MATH-GA 2210.001: Homework Number theory 3

1. Let $m, n \in \mathbb{Z}$ with $n \geq 1$ and let $L \subset \mathbb{R}^2$ be the lattice $L = \{(a,b) \in \mathbb{Z}, a \equiv mb \bmod n\}$. Find a $\mathbb{Z}$-basis of L.

2. Show that $\{(a,b,c) \in \mathbb{Z}^3, a \equiv b \bmod 5, b \equiv a + c \bmod 2\}$ is a lattice in $\mathbb{R}^3$. Compute its covolume and give a $\mathbb{Z}$-basis.

3. Let p be a prime such that -6 is a square modulo p. Show that p (resp. $2p$) could be written as $p = a^2 + 6b^2$ iff $p \equiv \pm 1 \bmod 8$ (resp. $p \equiv \pm 3 \bmod 8$.)

4. (the lattice E_8) Let

$$D_8 = \{(x_1, \dots x_8) \in \mathbb{Z}^8, \sum x_i \equiv 0 \bmod 2\}$$

and let $e \in \mathbb{R}^8$ be the vector:

$$e = (\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}).$$

We consider the standard scalar product on $\mathbb{R}^8$.

(a) Show that D_8 is a lattice in $\mathbb{R}^8$, of covolume 2.

(b) Deduce that $E_8 := \mathbb{Z}e + D_8$ is a lattice in $\mathbb{R}^8$ of covolume 1.

(c) Verify that for any $v, w \in E_8$, one has $v \cdot v \in 2\mathbb{Z}$ and $v \cdot w \in \mathbb{Z}$.

(d) Deduce that E_8 is not of the form $g(\mathbb{Z}^8)$ for g in the orthogonal group $g \in O_8(\mathbb{R})$.