2 = (-1)^{q+1}\det(\Lambda)$, we are done. □

5. Enlargements and Extension of Lattices.

In this section, we establish a few standard results to be used in next section. We still denote by Λ an integral lattice of signature (p, q) and dimension $n = p + q$ contained in an n-dimensional $\mathbb{Q}$-vector space V.

Definition 5.1. We say that a lattice Λ' is an *enlargement of* Λ if $\Lambda \subset \Lambda' \subset V$. We say that Λ is a *maximal lattice* if it is not strictly contained in any integral lattice in V. We say that Λ' is an *extension of* Λ if Λ' is a lattice in some vector space $V' \supset V$ such that $\Lambda = \Lambda' \cap V$; we also say that Λ is a *section* of Λ'. Finally, we say that Λ is *elementary* if Λ^*/Λ is ℓ-elementary for every prime ℓ.

An embedding $\Lambda \hookrightarrow \Lambda'$ is done via an enlargement $\Lambda \hookrightarrow M$ with $M \subset V$ followed by an extension $M \hookrightarrow \Lambda'$. In what follows, we shall essentially consider enlargements; extensions will then occur as enlargements of direct sums $\Lambda \bigoplus P$ for some low-dimensional lattices P.

Lemma 5.2. *A maximal lattice M is elementary and for every prime ℓ, we have $v_\ell(\det(M)) \le 2$, and even $v_2(\det(M)) \le 1$.*

Proof. Let Λ be an integral lattice and let ℓ be a prime.

If Λ is not ℓ-elementary, there exists $e \in \Lambda^*$ such that $\ell^2 e \in \Lambda \smallsetminus \ell\Lambda$. Then $\langle \Lambda, \ell e\rangle$ is an integral lattice which contains Λ to index ℓ.

Suppose now that Λ is ℓ-elementary, and consider the quadratic form φ induced by the norm on $(\ell\Lambda^* \cap \Lambda)/\Lambda$. If it represents zero on the image of a vector $e \in \Lambda$, then $\langle \Lambda, e\rangle$ is again an integral lattice containing Λ to index ℓ. Since every quadratic form in at least 3 variables on a finite field represents zero, Λ is not maximal if $v_\ell(\det(M)) \ge 3$, and this bound can be lowered to 2 when $\ell = 2$ since our quadratic form is then the square of a linear form.

[To unify the case $\ell = 2$ and ℓ odd, one should consider even lattices, and equip $(\ell\Lambda^* \cap \Lambda)/\Lambda$ with the quadratic form induced by $\frac{1}{2}N(x)$.] □

Lemma 5.3. *Any lattice Λ of signature (p, q) can be embedded into lattices Λ_1 of signature $(p + 1, q)$ and Λ_2 of signature $(p, q + 1)$ which both have the same square-free odd determinant.*

Proof. Embedding Λ in a maximal lattice, we may assume that Λ is ℓ-elementary for all ℓ and that its determinant d satisfies the conditions $v_\ell(d)=0$, 1, or 2 for odd ℓ and $v_2(d)=0$ or 1. Let

$$a=2^{v_2(d)}\prod_{v_\ell(d)=2}\ell\,.$$

Applying Lemma 5.2, we see that maximal lattices containing $\Lambda\perp{}^a\mathbb{Z}$ or $\Lambda_2=\Lambda\perp{}^{-a}\mathbb{Z}$ have odd determinants which are (up to sign) the same product of distinct odd primes. $\square$

To obtain lattices with determinants prime to ℓ, we shall have to know when does an orthogonal sum of lattices with $t_\ell=1$ can be enlarged to a lattice whose determinant is prime to ℓ. To this end, we introduce a *Legendre symbol* $\left(\frac{\Lambda}{\ell}\right)$ defined for odd primes ℓ and lattices Λ with $t_\ell(\Lambda)=1$ or 2, using the form φ defined in the proof of Lemma 5.2. If $t_\ell=1$, let $\varphi=ax^2$. We then set $\left(\frac{\Lambda}{\ell}\right)=\left(\frac{a}{\ell}\right)$. If $t_\ell=2$, we set $\left(\frac{\Lambda}{\ell}\right)=0$ if the form is degenerate (which amounts to saying that Λ is not ℓ-elementary), and otherwise, $\left(\frac{\Lambda}{\ell}\right)=+1$ if φ represents zero, and -1 if it does not.

As usual we extend the definition of the symbol to all odd denominators by setting $\left(\frac{\Lambda}{m}\right)=\prod_{i=1}^r\left(\frac{\Lambda}{\ell_i}\right)$ if $m=\prod_{i=1}^r\ell_i$ where the ℓ_i are odd primes.

Lemma 5.4. *Let L_1 and L_2 be two lattices with $t_\ell=1$. Then,*

$$\left(\frac{L_1\perp L_2}{\ell}\right)=(-1)^{(\ell-1)/2}\left(\frac{L_1}{\ell}\right)\left(\frac{L_2}{\ell}\right).$$

Proof. If $\left(\frac{L_i}{\ell}\right)$ is zero for $i=1$ or 2, both sides are zero. Otherwise, if the ℓ-part of $\mathrm{Smith}(L_i)$ is ℓa_i, the quadratic form modulo ℓ attached to $L_1\perp L_2$ is $a_1x_1^2+a_2x_2^2$, and it represents zero if and only if $\left(\frac{-a_1a_2}{\ell}\right)=-1$. $\square$

Lemma 5.5. *Let ℓ be an odd prime and let $a\in\{\pm1\}$. If $\ell\equiv-1 \mod 4$ or if $a=+1$ there exist lattices L, both odd of dimension 1 and even of dimension 2, such that $\left(\frac{L}{\ell}\right)=a$. Odd (resp. even) lattices of dimension 2 (resp. 4) with $\left(\frac{L}{\ell}\right)=a$ exist unconditionally.*

Proof. We first prove what concerns odd lattices. For $m\equiv0 \mod \ell$, we have $\left(\frac{{}^m\mathbb{Z}}{\ell}\right)=+1$ and $\left(\frac{{}^{-m}\mathbb{Z}}{\ell}\right)=\left(\frac{-1}{\ell}\right)$, so that we are left with the case where $a=-1$ and $\ell\equiv+1 \mod 4$. Let $L_1={}^{\ell'\ell}\mathbb{Z}$ where ℓ' is a prime such that $\ell'\equiv-1 \mod 4$ and $\left(\frac{\ell'}{\ell}\right)=-1$. By the previous case, there exists a 1-dimensional lattice L_2 such that $\left(\frac{L_2}{\ell}\right)=\left(\frac{L_1}{\ell}\right)$. Then $L_1\perp L_2$ is contained to index ℓ' in a lattice L, and we have $\det(L)=\ell$ and

$$\left(\frac{L}{\ell}\right)=\left(\frac{L_1\perp L_2}{\ell}\right)=\left(\frac{L_1}{\ell}\right)=\left(\frac{\ell'}{\ell}\right)=-1\,.$$

To handle the case of even lattices, we start with a lattice L having a basis (e_1, e_2) with Gram matrix $\begin{pmatrix} 2 & -1 \\ -1 & \frac{m+1}{2} \end{pmatrix}$ where m is any integer congruent to -1 modulo 4. The lattice L is even of determinant m. Then $(e_1 + 2e_2, e_2)$ has Gram matrix $\begin{pmatrix} 2m & m \\ m & \frac{m+1}{2} \end{pmatrix}$, hence $\left(\frac{L}{\ell}\right) = \left(\frac{2m/\ell}{\ell}\right)$ for every odd prime divisor ℓ of m. Taking $m = \ell$, we have $\left(\frac{L}{\ell}\right) = +1$ and $\left(\frac{L^-}{\ell}\right) = (-1)^{(\ell-1)/2}$. Thus we are again left with the case where $\ell \equiv +1 \mod 4$ and $a = -1$. We then take $m = \ell'\ell$ where ℓ' is a prime congruent to -1 modulo 4 and such that $\left(\frac{2\ell'}{\ell}\right) = -1$. The corresponding lattice L_1 has $\left(\frac{L_1}{\ell}\right) = -1$. We then consider a lattice L_2 of determinant ℓ' such that $L_1 \perp L_2$ embeds to index ℓ' in an integral lattice L. Then L is even and has determinant ℓ and Legendre symbol -1. □

6. Some congruences modulo 8.

The results we are going to prove are generally well-known in the case of even lattices, where they can be obtained by making use of *Milgram's formula*; see [M-H], Appendix 4; we could also reduce to positive lattices and then use modular forms. The proof we present below are general and do not make use of analytic tools. The method of extension we use below plays a key rôle in Conway and Sloane's results of [C-S1] and [C-S2].

We keep the notation of the previous section.

Theorem 6.1. *If* $\det(\Lambda) = \pm 2$*,* Λ *has two parity classes, whose norms are congruent to* $p - q - 1$ *and* $p - q + 1$ *modulo* 8*.*

Proof. Since the determinant of Λ has the sign of $(-1)^q$, we have $(-1)^q \det(\Lambda) = +2$.

Assume first that $p > 0$. By Theorem 5.3, Λ can be embedded in unimodular lattices Λ' of signature $(p, q+1)$. Since it is indefinite, this lattice is isometric to $I_{p,q+1}$, and Theorem 6.1 results from Theorem 4.4.

Assume now that $p = 0$. Then, Λ^- has signature $(q, 0)$ and determinant $(-1)^q \det(\Lambda) = +2$. By the result above, parity vectors e^- for Λ^- have norms $q \pm 1$. We can take for e^- any parity vector e for Λ, but since we have negated the scalar product, its norm is now given by the formula $N(e^-) = -N(e)$. This shows that the set of norms on Λ is now $-(q \pm 1) = -q \mp 1 = p - q \mp 1$ since $p = 0$. □

Corollary 6.2. *The signature of an even lattice of determinant* ± 2 *satisfies one of the the congruences* $p - q \equiv \pm 1 \mod 8$*.*

Proof. We have $0 \equiv p - q \pm 1 \mod 8$. □

We now consider lattices with odd, square-free level, as defined in Definition 2.1.

Theorem 6.3. *A lattice Λ of signature (p,q), determinant d and odd square-free level has a single parity class $\mathcal{C}$, whose norm modulo 8 is given by the following formulae:*

- *If $d \equiv -1 \mod 4$, $N(\mathcal{C}) \equiv (p-q)+(d-1)\big(\frac{\Lambda}{d}\big)$.*
- *If $d \equiv +1 \mod 4$, $N(\mathcal{C}) \equiv (p-q)+d+1-2\big(\frac{\Lambda}{d}\big)$.*

Proof. We shall use induction on the number r of prime factors of d, noting that for $r=0$, the theorem we want to prove results from Theorem 4.3. Suppose now that $r \geq 1$, and denote by e a parity vector for Λ.

Let $\ell = \ell_r$, et let L be the even lattice of determinant ℓ and such that $\big(\frac{L}{\ell}\big) = (-1)^{(\ell-1)/2}\big(\frac{\Lambda}{\ell}\big)$ of Lemma 5.5. Denote by (p',q') its signature and let f be a parity vector for L. The way we constructed L shows that if $\ell \equiv -1$ (resp. $+1$) $\mod 4$, we have $q'-p' \equiv -2$ or $+2 \mod 8$ (resp. $q'-p' \equiv 0$ or $4 \mod 8$). Applying Lemma 5.4, we may enlarge $\Lambda \perp L$ to an integral lattice Λ' of determinant $d' = \frac{d}{\ell}'$; its signature is $(p+p', q+q')$, and $e+f$ is a parity vector for Λ', of norm $N(e)+N(f)$. Now, the formulae in Theorem 6.3 hold for L by an immediate verification and for Λ' by the induction hypothesis. Lemma 5.4 then shows that they hold for Λ. □

Corollary 6.4. *Let Λ be an even lattice with odd determinant d. Then if $d \equiv -1$ (resp. $+1$) $\mod 4$, the signature of Λ satisfies the congruence $q \equiv p+2$ (resp. $q \equiv p$) $\mod 4$.*

Proof. Use the fact that 0 is a parity vector, and notice that $q \equiv p \pm 2 \mod 8$ amounts to $q \equiv p+2 \mod 4$ and $q \equiv p$ or $p+4 \mod 8$ amounts to $q \equiv p \mod 4$. □

7. Modular lattices.

Let a be a positive integer. We say that a lattice Λ is *a-modular* if there exists a similarity σ with multiplier a which maps Λ^* onto Λ; we say that Λ is *modular* if it is modular for some a. We then have $\det(\Lambda) = a^n \det(\Lambda^*)$, i.e. $\det(\Lambda) = a^{n/2}$. In particular, if a is square-free, n must be even, which amounts to $p \equiv q \mod 2$. (For $a=1$, observe that "1-modular" $\iff$ "unimodular".)

By what we proved in the previous section, if a is odd and square-free, the norms modulo 8 of the parity vectors can be calculated in terms of the quadratic characters $\big(\frac{\Lambda}{\ell}\big)$, $\ell \mid a$. We shall now consider 2-modular lattices.

We begin with a canonical construction which transforms a lattice Λ of signature (p,q) and even level N into one of signature $(2p,2q)$ and level $\frac{N}{2}$. Start with $\Lambda \perp \Lambda$, then adjoin to it all vectors of the form $\frac{(x,x)}{2}$ for all $x \in 2\Lambda^* \cap \Lambda$. This new lattice Λ' is integral, for $\frac{(x,x)}{2} \cdot (y,z)$ and $N(\frac{(x,x)}{2}) = \frac{x \cdot x}{2}$ are integers, because the scalar products $x \cdot y$, $x \cdot z$ and $x \cdot x$ are even for all $x \in 2\Lambda^* \cap \Lambda$ and $y,\, z \in \Lambda$.

Proposition 7.1. *If Λ is 2-modular, the lattice Λ' is unimodular and has the same parity as Λ.*

Proof. We denote by σ a similarity of multiplier 2 which maps Λ onto Λ^*. The lattice Λ' is integral, and obviously odd if Λ is. If Λ is even, for every $x \in 2\Lambda^* \cap \Lambda$, σx belongs to 2Λ, hence $N(\frac{\sigma x}{2}) = \frac{N(x)}{2}$ is even, which implies $N(x) \equiv 0 \mod 4$, whence $N\big(\frac{(x,x)}{2}\big) \equiv 0 \mod 2$.
Finally, since $[\Lambda' : \Lambda \perp \Lambda] = 2^{n/2}$, we have $\det(\Lambda') = 1$. □

The following corollary is well known, at least for positive lattices, and could be also proved using Milgram's formula:

Corollary 7.2. *If Λ is an even, 2-modular lattice, then $p \equiv q \mod 4$.*

Proof. Indeed, Λ' is a unimodular lattice of signature $(2p,2q)$, hence $2p - 2q \equiv 0 \mod 8$. □

However, for odd lattices, we cannot prove more on the norms of parity vectors than the general congruence $N(e) \equiv n \mod 2$. Indeed, let e be any parity vector. Then the set of parity vectors for Λ is $\mathcal{E} = \{e + x \mid x \in 2\Lambda^*\}$, and since $y \cdot x$ is even for any $x \in 2\Lambda^*$, we have $N(e+x) - N(e) \equiv N(x) \mod 4$. Since Λ is odd, there exists $x \in \Lambda$ with $N(x) \equiv 1 \mod 2$. Then the σx belongs to $2\Lambda^* \cap \Lambda$ and its norm is 2 mod 4, so that e and $e + \sigma x$ have different norms modulo 4. Direct sums of lattices ${}^2\mathbb{Z} \perp \mathbb{Z}$ provide examples with signature $(n,0)$ for any even dimension $n = 2r$ which for any $n \geq 8$ have parity vectors of any norm $N \mod 8$ congruent to $t_2 = r$ modulo 2.

Proposition 7.3. *If Λ is positive definite, then $\min \Lambda' = \min \Lambda$.*

Proof. We argue as in [M], Chapter 8, Section 8. Let $m = \min \Lambda$. We of course have $\min(\Lambda \perp \Lambda) = \min \Lambda = m$. Let $e \in \Lambda' \smallsetminus (\Lambda \perp \Lambda)$. We have $e = \frac{(x+2y,x+2z)}{2}$ for some $x \in 2\Lambda^* \cap \Lambda$ and $y, z \in \Lambda$. The vectors $x + 2y$ and $x + 2z$ are non-zero, for if $x + 2y = 0$, say, then $e = (0, z - y)$ belongs to $\Lambda \perp \Lambda$. Since they both belong to $2\Lambda^* \cap \Lambda$, their norms are at least $2m$. □

The canonical automorphism $\tau : (x,y) \mapsto (-y,x)$ of $\Lambda \perp \Lambda$ has square $-\mathrm{Id}$ (otherwise stated, it induces on $\Lambda \perp \Lambda$ and on $V \perp V$ a structure of module over the ring $\mathbb{Z}[i]$ of *Gaussian integers*). It clearly stabilizes the unimodular lattice Λ' that we canonically attached to Λ. Hence, following [M], Chapter 8, Section 8, we can continue with it a sequence *à la Barnes-Wall* of $\mathbb{Z}[i]$-lattices having dimensions $4n$, $8n$, etc. which are alternatively 1- and 2-modular, and even from dimension $4r$ onwards; moreover, in the Euclidean case, the minimum doubles when passing from 1- to 2-modular lattices, and is preserved otherwise.

It is not difficult to list the pairs $(n, 2n)$ of dimensions for which the doubling construction could produce *extremal ℓ-modular lattices*, $\ell = 1$ or 2, that is even lattices whose minimum attains Quebbemann's bound, namely $2 + 2\left\lfloor \frac{(\ell+1)\,n}{48} \right\rfloor$. [**Warning**. In the formula given in [M], Th. 16.4.1, the term "2+" is missing.]

The case $(32, 64)$ (2- to 1-modular) is especially interesting: four even, 2-modular extremal lattices are known in dimension 32, due to Quebbemann (2), Bachoc, and Nebe. The construction $\Lambda \mapsto \Lambda'$ thus produces four extremal unimodular lattices of dimension 64. Up to know, two examples (or maybe only one), constructed by Quebbemann and by Nebe, were known. However, I do not know how to prove that "my" four lattices are mutually non-isometric.

Another interesting case concerns the analogous transition from dimension 20 to 40. There are three 2-modular, extremal 20-dimensional lattices, from which we can construct three unimodular, extremal 20-dimensional lattices (all of minimum 4). However, I do not know ...

These three lattices in dimension 20 where found by Nebe (2) and R. Scharlau-B -Hemkemeimer (in [V], Section 19, they are however all attributed to Nebe); uniqueness was proved by Bachoc and Venkov in [B-V], Section 5.

Such constructions are also useful to produce odd lattices. For instance, from Kneser's 14-dimensional unimodular lattice with root system $2\boldsymbol{E}_7$, we obtain a 2-modular, 28-dimensional lattice of minimum 4, most certainly the lattice described in [N-S].

Gram matrices for some of the lattices considered above can be found in Nebe and Sloane's catalogue [N-S]. Constructions for the three lattices of Quebbemann referred to above can be found in [C-S].

References

[B-V] C. Bachoc, B. Venkov, *Modular forms, lattices and spherical designs*, in Réseaux euclidiens, designs sphériques et groupes, L'Ens. Math., Monographie **37**, J. Martinet, ed., Genève (2001), 87–111.

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

[C-S1] J.H. Conway, N.J.A. Sloane, *Low-Dimensional Lattices. I. Quadratic Forms of Small Determinant*, Proc. Royal Soc. London **A 418** (1988), 17–41.

[C-S2] J.H. Conway, N.J.A. Sloane, *Low-Dimensional Lattices V. Integral Coordinates for Integral Lattices*, Proc. Royal Soc. London **A 426** (1989), 211–232.

[El1] N. Elkies, *A characterization of the $\mathbb{Z}^n$ lattice*, Math. Res. Lett. **2** (1995), 321–326.

[El2] N. Elkies, *Lattices and codes with long shadows*, Math. Res. Lett. **2** (1995), 643–651.

[M] J. Martinet, *Perfect Lattices in Euclidean Spaces*, Grundlehren **327**, Springer-Verlag, Heidelberg (2003); English corrected and updated edition of the French book "Les réseaux parfaits des espaces euclidiens", Masson (now Dunod), Paris (1996).

[M-H] J. Milnor, D. Husemoller, *Symmetric Bilinear Forms*, Springer-Verlag, Ergebnisse **73**, Heidelberg (1973).

[N-S] G. Nebe, N.J.A. Sloane, *A Catalogue of Lattices*, http://www.research.att.com/~njas/lattices/index.html.

[N-V] G. Nebe, B. Venkov, *Unimodular lattices with long shadow*, J. Number Theory **99** (2003), 307-317.

[Se] J-P. Serre, *Cours d'arithmétique*, P.U.F., Paris (1970), translated into English as: *A Course in Arithmetic*, Graduate Texts in Math. **7**, Springer-Verlag, Heidelberg (1973).

[V] B.B. Venkov, *Réseaux et "designs" sphériques* (Notes by J. Martinet), in Réseaux euclidiens, designs sphériques et groupes, L'Ens. Math., Monographie **37**, J. Martinet, ed., Genève (2001), 10–86.

Jacques Martinet
A2X, Institut de Mathématiques
Université Bordeaux 1
351, cours de la Libération
F–33405 TALENCE cedex
E-mail : martinet@math.u-bordeaux.fr