Jordan Splittings of Almost Unimodular Integral Quadratic Forms

C. RIEHM*

Department of Mathematics, McMaster University, Hamilton, Ontario L8S 4K1, Canada

Communicated by H. Zassenhaus

Received March 9, 1979; revised July 30, 1979

Necessary and sufficient conditions for the existence of such splittings in the indefinite case are given in [Hambleton and Riehm, Invent. Math. 45 (1978), 19–33] so we restrict ourselves mainly to the definite case, in fact also to those forms which are represented by a unimodular form of the same rank. In this context a natural equivalence relation on such forms is related to a problem over a finite field, and this in turn is investigated more thoroughly in the case when the unimodular representing form is \( \sum_{i=1}^{n} x_i^2 \); the number of equivalence classes is counted for small values of \( n \), and it is shown that very few forms have Jordan splittings over \( \mathbb{Z} \). A calculation of the Grothendieck and Witt groups of almost unimodular forms is also given.

Let \( L \) be a lattice with a symmetric bilinear form

\[ f: L \times L \to \mathbb{Z} \]

and let \( p \) be a prime. We say that \( f \) is almost unimodular (with respect to \( p \)) if \( pF^{-1} \) is integral, where \( F \) is the matrix of \( f \) with respect to an arbitrary basis. This is equivalent to saying that \( L_q = \mathbb{Z}_q \otimes L \) is unimodular over the \( q \)-adic integers \( \mathbb{Z}_q \) when \( q \neq p \), and that, over \( \mathbb{Z}_p \),

\[ L_p = L_0 \perp L_1 \quad (1) \]

with \( L_0 \) unimodular and \( L_1 \) \( p \)-modular ("Jordan splitting" over \( \mathbb{Z}_p \)). The genesis of this paper is the question of the existence of a Jordan splitting

\[ L = L_0 \perp L_1 \]

over \( \mathbb{Z} \) itself, again with \( L_0 \) unimodular and \( L_1 \) \( p \)-modular. In [2], a complete solution can be found when \( f \) is indefinite.

* Research supported by NSERC (Canada) Grant A8778.
We begin (Theorem 2) by giving necessary and sufficient conditions for the genus of a positive definite form to contain a form with a Jordan splitting. According to Watson [9], any definite form in 14 or more variables has an indecomposable form in its genus, which implies that our conditions cannot be sufficient for the form itself to have a Jordan splitting.

A geometric almost unimodular lattice (gaul) is a pair \( L \subseteq M \) with \( L \) almost unimodular, \( M \) unimodular and rank \( L = \text{rank } M \). This is exactly the situation which obtains in the topological context in which the problem of global Jordan splittings arose (see [2]).

The gauls \( L \subseteq M \) and \( L' \subseteq M' \) are called equivalent if there is an isometry \( \phi: M \to M' \) which carries \( L \) onto \( L' \). In Section 2 we characterize the equivalence classes of gauls \( L \subseteq M \) with \( M \) fixed. In Section 3 we use this characterization to count the equivalence classes in the case \( L \) definite of discriminant \( p^2 \) and rank 3, 4 or 5; for arbitrary rank \( n \) and \( M \approx I_n \) (i.e., the quadratic form belonging to \( M \) is \( x_1^2 + \cdots + x_n^2 \)) we show that very few of the equivalence classes have a Jordan splitting (see Corollary 13 and Remark 14). In Example 15 the effectiveness of our procedure is illustrated in a particular case. In Section 4, the classes and genera of the special forms of Section 3 are investigated.

In Section 5, calculations of the Grothendieck and Witt groups of almost unimodular forms are provided.

1. Existence of a Jordan Splitting in a Genus

Let \( n \) denote the rank of \( L \) and \( n_0 \) and \( n_1 \) the \( \mathbb{Z}_p \)-ranks of the unimodular and \( p \)-modular Jordan components \( L_0 \) and \( L_1 \) of \( L_p \), (1). We say \( L \) is even if \( f(x, x) \in 2\mathbb{Z} \) for all \( x \) in \( L \), otherwise \( L \) is odd. When \( p = 2 \), we say, for example, that \( L \) is odd/even if \( L_0 \) is an odd \( \mathbb{Z}_2 \)-lattice and \( L_1 \) is an even lattice scaled by 2. The dual lattice \( L^* \) is the lattice \( \{ x \in \mathbb{Q}L : f(x, L) \subseteq \mathbb{Z} \} \). An analogous definition is made for a lattice over \( \mathbb{Z}_q \). The \( \mathbb{Z} \)-lattice \( L \) is almost unimodular iff \( f(L, L) \subseteq \mathbb{Z} \) and \( f(L^*, L^*) \subseteq (1/p)\mathbb{Z} \).

**Lemma 1.** Let \( L_2 \) and \( M_2 \) be almost unimodular \( \mathbb{Z}_2 \)-lattices. Then \( L_2 \approx M_2 \) iff

(a) \( L_2 \approx M_2 \) over \( \mathbb{Q}_2 \),

(b) corresponding Jordan components have the same parity,

(c) when \( L_2 \) and \( M_2 \) are even/even, corresponding Jordan components are equivalent.

**Proof.** We apply Theorem 93:29 of [7] to our special case. The necessity of (a) and (b) follows readily while for (c) we first note that the 2-modular Jordan components \( L_0 \) and \( M_0 \) of \( L_2 \) and \( M_2 \) are orthogonal sums of hyper-
SPLITTINGS OF ALMOST UNIMODULAR FORMS

bolic planes \((0, 1)\) plus possibly one copy of \((1, 1)\). By (i) of 93:29, their determinants are congruent mod 8, hence equal (modulo square units). Thus these orthogonal decompositions both contain \((1, 1)\) or both do not, so \(L_0 \simeq M_0\). Therefore their 2-modular Jordan components also have equal determinants, and so must be equivalent.

The sufficiency is trivial when \(L\) and \(M\) are even/even, and follows readily from 93:29 when they are even/odd or odd/odd. Suppose they are odd/odd. Then the forms of the duals \(L'_2\) and \(M'_2\), when multiplied by 2, are almost unimodular and even/odd. By a previous case \(L'_2 \simeq M'_2\) so \(L_2 \simeq M_2\).

The necessary and sufficient conditions for an indefinite form to have a global Jordan splitting, given in Theorems 19 to 24 of [2], are necessary in the definite case as well. But they can be greatly simplified and yield the following theorem:

**Theorem 2.** If \(L\) is positive definite, the genus of \(L\) contains a Jordan split lattice if and only if

\[
\begin{align*}
n_0 &= n_1 = 0 \pmod{8} & \text{when } p \text{ is odd and } L \text{ is even}, \\
\det L_0 &= 1 & \text{when } p \text{ is odd and } L \text{ is odd}, \\
n_0 &\equiv 0 \pmod{8} & \text{when } p = 2 \text{ and } L \text{ is even/odd}, \\
n_1 &\equiv 0 \pmod{8} & \text{when } p = 2 \text{ and } L \text{ is odd/even}.
\end{align*}
\]

We note that \(\text{gen } L\) always contains a Jordan split lattice when \(L\) is positive definite, \(p = 2\), and \(L\) is odd/odd.

**Proof.** The necessity of the congruences mod 8 follows from the fact that an even definite lattice of odd determinant has rank \(\equiv 0 \pmod{8}\) [8]. And in every case it is clear that \(\det L_0 = 1\) is necessary since every sublattice of \(L\) is positive definite. Consider the sufficiency. Let \(L_8\) be the unique even positive definite lattice of rank 8. By using copies of it and of \(\langle 1 \rangle\) (the unary lattice with form \(X^2\)), we can construct a positive definite almost unimodular lattice \(M\) such that the following (generic) invariants are the same for \(M\) and for \(L\): \(n, n_0, n_1\), parity, and parity of 2-adic Jordan components in case \(p = 2\). This is possible because of the conditions imposed on \(L\). Consider now the case \(p = 2\) and \(L\) even/even. Since \(\det M = 2^n = \det L\), \(M\) and \(L\) are equivalent over \(\mathbb{Z}_q\) for all odd \(q\) (92:1 of [7]) as well as over \(\mathbb{R}\). By Hilbert reciprocity they are also equivalent over \(\mathbb{Q}_2\). By Proposition 20 of [2], their 2-modular Jordan components over \(\mathbb{Z}_2\) are hyperbolic and hence have the same determinant, so their unimodular Jordan components also have the same determinant. Therefore by Lemma 1, \(L \simeq M\) over \(\mathbb{Z}_2\) and so they are in the same genus.

The remaining cases of the theorem are similar and generally easier.
2. GEOMETRIC ALMOST UNIMODULAR LATTICES

PROPOSITION 3. Let $L$ be almost unimodular with respect to $p$. Then $L$ is contained in a unimodular lattice of the same rank if and only if the $p$-modular Jordan component of $L$ over $\mathbb{Z}_p$ has even rank and, when $p$ is odd, is hyperbolic.

Proof. Necessity. Suppose $L$ is contained in the unimodular lattice $M$. Take a Jordan splitting (1) of $L_p$. Since the determinants of the unimodular lattices $M_p$ and $L_p$ are units, $\det L_1$ is a unit times a square, so $\dim L_1$ is even. Suppose $p$ is odd. Since $Q_p L_p$ supports a unimodular lattice, its image in the Witt group $W(\mathbb{Z}_p/p\mathbb{Z}_p)$ under the "second residue class homomorphism" must be 0 (cf. [6, Sect. 1, Chap. 6]); but this image is also the image of $Q_p L_1$ which implies that $L_1$ is hyperbolic (say, by determinants).

Sufficiency. When $p = 2$, 93:10 and 93:18 in [7] show that any 2-modular $\mathbb{Z}_2$-lattice of even rank is an orthogonal direct sum of binary lattices with matrices \begin{pmatrix} a & b \\ b & a \end{pmatrix} where $a \in 2\mathbb{Z}_2$ and $b \in 4\mathbb{Z}_2$; since it is clear that any such binary lattice is contained in a unimodular binary lattice, this implies that $L_2$ is contained in a unimodular lattice $L_2'$ on $\mathbb{Q}_2 L_2$ and so by 81:14 of [7], $L$ itself is contained in the unimodular $\mathbb{Z}$-lattice $M$ defined by

\[ M_q = L_2' \quad \text{for} \ q = 2, \]

\[ = L_o \quad \text{otherwise}. \]

Suppose $p$ is odd. Then $L_1$ is by hypothesis an orthogonal sum of hyperbolic planes and the proof follows easily along the same lines as $p = 2$.

For the rest of this section, we deal with a unimodular lattice $M$ and try to find the sublattices (of the same rank $n$ as $M$) which are almost unimodular with respect to $p$, and also the equivalence classes of gauls $(L, M)$.

The unimodular form $f$ on $M$ induces a non-singular symmetric bilinear $\mathbb{F}_p$-form $\tilde{f}$ on $M/pM$ via $\tilde{f}(x + pM, y + pM) = f(x, y) + p\mathbb{Z}$. A totally degenerate subspace of $M/pM$ is one on which $\tilde{f}$ is identically 0.

THEOREM 4. The mapping $L \rightsquigarrow pL^*/pM$ is a bijection between the set of almost unimodular sublattices of $M$ and the set $\mathcal{Y}$ of totally degenerate subspaces of $M/pM$. The inverse mapping is $W \rightsquigarrow ((1/p)W)^*$ where $W$ is the inverse image of $W$ under $M \rightarrow M/pM$. An almost unimodular lattice $L$ whose $p$-adic $p$-modular Jordan component has rank $n_1$ corresponds to a totally degenerate subspace of $M/pM$ of rank $\tilde{n}_1$. $L$ has a Jordan splitting iff $M$ has an orthogonal component $L'$ of rank $n - n_1$ whose image in $M/pM$ is orthogonal to $pL^*/pM$, i.e., $f(L', pL^*) = 0 \pmod{p}$.
Proof. Now \( f(L^*, L^*) \subseteq (1/p)\mathbb{Z} \) and it follows easily that \( pL^*/pM \) is totally degenerate. Let \( n_0 \) and \( n_1 \) be the ranks of the \( \mathbb{Z}_p \)-Jordan components of \( L_p \). Now \( [M:L] = p^{n_1/2} \) so \( [L^*:M] = p^{n_1/2} = [pL^*:pM] \) so \( pL^*/pM \) has rank \( \frac{1}{2}n_1 \) over \( \mathbb{F}_p \). It is easily checked that \( W \) totally degenerate implies 
\[
f((1/p)W', (1/p)W') \subseteq (1/p)\mathbb{Z};
\]
furthermore since \( W' \supseteq pM, (1/p)W' \supseteq M \) and so \( ((1/p)W')^* \subseteq M = M \), hence

\[
f\left(\left(\frac{1}{p} W'\right)^*, \left(\frac{1}{p} W'\right)^*\right) \subseteq \mathbb{Z}.
\]

Thus \( ((1/p)W')^* \) is almost unimodular. The inverse image of \( pL^*/pM \) is \( pL^* \) (since \( pM \subseteq pL^* \subseteq M \)) so the lattice corresponding to the totally degenerate subspace \( pL^*/pM \) is \( ((1/p) \cdot pL^*)^* = L \). On the other hand if \( W \) is a totally degenerate subspace of \( M/pM \),

\[
p \left( \left(\frac{1}{p} W'\right)^* \right)^* = W'
\]

so the lattice \( ((1/p)W')^* \) corresponds to \( W \). Thus the two correspondences are mutually inverse and so are bijective.

Suppose now that \( L \) has a global Jordan splitting \( L = L' \perp L'' \) with \( L' \) unimodular and \( L'' \) \( p \)-modular. Since \( L' \subseteq M, L' \) is an orthogonal component of \( M \) of rank \( n_0 \) satisfying \( f(L', pL^*) \equiv 0 \pmod{p} \) since \( pL^* = pL' \perp L'' \).

Conversely if \( L' \) has these properties, \( f(L', L'^*) \) is integral so \( L' \subseteq L \) and splits \( L \) orthogonally. By ranks, the orthogonal complement is \( p \)-modular and so we have a Jordan splitting.

The orthogonal group \( O(M) \) operates via isometries on \( M/pM \), hence is a group of operators on \( \mathcal{X} \).

Theorem 5. The equivalence classes of gauls \((L, M)\) with \( M \) fixed are in bijective correspondence with the orbit space \( O(M) \backslash \mathcal{X} \).

Proof. If \((L, M) \simeq (L', M)\), there is \( \sigma \in O(M) \) with \( \sigma L = L' \), whence \( \sigma(pL^*/pM) = pL'^*/pM \). Conversely if this last equation holds for \( \sigma \in O(M) \) then \( \sigma pL'' = pL'^* \) whence \( \sigma L = L' \).

3. \( M \) Has Form \( X_1^2 + X_2^2 + \cdots + X_n^2 \)

Thus \( M \) has an orthogonal basis \( e_1, \ldots, e_n \). It follows from Eichler's Theorem [4] on the uniqueness of the decomposition of a definite lattice into indecomposables that \( G_n := O(M) \) is a semi-direct product

\[
G_n = \{ \pm 1 \}^n \times S_n,
\]
where \( S_n \) is the symmetric group. We write elements of \( G_n \) in the form 
\[(\varepsilon_1, \ldots, \varepsilon_n)\sigma \]
where \( \varepsilon_i = \pm 1 \) and \( \sigma \in S_n \). We call \((\varepsilon_1, \ldots, \varepsilon_n)\) a multisign. The action of \( G_n \) on \( M \) is therefore described by
\[(\varepsilon_i)\sigma e_j = \varepsilon_{\sigma(j)} e_{\sigma(j)}.\]

If \( \sigma \) is a cycle, say \( \sigma = (i_1, i_2, \ldots, i_k) \), then an element of the form \((\varepsilon_{i_1}, \ldots, \varepsilon_{i_k})(i_1 \cdots i_k)\) is called a signed cycle (of length \( k \)) where it is understood that
\[(\varepsilon_{i_1}, \ldots, \varepsilon_{i_k}) e_j = e_j \quad j = i_1, \ldots, i_k,\]
\[= e_j \quad \text{otherwise};\]
the sign of a signed cycle is the product \( \varepsilon_{i_1} \cdots \varepsilon_{i_k} \). It is clear that every element of \( G_n \) can be written uniquely as a product of (commuting) disjoint signed cycles, and that the order of \( G_n \) is
\[|G_n| = 2^n(n!).\]

To each element of \( G_n \) we associate the sequence \((\mu_1, \mu_2, \ldots, \mu_n)\) of multiplicities of the signed cycle lengths in its signed cycle decomposition where, by including signed cycles of the form \((-1)(i)\), we may assume that \( \sum \mu_i = n \). It is easy to see that two elements of \( S_n \) are conjugate in \( S_n \) if and only if their cycle multiplicities are identical, and that the cardinality of a conjugacy class in \( S_n \) is
\[n!/\prod \mu_i! \prod \frac{2^{(i-1)\mu_i}}{i^{\mu_i} \cdot \mu_i! \cdot (\mu_i - \pi_i)!}.\]

If \( \sigma \in G_n \), we define its positive cycle multiplicity to be \((\pi_1, \ldots, \pi_n)\) where \( \pi_i \) is the number of signed cycles of sign +1 and length \( i \) in the signed cycle decomposition of \( \sigma \); thus \( 0 \leq \pi_i \leq \mu_i \).

**Proposition 6.** Two elements of \( G_n \) are conjugate iff their cycle and positive cycle multiplicities are respectively identical. The cardinality of a conjugacy class is
\[n! \prod \frac{2^{(i-1)\mu_i}}{i^{\mu_i} \cdot \pi_i! \cdot (\mu_i - \pi_i)!}.\]

**Proof.** Let \( \tau \) be an arbitrary element of \( G_n \), \( \tau(\varepsilon_i) = \delta_{\tau(i)} \varepsilon_{\tau(i)} \), where \( t \) is a permutation and \( \delta_j = \pm 1 \), and let \( \sigma = (\varepsilon_1, \ldots, \varepsilon_k)(1 \cdots k) \). It is easy to see that
\[\tau \sigma \tau^{-1} = (\delta_{\tau(i)} \varepsilon_i \delta_{\tau^{-1}(i)})(t(1) \cdots t(k)).\]
where \( \ell(0) = \ell(k) \). Note that the sign of \( \tau \sigma \tau^{-1} \) is the same as the sign of \( \sigma \). The proposition follows in a straightforward manner.

We take as basis of \( M/pM \) the reduction mod \( p \) of the orthonormal basis of \( M \), and thereby identify

\[
M/pM = \mathbb{F}_p^n.
\]

We are interested in the orbits of the totally degenerate subspaces of \( \mathbb{F}_p^n \) under the action of \( G_n \)

\[
(\varepsilon_1, \ldots, \varepsilon_n) \sigma(x_1, \ldots, x_n) = (\varepsilon_1 x_{\sigma^{-1}(1)}, \ldots, \varepsilon_n x_{\sigma^{-1}(n)}).
\]

We may view these totally degenerate subspaces as projective subspaces of the \( (n - 1) \)-dimensional projective space \( P_{n-1}(\mathbb{F}_p) \) which lie on the quadric hypersurface

\[
C_n = \left\{ [x_1, \ldots, x_n] \in P_{n-1}(\mathbb{F}_p) : \sum x_i^2 = 0 \right\},
\]

where \( [x_1, \ldots, x_n] \) are homogeneous coordinates. \( C_n \) is stable under \( G_n \) and we are interested in the orbits of \( G_n \) lying in \( C_n \). From now on we consider only the orbits of points; by Theorem 4 these correspond to gauls \( (L, M) \) with \( n_1 = 2 \).

A point \( x = [x_1, \ldots, x_n] \) of \( P_{n-1}(\mathbb{F}_p) \) is said to have extent \( k \), \( 1 \leq k \leq n \), if exactly \( k \) of its coordinates \( x_1, \ldots, x_n \) are non-zero. The subset of \( C_n \) of points of extent \( k \) is clearly \( G_n \)-stable. If \( n' \geq k \), it is also clear that there is a canonical bijection between the \( G_n \)-orbits of points of extent \( k \) in \( C_n \) and the \( G_{n'} \)-orbits of points of extent \( k \) in \( C_{n'} \). We therefore investigate the subset \( C_n^* \) of \( C_n \) consisting of the points of extent \( n \) and we let \( c_n^* \) be their cardinality \( |C_n^*| \) and \( c_n = |C_n| \). Then

\[
c_n = \sum_{k=1}^{n} \binom{n}{k} c_k^*
\]

where \( c_1^* = 0 \). By [1, p. 146], when \( p \) is odd

\[
c_n = \frac{p^{n-1} - 1}{p - 1} = 1 + p + \ldots + p^{n-2}
\]

for odd \( n \) while for even \( n \)

\[
c_n = \frac{p^{n/2} - \lambda^{n/2}}{p^{(n/2) - 1} + \lambda^{n/2}}/\left(1 - \lambda\right)
= 1 + p + \ldots + p^{n-2} + \lambda^{n/2} p^{(n/2) - 1}
\]

where \( \lambda \) is the Legendre symbol \((-1/p)\).
LEMMA 7. If $p$ is odd,

$$c^*_n = \frac{(p - 1)^{n-1} - (-1)^{n-1}}{p} + \lambda(-1)^n \sum_{i=1}^{\infty} \binom{n}{2i} (\lambda p)^{i-1}$$

$$= (-1)^n \sum_{i=1}^{\infty} \left( \lambda^i \left( \binom{n}{2i} + (-1)^{i-1} \binom{n-1}{i} \right) \right) p^{i-1}.$$

These are of course finite sums since the binomial coefficient $\binom{n}{r} = 0$ when $n < r$.

**Proof.** The relationship (2) defines $c^*_n$ uniquely as a linear function of $c_1, \ldots, c_n$ for any choice of the $c_i$'s. We therefore begin by solving (2) when $c_n = (p^{n-1} - 1)/(p - 1)$ for all $n$ and show by induction on $n$ that the corresponding $c^*_n$ is

$$c^*_n = \frac{(p - 1)^{n-1} - (-1)^{n-1}}{p}.$$

For $n = 1, c_1 = c^*_1 = 0$. Suppose $n > 1$. Then

$$c^*_n = c_n - \sum_{k=1}^{n-1} \binom{n}{k} c^*_k = \frac{p^{n-1} - 1}{p - 1} - \sum_{k=1}^{n-1} \binom{n}{k} \left( \frac{p - 1)^{k-1} - (-1)^{k-1}}{p} \right)$$

by the induction hypothesis. One now uses the identities

$$\sum_{k=1}^{n} \binom{n}{k} (p - 1)^{k-1} = 1 + \frac{p^n - p}{p - 1}, \quad \sum_{k=0}^{n} \binom{n}{k} (-1)^k = 0$$

to finish the induction step. We now consider instead

$$c_n = 0 \quad n \text{ odd}$$

$$= r^{n/2} \quad n \text{ even}$$

for any number $r$ and show that the corresponding $c^*_n = (-1)^n \sum_{i=0}^{\infty} \binom{n}{2i} r^i$. It holds for $n = 1$ so suppose $n > 1$. Using (2) as above we get

$$c^*_n = c_n - \sum_{i=1}^{\infty} \sigma_i r^i \quad \text{where} \quad \sigma_i = \sum_{k=1}^{n-1} (-1)^k \binom{n}{k} \binom{k}{2i}.$$

Now $\sigma_i = 0$ for $i \geq n/2$, and if $i < n/2$ one can show that $\sigma_i = \binom{n}{2i}(-1)^{n-1}$, whence the formula for $c^*_n$.

Using the linearity of $c^*_n$ as a function of the $c_n$'s and putting $r - \lambda p$, we get (for the original $c^*_n$)
SPLITTINGS OF ALMOST UNIMODULAR FORMS

\[ c_n^* = \frac{(p - 1)^{n-1} - (-1)^{n-1}}{p} + \frac{1}{p} (-1)^n \sum_{i=1}^\infty \left( \frac{n}{2i} \right) \lambda^i p^i \]

as desired. The second expression for \( c_n^* \) follows easily from the first.

We use Lemma 7 to record the first few values of \( c_n^* \) (\( c_1^* = 0 \)) when \( p \) is odd:

\[
\begin{align*}
    c_2^* &= 1 + (-1/p), \\
    c_3^* &= p - 2 - 3(-1/p), \\
    c_4^* &= p^2 - 2p + 3 + 6(-1/p), \\
    c_5^* &= p^3 - 4p^2 + p - 4 - 10(-1/p).
\end{align*}
\]

When \( p = 2 \), it is obvious that \( c_n^* \) is zero when \( n \) is odd and equals one when \( n \) is even.

Let \( p \) be odd and let \( \Delta \) be a non-square in \( \mathbb{F}_p \). We define \( c_{r,s}^* \) to be the number of projective solutions of \( \sum_i x_i^2 + \Delta \sum_i y_i^2 = 0 \) of extent \( r + s \).

Thus

\[
c_{r,s}^* = c_{s,r}^*, \quad c_n^* = c_{n,0}^* = c_{0,n}^*, \quad c_{1,1}^* = 1 - \left( -\frac{1}{p} \right),
\]

the latter following from: \( x^2 + \Delta y^2 \) is hyperbolic iff \((-1/p) = -1\). Also for any \( \alpha \neq 0 \) in \( \mathbb{F}_p \), one can show, using the norm from \( \mathbb{F}_p((-\Delta)^{1/2}) \) to \( \mathbb{F}_p \), that the number of affine solutions of \( x^2 + \Delta y^2 = \alpha \) of extent 2 is \( p - 2 + (-1/p) \). Now it is clear that \((p - 1)c_{r,s}^*\) is the number of affine solutions of \( \sum_i x_i^2 + \Delta \sum_i y_i^2 = -x_r^2 - \Delta y_s^2 \) of extent \( r + s \), which is the sum, over all \( \alpha \) in \( \mathbb{F}_p \), of the product of the number of affine solutions of \( \sum_i x_i^2 + \Delta \sum_i y_i^2 = \alpha \) of extent \( r + s - 2 \) and the number of affine solutions of \(-x_r^2 - \Delta y_s^2 = \alpha \) of extent 2. The first multiplicand is \( c_{r,s-1}^* \) if \( -\alpha \) is a square \( \neq 0 \), \( c_{r,s-1}^* \) if \(-\alpha \) is a non-square. We easily get

**Lemma 8.** If \( r, s \geq 1, r + s \geq 3 \), and \( p \) is odd,

\[
c_{r,s}^* = (p - 1) \left( 1 - \left( -\frac{1}{p} \right) \right) c_{r-1,s-1}^* + \frac{1}{2} \left( p - 2 + \left( -\frac{1}{p} \right) \right) (c_{r,s-1}^* + c_{r-1,s}^*).
\]

The first few values of \( c_{r,s}^* \) are (\( p \) odd)

\[
\begin{align*}
    c_{2,1}^* &= p - 2 + \left( -\frac{1}{p} \right), \\
    c_{2,2}^* &= p^2 - 2p + 3 - 2 \left( -\frac{1}{p} \right) \\
    c_{3,1}^* &= p^2 - 4p + 3.
\end{align*}
\]
To count the number of orbits of $G_n$ in $C_n^*$ we shall apply Burnside's Theorem [3, p. 39],

$$|G_n \setminus C_n^*| = \frac{1}{|G_n|} \sum_{\tau \in G_n} |C_n^{*\tau}|,$$

where $C_n^{*\tau}$ is the set of points in $C_n^*$ fixed by $\tau$.

For any integer $t \neq 0$ let $\text{ord}_2 t$ be the exponent of the largest power of 2 dividing $t$. The following lemma is proved by decomposing the cyclic group $\mathbb{F}_p^\times$ into its primary components.

**Lemma 9.** Let $d_1, \dots, d_k$ be positive integers and $E_i = \pm 1$ for $1 \leq i \leq k$. If $p$ is odd the system of equations

$$x^{d_1} = E_1, \ldots, x^{d_k} = E_k$$

has a solution in $\mathbb{F}_p^\times$ iff for all $i$ and $j$

$$E_i = E_j = -1 \Rightarrow \text{ord}_2 d_i = \text{ord}_2 d_j < \text{ord}_2(p - 1),$$
$$E_i = -1, E_j = 1 \Rightarrow \text{ord}_2 d_i < \text{ord}_2 d_j.$$  

Consider first $\tau = (E_1, \ldots, E_k)(12 \cdots n)$ and suppose that $x^\tau = x$ where $x = [x_1, \ldots, x_n]$ with $x_i \neq 0$ for all $i$. This means that there is a (uniquely determined) $\zeta$ in $\mathbb{F}_p^\times$ such that $E_i x_i = \zeta x_{i+1}$ for $1 \leq i \leq n$ (indices mod $n$), in particular

$$\zeta^n = E,$$

where $E = \prod E_i$, and

$$x = [x_1, \zeta^{-1} E_2 x_1, \zeta^{-2} E_2 E_3 x_1, \ldots, \zeta^{-(n-1)} E_2 \cdots E_n x_1].$$

Conversely if $x$ is of this form with $\zeta$ satisfying (5), then $x^\tau = x$. And for any such $x$,

$$\sum_{i=1}^n x_i^2 = 0 \quad \text{if} \quad \zeta \neq \pm 1,$$
$$= n x_1^2 \quad \text{if} \quad \zeta = \pm 1.$$  

Now suppose $\tau$ is an arbitrary element of $G_n$. Express $\tau$ as a product of disjoint signed cycles, with signs $E_1, \ldots, E_k$ and lengths $d_1, \ldots, d_k$, respectively. Define

$$d = \gcd \text{ of } p - 1, d_1, \ldots, d_k,$$
$$d_0 = 1 \quad \text{if } d \text{ is odd},$$
$$= 2 \quad \text{if } d \text{ is even and } E_i = 1 \text{ for all } i,$$
$$= 0 \quad \text{otherwise}.$$
Let $c^* \langle d_1, \ldots, d_k \rangle$ be the number of solutions of $\sum d_i x_i^2 = 0$ in $P_{n-1} (\mathbb{F}_p)$ of extent $k$.

**Lemma 10.** When $p$ is odd, $C_n^{*+} \neq \emptyset$ iff (4) holds, and then

$$|C_n^{*+}| = (d - d_0)(p - 1)^{k-1} + d_0 c^* \langle d_1, \ldots, d_k \rangle.$$

Proof. Consider the signed cycle decomposition of $\tau$. We can apply the above analysis for $(\varepsilon_1, \ldots, \varepsilon_n)(12 \cdots n)$ to each of these signed cycles and the corresponding subsets of the coordinates on which they operate. If $x^\tau = x$, this yields for each $i$, a $\zeta_i$ such that $\zeta_i^n = E_i$. But of course the same $\zeta$ must work for all the coordinate subsets if $x^\tau = x$, so $\zeta$ is a solution of (3) hence (4) is satisfied. It is easy to see that if (3) has at least one solution, then the number of solutions is $d$ and the number of solutions equal to $\pm 1$ is $d_0$. The desired formula now follows from (6) and (7).

We now consider low values of $n$. Each element in the conjugacy class of $\tau$ fixes the same number of points as $\tau$—in fact so does every element in the conjugacy class of $-\tau$. We therefore make tables with each line consisting of the following: an element $r$ of $G_n$, the number of elements in the union of the conjugacy classes of $r$ and $-r$ (as determined by Proposition 6, e.g.) and the number of points in $C_n^*$ fixed by $r$ (as determined by Lemma 10 and the formulas for $c_n^*$ and $c_n^{*+}$). (It is understood of course that each conjugacy class appears exactly once in the list.) We note that $c^* \langle d_1, \ldots, d_k \rangle$ can be calculated from the $c_{r,s}^*$. For example, $c^* \langle d_1, d_2, d_3 \rangle$ is a sum of several terms of which

$$\frac{1}{8} \left(1 + \left(\frac{d_1}{p}\right)\right)\left(1 - \left(\frac{d_2}{p}\right)\right)\left(1 + \left(\frac{d_3}{p}\right)\right) c_{2,1}^*$$

is typical—it arises from the case of all $d_i \neq 0 \pmod{p}$ with $d_1$ and $d_3$ squares and $d_2$ non-square, mod $p$.

For brevity we write $+$ for $+1$ and $-1$ in multisigns.

$n = 2$.

<table>
<thead>
<tr>
<th>Identity</th>
<th>$(+, -)$</th>
<th>$(12)$</th>
<th>$(+, -)(12)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

By Burnside's Theorem the number of orbits of extent 2 is

$$\frac{1}{8}(4(1 + (-1/p))) = \frac{1}{4}(1 + (-1/p)).$$
\(n = 3.\)

\[
\begin{array}{ccc}
\text{identity} & 2 & p - 2 - 3(-1/p) \\
(+ + -) & 6 & 0 \\
(12) & 12 & 1 + (-2/p) \\
(+ - +)(12) & 12 & 0 \\
(123) & 16 & 1 + (-3/p)
\end{array}
\]

Thus the number of orbits of extent 3 is
\[
\frac{1}{24} \left( p + 12 - 3 \left( \frac{-1}{p} \right) + 6 \left( \frac{-2}{p} \right) + 8 \left( \frac{-3}{p} \right) \right).
\]

In the tables for \(n = 4\) and 5, we omit conjugacy classes with empty fixed point sets.

\(n = 4.\)

\[
\begin{array}{ccc}
\text{identity} & 2 & p^2 - 2p + 3 + 6(-1/p) \\
(12) & 24 & p - 2 - (-1/p) - 2(-2/p) \\
(12)(34) & 12 & 2 + 2(-1/p) \\
(- + - +)(12)(34) & 12 & (p - 1)(1 + (-1/p)) \\
(123) & 64 & 0 \text{ when } p = 3, \\
& & 1 + (-3/p) \text{ when } p \neq 3 \\
(1234) & 48 & 1 + (-1/p) \\
(- + + +)(1234) & 48 & 1 + (-1/p) + (-2/p) + (2/p)
\end{array}
\]

Thus the number of orbits of rank 4 is
\[
\frac{1}{192} \left( p^2 + 16p + 6p \left( \frac{-1}{p} \right) + 65 + 48 \left( \frac{-1}{p} \right) + 24 \left( \frac{2}{p} \right) + 32 \left( \frac{-3}{p} \right) \right)
\]

when \(p \neq 3, 0 \text{ when } p = 3.\)

\(n = 5.\)

\[
\begin{array}{ccc}
\text{identity} & 2 & p^3 - 4p^2 + p - 4 - 10(-1/p) \\
(12) & 40 & p^2 - 3p + 3 + p(2/p) + 3(-1/p) + 3(-2/p) \\
(12)(34) & 120 & p - 2 - (-1/p) - 2(-2/p) \\
(12)(345) & 320 & 1 + (-6/p) \text{ when } p \neq 3 \\
& & 0 \text{ when } p = 3 \\
(123) & 160 & p - 2 - (-1/p) - 2(-3/p) \text{ when } p \neq 3 \\
& & 0 \text{ when } p = 3 \\
(1234) & 480 & 1 + (-1/p) \\
(12345) & 768 & 1 \text{ when } p = 5 \\
& & (p - 1, 5) - 1 \text{ when } p \neq 5
\end{array}
\]
Here \((p - 1, 5)\) is the gcd of \(p - 1\) and 5. The number of orbits of extent 5 is 0 when \(p = 3\), 1 when \(p = 5\) and

\[
\frac{1}{1920} \left\{ p^3 + 16p^2 + 81p + 20p \left( \frac{2}{p} \right) - 208 + 150 \left( \frac{-1}{p} \right) - 60 \left( \frac{-2}{p} \right) \\
+ 160 \left( \frac{-6}{p} \right) - 160 \left( \frac{-3}{p} \right) + 384(p - 1, 5) \right\}
\]

for \(p > 5\).

By Theorems 4 and 5, these formulas for \(n = 2, 3, 4, 5\) will enable us to calculate, for the same values of \(n\) and \(p\) odd, the number \(H_{p,n}\) of equivalence classes of geometric almost unimodular lattices \((L, M)\) with \(\det L = p^2\) and \(M \cong I_n\). We note first that it follows directly from the fact that 1 is the only non-zero square in \(\mathbb{F}_2\) or \(\mathbb{F}_3\), and Theorems 4 and 5, that

\[
H_{2,n} = \left\lfloor \frac{n}{2} \right\rfloor, \quad H_{3,n} = \left\lfloor \frac{3n}{2} \right\rfloor.
\]

The second through fifth columns in Table I give the number of orbits of extent 2 through 5, respectively, calculated from our formulas. From these we calculate the corresponding \(H_{p,n}\). For example \(H_{13,4}\) is the sum

\[
1 + 1 + 3 = 5
\]

of the numbers of orbits of extents 2, 3 and 4 for \(p = 13\).

**Remark 11.** Since there is one orbit of extent 2 iff \(p = 2\) or \(p \equiv 1\) (mod 4), and no such orbit otherwise, it follows from Theorem 4 that in any dimension \(n \geq 3\) there is a Jordan split gaul iff \(p = 2\) or \(p \equiv 1\) (mod 4), and in this case there is exactly one. This of course holds only in the special case under consideration at the moment \((M \cong I_n, \det L = p^2)\).

One can carry on this computation for higher values of \(n\) but it clearly

<table>
<thead>
<tr>
<th>(p)</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>(H_{p,3})</th>
<th>(H_{p,4})</th>
<th>(H_{p,5})</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>7</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>11</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>13</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>5</td>
<td>8</td>
</tr>
<tr>
<td>17</td>
<td>1</td>
<td>1</td>
<td>4</td>
<td>6</td>
<td>2</td>
<td>6</td>
<td>12</td>
</tr>
<tr>
<td>19</td>
<td>0</td>
<td>2</td>
<td>3</td>
<td>7</td>
<td>2</td>
<td>5</td>
<td>12</td>
</tr>
<tr>
<td>23</td>
<td>0</td>
<td>1</td>
<td>4</td>
<td>12</td>
<td>1</td>
<td>5</td>
<td>17</td>
</tr>
<tr>
<td>29</td>
<td>1</td>
<td>1</td>
<td>8</td>
<td>21</td>
<td>2</td>
<td>10</td>
<td>31</td>
</tr>
<tr>
<td>31</td>
<td>0</td>
<td>2</td>
<td>7</td>
<td>26</td>
<td>2</td>
<td>9</td>
<td>35</td>
</tr>
</tbody>
</table>
becomes very laborious. Instead we give some qualitative results, still in the
special case when the form of $M$ is $X_1^2 + \cdots + X_n^2$.

Let $m$ be an integer $\geqslant 1$. A polynomial of modulus $m$ is a function $\mathbb{Z} \to \mathbb{Q}$
of the form

$$a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0,$$

where $X$ is the identity function on $\mathbb{Z}$ and, for all $i$, $a_i : \mathbb{Z} \to \mathbb{Q}$ is constant on
each residue class mod $m$; if $a_n$ is not identically zero, $n$ is the degree of the
function. The collection $\mathbb{Q}[X]_m$ of polynomials of modulus $m$ is a ring and
$\mathbb{Q}[X]_m \subseteq \mathbb{Q}[X]_{m'}$, if $m$ divides $m'$. The union (direct limit) of the $\mathbb{Q}[X]_m$ for
all $m$ is a ring $\mathbb{Q}[X]_0$. Note that

$$\mathbb{Q}[X]_m + \mathbb{Q}[X]_{m'} \subseteq \mathbb{Q}[X]_l,$$

$\mathbb{Q}[X]_m \cdot \mathbb{Q}[X]_{m'} \subseteq \mathbb{Q}[X]_l$,

where $l$ is any common multiple of $m$ and $m'$.

The zero function or a polynomial of modulus $m$ and degree 0 will be
called a constant of modulus $m$.

By $O_m(X^n)$ is meant an element of $\mathbb{Q}[X]_m$ of degree $\leq r$; its value for $p \in \mathbb{Z}$
is denoted by $O_m(X^n)(p)$.

**Theorem 12.** Let $n$ be an integer $\geqslant 4$ and let $n' = q \cdot (\text{lcm of } n \text{ and } 8)$,
where $q$ is the product of all odd primes $< n$ which do not divide $n$. Then
there is a monic polynomial $P$ of modulus $n'$ and degree $n - 2$ such that, for
all primes $p \geqslant 5$,

$$|G_n \setminus C_n^*| = (1/2^{n-1}n!)P(p).$$

Moreover

$$P = \sum \gamma(d_1, \ldots, d_k) c^*(d_1, \ldots, d_k) + O_n(X^{(n/2)\cdot 1})(p),$$

where the sum is over all partitions ("unordered") $n = \sum d_i$ of $n$ into more
than $\lfloor \frac{1}{2}n \rfloor$ positive integers $d_1, d_2, \ldots$,

$$\gamma(d_1, \ldots, d_k) = n! \cdot 2^{n-k}/d_1 \cdots d_k \cdot \mu_1! \cdots \mu_n!$$

and $\mu_i$ is the multiplicity of $i$ in $d_1, \ldots, d_k$.

**Proof.** We first extend the Legendre symbol $(-1/p)$ in some way from a
function on the odd primes to a constant of modulus 4. Then by Lemma 7,
$c^*_n$ (for odd primes) is given by a monic polynomial of modulus 4 and degree
$n - 2$ if $n \geqslant 3$; by Lemma 8 and induction, $c^*_r, s$ is given by a monic
polynomial of modulus 4 and degree $r + s - 2$ if $r + s \geqslant 3$. Consider
$c^*(d_1, \ldots, d_k)$ and for a given prime $p \geqslant 5$, let $r, s$ and $t$ be resp. the number of
for which \((d_i/p) = 1, -1\) and 0; clearly \(r + s + t = k\) and, since all \(d_i\) are \(\leq n\), the integers \(r\), \(s\) and \(t\) are determined by the residue class of \(p \pmod{n'}\). Furthermore it is easy to see that

\[
\begin{align*}
    c^*(d_1, \ldots, d_k) &= c^*_{r,s} \cdot (p - 1)^t & \text{if } t < k \\
    &= (p - 1)^{k - 1} & \text{if } t = k
\end{align*}
\]

and so is given by a polynomial of modulus \(n'\) and degree \(\leq k - 1\). Suppose now that \(k > \frac{1}{2}n\). If no more than 2 of the \(d_i\) are \(\neq 0 \pmod{p}\), \(2 + 5(k - 2) \leq n\) which contradicts \(k > \frac{1}{2}n\) and \(n \geq 4\). Thus at least 3 of the \(d_i\) are \(\neq 0 \pmod{p}\) and it follows that \(c^*(d_1, \ldots, d_k) = c^*_{r,s}(p - 1)^t\) and is monic of degree \(k - 2\) and modulus \(n'\).

We now consider the functions \(d\) and \(d_0\) defined before Lemma 10. \(d\) has modulus \(= \gcd\) of \(d_1, \ldots, d_k\), hence also has modulus \(n'\) since \(n = \sum d_i\). It follows that \(d_0\) also has modulus \(n'\).

Now let \(\tau \in G_n\) have signed cycle lengths \(d_1, \ldots, d_k\) with \(k > n/2\). Then \(d_i = 1\) for all least one value of \(i\) and so, if \(C^*_{\tau} \neq \emptyset\) and any of the signs of the signed cycles of \(\tau\) are \(-1\), it follows from Lemma 10 that those with sign \(-1\) are precisely the signed cycles of odd length. Since we are interested in computing \(|C^*_{\tau}|\) we may replace \(\tau\) by \(-\tau\) and also by a conjugate if necessary and thereby suppose that \(\tau \in S_n\) (see Proposition 6 and its proof).

Note that the conjugacy classes of \(\tau\) and \(-\tau\) in \(G_n\) are equipotent but distinct, and that they are the only two conjugacy classes of signed cycles with cycle lengths \(d_1, \ldots, d_k\) and non-empty fixed point sets in \(C^*_{\tau}\). The cardinality of the conjugacy class of \(\tau\) (or \(-\tau\)) is \(\gamma(d_1, \ldots, d_k)\) by Proposition 6. Since \(d = d_0 = 1\) when at least one \(d_i = 1\), the theorem now follows from Burnside's Theorem and Lemma 10.

**Corollary 13.** Let \(n \geq 4\) and let \(M\) be a lattice with form \(X_1^2 + \cdots + X_n^2\). The number of equivalence classes of gauls \((L, M)\) is \([\frac{1}{2}n]\) if \(p = 2\), \([\frac{1}{3}n]\) if \(p = 3\), and, if \(p \geq 5\), is given by a polynomial of modulus \(n'\), leading coefficient \(= 1/2^{n-1}n!\), and degree \(n - 2\). None of these equivalence classes has a Jordan splitting if \(p \equiv 3 \pmod{4}\), and exactly one has a Jordan splitting if \(p = 2\) or \(p = 1 \pmod{4}\).

**Proof.** The formulas for \(p = 2\) and 3 were mentioned before Table 1, and the statement for \(p \geq 5\) follows readily from Theorem 13. For the last statement, see Remark 11.

**Remark 14.** It follows that if \(n\) is fixed the number of equivalence classes \(\rightarrow \infty\) as \(p \rightarrow \infty\). It follows from the Corollary and Theorem 20 and its proof that when \(n \geq 5\), the number of equivalence classes of geometric almost unimodular lattices \((L, M)\) with \(\det L = p^2\) and \(M \simeq I_n\) is \([\frac{1}{2}n]\) when \(p = 2\), \([\frac{1}{3}n]\) when \(p = 3\), \(\geq n - 2\) when \(p \geq 5\) (in fact the number of isometry
classes of such almost unimodular lattices in \( M \cong I_n \) satisfies the same equalities and inequalities). Thus the number of these equivalence classes goes to \( \infty \) with \( n \) as well.

**Example 15.** We show how the methods of this section can be applied in particular cases to obtain explicit results. Consider \( p = 7 \). There are no solutions to \( X_1^2 + X_2^2 = 0 \) in \( F_7 \). There is one orbit of extent 3 isotropic points (see Table I), represented by \([1, 2, 3]\). \( M + Z \frac{1}{7}(2e_1 + 2e_2 + 3e_3) \) has basis \( \frac{1}{7}(e_1 + 2e_2 + 3e_3) \), \( e_2, e_3 \); if \( A \) is the matrix of the bilinear form with respect to this basis,

\[
A^{-1} = \begin{bmatrix}
49 & -14 & -21 \\
-14 & 5 & 6 \\
-21 & 6 & 10
\end{bmatrix}
\]

and so the associated almost unimodular quadratic form in three variables is

\[
q_3 = 49X_1^2 + 5X_2^2 + 10X_3^2 - 28X_1X_2 - 42X_1X_3 + 12X_2X_3.
\]

Now consider isotropic points of extent 4. The same procedure as above can be used here. However there is a simpler way which avoids the inversion of a matrix. There is again only one orbit, represented by \([3, 3, 3, 1]\). The associated lattice \( L \) therefore consists of

\[
\left\{ \sum x_ie_i \in M : 3x_1 + 3x_2 + 3x_3 + x_4 \equiv 0 \pmod{7} \right\}.
\]

By considering the conditions obtained by putting some of the \( x_i = 0 \), we obtain the vectors

\[
e'_1 = e_1 - e_2, \quad e'_2 = e_2 - e_3, \quad e'_3 = e_3 - 3e_4, \quad e'_4 = 7e_4
\]

(8)

which are easily seen to generate \( L \), hence to form a basis. We then calculate the matrix of the bilinear form with respect to this basis and get the quadratic form

\[
q_4 = 2X_1^2 + 2X_2^2 + 10X_3^2 - 2X_1X_2 - 2X_1X_3 - 42X_2X_3.
\]

Of course we also get the form \( q_4' = q_3 + X_4^2 \) in dimension 4.

The only orbit of solutions of extent 5 is represented by \([3, 3, 1, 1, 1]\) and the associated form is

\[
q_5 = 2(X_1^2 + X_2^2 + X_3^2) + 10X_2^2 + 49X_3^2 - 2X_1X_2 - 6X_2X_3 - 2X_3X_4 - 14X_4X_5.
\]
The other forms of 5 variables are $q_4 + X_2^2$, $q_3 + X_4^2 + X_2^2$. We note in passing that the class number of $q_4$ is 1, that of $q_3$ is 2 and the other form in its genus is $q_2 + X_2^2$, and that of $q_4$ is 3 with $q_3 + X_4^2 + X_2^2$ and $q_4 + X_2^2$ being the other forms in the genus. See Remark 22.

One can similarly determine the forms belonging to totally degenerate subspaces of $M/7M$ of dimension $> 1$. For example, consider the totally degenerate plane in $M/7M$ spanned by $(3, 3, 3, 1)$ and $(1, 2, -3, 0)$. The lattice $L$ consists of all vectors in $M$ whose inner products with these two vectors, now considered as vectors in $M$, are $\equiv 0 \pmod{7}$. We have already found a basis (8) for the lattice determined by the first congruence. A typical vector in it is

$$\sum x_i e'_i = x_1 e_1 + (x_2 - x_1) e_2 + (x_3 - x_2) e_3 + (7x_4 - 3x_3) e_4$$

so its inner product with $(1, 2, -3, 0)$ is $-x_1 + 5x_2 - 3x_3$, and we find a basis for $L$ in the same way as before:

$$-e'_1 + 4e'_2 = -e_1 + 6e_2 - 4e_3, \quad e'_2 - 3e'_3 = e_2 - 4e_3 + 9e_4,$$

$$7e'_3 = 7e_3 - 21e_4, \quad e'_4 = 7e_4.$$ 

Then one can easily calculate the associated quadratic form (which will necessarily be 7-modular):

$$42X_2^2 + 98X_3^2 + 490X_5^2 + 49X_2^2 + 42X_1X_3 - 56X_4X_3 - 434X_2X_3,$$

$$+ 126X_2X_4 - 294X_3X_4.$$ 

The method used above yields easily:

**Theorem 16.** Let $[a_1, \ldots, a_n] \in C_n$ have extent $n$, where the $a_i$ are integers considered $\pmod{p}$, and let $b_1, \ldots, b_n$ be solutions of $a_1 + a_2b_2 \equiv 0, \ldots, a_{n-1} + a_nb_n \equiv 0 \pmod{p}$. Then the almost unimodular quadratic form corresponding to $[a_1, \ldots, a_n]$ is

$$\sum_{i=1}^{n-1} (1 + b_{i+1}^2)X_i^2 + p^2X_n^2 + 2 \sum_{i=1}^{n-1} b_{i+1}X_iX_{i+1} + 2pb_nX_{n-1}X_n.$$ 

The more general case of $[a_1, \ldots, a_n]$ not necessarily of extent $n$ reduces easily to this one.
4. APPLICATIONS TO CLASS NUMBERS

**Theorem 17.** Let \( M \) be \( \sim I_n \) and let \( L \) (resp. \( K \)) be an almost unimodular sublattice of \( M \) corresponding to a vector of \( M/pM \) of extent \( l \) (resp. \( k \)), (cf. Theorem 4). Then

(a) \( L \cong K \Rightarrow l = k \); if \( p = 2 \) or \( 3 \), the converse also holds.

(b) \( L \) is the orthogonal sum of a sublattice \( \simeq I_{n-1} \) and a lattice \( L' \) of rank \( l \) and determinant \( p^3 \).

(c) \( L' \) is even when \( p = 2 \), otherwise odd.

(d) if \( p = 2 \) or \( 3 \), \( L' \) is indecomposable.

(e) if \( p \geq 5 \), \( L' \) is either indecomposable or the orthogonal sum of two indecomposable lattices of determinant \( p \).

**Proof.** Let \( e_1, \ldots, e_n \) be an orthonormal basis for \( M \). Suppose first that \( l = n \). If \( J \) is a non-zero unimodular orthogonal component of \( L \), then \( J \) is also an orthogonal component of \( M \) and hence contains at least one of the \( e_i \); since \( J \) is an orthogonal component of \( L^* \) too and \( pJ \) has image 0 in \( M/pM \), it is easy to see that \( L \) could not correspond to an isotropic vector of \( M/pM \) of extent \( n \). Thus \( L \) has no non-zero unimodular component and, since it has determinant \( p^2 \), it must be either indecomposable or the orthogonal sum of two indecomposables of determinant \( p \). If \( p \) is odd, \( L \) is odd since it contains \( pe_1 \).

In the case \( p = 2 \) or \( 3 \), it is easy to see that by replacing \( (L, M) \) by an equivalent gaul, we may suppose that

\[
L = \left\{ \sum x_i e_i \in M : \sum x_i \equiv 0 \pmod{p} \right\}.
\]

In particular \( L \) is unique up to isometry, and is obviously even when \( p = 2 \). Any vector \( e_i - e_j \) \((i \neq j)\) is in \( L \) and satisfies \( f(e_i - e_j, e_i - e_j) = 2 \). Since the sublattice generated by a vector of length 1 would be unimodular, \( e_i - e_j \) must be orthogonally indecomposable. It follows that the \( e_i - e_j \) must all be in the same indecomposable component of \( L \), which is necessarily \( = L \) since they generate \( L \).

In the general case \( l \leq n \), we may assume that the vector of \( M/pM \) corresponding to \( L \) is a linear combination of \( e_i + pM, \ldots, e_i + pM \) and it follows that \( J = \sum_{i>1} z_i e_i \) is in \( L \), hence \( L = L' \perp J \) with \( L' \subseteq \sum_{i=1}^l z_i e_i = M' \) and of rank \( l \). It is easy to see that \( L' \) is an almost unimodular lattice in \( M' \) corresponding to the same line in \( M'/pM' \subseteq M/pM \) as \( L \) does, so this case follows from the case \( l = n \). Note that the first part of (a) follows from (b), (d) and (e).

**Remark 18.** We shall show by means of an example that the decomposable case really does occur (when \( l \equiv 0 \pmod{p} \), it is easy to give
SPLITTINGS OF ALMOST UNIMODULAR FORMS

examples of indecomposable ones by the method in the proof of Theorem 17 for \( p = 2 \) and 3). It would be interesting to know what the conditions on \([a_1, ..., a_l]\) are which determine the decomposability of the corresponding \( L' \).

Let \( p = 5 \) and consider the lattice

\[
L \simeq \left( \begin{array}{cc} 15 & 5 \\ 5 & 2 \end{array} \right) \perp \left( \begin{array}{cc} 15 & 5 \\ 5 & 2 \end{array} \right).
\]

Each of the summands has determinant 5 and is easily seen to be almost unimodular and indecomposable (cf. [2, Example 8]). The (binary) \( p \)-modular Jordan component of \( L \), has determinant \( 5^2 \) since it is the sum of two equivalent unary lattices, and hence is a hyperbolic plane since \(-1\) is a square in \( \mathbb{Z}_5 \). By Proposition 3, \( L \) is contained in a unimodular lattice \( M \) of rank 4 on \( \mathbb{Q}L \). Of course \( M \simeq I_4 \), say, in the basis \( e_1, ..., e_4 \) [7, 106:10]. Now

\[
L' = \left( \begin{array}{c} 3/5 \\ 1 \\ 2 \end{array} \right) \parallel \left( \begin{array}{c} 3/5 \\ 1 \\ 2 \end{array} \right) = \text{matrix } A
\]

in the basis \( e'_1, ..., e'_4 \), say. Thus \( e_j = \sum_{i=1}^4 b_{ij} e'_i \) for integers \( b_{ij} \) so

\[
I_4 = 'BAB,
\]

where \( B = (b_{ij}) \). Thus \('BA = B^{-1} \) so

\[
5B^{-1} = 'B(5A) \equiv \left[ \begin{array}{ccc} 3b_{11} & 0 & 3b_{31} & 0 \\ 3b_{12} & 0 & 3b_{32} & 0 \\ 3b_{13} & 0 & 3b_{33} & 0 \\ 3b_{14} & 0 & 3b_{34} & 0 \end{array} \right] \pmod{5}.
\]

Now \( e_j \notin L \) since otherwise \( \mathbb{Z}e_j \) would split \( L \) orthogonally, so at least one of \( b_{1j} \) and \( b_{3j} \) is \( \neq 0 \pmod{5} \), hence both are since \( f(e_j, e_j) \) is integral. Since the matrix of coefficients of the basis \( 5e'_1, ..., 5e'_4 \) of \( 5L' \) in terms of the basis \( e_1, ..., e_4 \) of \( M \) is \( 5B^{-1} \), the totally degenerate subspace of \( \mathbb{F}_5^4 \) corresponding to \( L \) is generated by the image of \( \sum_{i=1}^4 b_{1j} e_j \), which has extent 4.

Remark 19. It is possible to generalize part of Theorem 17. Namely, let \( M \) be a positive definite lattice with decomposition \( M = M_1 \perp M_2 \perp ... \perp M_n \) into indecomposables. Say that a totally degenerate subspace \( S \) of \( M/pM \) has extent \( l \) if \( S \) is contained in the image of a sum of \( l \) of the \( M_i \) and no fewer. If \( m \) is the dimension of \( S \) and \( L \) is the corresponding almost unimodular sublattice of \( M \), one can easily show that \( L = M' \perp L' \), where \( M' \) is the sum of \( n-l \) of the \( M_i \) and \( L' \) is the orthogonal sum of at most \( 2m \) indecomposable almost unimodular lattices, each with determinant \( = 0 \pmod{p} \).
THEOREM 20. Let $p$ be odd. Assume $n \geq 2$ if $p \equiv 1 \pmod{4}$ and $n \geq 3$ if $p \equiv 3 \pmod{4}$. Then there is one and only one genus $G_{p,n}$ of quadratic forms of rank $n$ with the following two properties:

(i) the forms in $G_{p,n}$ are odd, positive definite, and almost unimodular.

(ii) the $p$-modular $\ell_{p}$-Jordan component of each form is $\simeq (0,0)$. The class number $h_{p,n}$ of $G_{p,n}$ satisfies

$$H_{p,n}^{0} \leq h_{p,n} \quad (\text{all } n),$$

where $H_{p,n}^{0}$ is the cardinality of $\{k \leq n: c_{k}^{*} \neq 0\}$. Furthermore

$$h_{p,n} \leq H_{p,n} \quad (n \leq 8).$$

(cf. preamble to Table I). We have

$$H_{3,n}^{0} = \lfloor n/3 \rfloor, \quad H_{5,2}^{0} = 1, \quad H_{5,n}^{0} = n - 2 \quad (n \geq 3),$$

$$H_{p,n}^{0} = \frac{1}{2}(1 + (-1/p)) + n - 2 \quad (n \geq 2, p > 5).$$

Proof. We begin with the last part. In $F_{3}$, 1 is the only non-zero square and so $H_{p,n}^{0} = \lfloor n/3 \rfloor$ for all $n$. If $p > 3$ and $3 \leq k \leq 6$, one can check from the formulas for $c_{k}^{*}$ that $C_{k}^{*} \neq \phi$ except for $C_{3}^{*}$ when $p = 5$. We note also that $C_{2}^{*} \neq \phi$ when $p = 5$. Since every integer $\geq 5$ can be expressed as a non-negative integral linear combination of 3, 4, and 5, and also of 2, 4, and 5, the formulas for $H_{p,n}^{0}$ follow easily since $H_{p,n}^{0} = \frac{1}{2}(1 + (-1/p))$.

Since $H_{p,n}^{0} > 0$ for $n \geq 2$ resp. $3$ when $p \equiv 1$ resp. $3 \pmod{4}$, there are lattices of rank $n$ satisfying (i) and (ii) by Theorem 4 applied to $M \simeq I_{n}$, and Proposition 3. If $L$ and $L'$ are two of them, $L_{q} \simeq L'_{q}$ for all odd $q \neq p$ by determinants, $L_{p} \simeq L'_{p}$ since the determinants of their respective Jordan components are equal by (ii), $L_{\infty} \simeq L'_{\infty}$ since both are positive definite, hence $L_{2} \simeq L'_{2}$ over $\mathbb{Q}_{2}$ by Hilbert reciprocity, hence over $\mathbb{Z}_{2}$ since both are odd and unimodular. Thus $L$ and $L'$ are in the same genus so there is only one genus.

The inequality $h_{p,n} \geq H_{p,n}^{0}$ follows from Theorem 17(a). By Proposition 3, any $L \in G_{p,n}$ is contained in a unimodular lattice $M$; if $n \leq 8$, $M \simeq I_{n}$ by [7, 106:10] and so $h_{p,n} \leq H_{p,n}$ is evident.

COROLLARY 21. When $p$ is odd, the almost unimodular sublattices of determinant $p^{2}$ in $M \simeq I_{n}$ fall in the same genus.

Remark 22. If $H_{p,n}^{0} = H_{p,n}$ with $p$ odd and $n \leq 8$, both are of course equal to the class number $h_{p,n}$. It is easy to see that this happens if and only if the number $|G_{k}\backslash C_{k}^{*}|$ of orbits of extent $k$ is 0 or 1 for all $k \leq n$, e.g., when
p = 3. Also one can see from Table I that \( h_{7,3} = 1, h_{7,4} = 2 \) and \( h_{7,5} = 3 \). The six forms involved here are given explicitly in Example 15.

In order to give a similar result when \( p = 2 \), we give descriptions of five (possible) genera \( G_1, G'_1, G''_1, G_2, G'_2 \) on a quadratic space equivalent to \( I_n \) over \( \mathbb{Q} \). Each of the genera is almost unimodular with determinant \( = 4 \).

\[ G_1: \text{ each lattice in } G_1 \text{ is even and has a Jordan splitting } \]
\[ L_0 \perp L_1 \text{ over } \mathbb{Z}_2 \text{ with } L_1 \simeq \left( \begin{smallmatrix} 0 & 2 \\ 2 & 0 \end{smallmatrix} \right). \]
\[ G'_1: \text{ same as } G_1 \text{ except that } L_1 \simeq \left( \begin{smallmatrix} 1 & 2 \\ 1 & 0 \end{smallmatrix} \right). \]
\[ G''_1: \text{ same as } G_1 \text{ except that } L_1 \simeq \left( \begin{smallmatrix} 1 & 2 \\ 2 & 0 \end{smallmatrix} \right). \]
\[ G_2: \text{ same as } G_1 \text{ except each lattice is odd.} \]
\[ G'_2: \text{ same as } G_2 \text{ except } L_1 \simeq \left( \begin{smallmatrix} 1 & 2 \\ 2 & 0 \end{smallmatrix} \right). \]

**Theorem 23.** The five genera exist in the following dimensions and only in them.

\[ G_1: \quad n \equiv 2 \pmod{4}, \]
\[ G'_1: \quad n \equiv 0 \pmod{8}, \]
\[ G''_1: \quad n \equiv 4 \pmod{8}, \]
\[ G_2: \quad n \geq 3, \]
\[ G'_2: \quad n \geq 5. \]

They are distinct and are uniquely determined by the given conditions.

**The class numbers of** \( G_2 \) **and** \( G'_2 \) **satisfy**

\[ h_2 \geq \left\lceil \frac{(n + 1)}{4} \right\rceil, \quad h'_2 \geq \left\lceil \frac{(n - 1)}{4} \right\rceil, \]

resp; equality holds for \( 3 \leq n \leq 8 \). The class numbers of \( G_1, G'_1 \) and \( G''_1 \) are 1 if \( 2 \leq n \leq 6 \).

**Proof.** Let \( M \simeq I_n \) in the basis \( e_1, \ldots, e_n \). Suppose first that \( n \) is even and let \( L^{(n)} \) be the (indecomposable) lattice corresponding to the isotropic vector in \( M/2M \) of extent \( n \). Then the \( \mathbb{Z}_2 \)-lattice \( L_1 = \mathbb{Z}_2(e_1 + \cdots + e_n) + \mathbb{Z}_2(2e_1) \) is \( \simeq \left( \begin{smallmatrix} n & 2 \\ 2 & n \end{smallmatrix} \right) \), is 2-modular and splits \( L_2^{(n)} = \mathbb{Z}_2 \otimes L^{(n)} \) orthogonally, \( L_2^{(n)} - L_0 \perp L_1 \), since \( L^{(n)} \) consists of all vectors \( \sum a_i e_i \in M \) with \( \sum a_i \equiv 0 \pmod{2} \) — see [7, 82:15]. Note that \( \det L_0 = -1 + n \). By the local square theorem [7, 63:1], \(-1 + n \equiv -1 + n' \pmod{(2^2)} \) iff \( n \equiv n' \in \mathbb{Z}_2 \) (mod 8). It follows that the four binary lattices \( \left( \begin{smallmatrix} n' & 2 \\ 2 & n' \end{smallmatrix} \right) \) with \( n' = 0, 2, 4, 6 \) represent all the possibilities for \( L_1 \) up to isometry [7, 93:16], and they are distinct. Now \( L_0 \) is even, and so if \( n \geq 6 \), it splits off a plane \( P \simeq \left( \begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix} \right) \); if \( n \equiv 6 \pmod{8} \) we add the first basis vector of \( L_1 \) to the first basis vector of \( P \) and, letting \( P' \) be the unimodular plane spanned by this new vector and the second basis vector of \( P \), we obtain a splitting \( P \perp L_1 = P' \perp L'_1 \) and thence a Jordan splitting \( L_2^{(n)} = L'_0 \perp L'_1 \), with \( L'_1 \simeq \left( \begin{smallmatrix} 1 & 2 \\ 2 & 0 \end{smallmatrix} \right) \) by determinants. Thus the genera \( G_1, G'_1 \) and \( G''_1 \) exist in the stated dimensions.
Every even unimodular $\mathbb{Z}_2$-lattice is equivalent to an orthogonal sum of hyperbolic planes $\simeq (0, 1)$ and at most one lattice $\simeq (1, 1)$. Now if $G_1$ exists in dimension $n$, $\det L_0 = 1$ since $\det L_1 = 4$ (see definition of $G_1$), so $L_0$ must be an orthogonal sum of hyperbolic planes, which implies that $n \equiv 2 \pmod{4}$ by determinants. If $G'_1$ exists in dimension $n$, a similar argument shows that $n = 0 \pmod{4}$ and that $L_0$ is a direct sum of hyperbolic planes; a straightforward computation of Hasse symbols (cf. Sections 63B and 73 of [7]) shows that $S_2(G'_1) = -1$ if $n \equiv 4 \pmod{8}$, contradicting $M \simeq I_n$, so $n \equiv 0 \pmod{8}$. Similarly if $G''_1$ exists in dimension $n, n \equiv 4 \pmod{8}$.

Now let $n$ be arbitrary. One can easily check, using Lemma 2, that all 5 genera are distinct and that they are uniquely determined by the given conditions. An almost unimodular but not unimodular sublattice $L$ of $M$ must be of the form $L_{2k} \perp J$ where $J \simeq I_{n-2k}$ and $2k$ is the extent of the vector in $M/2M$ corresponding to $L$. If $n = 2k$ then $L = L_{2k}$ is in $G_1$, $G'_1$ or $G''_1$. Suppose $n > 2k$. If $2k \equiv 0 \pmod{4}$, it is easy to see that $L$ is in $G_2$ or $G'_2$ resp. Suppose $2k \equiv 4 \pmod{8}$. Then there is a binary $\mathbb{Z}_2$-lattice $\mathbb{Z}_2 y_1 + \mathbb{Z}_2 y_2 \simeq (4, 4)$ which splits $L_{2k}$ and a vector $y_3 \in J$ with $f(y_1, y_3) = 1$. It is easy to see that the lattice

$$\mathbb{Z}_2 (y_1 + 2y_3) + \mathbb{Z}_2 y_2 \simeq \begin{pmatrix} 8 & 2 \\ 4 & 4 \end{pmatrix}$$

is 2-modular, splits $L_2$ orthogonally [7, 82:15], and is $\simeq (0, 2)$ [7, 93:11]. Thus $L$ is in $G'_2$ in this case as well. It is easy to see therefore that $G_2$ and $G'_2$ exist in the stated dimensions.

It is evident from the definition that $G_2$ and $G'_2$ can only exist when $n \geq 3$. Suppose that $L \in G'_2$ for $n = 3$ or 4 and let $L = L_0 \perp L_1$ with $L_1 \simeq (0, 2)$. Then $\det L_0 = -1$ so $\mathbb{Q}_2 L_0 \simeq \langle -1 \rangle$ or $\langle 0, 2 \rangle$. But this implies $S_2(L_0) = -1$, which is not true. Thus $G'_2$ exists only when $n \geq 5$.

Consider $G_2$ for a given rank $n$. Then the lattices

$$L^{(2)} \perp I_{n-2}, L^{(6)} \perp I_{n-6}, \ldots, L^{(2k)} \perp I_{n-2k},$$

(9)

where $2k$ is the largest integer $<n$ which is $\equiv 2 \pmod{4}$, are all in $G_2$ and are in distinct classes (since $L^{(2l)}$ is indecomposable for any $l$). Thus $h_2 \geq [(n+1)/4]$. If $L \in G_2$ then $L$ is contained in a unimodular lattice by Proposition 3, and hence in a lattice $\simeq I_n$ if $n \leq 8$; by Theorem 5, $L$ must be equivalent to one of the lattices in (9), so $h_2 = [(n+1)/4]$. The remaining cases can be handled similarly.

**Corollary 24.** The almost unimodular sublattices of determinant 4 of $M \simeq I_n$ fall into a single genus when $n = 2$ or 3, two genera when $n = 4$ or $n$ is odd and $\geq 5$, three genera when $n$ is even and $\geq 6$. 
5. Grothendieck and Witt Groups

Let $G_p$ be the Grothendieck group of almost unimodular forms with respect to a fixed prime $p$. Thus the elements of $G_p$ are formal differences $[L] - [K]$ of equivalence classes of almost unimodular lattices where $L \sim L'$ iff there exists an almost unimodular lattice $J$ such that $L \perp J \sim L' \perp J$. We denote by $[a]$ the equivalence class of the lattice with form $aX^2$, $a = \pm 1$ or $\pm p$.

**Proposition 25.** If $p = 2$ or $p \equiv 3 \pmod{4}$, $G_p$ is generated by the 4 elements $[1], [-1], [p], [-p]$.

**Proof.** Let $[L] \in G_p$. Since $p = 2$ or $p \equiv 3 \pmod{4}$, $L \perp \langle 1, -p \rangle$ has a Jordan splitting by Theorems 25 or 21 of [2]; the proposition then follows from the fact that the Grothendieck group of unimodular forms is generated by $[1]$ and $[-1]$ [8, Theorem 1, p.52].

**Theorem 26.** If $p \equiv 3 \pmod{4}$, $G_p$ is the free Abelian group on $[1], [-1], [p], [-p]$ modulo the relationship $2([1] - [-1] - [p] + [-p]) = 0$. There is an isomorphism

$$G_p \rightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}^3$$

given by the direct product of the following four mappings:

(i) $G_p \rightarrow \mathbb{Z}/2\mathbb{Z}$ given by sending $[L]$ to the determinant of a unimodular Jordan component of $L_p$.

(ii) $G_p \rightarrow \mathbb{Z}$ given by the rank of a maximal negative definite subspace of $L_\infty$.

(iii) the ranks of a unimodular and a $p$-modular Jordan component of $L_p$.

**Proof.** It is clear by the local integral classification theory [7, 61:1, 91:9 and 92:2] that the maps are well defined. The images of $[1], [-1], [p], [-p]$ under the product map $\pi$ are, respectively, $(0, 0, 1, 0)$, $(1, 1, 1, 0)$, $(0, 0, 0, 1)$, and $(0, 1, 0, 1)$ so it is easy to check that $\pi$ is surjective. Suppose $\sum a_i[i] \in \ker \pi$. Clearly $a_{-1} \in 2\mathbb{Z}$. Therefore since $(0, 1, 0) - (1, 1, 0) - (0, 0, 1) + (1, 0, 1) = 0$ is, up to a scalar, the unique linear relationship among these four vectors in $\mathbb{Z}^3$, $\sum a_i[i] \in \ker \pi$ iff $(a_{-1}, a_1, a_p, a_{-p})$ is an integral multiple of $(2, -2, -2, 2)$. Now the integral forms $\langle 1, 1, -p, -p \rangle$ and $\langle -1, -1, p, p \rangle$ are in the same genus by local equivalence theory, hence in the same class [5, Satz 5], so $2([1] - [-1] - [p] + [-p]) = 0$ in $G_p$. The theorem follows easily.
THEOREM 27. If \( p = 2 \), \( G_p \) is the free Abelian group on \([1], [-1], [2], [-2] \) modulo the relationship \([1] - [-1] - [2] + [-2] = 0\). There is an isomorphism

\[ G_2 \to \mathbb{Z}^3 \]
given by the product of the three mappings defined in (ii) and (iii) of Theorem 26.

Proof. As in Theorem 26, one determines the image of the four generators under the product map \( \pi \); this shows that \( \pi \) is onto and that \( \sum a_i[i] \in \ker \pi \) iff \((a_1, a_{-1}, a_2, a_{-2})\) is a multiple of \((1, -1, -1, 1)\). But \( (1, 1, -2) \geq (1, -1, 2) \) since it is true locally at each prime \( q \neq 2 \), hence over \( \mathbb{Q}_2 \) by Hilbert reciprocity, hence over \( \mathbb{Z}_2 \) (Lemma 2), hence over \( \mathbb{Z} \) \([5, \text{ Satz 5}]\). Thus \([1] + [-2] = [-1] + [2] \) so \( \pi \) is an isomorphism.

PROPOSITION 28. Let \( p \equiv 1 \pmod{4} \).

(a) There is an odd binary positive definite lattice of determinant \( p \) which does not represent \( 1 \) over \( \mathbb{Z}_p \).

(b) If \( K \) is any such lattice,

\[ K \perp K \perp (-1) \simeq (1, 1, -1, p, p) \]

and \( G_p \) is generated by \([K], \langle 1 \rangle, (-1), \langle p \rangle\).

Proof. Let \( \Delta \) be a non-square unit in \( \mathbb{Z}_p \) and define the \( \mathbb{Z}_p \)-lattice \( J_p = \langle \Delta, \Delta p \rangle \). Similarly define \( J_q = \langle -1, -p \rangle \) and, for \( q \neq p \) or 2, \( J_q = \langle 1, p \rangle \).

Using the rules for the Hasse symbols \( S_q \) given in Sections 63B and 73 in \([7]\), one can easily check that \( \prod_q S_q(J_q) = 1 \) and so there is a binary space \( V \) over \( \mathbb{Q} \) each of whose completions \( V_q \) contains a lattice \( M_q \simeq J_q \) (see \([7, \text{ 72.1}]\)). It is easy to see that \( V_p \) does not represent \( 1 \), so neither does \( V \). We can choose a basis \( u, v \) of \( V \) with respect to which \( V \simeq \langle \delta, \delta p \rangle \) with \( \delta \) a \( \mathbb{Z}_p \)-unit in \( \mathbb{Z} \). Put \( \delta = (z u + z v) \) and define \( K \) to be the lattice on \( V \) with \( K_u = M_u \) if \( q \) divides \( \delta \), otherwise \( K_u = M_u \). It is easy to see that \( K \) is odd with determinant \( p \), hence almost unimodular.

We now consider (b). The relationship (10) holds at \( \infty \), and also over \( \mathbb{Z}_q \), \( q \neq p \) or 2, since both sides have determinant \( -p^2 \). Since \( \langle K_p \rangle \simeq \langle \Delta, \Delta p \rangle \) and \( \langle \Delta, \Delta \rangle \simeq \langle 1, 1 \rangle \), (10) also holds over \( \mathbb{Z}_p \), hence over \( \mathbb{Q}_2 \) by Hilbert reciprocity, hence over \( \mathbb{Z}_2 \) since both sides are odd and unimodular there. Thus both sides are in the same genus; but the class number is 1 in this case (see \([5, \text{ Satz 5}]\) so (10) holds over \( \mathbb{Z} \).

Let \( L \) be any almost unimodular lattice. Since a \( p \)-modular Jordan component of \( K_p \) is \( \simeq \langle \Delta p \rangle \), one of \( L \perp \langle 1 \rangle \perp \langle p \rangle \) and \( L \perp \langle -1 \rangle \perp K \) has a \( p \)-modular \( \mathbb{Z}_p \)-Jordan component with determinant = a power of \( p \), and so
also has a Jordan splitting over \( \mathbb{Z} \) by Theorem 21 of [2]. Thus, as in Proposition 25, \( G_p \) is generated by \([K], [1], [-1], [p] \) and \([-p] \). But \([-p] \), e.g., can be omitted since

\[
\langle 1, -1, p \rangle \simeq \langle 1, 1, -p \rangle
\]

over \( \mathbb{Z} \) by the same method used to prove (10).

**Theorem 29.** If \( p \equiv 1 \) (mod 4), \( G_p \) is the free Abelian group on \([K], [1], [-1], [p] \) modulo the relationship \( 2([K] - [1] - [p]) = 0 \). The mapping

\[
G_p \rightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}^3
\]

defined in Theorem 26 is an isomorphism.

The proof is entirely similar to that of Theorem 26, taking into account the relationship \( 2[K] = 2[1] + 2[p] \) implied by (10).

We now define the Witt group \( W_p \) to be the factor group \( G_p \) modulo the subgroup \( H_p \) generated by the binary isotropic forms. Such forms are either unimodular or \( p \)-modular (since the determinant cannot be \( \pm p \)). If \( a \in \mathbb{Z} \), then \( \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \) \( \langle 1 \rangle \simeq \langle 1, -1, 1 \rangle \) so a binary isotropic (almost unimodular) lattice is \([1] + [-1] \) or \([p] + [-p] \) in \( G_p \). Therefore we may view \( G_p \) as \( \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}^3 \) (\( p \) odd) or \( \mathbb{Z}^3 \) (\( p = 2 \)) and \( H_p \) as the subgroup \( \mathbb{Z}(1, 1, 2, 0) + \mathbb{Z}(0, 1, 0, 2) \) when \( p \equiv 3 \) (mod 4), \( \mathbb{Z}(0, 1, 2, 0) + \mathbb{Z}(0, 1, 0, 2) \) when \( p \equiv 1 \) (mod 4), \( \mathbb{Z}(1, 2, 0) + \mathbb{Z}(1, 0, 2) \) when \( p = 2 \). An application of elementary divisor theory yields:

**Theorem 30.**

\[
W_p \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}, \quad p \equiv 3 \) (mod 4),
\]
\[
\simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}, \quad p \equiv 1 \) (mod 4),
\]
\[
\simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}, \quad p = 2.
\]

The “reduced Witt group” \( W^0_p \) defined to be \( W_p \) modulo the subgroup generated by the unimodular forms, i.e., modulo \( \mathbb{Z}[1] + \mathbb{Z}[-1] \), is of interest in topology. By the same technique as above, one easily shows that

\[
W^0_p \simeq \mathbb{Z}/4\mathbb{Z}, \quad p \equiv 3 \) (mod 4),
\]
\[
\simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \quad p = 1 \) (mod 4),
\]
\[
\simeq \mathbb{Z}/2\mathbb{Z}, \quad p = 2.
\]

Furthermore by tracing through this isomorphism explicitly and applying Proposition 3, one can show that a lattice \( L \) is 0 in \( W^0_p \) iff it is contained in a
unimodular lattice of the same rank. Thus the forms which arise in topology are $0$ in $W^0$.

ACKNOWLEDGMENTS

I would like to thank my colleagues, J. Csima, T. M. K. Davison, and A. Rosa, for helpful comments.

REFERENCES