Appendix to "Reduction Modulo 2 and 3 of Euclidean Lattices": the Proof

The aim of this appendix is to prove the following theorem:

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:*

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

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

We consider a lattice Λ of norm 3 such that all classes modulo 2 possess representatives of norm at most $2N(\Lambda) = 6$.

A.2. Lemma. *Let Λ be a lattice of norm 3 such that all classes modulo 2 possess representatives of norm at most $2N(\Lambda) = 6$.*

(1) *Λ contains no norm 7 vectors.*

(2) *Any vector of norm 8 (resp. 9) in Λ is of the form $x = e + 2y$ with $N(e) = 4$ (resp. $N(e) = 5$), $N(y) = 3$, and $e \cdot y = -2$.*

Proof. Any vector $x \in \Lambda \smallsetminus 2\Lambda$ must be congruent modulo 2 to a vector $e \neq 0$ with norm $N(e) \leq 6$. This norm must be one of the integers 3, 4, 5, or 6, and is well defined by its value modulo 4. The congruence $N(x) \equiv N(e) \mod 4$ shows that the norm of e is itself well defined.

Changing e into $-e$ if need be, we may assume that $e \cdot x \geq 0$. Let $y = \frac{1}{2}\,(x - e)$. If $N(x) \leq 10$, we have $N(x) = N(e) + 4$, hence

$$N(x) \leq 10 \text{ and } x \notin 2\Lambda \implies N(y) \leq \frac{1}{4}\,(N(x) + N(e)) = 1 + \frac{1}{2}\,N(e)\,.$$

Applied to an x of norm 7, this inequality yields the upper bound $N(y) < 3$, hence $y = 0$. This is plainly impossible, whence (1).

Calculating $e \cdot y$ from the identity $N(x) = N(e) + 4\,e \cdot y + 4\,N(y)$, we obtain

$$N(x) \leq 10 \text{ and } x \notin 2\Lambda \implies e \cdot y = 1 - N(y)\,.$$

If $N(x) = 8$ (resp. if $N(x) = 9$), we have $N(e) = 4$ (resp. $N(e) = 5$), hence $N(y) < 4$, i.e. $N(y) = 3$, whence (2). $\square$

[The proof above shows that vectors of norm 8 (resp. 9) must be sums of one vector of norm 3 (resp. 4) and of one vector of norm 3, namely $e + y$ and y.]

We now consider well rounded lattices Λ of norm 3, and investigate necessary conditions for Λ to possess representatives modulo 2 of norm at most 6. Note that the scalar products $e \cdot e'$ for $e, e' \in S(\Lambda)$ are equal to ± 3 if e and e' are proportional, and to 0 or ± 1 otherwise. Recall that for $n \leq 4$, n independent minimal vectors of a lattice L constitute a basis of L, except perhaps if $n = 4$ and L is similar to the root lattice $\mathbb{D}_4$. (See [M], Chapter VI, Corollary 2.3.) Since a scaled copy of $\mathbb{D}_4$ with minimum 3 is not integral, this exception shall never occur.

We shall now study when $r \le 4$ the possibility for r independent vectors of Λ to occur as minimal vectors. There is not much to say if $r = 2$: two minimal vectors span a lattice L which is defined up to isometry by one of the Gram matrices

$$M_2 = \begin{pmatrix} 3 & 1 \\ 1 & 3 \end{pmatrix} \quad \text{or} \quad M_2' = \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix},$$

and $\Lambda/2\Lambda$ possesses representatives of norms 3 and 4, or 3 and 6. Moreover, the discussion below will show that such lattices may be embedded in 3- and 4-dimensional lattices Λ as in Theorem A.1.

Next, we consider the lattice L generated by $r = 3$ independent vectors e_1, e_2, e_3 of $S(\Lambda)$. (It would indeed suffice to suppose that no two of them are proportional.)

A.3. Lemma. *A lattice L generated by three minimal vectors in some lattice Λ of dimension $n \ge 3$ possesses a Gram matrix equal to one of the matrices*

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

A lattice with Gram matrix M_3 is isometric to $\mathbb{A}_3^*$. For M_3 (resp. M_3'), we have $s_3 = 4$, $s_4 = 3$, $s_5 = s_6 = 0$ (resp. $s_3 = 3$, $s_4 = 2$, $s_5 = 1$, $s_6 = 2$). The weighted formulae for classes modulo 2 are $3 + 4 = 2^3 - 1$ and $3 + 2 + 1 + \frac{1}{2}2 = 2^3 - 1$ respectively.

Proof. Replacing e_1 by $-e_1$ transforms M_3 into a matrix with entries -1 outside the diagonal, which is indeed a Gram matrix for $\mathbb{A}_3^*$ (see [M], Chapter IV, proof of Proposition 2.3). The data for M_3 and M_3' are easy to calculate, and we are left we the classification assertions, for the proofs of which we distinguish four cases according to the number $(0, 1, 2$ or $3)$ of scalar products $e_i \cdot e_j$, $i < j$ which are zero.

In the first two cases, we may assume that $e_1 \cdot e_2 = e_1 \cdot e_3 = +1$. Then, the value $e_2 \cdot e_3 = -1$ must be excluded, since it implies $N(e_1 + 2_2 - e_3) = 7$, and we are left with the Gram matrices M_3 and M_3'.

In the last two cases, we may assume that $e_1 \cdot e_3 = e_2 \cdot e_3 = 0$. If $e_1 \cdot e_2 = \pm 1$, then $N(e_1 \mp e_2 + e_3) = 7$. We must thus have $e_1 \cdot e_2 = 0$. We shall prove that the vector $x = e_1 + e_2 + e_3$ of norm 9 cannot be congruent modulo 2 to a vector $e \in \Lambda$ of smaller norm.

Suppose that we have in Λ an equality $x = e + 2y$ with $N(e) < 9$. Then, as in lemma 2, we have $N(e) = 5$ and $N(y) = 3$, and we may assume that $x \cdot e \ge 0$, which implies $e \cdot x = \pm 1$. Since the congruence $x' \equiv e \mod 2$ holds for any $x' = \pm e_1 \pm e_2 \pm e_3$, we always have $e' \cdot x = +1$ or $e' \cdot x = -1$. If $(e_1 + e_2 - e_3) \cdot e = +1$, then $e \cdot e_3 = 0$. This is impossible, since we would have $3 = e_3 \cdot x = 2e_3 \cdot y$. We thus have $(e_1 + e_2 - e_3) \cdot e = -1$, and similarly $(e_1 - e_2 + e_3) \cdot e = (-e_1 + e_2 + e_3) \cdot e = -1$, which implies $e_1 \cdot e = e_2 \cdot e = e_3 \cdot e$, hence $e_i \cdot e = \frac{1}{3} x \cdot e = \frac{1}{3}$. This is again impossible, $\square$

Next we consider systems of four independent minimal vectors $e_1, e_2, e_3, e_4 \in \Lambda$.

A.4. Lemma. *A lattice L generated by four independent minimal vectors in some norm 3 latice Λ of dimension $n \geq 4$ possesses a Gram matrix equal to*

$$M_4 = \begin{pmatrix} 3 & 0 & 1 & 1 \\ 0 & 3 & 1 & 1 \\ 1 & 1 & 3 & 0 \\ 1 & 1 & 0 & 3 \end{pmatrix}.$$

The invariants s_m for M_4 are $s_3 = 4$, $s_4 = 5$, $s_5 = s_6 = 4$, and the weighted formula for M_4 is $4 + 5 + 4 + \frac{1}{2}4 = 2^4 - 1$.

Proof. Let t be the number of zeroes among the scalar products $e_i \cdot e_j$, $i < j$.

If $t \leq 1$, we may assume that $e_1 \cdot e_2 = e_1 \cdot e_3 = e_1 \cdot e_4 = +1$ and that $e_i \cdot e_j \neq 0$ for $i < j$ except possibly for $e_3 \cdot e_4 = 0$. lemma 3 shows that we must have $e_2 \cdot e_3 = e_2 \cdot e_4 = -1$ and $e_3 \cdot e_4 = 0$ or 1, which yields the Gram matrices

$$M = \begin{pmatrix} 3 & 1 & 1 & 1 \\ 1 & 3 & -1 & -1 \\ 1 & -1 & 3 & -1 \\ 1 & -1 & -1 & 3 \end{pmatrix} \quad \text{and} \quad M' = \begin{pmatrix} 3 & 1 & 1 & 1 \\ 1 & 3 & -1 & -1 \\ 1 & -1 & 3 & 0 \\ 1 & -1 & 0 & 3 \end{pmatrix}.$$

These two possibilities must be excluded, the first one because $\det(M) = 0$ (the firts row of M is the sum of the three other ones), and the second one because $N(-e_1 + e_2 + e_3 + e_4) = 2$.

We thus have $t \geq 2$. We must exclude the possibility $e_i \cdot e_j = e_i \cdot e_k = 0$, which would contradict lemma A.3. Hence, after permuting the indices, we may assume that $e_1 \cdot e_2 = e_3 \cdot e_4 = 0$ and that $t = 2$. Replacing e_i by $-e_i$ for some indices $i \in \{2, 3, 4\}$, we may then assume that $e_1 \cdot e_3 = e_1 \cdot e_4 = e_2 \cdot e_3 = +1$, and we are left with two possible Gram matrices, namely

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

The values of s_3, s_4, s_5, s_6 are easily calculated for M_4 and for M_4', and this immediately proves the assertions about M_4 which are stated in the lemma. For M_4', we have $s_3 = s_4 = s_5 = s_6 = 4$, and the four pairs of vectors of norm 6 are $\pm(e_1 \pm e_2)$ and $\pm(e_3 \pm e_4)$. They represent exactly two classes in $L/2L$, and the corresponding weight formula is $4 + 4 + 4 + \frac{1}{2}4 = 14 < 2^4 - 1$. Hence, if M_4' occurs in some lattice Λ, its dimension must be at least 5.

The next invariants s_m of M_4' are $s_7 = 0$ and $s_8 = 8$, and vectors of norm 8 share out among two types: 4 pairs are of the form $e_i \pm e_j$; these are congruent modulo 2 to the vectors $e_i \mp e_j$, of norm 4, and 4 pairs which all represent the missing class of L modulo 2. A typical vector of this last type is $x = e_1 + e_2 - e_3 - e_4$. We shall show that no congruence $x \equiv e \mod 2\Lambda$ with $N(e) < N(x)$ may exist in Λ.

Otherwise, write $x = e + 2y$. As in lemma 2, we may assume that we have $x \cdot e \geq 0$, which implies $N(e) = 4$, $N(y) = 3$, and $e \cdot y = -2$. Since e (of norm 4) and the e_i (of norm 3) are not proportional, we have $N(e \pm e_i) \geq 3$, hence $|e \cdot e_i| \leq 2$ for all i. Similarly, since y and the e_i may not be proportional (because y is independent from the e_i), we have $|y \cdot e_i| \leq 1$. We now consider the Gram matrix of the vectors e_1, e_2, e_3, e_4 and $e_5 = y$. Taking into account the values of the $e_i \cdot x$ (respectively, $1, 3, -1, -3$), and making use of the inequalities above, we easily see that the possibilities for the scalar product $e_i \cdot y$ are $e_2 \cdot y = +1$, $e_4 \cdot y = -1$, $e_1 \cdot y = 1$ or 0 and $e_3 \cdot y = -1$ or 0. If $e_1 \cdot y$ were equal to 0, we would obtain for e_1, e_2, e_5 an impossible 3×3 Gram matrix ($e_1 \cdot e_2 = e_1 \cdot e_5 = 0$). Hence, we have $e_1 \cdot y = 1$ and similarly $e_4 \cdot y = -1$. But such a matrix may not occur, since the Gram matrix of e_1, e_3, e_4, e_5 then possesses a single set $\{i, j\}$ with $e_i \cdot e_j = 0$, a possibility that we have excluded at the beginning of the proof. $\square$

Proof of theorem A.1. Taking into account the two lemmas above, we just have to prove that there does not exist lattices Λ as in Theorem A.1 in dimension $n \geq 5$. We prove this by showing that the Gram matrix of 5 independent minimal vectors of Λ must contains non-admissible sub-matrices in dimension 3 or 4. Up to equivalence, we may assume that the 4×4 matrix in the upper left corner of the Gram matrix M' of n independent minimal vectors of Λ is the matrix M_4. It is thus possible to extract from M' a matrix of the form

$$M = \begin{pmatrix} 3 & 0 & 1 & 1 & x \\ 0 & 3 & 1 & 1 & y \\ 1 & 1 & 3 & 0 & z \\ 1 & 1 & 0 & 3 & t \\ x & y & z & t & 3 \end{pmatrix}$$

with $x, y, z, t \in \{0, \pm 1\}$. Since the Gram matrices of e_1, e_2, e_5 and of e_3, e_4, e_5 may not contain two zeroes in the same row, x, y, z, t are all non-zero. But this is not possible, since the Gram matrix of e_1, e_3, e_4, e_5 would then contain a single zero scalar product $e_i \cdot e_j$ with $i < j$. $\square$

It would be interesting to look at lattices with an odd minimum $N = 5, 7, \ldots$.