EUCLIDEAN VERSUS LORENTZIAN LATTICES

JACQUES MARTINET

Abstract. It is known that indefinite, odd, unimodular lattices are classified up to isometry by their signature (p,q), $p,q>0$. We consider n-dimensional Euclidean lattices embedded into a Lorentzian lattice of signature $(n,1)$. We attach this way a *weight* to unimodular Euclidean lattices.

Foreword —Warning

In 2001 I wrote down AmSTeX-files accounting for work done during the academic year 1999-2001 on embedding a Euclidean, n-dimensional lattice into a Lorentzian lattice of signature $(n,1)$, with the help of Christian Batut, who wrote various *PARI*-programs. In particular I introduced the notion of a *weight* for a unimodular lattice, which can be viewed as a kind of measure of complexity.

Fifteen years later I decided to put on line this LaTeX-file which accounts for the essential of the work done in those days. This is not intended for publication. However I believe it might be of some use for those who are interested in the interface between Euclidean and odd Lorentzian lattice.

1. Introduction

Let $p,q\geq 0$ be integers, and let V be a real vector space equipped with a quadratic form of signature (p,q) (thus $n:=\dim V=p+q$), with corresponding bilinear form denoted by $(x,y)\mapsto x\cdot y$ (the "*scalar product*" on V). A *lattice in* V is a $\mathbb{Z}$-submodule of V of rank $\dim V$. Unless otherwise stated, the word "lattice" will denote a *Euclidean lattice*, that is a lattice in a space of signature $(n,0)$, When V has signature (p,q), we say *lattice of signature* (p,q), and a *Lorentzian lattice* is a lattice of signature $(n,1)$, $n\geq 1$. We say that V, or its scalar product, is *indefinite* if both p and q are strictly positive. Negating $x\cdot y$ changes a lattice L of signature (p,q) into a lattice L^- of signature (q,p). We also set $L^+=L$.

2000 *Mathematics Subject Classification.* 11H55, 11H71.

Key words and phrases. Euclidean lattices, Lorentzian lattices, quadratic forms
First version: May 28th, 2016 (correction: June 2nd, 2016).

We say that a lattice L (of any signature) is *integral* if the scalar product takes integral values on L, and that an integral L is even (resp. odd) if the *norm* $x \cdot x$ takes only even values on L (resp. takes odd values on some vectors of L). The *determinant* $\det(L)$ *of* L is the determinant of the Gram matrix of one of its bases. Its sign is that of $(-1)^q$, and $\det(L)$ is an integer when L is integral. We say that L is *unimodular* if its determinant is ± 1, indeed $(-1)^q$ if L has signature (p, q). An important reference for Lorentzian, unimodular lattices is Chapter 26 of [C-S].

Definition 1.1. Let $\mathbb{Z}^+$ (resp. $\mathbb{Z}^-$) be the module $\mathbb{Z}$ equipped with the form $+xy$ (resp. $-xy$). We denote by $I_{p,q}$ the $\mathbb{Z}$-module $(\mathbb{Z}^+)^p \perp (\mathbb{Z}^-)^q$ (an orthogonal sum of p copies of $\mathbb{Z}^+$ and q copies of $\mathbb{Z}^-$), viewed as a lattice in $V = \mathbb{R} \otimes I_{p,q}$. If $q = 0$, this is a Euclidean lattice simply denoted by $\mathbb{Z}^n$.

The basic result we shall use is the following theorem, a proof of which can be read in [Se], Chapter IV, or [M-H], Chapter II, Section 4):

Theorem 1.2. *An odd, indefinite unimodular lattice of signature* (p, q) *is isometric to* $I_{p,q}$. □

Let now Λ be a unimodular, n-dimensional lattice in a Euclidean space E, let $V = E \perp (\mathbb{R}, -xy)$, and let $L = \Lambda \perp \mathbb{Z}^-$. Then L is an odd unimodular Lorentzian lattice. Hence by Theorem 1.2, there exists an isometry

$$\varphi : \Lambda \perp \mathbb{Z}^- \to I_{n,1}\,.$$

This isometry is far from being canonical, and any other such isometry φ' is of the form $\varphi' = \varphi \circ u$ where u is an automorphism of $I_{n,1}$, that is, an element of the orthogonal group $\mathrm{O}_{n,1}(\mathbb{Z})$. We identify this way Λ with the orthogonal $v^\perp$ of a vector $v \in I_{n,1}$ of norm -1, and lattices up to isometry are in one-to-one correspondence with orbits of vectors of norm -1 in $\mathrm{O}_{n,1}(\mathbb{Z})$. Vectors $x \in I_{n,1}$ will be written in the form

$$x = (x_1, \dots, x_n; x_0)$$

and thus have norm $N(x) = x_1^2 + \cdots + x_n^2 - x_0^2$. We write

$$v = (v_1, \dots, v_n; v_0) \;\text{ with } v_1^2 + \cdots + v_n^2 - v_0^2 = -1\,.$$

Without loss of generality, we may assume that the v_i are non-negative. Among all vectors v orthogonal to Λ, there exist finitely many for which v_0 attains its minimum.

Definition 1.3. The smallest possible value of $|v_0|$ for a vector $v \in \Lambda^\perp$ is called the *weight of* Λ, denoted by $\mathrm{wt}(\Lambda)$.

Problem 1.4. *To find good bounds for the the weight of n-dimensional unimodular lattices of minimum m.*

In a given dimension the weight seems to be a measure of the complexity of the lattice. For example, among the even, 24-dimensional lattices, the weight has the value 145 for the Leech lattice which does not contain norm 2 vectors, 73 for the lattice which contains only 24 pairs of such vectors, and is ≤ 51 otherwise; see Section 7, Table 2.

Note that such a weight can also be attached to those lattices Λ of determinant d which can be embedded in $I_{n,1}$, and thus can then be realized as the orthogonal of a vector of norm $-d$.

2. Parity Classes

In this section Λ stands for an integral lattice of any signature (p, q). Integrality is equivalent to the inclusion

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

The map $x \mapsto N(x) \mod 2$ is a homomorphism of Λ into $\mathbb{Z}/2\mathbb{Z}$. Hence there exists $e' \in \Lambda^*$, such that $N(x) \equiv e' \cdot x \mod 2$ for every $x \in \Lambda$, and e' is uniquely defined modulo $2\Lambda^*$. We call the class of e' modulo $2\Lambda^*$ the *parity class of* Λ *in* Λ^*.

Let $d = \det(\Lambda)$; this is the product of the elementary divisors of (Λ^*, Λ). If d is odd, the map $s \mapsto dx$ induces an isomorphism pf $\Lambda^*/2\Lambda^*$ onto $\Lambda/2\Lambda$. This shows that there exist parity vectors in Λ (e.g., $e := de'$), and that these parity vectors constitute a class modulo 2 in Λ. This is the *parity class of* Λ.

[In general there are 2^k parity classes in Λ, where k is the number of even elementary divisors of (Λ^*, Λ).]

Note that Λ is even if and only if 0 is a parity class of Λ.

Proposition 2.1. (1) *On a given parity class the norm is an invariant modulo* 8.
(2) *If* Λ *is unimodular this invariant is congruent to* $p-q$ *modulo* 8.
(3) *The signature of an even, unimodular lattice satisfies the congruence* $q \equiv p \mod 8$.

Proof. (1) follows from the identity $N(e+2x) = N(e)+4(e\cdot x+N(x))$, and (3) is a consequence of (2), observing that Λ is even if and only if 0 is a parity class of Λ.

(2) Let e be a parity vector of Λ. If $\Lambda = I_{p,q}$, we may chose for e the all ones vector, of norm $p - q$. This proves (2) for $\Lambda = I_{p,q}$. To prove (2) in general consider the lattices $\Lambda \perp \mathbb{Z}^+$ and $\Lambda \perp \mathbb{Z}^-$. Both are odd, and at least one of them is indefinite, hence isometric to $I_{p+1,q}$

or $I_{p,q+1}$ by Theorem 1.2, which implies either $N(e)+1 \equiv (p+1)-q$ or $N(e)-1 \equiv p-(q+1)$, that is $N(e) \equiv p-q \mod 2$. □

Let $v=(v_1,\dots,v_{p+q}) \in I_{p,q}$ be a vector of odd norm d, and let H be the hyperplane orthogonal to v in V. Then $\Lambda := I_{p,q} \cap H$ is a lattice of determinant d in H, hence has a unique parity class.

Proposition 2.2. *Let $v=(v_1,\dots,v_{p+q}) \in I_{p,p}$, of norm ± 1, let H the hyperplane $v^\perp \subset V$, and let $\Lambda = H \cup I_{p,p}$. Then the parity class of Λ is that of the vectors e with components $e_i \equiv v_i + 1 \mod 2$.*

Proof. Consider more generally the case of a vector v of norm $d \neq 0$, assumed to be primitive (this is automatic if $d = \pm 1$), so that $\det(\Lambda) = (-1)^q d$. The norm of $x=(x_i) \in I_{p,p}$ is $N(x) = \sum_i \varepsilon_i x_i^2$ where $\varepsilon_i = \pm 1$ and $\sum \varepsilon_i = p-q$. Hence

$$N(x) \equiv e \cdot x \mod 2 \iff \textstyle\sum_i (e_i-1)x_i \equiv 0 \mod 2\,.$$

Taking $x = \varepsilon_i v_j - \varepsilon_j v_i \in \Lambda$, we obtain

$$\forall\, i,\ \forall\, j,\ (e_i-1)v_j \equiv (e_j-1)v_i \mod 2\,.$$

Pick i with v_i odd (such an i exists since v is primitive). We then see that we must have $e_j \equiv 1 \mod 2$ if v_j is even, and $e_j \equiv e_i \mod 2$ if v_j is odd. This shows that e belongs to one of the two classes C_1, C_2 modulo 2 defined as follows:

$$v_i \text{ even: } e_i \equiv 1 \text{ on } C_1 \text{ and } C_2\,;$$
$$v_i \text{ odd: } e_i \equiv 0 \text{ on } C_1,\ e_i \equiv 1 \text{ on } C_2.$$

When d is even, there are two parity classes, necessarily C_1 and C_2. When d is odd, we make use of the fact that for any integral lattice of odd determinant, the norm of parity vectors is congruent to the dimension modulo 2 (a consequence of Proposition 2.1 if $d=\pm 1$). Here we must have $N(e) \equiv p+q-1 \mod 2$, whereas the all ones vector has norm $p-q \mod 2$.

[Direct proof: $e+v$ is a parity vector for $\Lambda \perp \mathbb{Z}v$, and because of the double inclusion $d\Lambda \subset \Lambda \perp \mathbb{Z}v \subset \Lambda$, $e+v$ is a parity vector for Λ.] □

Corollary 2.3. *The lattice Λ is even if and only if all components of v are odd.* □

3. Small Norms and Small Weights

From now on, and unless otherwise stated, we study unimodular lattices inside $V := \mathbb{R} \otimes I_{n,1}$, defined as the orthogonal of a vector $v = (v_1,\dots,v_n; v_0)$ of norm -1, i.e., we have $v_1^2 + \cdots + v_n^2 - v_0^2 = -1$. In this section we essentially consider questions related to the existence of vectors of norm 1 or 2.

3.1. **Lattices of Weight 1.** This question is closely related to the existence of norm-1 vectors. In an integral lattice L (of any signature), vectors of norm ± 1 have the following two properties:
(1) If $N(x) = N(y) = \pm 1$ and $y \neq \pm x$, then we have $|x \cdot y| < 1$, hence $x \cdot y = 0$;
(2) If $N(e) = \pm 1$, the identity $x = (x \mp (e \cdot x)e) + (e \cdot x)e$ shows that L splits as an orthogonal sum $\mathbb{Z}e \perp L'$.
As a consequence the existence of k distinct pairs $\pm x$ of vectors of norm ± 1 factors out from L an orthogonal sum of k lattices $\mathbb{Z}^{\pm}$.

To state the theorem below, we need to identify a lattice defined by orthogonality with the celebrated lattice $\mathbb{E}_8$, the definition of which we recall in Subsection 3.2 below. Suffices to know that $\min E_8 = 2$ and $s(\mathbb{E}_8) = 120$ ($s > 64$ suffices).

Proposition 3.1. *The lattice orthogonal to* $(1^8; 3)$ *is isometric to* $\mathbb{E}_8$.

Proof. Indeed this lattice is even and possesses $28 + 56 + 28 + 8 = 120$ pairs of norm 2 vectors, obtained as permutations of the following four types: $(1, -1, 0^6; 0)$, $(1^3, 0^5; 1)$, $(1^6, 0^2; 2)$ and $(2, 1^7; 3)$, dividing its set S of minimal vectors into four subsets S_1, S_2, S_3, S_4; see the proof of Theorem 3.3. □

Theorem 3.2. *Let* Λ *be an* n*-dimensional unimodular, Euclidean lattice. Then either* $\mathrm{wt}(\Lambda) = 1$*, and* Λ *is isometric to* $\mathbb{Z}^n$*, or* $\mathrm{wt}(\Lambda) \geq 3$*, and* $n \geq 8$*; and if* $\mathrm{wt}(\Lambda) = 3$*,* Λ *is isometric to* $\mathbb{E}_8 \perp \mathbb{Z}^{n-8}$.

Proof. Observe that if $v_i = 0$ for some i then the vector e_i with component 1 at i and 0 otherwise is a norm 1 vector, orthogonal to all vectors x with $x_i = 0$. Thus if v has k components equal to 0 then Λ is isometric to a direct sum $\Lambda' \perp \mathbb{Z}^k$. If $v_0 = 1$, the vectors e_i constitute an orthogonal basis for Λ, which shows that $\Lambda \simeq \mathbb{Z}^n$.

Assume now that $v_0 = 2$. Then v extends the vector $w := (1, 1, 1; 2)$ with $v_i = 0$ for $i = 4, \dots, n$. It thus suffices to consider w itself. Then the three vectors $(1, 1, 0; -1)$, $(1, 0, 1; -1)$ and $(0, 1, 1; -1)$ have norm 1 and are pairwise orthogonal. This proves that weights never take the value 2.

Assume finally that $v_2 = 3$. Then it suffices to consider three possible vectors v, namely $(2, 2; 3)$ $(n = 2)$, $(2, 1^4; 3)$ $(n = 5)$ and $(1^8; 3)$ $(n = 8)$, and to show that the first two define $\mathbb{Z}^n$. This is achieved by considering the two vectors $(2, 1; 2)$ and $(1, 2; 2)$ in the first case, and the vectors $e_1 := (1, 1, 1, 1, 1; 2)$, and e_i, $i = 2, 3, 4, 5$ having components 1 at 0, 1, i and 0 otherwise in the second case. □

3.2. **Roots.** Let e be a vector of non-zero norm in an integral lattice L (of arbitrary signature). The *symmetry* σ_e *along* e (or *with respect to the hyperplane* $e^\perp$) is given by the formula

$$\sigma_e(x) = x - \frac{2(e\cdot x)}{e\cdot e}\, e\,,$$

so that reflections defined by vectors of norm ± 1 and ± 2 are automorphisms of L. These vectors are usually called the *roots of* L, though we shall often discard norms ± 1 (we have seen that they induce orthogonal decompositions),
[A general definition is that e is a root of L if e is *primitive*, and if $\sigma_e(L) = L$. Then $N(e)$ must divide the annihilator of L^*/L, so that when L is unimodular, roots are effectively vectors of norm dividing 2.]

In the Euclidean setting, a *root lattice* is an integral lattice generated by vectors of norm 2, its *roots* (even if some vectors of large norm may also be roots according to the general definition). A celebrated theorem is that root lattices are orthogonal sums of irreducible root lattices, which share out among two infinite series and three exceptional lattices.

Consider $\mathbb{Z}^{n+1}$ and $\mathbb{Z}^n$, equipped with their canonical bases (ε_i), $0 \le i \le n$ and $1 \le i \le n$, respectively. Then the infinite series are

$$\mathbb{A}_n = \{x \in \mathbb{Z}^{n+1} \mid \sum x_i = 0\}\ (n \ge 1)$$

and

$$\mathbb{D}_n = \{x \in \mathbb{Z}^n \mid \sum x_i \equiv 0 \mod 2\}\ (n \ge 4)\,.$$

[We did not consider $D_2 \simeq \mathbb{A}_1 \perp \mathbb{A}_1$ and $\mathbb{D}_3 \simeq A_3$.]

The Gram matrix of the basis $(\varepsilon_0 - \varepsilon_i)$ for $\mathbb{A}_n$ has entries 2 on the diagonal and 1 off the diagonal, which gives an easy way for characterizing $\mathbb{A}_n$ up to isomorphism. Replacing in this matrix 1 by 0 for *one* pair of entries $(i,j),(j,i)$, we obtain a Gram matrix for $\mathbb{D}_n$. (Consider the basis $\varepsilon_i + \varepsilon_j, \varepsilon_i - \varepsilon_k$, $k \ne i$.)

The roots of $\mathbb{A}_n$ are the $\frac{n(n+1)}{2}$ pairs $\pm(\varepsilon_i - \varepsilon_j)$, $i < j$ and those of $\mathbb{D}_n$ are the $n(n-1)$ pairs $\pm(\varepsilon_i \pm \varepsilon_j)$, $i < j$.

The exceptional lattices are then $\mathbb{E}_8 := \mathbb{D}_8^+$ (see below, *Coxeter lattices*) and its successive densest cross-sections $\mathbb{E}_7$ and $\mathbb{E}_6$. Their roots consist of 120, 63 and 36 pairs of norm-2 vectors, respectively.

For the sets of roots of the irreducible lattices, we use the notation $\boldsymbol{A}_n$, $\boldsymbol{D}_n$ and $\boldsymbol{E}_n$.

3.3. **Coxeter lattices.** Given an integral lattice L, a necessary condition for a lattice $M \supset L$ to be integral is that M should be contained in L^*, which gives some importance to the study of lattices M such that $L \subset M \subset L^*$. When L is an irreducible root lattice, lattices M as above are called *Coxeter lattices*.

When $L = A_n$, L^*/L is cyclic of order $\det(L) = n+1$, so that there exists for each divisor r of $n+1$ a unique Coxeter lattice containing $\mathbb{A}_n$ to index r, denoted by $\mathbb{A}_n^r$. Its determinant is $\frac{n+1}{r^2}$, so that it can be integral only when $r^2 \mid n+1$. This condition suffices, and in particular, $\mathbb{A}_n^r$ is unimodular if and only if $n+1 = r^2$.

When $L = \mathbb{D}_n$, we only find $\mathbb{Z}^n$ if n is odd, but two lattices distinct from $\mathbb{Z}^n$ if n is even, denoted by $\mathbb{D}_n^+$ and $\mathbb{D}_n^-$, equal to $\mathbb{D}_n \cup (\mathbb{D}_n + \frac{e^\pm}{2})$, where $e^+ = (1^n)$ and $e^- = (1^{n-1}, -1)$. These two lattices are isometric, half-integral and exchanged by duality if $n \equiv 2 \bmod 4$, unimodular otherwise, odd if $n \equiv 4 \bmod 8$, even if $n \equiv 0 \bmod 8$. We have $S(\mathbb{D}_n^+) = S(\mathbb{D}_n)$, except $\mathbb{D}_4^+ \simeq \mathbb{Z}^4$ and $\mathbb{D}_8^+$, which is the lattice $\mathbb{E}_8$. Similarly, one has $\min \mathbb{A}_n^r = 2$ except if $r = n+1$, $r = \frac{n+1}{2}$ and $(n,r) = (5,2)$ and then $S(A_n^r) = S(\mathbb{A}_n)$ except for $\mathbb{A}_7^2 \simeq \mathbb{E}_7$ and $\mathbb{A}_8^3 \simeq \mathbb{E}_8$.

We now construct the unimodular Coxeter lattices as orthogonal to a Lorentzian vector $v = (v_1, \dots, v_n; v_0)$ of norm -1.

Theorem 3.3. (1) *Let $r \geq 2$, let $n = r^2 - 1$ and let $v = (1^n; r)$. Then the orthogonal of v is isometric to $\mathbb{A}_n^r$.*
(2) *Let $n = 4m \geq 2$ and let $v = (m-1, 1^{n-1}; m+1)$. Then the orthogonal of v is isometric to $\mathbb{D}_n^+$.*

Proof. Consider any vector v.
(i) If $v_i = 1$ for some i, then x with $x_i = 2$ and $x_j = v_j$ if $j \neq i$ is a vector of norm 2.
(ii) If $v_{i_1} = \cdots = v_{i_k} = a$, say, for some $k \geq 2$, the vectors having components a permutation of $1, -1, 0^{k-2}$ at $i_1, \dots, i_k$ and 0 otherwise constitute a root system of type $\boldsymbol{A}_{k-1}$.
(iii) If $a = 1$, the vectors defined by (i) or (ii) constitute a system of type $\boldsymbol{A}_k$.
(iv) If $v_\ell = v_0 - 2$ for some ℓ, the vectors of (iii) together with vectors having components 1 at ℓ and two subscripts in $i_1, \dots, i_k$, -1 at 0, and 0 otherwise constitute a root system of type $\boldsymbol{D}_{k+1}$.
[Proof: one constructs a Gram matrix with the convenient entries 2 or 1 for systems $\boldsymbol{A}_?$, and one pair of entries 0 for systems $\boldsymbol{D}_?$, starting with $k-1$ vectors $(1, -1, 0^{n-2}; 0)$ for (ii), and completing them first by one vector of the form (i), and finally one vector of the form (iv).]

The proof of (1) is now easy. By (iii) above, $v^\perp$ is a unimodular lattice which contains $\mathbb{A}_n$, hence isometric to $\mathbb{A}_n^r$ with $r = \sqrt{n+1}$.

To prove (2), we extend using (iv) the root system of type $\boldsymbol{A}_{n-1}$ arising from $v_2, \dots, v_n$ to a system of type $\boldsymbol{D}_n$. This shows that $v^\perp$ is a unimodular lattice containing $\mathbb{D}_n$, hence isometric to $\mathbb{D}_n^+$ or $\mathbb{Z}^n$, thus to $\mathbb{D}_n^+$ if m is even, and in particular if $m = 2$.

Let $m \geq 3$. Then the vectors of norm 2 in both $\mathbb{Z}^n$ and $\mathbb{D}_n^+$ are exactly those of $\mathbb{D}_n$. Vectors of $\mathbb{Z}^n$ are then of the form $\frac{x+y}{2}$ for two orthogonal vectors of norm 2. It is easily checked that no sum $x + y$ has even components. (Transitivity of the automorphism group on the roots shows that we may even fix x, for instance, $x = e_1$.)
[With the notation of Proposition 3.1, in the identification of $\mathbb{E}_8$ with $\mathbb{A}_8^3$ (resp. $\mathbb{D}_8^+$), one has $S(\mathbb{A}_8) = S_1 \cup S_4$ (resp. $S(\mathbb{D}_8) = S_2$).] □

Coxeter-like lattices can also be considered inside reducible root lattices. Here are two examples, with which we exhaust all lattices occurring in Table 1 of Section 7.

We have $[\mathbb{E}_7^* : \mathbb{E}_7] = 2$, and may write $\mathbb{E}_7^* = \mathbb{E}_7 \cup (\mathbb{E}_7 + \frac{e}{2})$ where e may be chosen of norm 6. The formula

$$L_{14} = (\mathbb{E}_7 \perp \mathbb{E}_7) \cup (\mathbb{E}_7 \perp \mathbb{E}_7 + (e, e))$$

defines an odd, unimodular lattice with minimum 3 off $\mathbb{E}_7 \perp \mathbb{E}_7$.

Let $p \geq q \geq 2$. Write $\mathbb{D}_{4p}^* = \langle \mathbb{D}_{4p}, e, \varepsilon \rangle$, e as above, ε in the canonical basis for $\mathbb{Z}^{4p}$, and similarly $\mathbb{D}_{4q}^* = \langle \mathbb{D}_{4q}, e', \varepsilon' \rangle$. Then the formula

$$L_{4p,4q} = \langle \mathbb{D}_{4p} \perp \mathbb{D}_{4q}, e + \varepsilon', e' + \varepsilon \rangle$$

defines a unimodular lattice, with minimum $q + 1$ off $\mathbb{D}_{4p} \perp \mathbb{D}_{4q}$, even if p and q are odd (e.g., the lattice with root system $2\boldsymbol{D}_{12}$ of Table 2) and odd otherwise (e.g., the lattice with root system $2\boldsymbol{D}_8$ of Table 1).
[Among low-dimensional lattices of small weight, we may also quote lattices with root systems $\boldsymbol{A}_{11} + \boldsymbol{E}_6$ ($n = 17$, $w = 6$), $\boldsymbol{A}_{17} + \boldsymbol{A}_1$ ($n = 18$, $w = 5$), and $2\boldsymbol{A}_9$ ($n = 18$, $w = 7$).]

4. Orthogonal Sums

It is well-known and easy to prove that an isometric embedding $L \hookrightarrow M$ of a unimodular lattice L into an integral lattice M identifies L with a direct factor of M, a remark we previously made in Section 3.1 when $L = \mathbb{Z}$; and consideration of vectors of norm 1 shows the inequality $\mathrm{wt}(L \perp \mathbb{Z}^k) \leq \mathrm{wt}(L)$, that we generalize in the theorem below and its corollary.

Theorem 4.1. *Let*

$$v = (v_1, \dots, v_n; v_0) \in I_{n,1} \quad \textit{and} \quad v' = (v'_1, \dots, v'_n; v'_0) \in I_{n',1}$$

be primitive vectors, let $\Lambda = v^\perp$, *and let* $\Lambda' = v'^\perp$. *Let*

$$w = (v'_0 v_1, \dots, v'_0 v_n, v'_1, \dots, v'_n, ; v_0 v'_0) \in I_{n+n',1}\,.$$

Then, if Λ *is unimodular, the lattice orthogonal to* w *in* $I_{n+n',1}$ *is isometric to the orthogonal sum* $\Lambda \perp \Lambda'$.

Proof. Set $M = w^\perp$. The map

$$x = (x_1, \dots, x_n; x_0) \mapsto (x_1, \dots, x_n, 0 \dots, 0; x_0)$$

maps Λ isometrically onto a sublattice Λ_1 of M. Since Λ is unimodular, M is the direct sum of Λ_1 and of its orthogonal Λ_1' in M. Let V' be the orthogonal of Λ_1 in the rational vector space $V = \mathbb{Q} \otimes I_{n+n',1}$. Identify v with the vector $(v_1, \dots, v_n, 0 \dots, 0; v_0) \in V$. Then, V' is the space of vectors $u \in V$ of the form

$$u = \lambda v + (0, \dots, 0, \mu_1, \dots, \mu_{n'}; 0) = (\lambda v_1, \dots, \lambda v_n, \mu_1, \dots, \mu_{n'}; \lambda v_0)$$

with $\lambda, \mu_1, \dots, \mu_{n'} \in \mathbb{Q}$. We have

$$\begin{aligned} w \cdot u &= \lambda v_0' v_1^2 + \dots + \lambda v_0' v_n^2 + \mu_1 v_1' + \dots + \mu_{n'} v_{n'}' - \lambda v_0' v_0^2 \\ &= -\lambda v_0' + \mu_1 v_1' + \dots + \mu_{n'} v_{n'}' \,. \end{aligned}$$

Hence, Λ_1' is the set of elements of w which satisfy the following two conditions:

(1) $\mu_1 v_1' + \dots + \mu_{n'} v_{n'}' = \lambda v_0'$;
(2) $\lambda v_0, \lambda v_1, \dots, \lambda v_n, \mu_1, \dots, \mu_n \in \mathbb{Z}$.

Since v is primitive, the second condition means simply that λ, $\mu_1, \dots, \mu_n$ are integral. The map

$$(\mu_1, \dots, \mu_{n'}; \lambda) \mapsto \lambda v + (0, \dots, 0, \mu_1, \dots, \mu_{n'}; 0) : \Lambda' \to V'$$

is then clearly an isomorphism of Λ' onto Λ_1'. But we have

$$\begin{aligned} N((\lambda v_1, \dots, \lambda v_n, \mu_1, \dots, \mu_{n'}; \lambda v_0)) &= \lambda^2 (v_1^2 + \dots + v_n^2 - v_0^2) + \mu_1^2 + \ldots + \mu_{n'}^2 \\ &= \mu_1^2 + \ldots + \mu_n^2 - \lambda^2 = N((\mu_1, \dots, \mu_{n'}; \lambda)) \,. \end{aligned}$$

Hence, the isomorphism above is an isometry. □

Corollary 4.2. *If Λ and Λ' are unimodular, then*

$$\mathrm{wt}(\Lambda \perp \Lambda') \le \mathrm{wt}(\Lambda) \cdot \mathrm{wt}(\Lambda').$$

□

Question 4.3. *Does equality always hold in the corollary above? In particular, is it true that* $\mathrm{wt}(\Lambda \perp \mathbb{Z}^k) = \mathrm{wt}(\Lambda)$ *whatever Λ and k?* [Equality in the second question holds if $\mathrm{wt}(\Lambda) \le 7$.]

It should be noted that the construction of the vector w used Theorem 4.1 is not symmetric on direct sums. For instance, $\mathbb{D}_{16}^+ \perp \mathbb{E}_8$ and $\mathbb{E}_8 \perp \mathbb{D}_{16}^+$ give for the Niemeier lattice with root system $\boldsymbol{D}_{16} + \boldsymbol{E}_8$ the distinct representations $(9, 3^{15}, 1^8; 15)$ and $(5^8, 3, 1^{15}, 15)$. The other occurrences of distinct representations for a same Niemeier lattice are listed in Section 7.

5. Lower bounds for the weight

In this section we consider unimodular lattices Λ of minimum ≥ 3 (lattices without roots). The theorem below gives lower bounds for the weight of lattices of minimum ≥ 3, first in general, then in the particular case of even lattices. Note that this theorem does not give specific lower bounds for odd lattices of minimum ≥ 4.

Theorem 5.1. *Let Λ be an n-dimensional unimodular lattice.*

(1) *If* $\min\Lambda \geq 3$, *then* $\mathrm{wt}(\Lambda)^2 \geq \frac{(n+1)(n+2)(2n+3)}{6}$, *and equality holds only for one unimodular lattice of dimension* 23, *the* shorter Leech lattice O_{23}, *of weight* 70.

(2) *If Λ is* even *and if* $\min\Lambda \geq 4$, *then* $\mathrm{wt}(\Lambda)^2 \geq \frac{(n+1)(2n+1)(2n+3)}{3}$. *If $n = 24$, this implies* $\mathrm{wt}(\Lambda) \geq 145$, *and equality then holds if and only if Λ is isometric to the Leech lattice Λ_{24}.*

Proof. We express Λ as the orthogonal in $I_{n,1}$ of $v = (v_1, \dots, v_n; v_0)$ where $v_0 = \mathrm{wt}(\Lambda)$,

Set $S_2(m) = 1^2 + 2^2 + \cdots + m^2$ and denote by $S_{2,odd}(m)$ the sum of odd squares up to m. We have

$$S_2(m) = \frac{m(m+1)(2m+1)}{6}$$

and

$$S_{2,odd}(2m+1) = S_2(2m+1) - 2^2 S_2(m) = \frac{(m+1)(2m+1)(2m+3)}{3}.$$

Assertions (i) and (ii) at the beginning of the proof of Theorem 3.3 show that if $\min\Lambda \geq 3$, the components $v_1, \dots, v_n$ of v are distinct and at least 2, and Corollary 2.3 shows that they must be odd under condition (2). This proves the bounds $v_0 \geq S_2(n+1)$ under condition (1) and $v_0 \geq S_{2,odd}(2n+1)$ under condition (2), which are the lower bounds we need.

Putting $n = 23$ in (1), we obtain $v_0^2 \geq \frac{24\cdot 25\cdot 49}{6} = 70^2$. This shows that if equality holds in (1) for $n = 23$, then Λ is necessarily orthogonal to $v = (24, 23, \dots, 5, 3; 70)$ (up to a permutation of $v_1, \dots, v_n$)), but we cannot exclude *a priori* the existence of vectors of norm 1 or 2 in Λ. That $\min\Lambda$ is 3 was proved (Batut), using a program producing a Gram matrix for Λ and computing the minimum of Λ by standard Euclidean procedures. This identifies Λ with O_{23}, the only unimodular lattice of dimension ≤ 23 and minimum ≥ 3.

That $n = 23$ is the only possible choice is a consequence of the following theorem: *the only integral points with strictly positive coordinates on the elliptic curve* $6y^2 = x(x+1)(2x+1)$ *are* $(1, 1)$ *and* $(23, 70)$. [This is a theorem of G.N. Watson (1918); other proof by W. Ljunggren (1952); see [Mor], p. 258; nowadays one could use Baker's method.]

Finally putting $n = 24$ in (2), we obtain $v_0^2 \geq \frac{25\cdot 49\cdot 51}{3} = 20825$, hence $v_0 \geq 144.308\dots$, i.e. $v_0 \geq 145$. We observe that $145^2 - 20825 = 200 = 51^2 - 49^2$, which implies that if equality holds in (2) for $n = 24$, then Λ is necessarily orthogonal to $v = (51, 47, 45, \dots, 5, 3; 145)$. A computation with a Gram matrix shows that Λ has no roots. This identifies Λ with the Leech lattice Λ_{24}, the only unimodular lattice of dimension ≤ 24 and minimum ≥ 4. (That we can obtain Leech by this construction has been known for some time; see Chapter 26 of [C-S].) $\square$

It is somewhat puzzling that searching for lattices of minimum ≥ 3 among those having a small weight quickly forces the discovery of the remarkable lattices O_{23} and Λ_{24}. Up to dimension 26 there are four unimodular lattices of minimum ≥ 3, namely O_{23}, Λ_{24}, the *odd Leech lattice* O_{24}, and one lattice (discovered by Conway, uniqueness proved by Borcherds) that we shall denote by O_{26}. They are also easily found using Theorem 5.1.

For $n = 24$, we must have $\mathrm{wt}(\Lambda) \geq \sqrt{5525} = 74.33\dots$, and since $75^2 - 5525 = 100 = 26^2 - 24^2$, the minimal possible weight is ≥ 75, and 75 may occur only with $v = (26, 25, 23, 22, 21, \dots, 7, 5, 3; 75)$. It turns out that $v^\perp$ has minimum 3.

For $n = 26$, the lower bound is $\sqrt{6930} = 83.24\dots$. We must go up to $v_0 = 89$. Then we have $89^2 - 6930 = 991 = 28^2 + 29^2 - 25^2 - 3^2$, and we obtain this way a lattice of minimum 3.

Such lattices have been classified in dimensions 27 and 28 by Bacher and Venkov ([Bc-Ve]). We content ourselves with one example with $n = 27$, which needs $v_0 \geq \sqrt{7714} = 88$. Using the equality $91^2 - 7714 = 36^2 - 27^2$, we construct one of the Bacher-Venkov lattices ($s = 1332$, $|\mathrm{Aut}| = 7680$).

To finish this section we establish lower bounds for the weight of unimodular lattices with root system $n\boldsymbol{A}_1$.

Theorem 5.2. *Let Λ be an n-dimensional unimodular lattice with root system $n\boldsymbol{A}_1$. Then n is even, say, $n = 2m$, and we have*

$$\mathrm{wt}(\Lambda) \geq \frac{(m+1)(2m^2+4m+3)}{3},$$

and even

$$\mathrm{wt}(\Lambda)^2 \geq \frac{(2m+1)(4m^2+4m+3)}{3} = \frac{(n+1)(n^2+2n+3)}{3}$$

if Λ is even.

Proof. Let $\Lambda_0 = \mathbb{A}_1^{\perp n}$. We have $[\Lambda : \Lambda_0]^2 = \det(\Lambda_0) = 2^n$. Hence n is even. Set $n = 2m$, and write $\Lambda = v^\perp$ for some $v \in I_{n,1}$. Minimizing the sum $v_1^2 + \cdots + v_n^2$ under assertions (i) and (ii) at the beginning of the proof of Theorem 3.3, we see that the best we can do is to choose v with one component 1 and $m-1$ distinct pairs (v_j, v_j) with $v_j \ge 2$. This implies $v_0^2 \ge 1 + 1^2 + 2(2^2 + \cdots + m^2) + (m+1)^2$, which is the first inequality above. Similarly choosing all v_i odd implies $v_0^2 \ge 1 + 1^2 + 2(3^2 + \cdots + (2m-1)^2) + (2m+1)^2$, from which the second inequality follows. □

Here are examples of each of the lower bounds above.

Applied with $n = 22$ the first inequality reads $v_0^2 \ge 34^2$. This defines a lattice of minimum 2, thus the known lattice with root system $22\boldsymbol{A}_1$, which is consequently of weight 34.

Applied with $n = 24$ the second inequality implies $v_0 \ge \sqrt{5225} = 72.284\ldots$. Since $73^2 - 5225 = 27^2 - 25^2$, replacing in the proof of Theorem 5.2 the last term 25^2 by 27^2, we construct a lattice of minimum 2 (because it it even), whose root system contains, hence is equal to $24\boldsymbol{A}_1$.

Similar arguments apply to Niemeier lattices with root systems $12\boldsymbol{A}_2$ and $8\boldsymbol{A}_3$, giving for their weights the lower bounds 37, 49 from which we easily deduce the exact values wt $= 39$, 51 respectively.

6. More on Small Norms and Small Weights

We give here some complements to Section 3. We consider a vector $v = (v_1, \ldots, v_n; v_0) \in I_{n,1}$ of strictly negative norm $-d$, and assume that $v_1 \ge v_2 \ge \cdots \ge v_n$ and $v_0 > 0$.

6.1. **Small Norms.** Let $x = (x_1, \ldots, x_n; x_0)$ of norm $t > 0$ in $E = v^\perp$. Negating x if need be, we may moreover assume that x_0 is also non-negative. We have the following three relations between the v_i, x_i and t:

$$(1) \qquad v_1^2 + \cdots + v_n^2 = v_0^2 - d$$

$$(2) \qquad v_1 x_1 + \cdots + v_n x_n = v_0 x_0$$

$$(3) \qquad x_1^2 + \cdots + x_n^2 = x_0^2 + t\,.$$

This implies

$$(v_0x_0)^2 = (v_1x_1+\cdots+v_nx_n)^2 \le (v_1^2+\cdots+v_n^2)\,(x_1^2+\cdots+x_n^2) = (v_0^2-d)\,(x_0^2+t)\,,$$

whence the crude estimates

$$x_0^2 \le t\big(\tfrac{v_0^2}{d} - 1\big) \quad \text{and} \quad x_1^2 + \cdots + x_n^2 = x_0^2 + t \le \tfrac{tv_0^2}{d}\,,$$

which bound the components of x.

The combination $(1) - 2 \times (2) + (3)$ yields the following identity involving the Lorentz distance between x_0 and v_0:

$$(x_1 - v_1)^2 + \cdots + (x_n - v_n)^2 = (x_0 - v_0)^2 + t - d\,,$$

which shows the existence of a kind of symmetry exchanging the values 0 and v_0 in x: setting $y = x - v$ (thus, $y_i = x_i - v_i$) transforms the conditions "$x \cdot v = 0$ and $N(x) = t$" into "$y \cdot v = d$ and $N(y) = t - d$". [More generally, using combinations $\lambda^2(1) - 2\lambda\mu\,(2) + \mu^2(3)$, we obtain $(\mu x_1 - \lambda v_1)^2 + \cdots + (\mu x_n - \lambda v_n)^2 = (\mu x_0 - \lambda v_0)^2 + \mu^2 t - \lambda^2 d$.]

6.2. **Reduction.** Let us say that v is *reduced* if for every vector v' in the orbit of v we have $|v'_0| \geq v_0$. It would be interesting to find restrictive conditions on the v_i that satisfy reduced vectors v. Unfortunately I must content myself with the following two examples, proved using reflections along vectors $e = (e_1, \dots, e_n; e_0)$ of norm ± 2, that we assume to have a non-negative component e_0.

(1) If $N(e) = +2$ and $e_0 \geq 1$, then $e_1 v_1 + \cdots + e_n v_n \leq e_0 v_0$;
(2) If $N(e) = -2$ and $e_0 \geq 2$, then $e_1 v_1 + \cdots + e_n v_n \leq (e_0 - \frac{1}{e_0}) v_0$.

Taking $e = (1^3, 0^{n-3}, 1)$, (1) reads (1'): $v_1 + v_2 + v_3 \leq v_0$. We shall use this condition to prove the well-known classification result, easily proved by more usual methods (even under the less restrictive condition $n \leq 11$): *A unimodular lattice Λ of dimension $n \leq 9$ is isometric to $\mathbb{Z}^n$ or to $\mathbb{E}_8 \perp \mathbb{Z}^{n-8}$.*

Proof. Write $\Lambda = v^\perp$ with v reduced. We have

$$v_0^2 - 1 = v_1^2 + \cdots + v_n^2 = (v_1 + v_2 + v_3)^2 - T$$

where

$$T = (v_1 v_2 - v_4^2) + (v_1 v_2 - v_5^2) + (v_1 v_3 - v_6^2) + (v_1 v_3 - v_7^2) + (v_2 v_3 - v_8^2) + (v_2 v_3 - v_9^2)$$

is the sum of six non-negative terms. We have $v_1 + v_2 + v_3 \leq v_0$, If this inequality is strict, then we have

$$T = (v_1 + v_2 + v_3)^2 - v_0^2 + 1 \leq (v_0 - 1)^2 - v_0^2 + 1 = -2(v_0 - 1) \leq 0\,,$$

hence $v_0 = 1$ and $\Lambda \simeq \mathbb{Z}^n$. Otherwise, we have $v_1 + v_2 + v_3 = v_0$, hence $T = 1$, which implies $v_3 = v_1$. Writing $T = \sum_{i=4}^{9}(v_1^2 - v_i^2)$, we see that $v_1 = \cdots = v_8$, $v_9 < v_8$ and $v_8^2 - v_9^2 = 1$. Thus we must have $v_8 = 1$, $v_9 = 0$ and $v_0 = 3$. □

7. Tables

I reproduce here tables of unimodular lattices, first odd or even up to dimension 16 (with no component $\mathbb{Z}$), then even in dimension 24. These tables were computed by Christian Batut. His calculations do not provide any classification result; they were just intended to give the weight of all unimodular lattices either of dimension up to 16, or even and of dimension up to 24: indeed they make use of the known classification results, which can be read in [C-S], Chapter 16.

TABLE 1. Unimodular lattices of dimension $n \leq 16$

dim.	weight	vector	root system
0	1	$\emptyset$	$\emptyset$
8	3	1^8	$\boldsymbol{E}_8$
12	4	$2, 1^{11}$	$\boldsymbol{D}_{12}$
14	6	$2^7, 1^7$	$2\boldsymbol{E}_7$
15	4	1^{15}	$\boldsymbol{A}_{15}$
16	5	$3, 1^{15}$	$\boldsymbol{D}_{16}$
	9	$3^8, 1^8$	$2\boldsymbol{E}_8$
	6	$3^2, 2, 1^{13}$	$2\boldsymbol{D}_8$

In practice, to construct Table 2, say, we consider increasing odd weights $w = 3, 5, \dots$, and partitions $24 = a_1 + \cdots + a_k$ with non-negative a_i such that $a_1(w-2)^2 + a_2(w-4)^2 + \cdots + a_k 1^2 = w^2 - 1$, construct a Gram matrix M for the orthogonal to the vector $v = (v_1, \dots, v_{24}; w)$ with $v_i = w - 2$ for $1 \leq i \leq a_1$, $v_i = w - 4$ for $a_1 + 1 \leq i \leq a_1 + a_2$, etc, and test M for equivalence with matrices which have been previously found. The process stops when we have found the right number (24) of pairwise non-equivalent matrices.

Thanks to the weight calculations done at the end of Section 5 which gave the weights of lattices with root systems $\emptyset$, $24\boldsymbol{A}_1$, $12\boldsymbol{A}_2$, $8\boldsymbol{A}_3$, it actually suffices to consider weights only up to $w = 37$.

The *PARI-GP*-code below (an updated version of a code due to Batut) produces a Gram matrix for a given vector v, which can then be reduced to shorten its identification.
Input : a vector v with integer components;
Output: an $n \times n$ matrix with $n = length(v) - 1$.

```
{gramlz(v) =
local(m=#v,u,w);
v[m]=-v[m];u=matkerint(Mat(v));w=u;w[m,]=-w[m,];
w~*u;}
```

It was observed in Section 4 that the weight of the Niemeier lattice with root system $\boldsymbol{D}_{16} + \boldsymbol{E}_8$ could be produced by two distinct representations. Here are other examples:
$4\boldsymbol{A}5 + \boldsymbol{D}4$: $(9^4, 7^5, 5^4, 3^6, 1^5)$, $(9^4, 7^4, 5^6, 3^6, 1^4)$, $(9^3, 7^6, 5^6, 3^4, 1^5)$;
$\boldsymbol{D}_{10} + 2\boldsymbol{E}_7$: $(11, 5^{10}, 3^7, 1^6)$, $(7^7, 5, 3^7, 1^9)$;
$4\boldsymbol{E}_6$: $(15, 9^5, 7^6, 5^6, 3, 1^5)$, $(11^6, 9^2, 5^6, 3^5, 1^5)$, $(11^6, 9, 7^2, 5^5, 3^6, 1^4)$;
$8\boldsymbol{A}_3$: $(13^3, 11^4, 9^3, 7^3, 5^4, 3^4, 1^3)$, $(13^3, 11^3, 9^4, 7^4, 5^4, 3^3, 1^3)$.

Table 2. The 24 Niemeier lattices

weight	symbol	vector	Coxeter	root system
5	δ	1^{24}	$h=25$	$\boldsymbol{A}_{24}$
7	α	$5,1^{23}$	$h=46$	$\boldsymbol{D}_{24}$
9	ζ	$3^7,1^{17}$	$h=18$	$\boldsymbol{A}_{17}+\boldsymbol{E}_7$
11	θ	$5,3^9,1^{14}$	$h=16$	$\boldsymbol{A}_{15}+\boldsymbol{D}_9$
	κ	$3^{12},1^{12}$	$h=13$	$2\boldsymbol{A}_{12}$
13	ϵ	$7,3^{12},1^{11}$	$h=22$	$2\boldsymbol{D}_{12}$
15	β	$9,3^{15},1^8$	$h=30$	$\boldsymbol{D}_{16}+\boldsymbol{E}_8$
	λ	$5^6,3^7,1^{11}$	$h=12$	$\boldsymbol{A}_{11}+\boldsymbol{D}_7+\boldsymbol{E}_6$
	ν	$5^5,3^{10},1^9$	$h=10$	$2\boldsymbol{A}_9+\boldsymbol{D}_6$
17	o	$5^8,3^9,1^7$	$h=\ 9$	$3\boldsymbol{A}_8$
19	ι	$9,5^8,3^8,1^7$	$h=14$	$3\boldsymbol{D}_8$
21	η	$11,5^{10},3^7,1^6$	$h=18$	$\boldsymbol{D}_{10}+2\boldsymbol{E}_7$
	ρ	$7^4,5^7,3^7,1^6$	$h=\ 7$	$4\boldsymbol{A}_6$
	π	$7^5,5^5,3^7,1^7$	$h=\ 8$	$2\boldsymbol{A}_7+2\boldsymbol{D}_5$
25	η	$11,7^6,6^6,3^6,1^5$	$h=10$	$4\boldsymbol{D}_6$
27	γ	$9^8,3^8,1^8$	$h=30$	$3\boldsymbol{E}_8$
	σ	$9^4,7^5,5^4,3^6,1^5$	$h=6$	$4\boldsymbol{A}_5+\boldsymbol{D}_4$
31	υ	$11^2,9^4,7^5,5^4,3^5,1^4$	$h=5$	$6\boldsymbol{A}_4$
33	μ	$15,9^5,7^6,5^6,3,1^5$	$h=12$	$4\boldsymbol{E}_6$
37	τ	$15,11^4,9^4,7^4,5^4,3^4,1^3$	$h=6$	$6\boldsymbol{D}_4$
39	ϕ	$13^3,11^4,9^3,7^3,5^4,3^4,1^3$	$h=4$	$8\boldsymbol{A}_3$
51	χ	$17^3,15^2,13^3,11^3,9^2,7^3,5^3,3^3,1^2$	$h=3$	$12\boldsymbol{A}_2$
73	ψ	$27,23^2,21^2,19^2,17^2,15^2,13^2,11^2,9^2,7^2,5^2,3^2,1$	$h=2$	$24\boldsymbol{A}_1$
145	ω	$51,47,45,43,\ldots,9,7,5,3$	$h=0$	$\emptyset$

References

[Bc-Ve] R. Bacher, B. Venkov, *Réseaux entiers unimodulaires sans racines en dimension* 27 *et* 28, in Réseaux euclidiens, designs sphériques et formes modulaires, J. Martinet, ed., L'Ens. Math., Monographie **37**, Genève (2001), 212–267.

[C-S] J.H. Conway, N.J.A. Sloane, *Sphere Packings, Lattices and Groups*, Grundlehren **290**, Springer-Verlag, Heidelberg (1988); third edition: 1999.

[Mar] J. Martinet, *Perfect Lattices in Euclidean Spaces*, Grundlehren **327**, Springer-Verlag, Heidelberg, (2003).

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

[Mor] L.J. Mordell, *Diophantine Equations*, Academic Press, New-york (1969).

[PARI] *PARI/GP, a computer algebra system designed for fast computations in number theory*, url http://pari.math.u-bordeaux.fr/ .

[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).

Jacques Martinet,
Villa 30, Hameau de Noailles,
33400 Talence, France
E-mail address: Jacques.Martinet@math.cnrs.fr