JOURNAL
de Théorie des Nombres
de BORDEAUX
anciennement Séminaire de Théorie des Nombres de Bordeaux

Tathagata BASAK

Modular lattices from finite projective planes

Tome 26, n° 2 (2014), p. 269-279.

<http://jtnb.cedram.org/item?id=JTNB_2014__26_2_269_0>

Journal de Théorie des Nombres
de Bordeaux **26** (2014), 269–279

Modular lattices from finite projective planes

par Tathagata BASAK

Résumé. En utilisant la géométrie du plan projectif sur un corps fini $\mathbb{F}_q$, nous construisons un réseau hermitien de type Lorentz L_q de dimension (q^2+q+2) defini sur un certain anneau d'entiers $\mathcal{O}$ dépendant de q. Nous montrons qu'une infinité de ces réseaux sont p-modulaires, c'est-à-dire que $pL_q' = L_q$, où p est un premier de $\mathcal{O}$ tel que $|p|^2 = q$.

Les réseaux lorentziens L_q mènent parfois à la construction de réseaux définis positifs intéressants. En particulier, si $q \equiv 3 \bmod 4$ est tel que (q^2+q+1) est la norme d'un élément de $\mathbb{Q}[\sqrt{-q}]$, alors nous obtenons un réseau entier unimodulaire M_q défini positif et de dimension paire $2q(q+1)$ tel que $\mathrm{Aut}(M_q) \supseteq \mathrm{PGL}(3,\mathbb{F}_q)$. Nous prouvons que M_3 est le réseau de Leech.

Abstract. Using the geometry of the projective plane over the finite field $\mathbb{F}_q$, we construct a Hermitian Lorentzian lattice L_q of dimension (q^2+q+2) defined over a certain number ring $\mathcal{O}$ that depends on q. We show that infinitely many of these lattices are p-modular, that is, $pL_q' = L_q$, where p is some prime in $\mathcal{O}$ such that $|p|^2 = q$.

The Lorentzian lattices L_q sometimes lead to construction of interesting positive definite lattices. In particular, if $q \equiv 3 \bmod 4$ is a rational prime such that (q^2+q+1) is norm of some element in $\mathbb{Q}[\sqrt{-q}]$, then we find a $2q(q+1)$ dimensional even unimodular positive definite integer lattice M_q such that $\mathrm{Aut}(M_q) \supseteq \mathrm{PGL}(3,\mathbb{F}_q)$. We find that M_3 is the Leech lattice.

1. Introduction

1.1. Results: Let q be a rational prime power and $n = (q^2+q+1)$. Let $\mathcal{O}$ be either the ring of rational integers or the ring of integers in a quadratic imaginary number field or Hurwitz's ring of integral quaternions. Let $p \in \mathcal{O}$ be a prime element such that $|p|^2 = q$, and $\bar{z} = z \bmod p\mathcal{O}$ for all $z \in \mathcal{O}$. Given such a triple $(\mathcal{O}, p, q)$, we shall construct a Hermitian $\mathcal{O}$-lattice L_q of signature $(1,n)$ such that $\mathrm{PGL}(3,\mathbb{F}_q)$ acts naturally on L_q and $L_q \subseteq pL_q'$. If q happens to be a rational prime, then we show that L_q is p-modular, that is $L_q = pL_q'$ (see 2.8).

Manuscrit reçu le 31 décembre 2012, accepté le 3 septembre 2013.
Classification math. 11H56, 51E20, 11E12, 11E39.

If L_q contains a norm zero vector fixed by $\mathrm{PGL}(3,\mathbb{F}_q)$, then we can split L_q as direct sum of a definite lattice Λ_q and a hyperbolic cell, where Λ_q is stable under $\mathrm{PGL}(3,\mathbb{F}_q)$ action. If $p=\sqrt{-3}$, $q=3$ and $\mathcal{O}=\mathbb{Z}[\frac{1+p}{2}]$, then Λ_q is a form of Leech lattice defined over $\mathcal{O}$. We show that if $q\equiv 3 \bmod 4$ is a rational prime and n is norm of some element in $\mathbb{Q}[\sqrt{-q}]$, then Λ_q is p-modular and $\mathrm{Aut}(\Lambda_q)\supseteq \mathrm{PGL}(3,\mathbb{F}_q)$ (see 3.3, 3.6). An appropriately scaled real form of Λ_q gives us a positive definite even unimodular $2q(q+1)$ dimensional $\mathbb{Z}$-lattice M_q such that $\mathrm{PGL}(3,\mathbb{F}_q)$ naturally acts on M_q (see 3.7). Such examples exists for $q=3,47,59,71,131,\cdots$. General conjectures in analytic number theory (for example, the Bateman-Horn conjecture) suggest that there are infinitely many such primes.

So far, we have applications of our construction only for $q=3$ and $q=2$ (see 1.2 and 1.3). However the construction goes through for a general q with no extra work. So we have chosen to present it in that form.

1.2. Examples:

(1) Let q to be a rational prime; $q\equiv 3 \bmod 4$. Let $p=\sqrt{-q}$ and $\mathcal{O}=\mathbb{Z}[\frac{1+p}{2}]$. Then the assumptions in 1.1 is satisfied. So we get infinitely many p-modular Hermitian lattices L_q.

(2) Among the lattices in (1), the lattice L_3 obtained for $q=3$ seems to be especially interesting. The reflection group of L_3 gives us a complex hyperbolic reflection group in $PU(1,13)$ having finite co-volume. Thirteen is the largest dimension in which a finite co-volume discrete reflection group in $PU(1,n)$ is known. The lattice L_3 and its construction given here plays a major role in an ongoing project (see [1], [2], [5], [7]) trying to relate the complex reflection group of L_3 and the monster via the Conway-Ivanov-Norton presentation of the bimonster (see [9], [10], [14], [15]). The construction described here came up while studying this example.

(3) Our construction also goes through if $\mathcal{O}$ is the ring of Hurwitz's quaternionic integers and $p=(1-i)$. In this case, we obtain the direct sum of a quaternionic form of the Leech lattice and a hyperbolic cell. The reflection group of this lattice has properties analogous to the reflection group of the lattice L_3 mentioned in (2); see [6].

1.3. Remarks on the construction:

- Suppose z is a primitive vector of norm 0 in L_q fixed by $\mathrm{PGL}(3,\mathbb{F}_q)$ or some large subgroup of $\mathrm{PGL}(3,\mathbb{F}_q)$. The definite lattices $z^{\perp}/z$ are sometimes interesting. In the examples (2) (resp. (3)) of 1.2 this yields a complex (resp. quaternionic) form of the Leech lattice that makes $\mathrm{PGL}(3,\mathbb{F}_3)$ (resp. $\mathrm{PGL}(3,\mathbb{F}_2)$) symmetry visible.
- Using the construction given here, we were able to find generators and relations for the reflection groups of the complex and

quaternionic hyperbolic lattices described in 1.2(2) and 1.2(3). The Coxeter-Dynkin diagram determined by these generators and relations are the incidence graphs of $\mathbb{P}^2(\mathbb{F}_3)$ and $\mathbb{P}^2(\mathbb{F}_2)$ respectively (see [5], [6]).

- The definition of the lattices L_q given in 2.5 is similar to the definition of a root lattice. In this analogy, the incidence graph of $\mathbb{P}^2(\mathbb{F}_q)$ plays the role of a Dynkin diagram. This analogy has proved to be an useful one in understanding the reflection group of the lattice L_3 mentioned in 1.2(2), and its connection with the monster (see. [5]).
- Nice lattices are often constructed using nice error correcting codes. For example see [11], pp. 197-198 and pp. 211-212. One can view our construction in this spirit, with the code being given by the incidence matrix of the points and lines of $\mathbb{P}^2(\mathbb{F}_q)$.
- Bacher and Venkov, in [4], constructed a 28 dimensional integer lattices of minimal norm 3 whose shortest vectors are parametrized by the Lagrangian subspaces in 6 dimensional symplectic vector space over $\mathbb{F}_3$. This example also seems to be related to our construction (Boris Venkov, private communications).
- Alexey Bondal pointed out to me that the construction in this paper bears similarity with his method of construction of lattices in simple Lie algebras which are invariant under the automorphisms that preserve a decomposition of the Lie algebra into mutually orthogonal Cartan subalgebras. (for example, see [8] or [16], ch. 9).
- The lattices that satisfy $pL' = L$ are called p-modular. These behave much like unimodular lattices, for example, see [17]. Appropriately scaled real form of the lattices described in (2) and (3) of 1.2 are the even unimodular lattices $II_{2,26}$ and $II_{4,28}$ respectively.
- The construction given in 2.5 probably yields more examples of Hermitian lattices defined over other rings $\mathcal{O}$, for example, certain maximal orders in rational quaternion algebras. But for simplicity of presentation we shall restrict ourselves to $\mathcal{O}$ being a ring as in 1.1.

2. Lorentzian lattices with symmetries of finite projective planes

Definition 2.1 (Hermitian lattices)**.** Let $\mathcal{O}$ be a ring as in 1.1. Let $\mathrm{Frac}(\mathcal{O})$ be its fraction field. Let L be a projective $\mathcal{O}$-module of rank n with a $\mathcal{O}$-valued Hermitian form $\langle\ |\ \rangle : L \times L \to \mathcal{O}$. We shall always assume that the Hermitian form is linear in the second variable. The *dual* module of L, denoted L', is the set of all $\mathcal{O}$-valued linear functionals on L. The Hermitian form induces a natural map $L \to L'$ given by $x \mapsto \langle x|\ \rangle$. The kernel of this map is called the *radical* of L, and is denoted by $\mathrm{Rad}(L)$. We say $(L, \langle\ |\ \rangle)$ is *non-singular* if $\mathrm{Rad}(L) = 0$. If $(L, \langle\ |\ \rangle)$ is non-singular, then we say

$(L, \langle\ |\ \rangle)$ is an $\mathcal{O}$-*lattice* of rank n. If $\mathrm{Rad}(L) \neq 0$, we say $(L, \langle\ |\ \rangle)$ is a singular $\mathcal{O}$-lattice.

We shall denote a lattice $(L, \langle\ |\ \rangle)$ simply by L. The dual of a lattice is a lattice. We may identify a lattice inside its dual using the Hermitian form. One says that L is *unimodular* if $L' = L$. One says L is p-*modular* for some $p \in \mathcal{O}$, if $L' = p^{-1}L$. A lattice L has signature (m, k) if $L \otimes_{\mathcal{O}} \mathrm{Frac}(\mathcal{O})$ has a basis whose matrix of inner products have m positive eigenvalues and k negative eigenvalues. A lattice is *Lorentzian* if it has signature $(1, k)$.

We let $\mathcal{O}^{1,k}$ be the free $\mathcal{O}$-module of rank $(k+1)$ with the Hermitian form

$$\langle (u_0, u_1, \cdots, u_k) | (v_0, v_1, \cdots, v_k) \rangle = \bar{u}_0 v_0 - \bar{u}_1 v_1 - \cdots - \bar{u}_k v_k.$$

Then $\mathcal{O}^{1,k}$ is unimodular while $p\mathcal{O}^{1,k}$ is q-modular.

Definition 2.2. Let $(\mathcal{O}, p, q)$ be as in 1.1. Let $\mathbb{P}^2(\mathbb{F}_q)$ be the projective plane over $\mathbb{F}_q$. Let

$$n = q^2 + q + 1.$$

Let $\mathcal{P}$ be the set of points and $\mathcal{L}$ be the set of lines of $\mathbb{P}^2(\mathbb{F}_q)$. The sets $\mathcal{P}$ and $\mathcal{L}$ have n elements each. If a point $x \in \mathcal{P}$ is incident on a line $l \in \mathcal{L}$, then we write $x \in l$. Let D be the (directed) incidence graph of $\mathbb{P}^2(\mathbb{F}_q)$. The vertex set of D is $\mathcal{P} \cup \mathcal{L}$. There is a directed edge in D from a vertex l to a vertex x, if $x \in \mathcal{P}$, $l \in \mathcal{L}$ and $x \in l$.

Let L_q° be the free $\mathcal{O}$–module of rank $2n$ with basis vectors indexed by $D = \mathcal{P} \cup \mathcal{L}$. Let $r, s \in D$. Define a Hermitian form $\langle\ |\ \rangle : L_q^\circ \times L_q^\circ \to \mathcal{O}$ by

$$\langle r|s\rangle = \begin{cases} -q & \text{if} \quad r = s \in D, \\ p & \text{if} \quad r \in \mathcal{P}, s \in \mathcal{L}, r \in s, \\ \bar{p} & \text{if} \quad r \in \mathcal{L}, s \in \mathcal{P}, s \in r, \\ 0 & \text{otherwise.} \end{cases} \tag{2.1}$$

Lemma 2.3. *Given $l \in \mathcal{L}$, let $w_l = \bar{p}l + \sum_{x \in l} x$. Then $\langle x'|w_l\rangle = 0$ and $\langle w_l|l'\rangle = p$ for all $x' \in \mathcal{P}$ and $l' \in \mathcal{L}$.*

Proof. The inner products are easily calculated from equation (2.1). For example, since each line l has $(q+1)$ points on it, we have

$$\langle w_l|l\rangle = p.(-q) + (q+1)p = p.$$

If l and l' are two distinct lines, then they meet at one point. So

$$\langle w_l|l'\rangle = p.0 + p = p.$$

□

Proposition 2.4. *The radical of L_q^0 has rank $(n-1)$ and $\mathrm{Rad}(L_q^0) \otimes_{\mathcal{O}} \mathrm{Frac}(\mathcal{O})$ is spanned by the vectors $(w_{l_1} - w_{l_2})$ for l_1, l_2 in $\mathcal{L}$.*

Proof. If l_1, l_2 belong to $\mathcal{L}$, then lemma 2.3 implies that $(w_{l_1} - w_{l_2}) \in \mathrm{Rad}(L_q^\circ)$. Let U be the $\mathcal{O}$-module of rank $(n-1)$ spanned by $(w_{l_1} - w_{l_2})$ for all $l_1, l_2 \in \mathcal{L}$. Then L_q°/U is a $\mathcal{O}$–module of rank $(n+1)$. Since $U \subseteq \mathrm{Rad}(L_q^\circ)$, the Hermitian form on L_q° descends to a Hermitian form on L_q°/U, which is again denoted by $\langle\ |\ \rangle$. For each $l \in \mathcal{L}$, the vectors w_l have the same image in L_q°/U; call this image $w_\mathcal{P}$. Lemma 2.3 implies that $w_\mathcal{P}$ is orthogonal (in L_q°/U) to each $x \in \mathcal{P}$ and $\langle w_\mathcal{P}|l\rangle = p$ for all $l \in \mathcal{L}$. So

$$\langle w_\mathcal{P}|w_\mathcal{P}\rangle = \langle \bar{p}l + \sum_{x\in l} x|w_\mathcal{P}\rangle = p\langle l|w_\mathcal{P}\rangle = q.$$

The matrix of inner products of the $(n+1)$ vectors $\mathcal{P} \cup \{w_\mathcal{P}\}$ in L_q°/U is a diagonal matrix with diagonal entries $(-q, -q, \cdots, -q, q)$. So L_q°/U is a non-degenerate $\mathcal{O}$–module of signature $(1, n)$. It follows that

$$U \otimes_\mathcal{O} \mathrm{Frac}(\mathcal{O}) = \mathrm{Rad}(L_q^\circ) \otimes_\mathcal{O} \mathrm{Frac}(\mathcal{O}). \qquad \square$$

Definition 2.5. Let L_q be the quotient of L_q° by its radical. Then L_q is finitely generated and torsion free. So if $\mathcal{O}$ is a Dedekind domain, then L_q is projective. Over Hurwitz's integral quaternions $\mathcal{H}$, a finitely generated torsion-free module is free, since $\mathcal{H}$ is an Euclidean domain.

The proof of 2.4 shows that the Hermitian form on L_q° induces a non-degenerate Hermitian form on L_q of signature $(1, n)$. The basis vectors of L_q° defines $2n$ vectors in L_q indexed by the points and lines of $\mathbb{P}^2(\mathbb{F}_q)$. These will be denoted by $x_0, \cdots, x_{n-1}$ and $l_0, \cdots, l_{n-1}$ respectively.

We have two more distinguished vectors $w_\mathcal{P}$ and $w_\mathcal{L}$ in L_q. We already defined $w_\mathcal{P}$ above. For $x \in \mathcal{P}$, let $w_x = px + \sum_{x\in l} l$. As above, one checks that $(w_x - w_{x'}) \in \mathrm{Rad}(L_q^\circ)$ for $x, x' \in \mathcal{P}$. We let $w_\mathcal{L}$ be the image of the vectors w_x in L_q. So

$$w_\mathcal{P} = \bar{p}l + \sum_{x'\in l} x' \ \text{ and } \quad w_\mathcal{L} = px + \sum_{x\in l'} l', \tag{2.2}$$

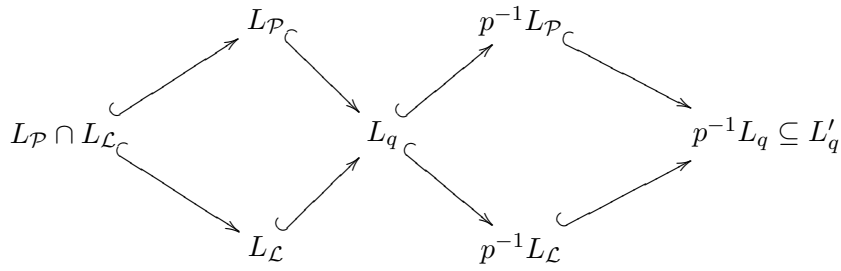
for any $x \in \mathcal{P}$ and $l \in \mathcal{L}$. Using equation (2.1) one checks that for all $x \in \mathcal{P}$ and $l \in \mathcal{L}$, we have,

$$\langle w_\mathcal{P}|x\rangle = \langle w_\mathcal{L}|l\rangle = 0, \ \ \langle w_\mathcal{P}|l\rangle = \langle x|w_\mathcal{L}\rangle = p, \tag{2.3}$$
$$|w_\mathcal{P}|^2 = |w_\mathcal{L}|^2 = q, \ \ \langle w_\mathcal{P}|w_\mathcal{L}\rangle = (q+1)p.$$

2.6. Line Coordinates on L_q: Let $L_\mathcal{L}$ and $L_\mathcal{P}$ be the sublattice of L_q spanned by $\{w_\mathcal{L}, l_0, \cdots, l_{n-1}\}$ and $\{w_\mathcal{P}, x_0, \cdots, x_{n-1}\}$ respectively. Then $L_q = L_\mathcal{P} + L_\mathcal{L}$. From equation (2.1) and (2.3), we observe that

$$L_\mathcal{P} \simeq L_\mathcal{L} \simeq p\mathcal{O}^{1,n}.$$

By looking at the inner products, we get the following inclusions:



Let us identify $p^{-1}L_{\mathcal{L}}$ with $\mathcal{O}^{1,n}$. Then L_q becomes a sub-lattice of the unimodular $\mathcal{O}$-lattice $\mathcal{O}^{1,n}$. Following [3], we call this the *line coordinates* on L_q. In other words, the line coordinates for $v = p^{-1}(v_\infty w_{\mathcal{L}} + v_0 l_0 + \cdots + v_{n-1} l_{n-1})$ is $(v_\infty; v_0, v_1, \cdots, v_{n-1})$. The following lemma is well known and it will help us decide when L_q is p-modular.

Lemma 2.7. *Let $(\mathcal{O}, p)$ be as in 1.1. Let M be an unimodular Hermitian $\mathcal{O}$-lattice. Then $W = M/pM$ is a $\mathcal{O}/p\mathcal{O}$-vector space. Let $\pi : M \to W$ be the projection. Let L be a sublattice of M. Let $X = \pi(L)$.*

(a) The Hermitian form on M induces a non-degenerate symmetric bilinear form on the $\mathcal{O}/p\mathcal{O}$-module W given by $(\pi(x), \pi(y)) = \langle x|y\rangle \bmod p\mathcal{O}$.

(b) X is isotropic if and only if $L \subseteq pL'$.

(c) There is a bijection between p-modular lattices L lying between M and pM and subspaces $X \subseteq W$ such that $X = X^\perp$, given by $X = \pi(L)$. Such subspaces X are maximal isotropic.

Proof. (a) Since M is unimodular, the form on W is non-degenerate. Since the form $\langle\ |\ \rangle$ on M is Hermitian and $\bar{z} \equiv z \bmod p\mathcal{O}$ for all $z \in \mathcal{O}$, the form on W is symmetric. This proves (a). Part (b) is clear.

(c) Since $pM \subseteq L \subseteq M$ and M is unimodular, $L' \subseteq p^{-1}M$; so $pL' \subseteq M$. Part (c) follows, once one verifies that $\pi^{-1}(X^\perp) = pL'$. □

Theorem 2.8. *Let $(\mathcal{O}, p, q)$ be as in 1.1. Suppose q is a rational prime and $\mathcal{O}/p\mathcal{O} \simeq \mathbb{F}_q$. Then the lattice L_q is p-modular, that is, $pL'_q = L_q$.*

Theorem 2.8 follows from theorem 2.9 quoted below. The proof of 2.9 uses the fact that *the incidence matrix of $\mathbb{P}^2(\mathbb{F}_q)$ generates a "cyclic difference set code"* (see [19]).

Theorem 2.9 ([13], theorem 2′, page 1067)**.** *Let $q = l^d$ be a power of a rational prime l. Then the $\mathbb{F}_q$-rank of the incidence matrix of $\mathbb{P}^2(\mathbb{F}_q)$ is equal to $\binom{l+1}{2}^d + 1$.*

proof of theorem 2.8. Identify L_q inside the unimodular lattice $p^{-1}L_{\mathcal{L}} = \mathcal{O}^{1,n} = M$ using the line coordinates. Then equation (2.2) implies that $x_i = (1; \epsilon_1, \cdots, \epsilon_n)$, where the ϵ_j's are either -1 or 0 and the -1's occur

at the coordinates corresponding to the lines that pass through x_i. Consider the subspace $X = L/pM$ of the $\mathbb{F}_q$-vector space M/pM. Since X is isotropic with respect to the induced non-degenerate form on M/pM, we have $\dim_{\mathbb{F}_q}(X) \leq \frac{1}{2}\dim_{\mathbb{F}_q}(M/pM) = \frac{1}{2}(n+1)$.

Note that X is spanned by the images of the vectors $x_0, \cdots, x_{n-1}$. Let $\tilde{A}$ be the $n \times (n+1)$ matrix whose i-th row is x_i. Let A be the matrix obtained from $\tilde{A}$ by deleting the first column of all 1's. Each row of $\tilde{A}$ add up to $-q$, so A and $\tilde{A}$ have the same $\mathbb{F}_q$-rank. Since $(-A)$ is the incidence matrix of $\mathbb{P}^2(\mathbb{F}_q)$, theorem 2.9 implies that $\mathrm{rank}_{\mathbb{F}_q}(A) = \frac{n+1}{2}$. So $\dim_{\mathbb{F}_q}(X) = \frac{n+1}{2}$. Thus X is maximal isotropic; so lemma 2.7 implies that L_q is p-modular. □

Corollary 2.10. *Suppose the assumptions of theorem 2.8 hold. Identify $p^{-1}L_{\mathcal{L}}$ with $\mathcal{O}^{1,n}$. Then*

$$L_q = \{v \in \mathcal{O}^{1,n} \colon \langle x|v\rangle \equiv 0 \mod p\mathcal{O} \text{ for all } x \in \mathcal{P}\}.$$

Remark 2.11. Let $\mathcal{O}$ be the ring of integers in a quadratic imaginary number field. Identify $p^{-1}L_{\mathcal{L}}$ with $\mathcal{O}^m$ as $\mathcal{O}$-modules. Then $(p\mathcal{O})^m \subseteq L_q \subseteq \mathcal{O}^m$. There exists a unique fractional ideal $I = [\mathcal{O}^m : L_q]$ of $\mathcal{O}$ such that the ideal class of I (called the Steinitz class of L_q) determines the isomorphism type of L_q as an $\mathcal{O}$-module (see [12], p. 94-95). Let J be a prime ideal of $\mathcal{O}$ different from p. Since $(p\mathcal{O})^m \subseteq L_q \subseteq \mathcal{O}^m$, the localization $(L_q)_J$ is equal to $\mathcal{O}_J^m$. It follows that $[\mathcal{O}^m : L_q]$ is some power of the principal ideal $p\mathcal{O}$ (see [12], p. 94-95). So the Steinitz class of L_q is trivial and L_q is a free $\mathcal{O}$-module.

3. Positive definite lattices with symmetry of finite projective planes

Lemma 3.1. *Let $(\mathcal{O}, p)$ be as in 1.1. Let L be a Hermitian $\mathcal{O}$-lattice such that $pL' = L$. If z is a primitive element of L, then $\langle L|z\rangle = p\mathcal{O}$. Since $\bar{p}\mathcal{O} = p\mathcal{O}$, we also have $\langle z|L\rangle = p\mathcal{O}$.*

Proof. The lemma holds when $\mathcal{O} = \mathcal{H}$ is the ring of Hurwitz integers since every ideal in $\mathcal{H}$ is principal. Otherwise, we may assume that $\mathcal{O}$ is a Dedekind domain. Suppose $\langle L|p^{-1}z\rangle = I$ is a proper ideal in $\mathcal{O}$. Suppose $I \cap \mathbb{Z} = s\mathbb{Z}$. There exists an ideal J such that $IJ = s\mathcal{O}$. Then, for all $j \in J$, we have $\langle L|s^{-1}p^{-1}jz\rangle \subseteq s^{-1}jI \subseteq s^{-1}JI \subseteq \mathcal{O}$. It follows that $s^{-1}p^{-1}jz \in L' = p^{-1}L$, so $s^{-1}jz \in L$ for all $j \in J$. Since z is primitive, $s^{-1}j \in \mathcal{O}$ for all $j \in J$, so $J \subseteq s\mathcal{O}$. But $IJ = s\mathcal{O}$, so $I = \mathcal{O}$. □

Lemma 3.2. *Let $(\mathcal{O}, p)$ be as in 1.1. Let L be a p-modular Lorentzian Hermitian $\mathcal{O}$-lattice. Let z be a primitive norm 0 vector in L. Then L splits off a hyperbolic cell containing z, that is, there exists a lattice H of signature $(1,1)$ containing z such that $L = H \oplus \Lambda$ for a definite lattice $\Lambda \simeq z^{\perp}/z$. Further, Λ is also p-modular.*

Proof. Lemma 3.1 implies that there exists $f \in L$ such that $\langle z|f\rangle = p$. Then $H = \mathcal{O}z + \mathcal{O}f$ is a hyperbolic cell. Note that π_H, given by

$$\pi_H(x) = (\bar{p}^{-1}\langle f|x\rangle - |p|^{-2}|f|^2\ \langle z|x\rangle)z + p^{-1}\langle z|x\rangle f$$

is the orthogonal projection of $L \otimes \mathrm{Frac}(\mathcal{O})$ to $H \otimes \mathrm{Frac}(\mathcal{O})$ and π_H maps L into H. It follows that $L = H \oplus \Lambda$, where $\Lambda = H^{\perp}$. So $z^{\perp} = \Lambda \oplus \mathcal{O}z$ and $z^{\perp}/z \simeq \Lambda$.

It remains to see that $p\Lambda' = \Lambda$. If $\lambda \in \Lambda$, then $\langle \lambda|L\rangle \in p\mathcal{O}$, so $\langle \lambda|\Lambda\rangle \in p\mathcal{O}$, that is $\Lambda \subseteq p\Lambda'$. Suppose $\phi \in \Lambda'$. Since $L = \Lambda \oplus H$, we can extend ϕ to an element of L' by defining ϕ to be 0 on H. Since $L' = p^{-1}L$, there exists $x \in L$ such that $\phi(\cdot) = \langle p^{-1}x|\cdot\rangle$. But then $\phi(\lambda) = \langle p^{-1}(x - \pi_H(x))|\lambda\rangle$ for all $\lambda \in \Lambda$ and $(x - \pi_H(x)) \in \Lambda$. □

3.3. Positive definite modular lattices with $\mathrm{PGL}(3, \mathbb{F}_q)$ symmetry: Let $(\mathcal{O}, p, q)$ be as in 1.1 and L_q be the lattice defined in 2.5 from this data. Suppose L_q has a primitive norm zero vector z fixed by $\mathrm{PGL}(3, \mathbb{F}_q)$. Suppose $g \in \mathrm{PGL}(3, \mathbb{F}_q)$ acts trivially on $z^{\perp}/z$. Since g has finite order, it must fix $z^{\perp}$ point-wise. But g also point-wise fixes the span of $w_{\mathcal{P}}$ and $w_{\mathcal{L}}$. So g must be trivial. So the automorphism group of $z^{\perp}/z$ contains $\mathrm{PGL}(3, \mathbb{F}_q)$. It follows that $z^{\perp}/z$ is a positive definite $(n-1) = q^2 + q$ dimensional $\mathcal{O}$-lattice, whose automorphism group contains $\mathrm{PGL}(3, \mathbb{F}_q)$. If L is p-modular, then lemma 3.2 implies that the positive definite lattice $z^{\perp}/z$ is also p-modular.

For example, if $\mathcal{O} = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ and $q = 3$, then we may take $z = w_{\mathcal{P}} + \frac{1}{2}(-1+p)\bar{p}w_{\mathcal{L}}$. To find more examples of z (see 3.6), we need the lemma below. It might be known in the literature but we include a proof since we could not find a references.

Lemma 3.4. *Let $q \equiv 3 \bmod 4$ be a rational prime, $n = q^2 + q + 1$. If p is a rational prime, write $n = p^{v_p(n)}m$ with $p \nmid m$. Then the following are equivalent:*

(a) The integer n is a norm of some element in $\mathbb{Q}[\sqrt{-q}]$.

(b) The ternary quadratic form

$$z^2 + qx^2 - ny^2 \tag{3.1}$$

represents 0 over $\mathbb{Z}$.

(c) If $v_p(n)$ is odd for some rational prime p, then $p \equiv 1 \bmod 4$.

Proof. The equivalence of (a) and (b) is clear. Assume (b). Let (z, x, y) be a zero of the ternary form $(z^2 + qx^2 - ny^2)$ over $\mathbb{Z}$ such that the greatest common divisor of x, y and z is equal to 1. Let p be a prime; $p \equiv 3 \bmod 4$. Suppose, if possible $v_p(n) = 2r + 1$. Since $q^3 \equiv 1 \bmod p$,

$$z^2 + (q^{-1}x)^2 \equiv z^2 + q^3(q^{-1}x)^2 \equiv z^2 + qx^2 \equiv 0 \bmod p,$$

where q^{-1} denotes the inverse of q modulo p. The equation $Z^2 + X^2 = 0$ has no nontrivial solution in $\mathbb{F}_p$. So p must divide both z and x and hence p does not divide y. So $v_p(z^2 + qx^2) = v_p(n) = 2r + 1$. If $v_p(z) \neq v_p(x)$, then $v_p(z^2 + qx^2) = 2\min\{v_p(z), v_p(x)\}$ is even, which is not possible. So let $v_p(z) = v_p(x) = j$. Writing $z = p^j z_1$ and $x = p^j x_1$ we find that $v_p(z_1^2 + qx_1^2) + 2j = 2r + 1$, so $v_p(z_1^2 + qx_1^2) > 0$. But this again leads to

$$z_1^2 + (q^{-1}x_1)^2 \equiv z_1^2 + qx_1^2 \equiv 0 \bmod p,$$

which is a contradiction, since p does not divide z_1 and x_1. Thus (b) implies (c).

Conversely, assume (c). The ternary form represents 0 over $\mathbb{R}$, so it suffices to check that it represents 0 over $\mathbb{Q}_p$ for all but one rational prime p, that is, the local Hilbert symbols $(-q, n)_p = 1$. Because of the product formula ([18] Ch. 3, theorem 3, pp. 23) we can omit one prime.

Note that $(q+1, 1, 1)$ is a nontrivial solution to $(z^2 - qx^2 - ny^2) = 0$ over $\mathbb{Z}$, so $(q, n)_p = 1$ for all prime p. So, for $p \neq 2$, using [18] Ch. 3, theorem 1, pp. 20, we get

$$(-q, n)_p = (-1, n)_p (q, n)_p = (-1, n)_p = \Big(\frac{-1}{p}\Big)^{v_p(n)}.$$

But our assumption states that if $v_p(n)$ is odd, then $p \equiv 1 \bmod 4$, so -1 is a quadratic residue modulo p. □

Remark 3.5. Suppose $q \neq 3$ is a prime such that the conditions of lemma 3.4 are satisfied. If q is of the form $3k + 1$, then $n = 9k^2 + 9k + 3$, so $v_3(n) = 1$, which is not possible. So if $q \neq 3$, then we must have $q \equiv -1 \bmod 12$. The first few primes q satisfying the conditions in 3.4(c), are $q = 3, 47, 59, 71, 131$. For example, if $q = 3$, then $(z, x, y) = (1, 2, 1)$ is a solution to the ternary form in (3.1). If $q = 47$, then $(z, x, y) = (47, 27, 4)$ is a solution. General conjectures like Schinzel's hypothesis H or Bateman-Horn conjecture imply that there are infinitely such primes.

Example 3.6. (1) Let $(\mathcal{O}, p, q)$ be as in 1.2(1). One verifies that the set of fixed points of the group $\mathrm{PGL}(3, \mathbb{F}_q)$ acting on $L_q \otimes_{\mathcal{O}} \mathbb{Q}[\sqrt{-q}]$ is the two dimensional subspace spanned by $w_{\mathcal{P}}$ and $w_{\mathcal{L}}$. So L_q contains a norm zero vector fixed by $\mathrm{PGL}(3, \mathbb{F}_q)$ if and only if $(w_{\mathcal{P}} + cw_{\mathcal{L}})$ has norm zero for some $c \in \mathbb{Q}[\sqrt{-q}]$. Using equation (2.3), one verifies that

$$|w_{\mathcal{P}} + cw_{\mathcal{L}}|^2 = |cp + q + 1|^2 - (q^2 + q + 1).$$

So $|w_{\mathcal{P}} + cw_{\mathcal{L}}|^2 = 0$ if and only if $(q^2 + q + 1)$ is a norm of some element of $\mathbb{Q}[\sqrt{-q}]$. Suppose q is such that the conditions in lemma 3.4 hold. Then there exists a primitive norm zero vector z in L_q fixed by $\mathrm{PGL}(3, \mathbb{F}_q)$. By lemma 3.1, there exists a lattice vector f such that $\langle z|f\rangle = p$. So we can take $H = \mathcal{O}z + \mathcal{O}f$. Writing $L_q = \Lambda_q \oplus H$ as in 3.2, we get a p-modular

Hermitian lattice Λ_q defined over $\mathbb{Z}[(1+p)/2]$, whose automorphism group contains $\mathrm{PGL}(3,\mathbb{F}_q)$. For $q=3$ we find that Λ_q is the Leech lattice defined over Eisenstein integers.

(2) Let $\mathcal{O}=\mathcal{H}$ be the ring of Hurwitz integers, $p=(1-i)$ and $q=2$. Let $L_2^{\mathcal{H}}$ be the lattice obtained from this data. (Of course in this case one has to be careful to phrase everything in terms of right modules or left modules.) The reflection group of $L_2^{\mathcal{H}}$ was studied in [6] where we always considered right $\mathcal{H}$-modules. One checks that $z=w_{\mathcal{P}}+w_{\mathcal{L}}\bar{p}(-1+i+j+k)/2$ is a primitive null vector in $L_2^{\mathcal{H}}$. So we can write $L_2^{\mathcal{H}}=\Lambda\oplus H$, so that $\Lambda\simeq z^{\perp}/z$ and H is a hyperbolic cell. The lattice Λ is a quaternionic form of Leech lattice defined of Hurwitz integers.

3.7. Even unimodular positive definite $\mathbb{Z}$-lattices with $\mathrm{PGL}(3,\mathbb{F}_q)$ symmetry: Let q be a rational prime; $q\equiv 3 \bmod 4$. Suppose q satisfies the conditions in lemma 3.4. Let Λ_q be the definite Hermitian $\mathcal{O}$-lattice from 3.6(1). Let M_q be the underlying $\mathbb{Z}$-module of Λ_q with the integral bilinear form

$$(x,y)=-2q^{-1}\,\mathrm{Re}\langle x|y\rangle.$$

Then M_q is a positive definite, even, unimodular $\mathbb{Z}$-lattice of dimension $2q(q+1)$ such that $\mathrm{Aut}(M_q)\supseteq \mathrm{PGL}(3,\mathbb{F}_q)$. If $q=3$, then M_q is the Leech lattice.

proof that M_q is unimodular: Identify the vector spaces $\Lambda_q\otimes_{\mathcal{O}}\mathbb{Q}(\sqrt{-q})$ and $M_q\otimes_{\mathbb{Z}}\mathbb{Q}$. All the lattices in question can be identified inside this vector space. Suppose $\mu\in M_q'$. Let $\langle\mu|y\rangle=(u+pv)/2$ with $u,v\in\mathbb{R}$. Since $(\mu,y)=-2q^{-1}\,\mathrm{Re}\langle\mu|y\rangle\in\mathbb{Z}$, we have $u\in q\mathbb{Z}$. Also

$$(\mu,\tfrac{(1+p)}{2}y)=-2q^{-1}\,\mathrm{Re}\langle\mu|\tfrac{(1+p)}{2}y\rangle=(qv-u)/2q\in\mathbb{Z}.$$

So $v\in q^{-1}u+2\mathbb{Z}$. It follows that $v\in\mathbb{Z}$ and $u\equiv v \bmod 2$. So $\langle\mu|y\rangle\in p\mathcal{O}$. So $p^{-1}\mu\in\Lambda_q'=p^{-1}\Lambda_q$, so $\mu\in\Lambda_q$, that is $\mu\in M_q$. □

References

[1] D. Allcock, *The Leech lattice and complex hyperbolic reflections*. Invent. Math. **140** (2000), 283–301.

[2] D. Allcock, *A monstrous proposal*. Groups and Symmetries: From neolithic Scots to John McKay (2009), AMS and Centre de Recherches Mathå£«atiques. arXiv:math/0606043.

[3] D. Allcock, *On the Y_{555} complex reflection group*. J. Alg. **322** (2009), 1454–1465

[4] R. Bacher and B. Venkov, *Lattices and association schemes: A unimodular example without roots in dimension 28*. Ann. Inst. Fourier, Grenoble. **45**, 5 (1995), 1163–1176.

[5] T. Basak, *The complex Lorentzian Leech lattice and the bimonster*. J. Alg. **309**, no. 1 (2007), 32–56.

[6] T. Basak, *Reflection group of the quaternionic Lorentzian Leech lattice*. J. Alg. **309**, no. 1 (2007), 57–68.

[7] T. Basak, *The complex Lorentzian Leech lattice and the bimonster (II)*. preprint (2012), arXiv:0811.0062, submitted.

[8] A. I. Bondal, *Invariant lattices in Lie algebras of type A_{p-1} (Russian)*. Vestnik Moskov. Univ. Ser. I Mat. Mekh. 93, no. 1 (1986), 52–54.

[9] J. H. Conway, S. P. Norton and L. H. Soicher, *The bimonster, the group Y_{555}, and the projective plane of order 3.* " Computers in Algebra" (M. C. Tangara, Ed.), Lecture Notes in Pure and Applied Mathematics, No 111, Dekker, New York, (1988), 27–50.
[10] J. H. Conway and C. S. Simons, *26 Implies the Bimonster.* J. Alg. **235** (2001), 805–814.
[11] J. H. Conway, and N. J. A. Sloane, *Sphere Packings, Lattices and Groups 3rd Ed.* Springer-Verlag, 1998.
[12] A. Fröhlich and M.J. Taylor, *Algebraic number theory.* Cambridge University Press, 1991.
[13] R. L. Graham and J. Macwilliams, *On the number of information symbols in the difference set cyclic codes.* The Bell System Technical Journal, Vol XLV, No. 7, 1966.
[14] A. A. Ivanov, *A geometric characterization of the monster.* Groups, Combinatorics and Geometry, edited by M. Liebeck and J. Saxl, London Mathematical Society Lecture Note Series, No. 165, Cambridge Univ. Press, (1992), 46–62.
[15] A. A. Ivanov, *Y–groups via transitive extension.* J. Alg. **218** (1999) 412–435.
[16] A. I. Kostrikin and H. T. Pham, *Orthogonal decompositions and integral lattices.* Walter de Gruyter, 1994.
[17] G. Nebe and K. Schindelar, *S-extremal strongly modular lattices.* J. Théor. Nombres Bordeaux, **19** no. 3, (2007), 68–701.
[18] J. P. Serre, *A course in Arithmetic.* Springer-Verlag, 1973.
[19] J. Singer, *A theorem in finite projective geometry and some applications to number theory.* Trans. A. M. S. **43**, No. 3 (1938), 377–385.

Tathagata Basak
Department of Mathematics
Iowa State University
Ames, IA 50011
E-mail: tathastu@gmail.com
URL: http://orion.math.iastate.edu/tathagat/