Positive binary forms representing the same arithmetic progressions

Byeong-Kweon Oh (SNU)

International Conference on the Algebraic and Arithmetic Theory of Quadratic Forms, Puerto Natales, Patagonia, Chile

Abstract

In 1938, Delone proved that $(x^2 + 3y^2, x^2 + xy + y^2)$ is the unique pair of non-isometric positive definite integral binary forms representing same integers. In this talk, we find all pairs of positive definite binary integral forms representing same integers in the set $A_{p,k} = \{pn + k : n \geq 0\}$ for any prime p and any non-negative integer k less than p.

Some notations

Some notations

- Let $f(x, y) = [a, b, c] = ax^2 + bxy + cy^2$ be a (positive definite integral) binary quadratic form with discriminant $d_f := b^2 - 4ac < 0$. We always assume that f is primitive, that is, $(a, b, c) = 1$.

Some notations

- Let $f(x, y) = [a, b, c] = ax^2 + bxy + cy^2$ be a (positive definite integral) binary quadratic form with discriminant $d_f := b^2 - 4ac < 0$. We always assume that f is primitive, that is, $(a, b, c) = 1$.
- The binary $\mathbb{Z}$-lattice corresponding to f is denoted by $L_f = \mathbb{Z}x + \mathbb{Z}y$. It satisfies $[Q(x), 2B(x, y), Q(y)] = [a, b, c]$. We always assume that the norm ideal of any binary lattice is $\mathbb{Z}$.

Some notations

- Let $f(x, y) = [a, b, c] = ax^2 + bxy + cy^2$ be a (positive definite integral) binary quadratic form with discriminant $d_f := b^2 - 4ac < 0$. We always assume that f is primitive, that is, $(a, b, c) = 1$.
- The binary $\mathbb{Z}$-lattice corresponding to f is denoted by $L_f = \mathbb{Z}x + \mathbb{Z}y$. It satisfies $[Q(x), 2B(x, y), Q(y)] = [a, b, c]$. We always assume that the norm ideal of any binary lattice is $\mathbb{Z}$.
- For two binary forms f and g, f is (properly) equivalent to g if there is a $T = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in GL_2(\mathbb{Z})$ $(SL_2(\mathbb{Z})$, respectively) such that $f(rx + sy, tx + uy) = g(x, y)$.

Some notations

- Let $f(x, y) = [a, b, c] = ax^2 + bxy + cy^2$ be a (positive definite integral) binary quadratic form with discriminant $d_f := b^2 - 4ac < 0$. We always assume that f is primitive, that is, $(a, b, c) = 1$.
- The binary $\mathbb{Z}$-lattice corresponding to f is denoted by $L_f = \mathbb{Z}x + \mathbb{Z}y$. It satisfies $[Q(x), 2B(x, y), Q(y)] = [a, b, c]$. We always assume that the norm ideal of any binary lattice is $\mathbb{Z}$.
- For two binary forms f and g, f is (properly) equivalent to g if there is a $T = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in GL_2(\mathbb{Z})$ $(SL_2(\mathbb{Z})$, respectively) such that $f(rx + sy, tx + uy) = g(x, y)$.
- If f is (properly) equivalent to g, then we write $f \sim g$ ($f \simeq g$, respectively).

Composition law

Composition law

- Let $\mathfrak{S}_d$ be the set of all proper equivalence classes of primitive binary forms with discriminant d. $h(d) = |\mathfrak{S}_d|$.

Composition law

- Let $\mathfrak{S}_d$ be the set of all proper equivalence classes of primitive binary forms with discriminant d. $h(d) = |\mathfrak{S}_d|$.
- For two classes $\mathfrak{C}_1, \mathfrak{C}_2 \in \mathfrak{S}_d$, there are $[a_1, b, c_1] \in \mathfrak{C}_1$ and $[a_2, b, c_2] \in \mathfrak{C}_2$ such that $(a_1, a_2) = 1$.

Composition law

- Let $\mathfrak{S}_d$ be the set of all proper equivalence classes of primitive binary forms with discriminant d. $h(d) = |\mathfrak{S}_d|$.
- For two classes $\mathfrak{C}_1, \mathfrak{C}_2 \in \mathfrak{S}_d$, there are $[a_1, b, c_1] \in \mathfrak{C}_1$ and $[a_2, b, c_2] \in \mathfrak{C}_2$ such that $(a_1, a_2) = 1$.
- The composition $\mathfrak{C}_1 \cdot \mathfrak{C}_2$ is the class in $\mathfrak{S}_d$ containing $[a_1 a_2, b, *]$.

Composition law

- Let $\mathfrak{S}_d$ be the set of all proper equivalence classes of primitive binary forms with discriminant d. $h(d) = |\mathfrak{S}_d|$.
- For two classes $\mathfrak{C}_1, \mathfrak{C}_2 \in \mathfrak{S}_d$, there are $[a_1, b, c_1] \in \mathfrak{C}_1$ and $[a_2, b, c_2] \in \mathfrak{C}_2$ such that $(a_1, a_2) = 1$.
- The composition $\mathfrak{C}_1 \cdot \mathfrak{C}_2$ is the class in $\mathfrak{S}_d$ containing $[a_1 a_2, b, *]$.
- Under this composition law, $\mathfrak{S}_d$ forms an finite abelian group.

Composition law

- Let $\mathfrak{S}_d$ be the set of all proper equivalence classes of primitive binary forms with discriminant d. $h(d) = |\mathfrak{S}_d|$.
- For two classes $\mathfrak{C}_1, \mathfrak{C}_2 \in \mathfrak{S}_d$, there are $[a_1, b, c_1] \in \mathfrak{C}_1$ and $[a_2, b, c_2] \in \mathfrak{C}_2$ such that $(a_1, a_2) = 1$.
- The composition $\mathfrak{C}_1 \cdot \mathfrak{C}_2$ is the class in $\mathfrak{S}_d$ containing $[a_1 a_2, b, *]$.
- Under this composition law, $\mathfrak{S}_d$ forms an finite abelian group.
- The identity class $\mathfrak{I}_d$ is the class containing a form representing 1.

Composition law

- Let $\mathfrak{S}_d$ be the set of all proper equivalence classes of primitive binary forms with discriminant d. $h(d) = |\mathfrak{S}_d|$.
- For two classes $\mathfrak{C}_1, \mathfrak{C}_2 \in \mathfrak{S}_d$, there are $[a_1, b, c_1] \in \mathfrak{C}_1$ and $[a_2, b, c_2] \in \mathfrak{C}_2$ such that $(a_1, a_2) = 1$.
- The composition $\mathfrak{C}_1 \cdot \mathfrak{C}_2$ is the class in $\mathfrak{S}_d$ containing $[a_1 a_2, b, *]$.
- Under this composition law, $\mathfrak{S}_d$ forms an finite abelian group.
- The identity class $\mathfrak{I}_d$ is the class containing a form representing 1.
- A class $\mathfrak{C}$ is called an ambiguous class if $\mathfrak{C}^{-1} = \mathfrak{C}$.

Composition law

- Let $\mathfrak{S}_d$ be the set of all proper equivalence classes of primitive binary forms with discriminant d. $h(d) = |\mathfrak{S}_d|$.
- For two classes $\mathfrak{C}_1, \mathfrak{C}_2 \in \mathfrak{S}_d$, there are $[a_1, b, c_1] \in \mathfrak{C}_1$ and $[a_2, b, c_2] \in \mathfrak{C}_2$ such that $(a_1, a_2) = 1$.
- The composition $\mathfrak{C}_1 \cdot \mathfrak{C}_2$ is the class in $\mathfrak{S}_d$ containing $[a_1 a_2, b, *]$.
- Under this composition law, $\mathfrak{S}_d$ forms an finite abelian group.
- The identity class $\mathfrak{I}_d$ is the class containing a form representing 1.
- A class $\mathfrak{C}$ is called an ambiguous class if $\mathfrak{C}^{-1} = \mathfrak{C}$.
- For binary forms $f_1 \in \mathfrak{C}_1$ and $f_2 \in \mathfrak{C}_2$, $f_1 \cdot f_2$ denotes a form in the class $\mathfrak{C}_1 \cdot \mathfrak{C}_2$.

Some notations

Some notations

- The isometry group $O(f)$ of f is defined by

$$O(f) = \left\{ \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in GL_2(\mathbb{Z}) : f(rx+sy, tx+uy) = f(x,y) \right\}.$$

Some notations

- The isometry group $O(f)$ of f is defined by

$$O(f) = \left\{ \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in GL_2(\mathbb{Z}) : f(rx + sy, tx + uy) = f(x, y) \right\}.$$

- The proper isometry group of f is denoted by $O^+(f)$.

Some notations

- The isometry group $O(f)$ of f is defined by

$$O(f) = \left\{ \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in GL_2(\mathbb{Z}) : f(rx + sy, tx + uy) = f(x, y) \right\}.$$

- The proper isometry group of f is denoted by $O^+(f)$.
- Note that $o^+(f) := |O^+(f)| = 2$ unless $d_f \neq -3, -4$. In the exceptional cases, $o^+([1,1,1]) = 6$ and $o^+([1,0,1]) = 4$.

Some notations

- The isometry group $O(f)$ of f is defined by

$$O(f) = \left\{ \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in GL_2(\mathbb{Z}) : f(rx + sy, tx + uy) = f(x, y) \right\}.$$

- The proper isometry group of f is denoted by $O^+(f)$.
- Note that $o^+(f) := |O^+(f)| = 2$ unless $d_f \neq -3, -4$. In the exceptional cases, $o^+([1, 1, 1]) = 6$ and $o^+([1, 0, 1]) = 4$.
- We define

$$R(a, f) = \{(x, y) \in \mathbb{Z}^2 : f(x, y) = a\}.$$

Some notations

- The isometry group $O(f)$ of f is defined by

$$O(f) = \left\{ \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in GL_2(\mathbb{Z}) : f(rx+sy, tx+uy) = f(x,y) \right\}.$$

- The proper isometry group of f is denoted by $O^+(f)$.
- Note that $o^+(f) := |O^+(f)| = 2$ unless $d_f \neq -3, -4$. In the exceptional cases, $o^+([1,1,1]) = 6$ and $o^+([1,0,1]) = 4$.
- We define

$$R(a,f) = \{(x,y) \in \mathbb{Z}^2 : f(x,y) = a\}.$$

- Note that $R(a,f)$ is a finite set. We define $r(a,f) = |R(a,f)|$.

Some notations

- The isometry group $O(f)$ of f is defined by

$$O(f) = \left\{ \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in GL_2(\mathbb{Z}) : f(rx + sy, tx + uy) = f(x, y) \right\}.$$

- The proper isometry group of f is denoted by $O^+(f)$.
- Note that $o^+(f) := |O^+(f)| = 2$ unless $d_f \neq -3, -4$. In the exceptional cases, $o^+([1, 1, 1]) = 6$ and $o^+([1, 0, 1]) = 4$.
- We define

$$R(a, f) = \{(x, y) \in \mathbb{Z}^2 : f(x, y) = a\}.$$

- Note that $R(a, f)$ is a finite set. We define $r(a, f) = |R(a, f)|$.
- $Q(f) = \{a \in \mathbb{Z} : r(a, f) \neq 0\}$.

Some notations

- The isometry group $O(f)$ of f is defined by

$$O(f) = \left\{ \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in GL_2(\mathbb{Z}) : f(rx + sy, tx + uy) = f(x, y) \right\}.$$

- The proper isometry group of f is denoted by $O^+(f)$.
- Note that $o^+(f) := |O^+(f)| = 2$ unless $d_f \neq -3, -4$. In the exceptional cases, $o^+([1,1,1]) = 6$ and $o^+([1,0,1]) = 4$.
- We define

$$R(a, f) = \{(x, y) \in \mathbb{Z}^2 : f(x, y) = a\}.$$

- Note that $R(a, f)$ is a finite set. We define $r(a, f) = |R(a, f)|$.
- $Q(f) = \{a \in \mathbb{Z} : r(a, f) \neq 0\}$.
- For a binary lattice L, $R(a, L)$ and $Q(L)$ are similarly defined .

Some known results

Some known results

- For any positive integer k with $(k, d) = 1$,

$$\sum_{\mathfrak{C} \in \mathfrak{S}_d} r(k, \mathfrak{C}) = w_d \sum_{n|k} \left(\frac{d}{n}\right),$$

where $(\cdot)$ is the Kronecker's symbol and $w_{-3} = 6, w_{-4} = 4$, otherwise $w_d = 2$.

Some known results

- For any positive integer k with $(k, d) = 1$,

$$\sum_{\mathfrak{C} \in \mathfrak{S}_d} r(k, \mathfrak{C}) = w_d \sum_{n|k} \left(\frac{d}{n} \right),$$

  where $(\cdot)$ is the Kronecker's symbol and $w_{-3} = 6, w_{-4} = 4$, otherwise $w_d = 2$.
- If $h(d) = 1$, then we can explicitly compute the number $r(k, f)$ for the binary form f with $d_f = d$.

Some known results

- For any positive integer k with $(k, d) = 1$,

$$\sum_{\mathfrak{C} \in \mathfrak{S}_d} r(k, \mathfrak{C}) = w_d \sum_{n|k} \left(\frac{d}{n}\right),$$

  where $(\cdot)$ is the Kronecker's symbol and $w_{-3} = 6, w_{-4} = 4$, otherwise $w_d = 2$.
- If $h(d) = 1$, then we can explicitly compute the number $r(k, f)$ for the binary form f with $d_f = d$.
- $h(d) = 1$ if and only if $d = -3, -4, -8, -11, -19, -43, -67, -163, -12, -16, -28, -27$.

Some remarks

Some remarks

- $f \sim g$ if and only if $L_f \simeq L_g$ if and only if $f \simeq g$ or $f \simeq g^{-1}$.

Some remarks

- $f \sim g$ if and only if $L_f \simeq L_g$ if and only if $f \simeq g$ or $f \simeq g^{-1}$.
- For a binary lattice L, the corresponding binary form f_L is well defined only up to equivalence.

Some remarks

- $f \sim g$ if and only if $L_f \simeq L_g$ if and only if $f \simeq g$ or $f \simeq g^{-1}$.
- For a binary lattice L, the corresponding binary form f_L is well defined only up to equivalence.
- For two binary lattices L and M, $f_L \cdot f_M$ is NOT defined.

Some remarks

- $f \sim g$ if and only if $L_f \simeq L_g$ if and only if $f \simeq g$ or $f \simeq g^{-1}$.
- For a binary lattice L, the corresponding binary form f_L is well defined only up to equivalence.
- For two binary lattices L and M, $f_L \cdot f_M$ is NOT defined.
- If either f_L or f_M is contained in an ambiguous class, then $f_L \cdot f_M$ is well defined up to equivalence.

Some remarks

- $f \sim g$ if and only if $L_f \simeq L_g$ if and only if $f \simeq g$ or $f \simeq g^{-1}$.
- For a binary lattice L, the corresponding binary form f_L is well defined only up to equivalence.
- For two binary lattices L and M, $f_L \cdot f_M$ is NOT defined.
- If either f_L or f_M is contained in an ambiguous class, then $f_L \cdot f_M$ is well defined up to equivalence.
- $r(a, f_L \cdot f_M) + r(a, f_L \cdot f_M^{-1})$ is independent of the choices of proper equivalences. Hence it is well defined.

Some remarks

- $f \sim g$ if and only if $L_f \simeq L_g$ if and only if $f \simeq g$ or $f \simeq g^{-1}$.
- For a binary lattice L, the corresponding binary form f_L is well defined only up to equivalence.
- For two binary lattices L and M, $f_L \cdot f_M$ is NOT defined.
- If either f_L or f_M is contained in an ambiguous class, then $f_L \cdot f_M$ is well defined up to equivalence.
- $r(a, f_L \cdot f_M) + r(a, f_L \cdot f_M^{-1})$ is independent of the choices of proper equivalences. Hence it is well defined.
- For a class $\mathfrak{C} \in \mathfrak{S}_d$ and a prime p, if $r(p, \mathfrak{C}) \neq 0$, then $r(p, \mathfrak{D}) = 0$ for any $\mathfrak{D} \in \mathfrak{S}_d - \{\mathfrak{C}, \mathfrak{C}^{-1}\}$.

Watson transformations

Watson transformations

- For any prime p, the Watson transformation $\Lambda_p(L)$ of a lattice L is defined by

$$\Lambda_p(L) = \{x \in L : Q(x+z) \equiv Q(x) \pmod{p}\ \forall z \in L\}.$$

Watson transformations

- For any prime p, the Watson transformation $\Lambda_p(L)$ of a lattice L is defined by

$$\Lambda_p(L) = \{x \in L : Q(x+z) \equiv Q(x) \pmod{p} \ \forall z \in L\}.$$

- Define $\mathbb{H} = [0, 1, 0]$.

Watson transformations

- For any prime p, the Watson transformation $\Lambda_p(L)$ of a lattice L is defined by

$$\Lambda_p(L) = \{x \in L : Q(x+z) \equiv Q(x) \pmod{p} \ \forall z \in L\}.$$

- Define $\mathbb{H} = [0, 1, 0]$.
- Note that

$$L_p = L \otimes \mathbb{Z}_p \not\cong \mathbb{H} \quad \text{if and only if} \quad Q(L) \cap p\mathbb{Z} = Q(\Lambda_p(L)).$$

Problem

Problem

- We write $(L, M) \simeq (L', M')$ if $L \simeq L', M \simeq M'$ or $L \simeq M', M \simeq L'$

Problem

- We write $(L, M) \simeq (L', M')$ if $L \simeq L'$, $M \simeq M'$ or $L \simeq M'$, $M \simeq L'$
- (Delone, Watson) $Q(L) = Q(M)$ if and only if $L \simeq M$ or $(L, M) \simeq ([1, 0, 3], [1, 1, 1])$.

Problem

- We write $(L, M) \simeq (L', M')$ if $L \simeq L', M \simeq M'$ or $L \simeq M', M \simeq L'$
- (Delone, Watson) $Q(L) = Q(M)$ if and only if $L \simeq M$ or $(L, M) \simeq ([1, 0, 3], [1, 1, 1])$.
- For a prime p and an integer k $(0 \leq k \leq p-1)$, define $A_{p,k} = \{pn + k : n \in \mathbb{Z}^+ \cup \{0\}\}$.

Problem

- We write $(L, M) \simeq (L', M')$ if $L \simeq L', M \simeq M'$ or $L \simeq M', M \simeq L'$
- (Delone, Watson) $Q(L) = Q(M)$ if and only if $L \simeq M$ or $(L, M) \simeq ([1, 0, 3], [1, 1, 1])$.
- For a prime p and an integer k $(0 \leq k \leq p - 1)$, define $A_{p,k} = \{pn + k : n \in \mathbb{Z}^+ \cup \{0\}\}$.
- (Problem) Find all non-isometric pairs (L, M) of binary lattices such that

$$Q(L) \cap A_{p,k} = Q(M) \cap A_{p,k} \neq \emptyset.$$

Remarks

Remarks

- In the representation point of view, it is convenient to consider "lattices" rather than "forms". However if we use the group structure, we have to consider the proper equivalence classes.

Remarks

- In the representation point of view, it is convenient to consider "lattices" rather than "forms". However if we use the group structure, we have to consider the proper equivalence classes.
- There is NO composition law between equivalences classes of lattices.

Remarks

- In the representation point of view, it is convenient to consider "lattices" rather than "forms". However if we use the group structure, we have to consider the proper equivalence classes.
- There is NO composition law between equivalences classes of lattices.
- Let p be an odd prime and a be any integer such that $-a$ is a quadratic non-residue modulo p.

Remarks

- In the representation point of view, it is convenient to consider "lattices" rather than "forms". However if we use the group structure, we have to consider the proper equivalence classes.
- There is NO composition law between equivalences classes of lattices.
- Let p be an odd prime and a be any integer such that $-a$ is a quadratic non-residue modulo p.
- If $L = [1, 0, a]$ and $M = [1, 0, p^2a]$, then

$$Q(L) \cap p\mathbb{Z} = Q(M) \cap p\mathbb{Z} = Q(p^2x^2 + ap^2y^2).$$

Remarks

- In the representation point of view, it is convenient to consider "lattices" rather than "forms". However if we use the group structure, we have to consider the proper equivalence classes.
- There is NO composition law between equivalences classes of lattices.
- Let p be an odd prime and a be any integer such that $-a$ is a quadratic non-residue modulo p.
- If $L = [1, 0, a]$ and $M = [1, 0, p^2 a]$, then

$$Q(L) \cap p\mathbb{Z} = Q(M) \cap p\mathbb{Z} = Q(p^2x^2 + ap^2y^2).$$

- Therefore there are infinitely many such pairs if $k = 0$.

Useful Lemmas

Useful Lemmas

- (Weber) For any (primitive) binary lattice L, there are infinitely many primes that are represented by L.

Useful Lemmas

- (Weber) For any (primitive) binary lattice L, there are infinitely many primes that are represented by L.
- (Meyer) For any binary lattice L, L represents infinitely many primes in the set $A_{n,k}$ if $Q(L) \cap A_{n,k} \neq \emptyset$.

Useful Lemmas

- (Weber) For any (primitive) binary lattice L, there are infinitely many primes that are represented by L.
- (Meyer) For any binary lattice L, L represents infinitely many primes in the set $A_{n,k}$ if $Q(L) \cap A_{n,k} \neq \emptyset$.
- (Pall's Lemma) Assume that $L_p \simeq \mathbb{H}$. Let T be the binary lattice such that $r(p, T) > 0$ and $d_T = d_L$. For any integer n,

$$r(pn, L) = r(n, f_L \cdot f_T) + r(n, f_L \cdot f_T^{-1}) - r\left(\frac{n}{p}, L\right).$$

Example

Example

- Note that $\mathfrak{C}_{-108} = \{[1, 0, 27], [4, 2, 7], [4, -2, 7]\}$.

Example

- Note that $\mathfrak{C}_{-108} = \{[1,0,27],[4,2,7],[4,-2,7]\}$.
- Let $n = 2^a 3^b k$ with $(k,6) = 1$.

Example

- Note that $\mathfrak{C}_{-108} = \{[1,0,27],[4,2,7],[4,-2,7]\}$.
- Let $n = 2^a 3^b k$ with $(k,6) = 1$.
- If $a > 0$ or $b > 0$, then

$$r(n, x^2 + 27y^2) = \omega \sum_{m|k} \left(\frac{-3}{m}\right),$$

where

$$\omega = \begin{cases} 2 & \text{if } a = 0 \text{ and } b \geq 2 \text{ or } a \geq 2 \text{ and } b = 0, \\ 6 & \text{if } a \text{ is positive even integer and } b \geq 2, \\ 0 & \text{otherwise.} \end{cases}$$

Example

Example

- Assume that $(n, 6) = 1$.

Example

- Assume that $(n, 6) = 1$.
- If we define

$$P = \{p : p \equiv 1 \pmod 3, 2 \text{ is a cubic residue modulo } p\},$$

then $r(p, [1, 0, 27]) > 0$ if and only if $p \in P$.

Example

- Assume that $(n, 6) = 1$.
- If we define

$$P = \{p : p \equiv 1 \pmod 3, 2 \text{ is a cubic residue modulo } p\},$$

  then $r(p, [1, 0, 27]) > 0$ if and only if $p \in P$.
- Let Q be the set of primes that are congruent to 1 modulo 3 and are not represented by $[1, 0, 27]$.

Example

- Assume that $(n, 6) = 1$.
- If we define

$$P = \{p : p \equiv 1 \pmod 3, 2 \text{ is a cubic residue modulo } p\},$$

then $r(p, [1, 0, 27]) > 0$ if and only if $p \in P$.

- Let Q be the set of primes that are congruent to 1 modulo 3 and are not represented by $[1, 0, 27]$.
- Let

$$n = \prod_{i=1}^{r} p_i^{e_i} \prod_{j=1}^{s} q_j^{f_j} \prod_{k=1}^{t} r_k^{g_k},$$

where $p_i \in P$ and $q_j \in Q$ and $r_k \equiv 2 \pmod 3$.

Example

- Assume that $(n, 6) = 1$.
- If we define

$$P = \{p : p \equiv 1 \pmod 3, 2 \text{ is a cubic residue modulo } p\},$$

  then $r(p, [1, 0, 27]) > 0$ if and only if $p \in P$.
- Let Q be the set of primes that are congruent to 1 modulo 3 and are not represented by $[1, 0, 27]$.
- Let

$$n = \prod_{i=1}^{r} p_i^{e_i} \prod_{j=1}^{s} q_j^{f_j} \prod_{k=1}^{t} r_k^{g_k},$$

  where $p_i \in P$ and $q_j \in Q$ and $r_k \equiv 2 \pmod 3$.
- If g_k is odd for some k, then $r(n, [1, 0, 27]) = 0$.

Example

Example

- Assume that g_k is even for any k.

Example

- Assume that g_k is even for any k.
- Then we have

$$r(n, x^2 + 27y^2) = \frac{2}{3} \prod_{i=1}^{r} (e_i + 1) \prod_{j=1}^{s} ((f_j + 1) + \epsilon),$$

where

$$\epsilon = \begin{cases} 0 & \text{if } \prod_{j=1}^{s} (f_j + 1) \equiv 0 \pmod 3, \\ 2 & \text{if } \prod_{j=1}^{s} (f_j + 1) \equiv 1 \pmod 3, \\ -2 & \text{otherwise.} \end{cases}$$

Sublattices with index p

Sublattices with index p

- Let $L = \mathbb{Z}x + \mathbb{Z}y$ be a binary lattice.

Sublattices with index p

- Let $L = \mathbb{Z}x + \mathbb{Z}y$ be a binary lattice.
- The set of sublattices of L with index p is denoted by $\Gamma_p(L)$.

Sublattices with index p

- Let $L = \mathbb{Z}x + \mathbb{Z}y$ be a binary lattice.
- The set of sublattices of L with index p is denoted by $\Gamma_p(L)$.
- Every lattice in $\Gamma_p(L)$ is of the form

$$L_{-1} := \mathbb{Z}(px) + \mathbb{Z}y \quad \text{and} \quad L_u := \mathbb{Z}(x + uy) + \mathbb{Z}(py),$$

where $0 \leq u \leq p - 1$.

Sublattices with index p

- Let $L = \mathbb{Z}x + \mathbb{Z}y$ be a binary lattice.
- The set of sublattices of L with index p is denoted by $\Gamma_p(L)$.
- Every lattice in $\Gamma_p(L)$ is of the form

$$L_{-1} := \mathbb{Z}(px) + \mathbb{Z}y \quad \text{and} \quad L_u := \mathbb{Z}(x + uy) + \mathbb{Z}(py),$$

  where $0 \leq u \leq p - 1$.
- Assume that p is odd.

Sublattices with index p

Sublattices with index p

- If L_p is isotropic unimodular, then each lattice in $\Gamma_p(L)$ is locally isometric to

$$\langle 1, -p^2 \rangle \left(\frac{p-1}{2}\right), \quad \langle \Delta_p, -\Delta_p p^2 \rangle \left(\frac{p-1}{2}\right) \text{ or } \langle p, -p \rangle \ (2).$$

Sublattices with index p

- If L_p is isotropic unimodular, then each lattice in $\Gamma_p(L)$ is locally isometric to

$$\langle 1, -p^2 \rangle \left(\frac{p-1}{2} \right), \quad \langle \Delta_p, -\Delta_p p^2 \rangle \left(\frac{p-1}{2} \right) \quad \text{or} \quad \langle p, -p \rangle \ (2).$$

- If L_p is anisotropic unimodular, then each lattice in $\Gamma_p(L)$ is locally isometric to

$$\langle 1, -\Delta_p p^2 \rangle \left(\frac{p+1}{2} \right) \quad \text{or} \quad \langle \Delta_p, -p^2 \rangle \left(\frac{p+1}{2} \right).$$

Sublattices with index p

- If L_p is isotropic unimodular, then each lattice in $\Gamma_p(L)$ is locally isometric to

$$\langle 1, -p^2 \rangle \left(\frac{p-1}{2}\right), \quad \langle \Delta_p, -\Delta_p p^2 \rangle \left(\frac{p-1}{2}\right) \quad \text{or} \quad \langle p, -p \rangle \ (2).$$

- If L_p is anisotropic unimodular, then each lattice in $\Gamma_p(L)$ is locally isometric to

$$\langle 1, -\Delta_p p^2 \rangle \left(\frac{p+1}{2}\right) \quad \text{or} \quad \langle \Delta_p, -p^2 \rangle \left(\frac{p+1}{2}\right).$$

- If $L_p = \langle \epsilon_1, \epsilon_2 p^t \rangle$ is not unimodular, then each lattice in $\Gamma_p(L)$ is locally isometric to

$$\langle \epsilon_1, \epsilon_2 p^{t+2} \rangle \ (p) \quad \text{or} \quad \langle \epsilon_1 p^2, \epsilon_2 p^t \rangle \ (1).$$

Sublattices with index p

Sublattices with index p

- For any binary lattice K with $p \mid d_K$, $u_p(K) := \left(\frac{a}{p}\right)$ for any $a \in Q(K) - p\mathbb{Z}$.

Sublattices with index p

- For any binary lattice K with $p \mid d_K$, $u_p(K) := \left(\frac{a}{p}\right)$ for any $a \in Q(K) - p\mathbb{Z}$.
- We define two subsets $\Gamma_{p,\pm 1}(L)$ of $\Gamma_p(L)$ by

$$\Gamma_{p,\pm 1}(L) := \{K \in \Gamma_p(L) : u_p(K) = \pm 1\}.$$

Sublattices with index p

- For any binary lattice K with $p \mid d_K$, $u_p(K) := \left(\frac{a}{p}\right)$ for any $a \in Q(K) - p\mathbb{Z}$.
- We define two subsets $\Gamma_{p,\pm 1}(L)$ of $\Gamma_p(L)$ by

$$\Gamma_{p,\pm 1}(L) := \{K \in \Gamma_p(L) : u_p(K) = \pm 1\}.$$

- The number of equivalence classes in $\Gamma_{p,\pm 1}(L) := \gamma_{p,\pm 1}(L)$.

Sublattices with index p

- For any binary lattice K with $p \mid d_K$, $u_p(K) := \left(\frac{a}{p}\right)$ for any $a \in Q(K) - p\mathbb{Z}$.
- We define two subsets $\Gamma_{p,\pm 1}(L)$ of $\Gamma_p(L)$ by

$$\Gamma_{p,\pm 1}(L) := \{K \in \Gamma_p(L) : u_p(K) = \pm 1\}.$$

- The number of equivalence classes in $\Gamma_{p,\pm 1}(L) := \gamma_{p,\pm 1}(L)$.
- (Lemma) For the action $\Phi : O(L) \times \Gamma_{p,\pm 1}(L) \mapsto \Gamma_{p,\pm 1}(L)$ defined by $\Phi(\sigma, M) = \sigma(M)$, each orbit $ob(M)$ consists of all lattices isometric to M. Furthermore $|ob(M)| = \frac{o(L)}{o(M)}$.

Number of equivalent classes

Number of equivalent classes

- Assume $o(L) = 4$ and $\tau_x \in O(L)$ for a primitive vector $x \in L$.

Number of equivalent classes

- Assume $o(L) = 4$ and $\tau_x \in O(L)$ for a primitive vector $x \in L$.
- If $\left(\frac{-d_L}{p}\right) = 1$, then

$$\gamma_{p,\left(\frac{Q(x)}{p}\right)}(L) = \mathbf{2} + \frac{p - 4 - \left(\frac{-1}{p}\right)}{4} \quad \text{and} \quad \gamma_{p,-\left(\frac{Q(x)}{p}\right)}(L) = \mathbf{0} + \frac{p - \left(\frac{-1}{p}\right)}{4},$$

Number of equivalent classes

- Assume $o(L) = 4$ and $\tau_x \in O(L)$ for a primitive vector $x \in L$.
- If $\left(\frac{-d_L}{p}\right) = 1$, then

$$\gamma_{p,\left(\frac{Q(x)}{p}\right)}(L) = \mathbf{2} + \frac{p - 4 - \left(\frac{-1}{p}\right)}{4} \quad \text{and} \quad \gamma_{p,-\left(\frac{Q(x)}{p}\right)}(L) = \mathbf{0} + \frac{p - \left(\frac{-1}{p}\right)}{4},$$

- If $\left(\frac{-d_L}{p}\right) = -1$, then

$$\gamma_{p,1}(L) = \gamma_{p,-1}(L) = \mathbf{1} + \frac{p - 2 + \left(\frac{-1}{p}\right)}{4}.$$

Number of equivalent classes

- Assume $o(L) = 4$ and $\tau_x \in O(L)$ for a primitive vector $x \in L$.
- If $\left(\frac{-d_L}{p}\right) = 1$, then

$$\gamma_{p,\left(\frac{Q(x)}{p}\right)}(L) = \mathbf{2} + \frac{p - 4 - \left(\frac{-1}{p}\right)}{4} \quad \text{and} \quad \gamma_{p,-\left(\frac{Q(x)}{p}\right)}(L) = \mathbf{0} + \frac{p - \left(\frac{-1}{p}\right)}{4},$$

- If $\left(\frac{-d_L}{p}\right) = -1$, then

$$\gamma_{p,1}(L) = \gamma_{p,-1}(L) = \mathbf{1} + \frac{p - 2 + \left(\frac{-1}{p}\right)}{4}.$$

- Finally, if p divides the discriminant of L, then

$$\gamma_{p,u_p(L)}(L) = \mathbf{1} + \frac{p-1}{2} \qquad \text{and} \qquad \gamma_{p,-u_p(L)}(L) = \mathbf{0}.$$

Number of equivalent classes

Number of equivalent classes

- If $L = [1, 0, 1]$, then

$$\gamma_{p,1}(L) = \frac{\mathbf{3} + \left(\frac{\mathbf{2}}{\mathbf{p}}\right)}{\mathbf{2}} + \frac{p - 2\left(\frac{2}{p}\right) - \left(\frac{-1}{p}\right) - 6}{8}$$

and

$$\gamma_{p,-1}(L) = \frac{\mathbf{1} - \left(\frac{\mathbf{2}}{\mathbf{p}}\right)}{\mathbf{2}} + \frac{p + 2\left(\frac{2}{p}\right) - \left(\frac{-1}{p}\right) - 2}{8}.$$

Number of equivalent classes

Number of equivalent classes

- If $L = [1, 1, 1]$ and $p \neq 3$ then

$$\gamma_{p,1}(L) = \frac{\mathbf{3} + \left(\frac{\mathbf{3}}{\mathbf{p}}\right)}{\mathbf{2}} + \frac{p - 3\left(\frac{3}{p}\right) - \left(\frac{p}{3}\right) - 9}{12}$$

and

$$\gamma_{p,-1}(L) = \frac{\mathbf{1} - \left(\frac{\mathbf{3}}{\mathbf{p}}\right)}{\mathbf{2}} + \frac{p + 3\left(\frac{3}{p}\right) - \left(\frac{p}{3}\right) - 3}{12}.$$

Number of equivalent classes

- If $L = [1,1,1]$ and $p \neq 3$ then

$$\gamma_{p,1}(L) = \frac{\mathbf{3} + \left(\frac{\mathbf{3}}{\mathbf{p}}\right)}{\mathbf{2}} + \frac{p - 3\left(\frac{3}{p}\right) - \left(\frac{p}{3}\right) - 9}{12}$$

and

$$\gamma_{p,-1}(L) = \frac{\mathbf{1} - \left(\frac{\mathbf{3}}{\mathbf{p}}\right)}{\mathbf{2}} + \frac{p + 3\left(\frac{3}{p}\right) - \left(\frac{p}{3}\right) - 3}{12}.$$

- Finally, if $L = [1,1,1]$ and $p = 3$, then $\gamma_{p,1}(L) = 1$ and $\gamma_{p,-1}(L) = 0$.

When $k \neq 0, p \neq 2$

When $k \neq 0, p \neq 2$

- Let L and M be binary $\mathbb{Z}$-lattices such that $L \not\cong M$ and $(L, M) \not\cong ([1,1,1],[1,0,3])$.

When $k \neq 0, p \neq 2$

- Let L and M be binary $\mathbb{Z}$-lattices such that $L \not\simeq M$ and $(L, M) \not\simeq ([1,1,1],[1,0,3])$.
- (Main result for $k \neq 0$, $p \neq 2$) Two lattices L and M satisfy the condition

$$Q(L) \cap A_{p,k} = Q(M) \cap A_{p,k} \neq \emptyset$$

if and only if

$$L_2 \simeq M_2 \text{ and every lattice in } \Gamma_{p,\left(\frac{k}{p}\right)}(L) \text{ is isometric to } M,$$

or $L = [1,0,3]$ and the pair $([1,1,1], M)$ instead of (L, M) satisfies the above condition. Furthermore in the former case, it is equivalent to the conditions given in Table I and II:

Table I

p	k	$o(L)$	d_L	$\left(\frac{Q(x)}{p}\right)$	M
3	1	2	$1 \pmod 3$	$\times$	$[L:M]=3,\ u_p(M)=1$
3	2	2	$1 \pmod 3$	$\times$	$[L:M]=3,\ u_p(M)=-1$
3	1	4	$1 \pmod 3$	$\times$	$[L:M]=3,\ u_p(M)=1$
3	2	4	$1 \pmod 3$	$\times$	$[L:M]=3,\ u_p(M)=-1$
3	1	4	$2 \pmod 3$	-1	$[L:M]=3,\ u_p(M)=1$
3	2	4	$2 \pmod 3$	1	$[L:M]=3,\ u_p(M)=-1$
5	$1,4$	4	$\pm 1 \pmod 5$	-1	$[L:M]=5,\ u_p(M)=1$
5	$2,3$	4	$\pm 1 \pmod 5$	1	$[L:M]=5,\ u_p(M)=-1$

Table I ($x \in L$ is a primitive vector such that $\tau_x \in O(L)$)

Table II

p	k	L	M	p	k	L	M
3	1	$[1,1,1]$	$[1,1,7]$	5	$1,4$	$[1,1,1]$	$[1,1,19]$
5	$2,3$	$[1,1,1]$	$[3,3,7]$	7	$1,2,4$	$[1,1,1]$	$[1,1,37]$
7	$3,5,6$	$[1,1,1]$	$[3,3,13]$	11	$2,6,7,8,10$	$[1,1,1]$	$[7,1,13]$
13	$2,5,6,7,8,11$	$[1,1,1]$	$[7,5,19]$	3	1	$[1,0,1]$	$[1,0,9]$
3	2	$[1,0,1]$	$[2,2,5]$	5	$1,4$	$[1,0,1]$	$[1,0,25]$
5	$2,3$	$[1,0,1]$	$[2,2,13]$	7	$1,2,4$	$[1,0,1]$	$[1,0,49]$

Table II

Sketch of proof

Sketch of proof

- Assume that $Q(L) \cap A_{p,k} = Q(M) \cap A_{p,k} \neq \emptyset$.

Sketch of proof

- Assume that $Q(L) \cap A_{p,k} = Q(M) \cap A_{p,k} \neq \emptyset$.
- Then $L_q \simeq M_q$ for any $q \neq 2, p$.

Sketch of proof

- Assume that $Q(L) \cap A_{p,k} = Q(M) \cap A_{p,k} \neq \emptyset$.
- Then $L_q \simeq M_q$ for any $q \neq 2, p$.
- $L_2 \simeq M_2$ or $(L_2, M_2) \simeq ([1,1,1],[1,0,3])$.

Sketch of proof

- Assume that $Q(L) \cap A_{p,k} = Q(M) \cap A_{p,k} \neq \emptyset$.
- Then $L_q \simeq M_q$ for any $q \neq 2, p$.
- $L_2 \simeq M_2$ or $(L_2, M_2) \simeq ([1,1,1],[1,0,3])$.
- Assume that $L_2 \simeq M_2$.

Sketch of proof

- Assume that $Q(L) \cap A_{p,k} = Q(M) \cap A_{p,k} \neq \emptyset$.
- Then $L_q \simeq M_q$ for any $q \neq 2, p$.
- $L_2 \simeq M_2$ or $(L_2, M_2) \simeq ([1,1,1],[1,0,3])$.
- Assume that $L_2 \simeq M_2$.
- If $L_p \simeq M_p$, then there is a prime $q \in Q(L) \cap A_{p,k}$. Since $d_L = d_M$, $L \simeq M$.

Sketch of proof

- Assume that $Q(L) \cap A_{p,k} = Q(M) \cap A_{p,k} \neq \emptyset$.
- Then $L_q \simeq M_q$ for any $q \neq 2, p$.
- $L_2 \simeq M_2$ or $(L_2, M_2) \simeq ([1,1,1],[1,0,3])$.
- Assume that $L_2 \simeq M_2$.
- If $L_p \simeq M_p$, then there is a prime $q \in Q(L) \cap A_{p,k}$. Since $d_L = d_M$, $L \simeq M$.
- Therefore we may assume that

$$L_p \simeq [\epsilon_1, 0, \epsilon_2 p^{\alpha}] \qquad \text{and} \qquad M_p \simeq [\epsilon_1, 0, \epsilon_2 p^{\beta}],$$

where $\epsilon_i \in \mathbb{Z}_p^{\times}$, $\beta - \alpha \in 2\mathbb{Z}^+$ and $\epsilon_1 k \in (\mathbb{Z}_p^{\times})^2$.

Sketch of proof

Sketch of proof

- The discriminant of each sublattice of L with index $p^{\frac{(\beta-\alpha)}{2}}$ equal to that of M.

Sketch of proof

- The discriminant of each sublattice of L with index $p^{\frac{(\beta-\alpha)}{2}}$ equal to that of M.
- By Meyer's theorem, the number of sublattices of L with index $p^{\frac{(\beta-\alpha)}{2}}$ is 1 up to isometry.

Sketch of proof

- The discriminant of each sublattice of L with index $p^{\frac{(\beta-\alpha)}{2}}$ equal to that of M.
- By Meyer's theorem, the number of sublattices of L with index $p^{\frac{(\beta-\alpha)}{2}}$ is 1 up to isometry.
- From this, we have $\gamma_{p,\left(\frac{k}{p}\right)}(L) = 1$.

Sketch of proof

- The discriminant of each sublattice of L with index $p^{\frac{(\beta-\alpha)}{2}}$ equal to that of M.
- By Meyer's theorem, the number of sublattices of L with index $p^{\frac{(\beta-\alpha)}{2}}$ is 1 up to isometry.
- From this, we have $\gamma_{p,\left(\frac{k}{p}\right)}(L) = 1$.
- To consider the case when $(L_2, M_2) \simeq ([1,1,1],[1,0,3])$, we need some modification of the above argument.

When $k \neq 0, p = 2$

When $k \neq 0, p = 2$

- (Main result for $k \neq 0$, $p = 2$) For two binary $\mathbb{Z}$-lattices L, M,

$$Q(L) \cap A_{2,1} = Q(M) \cap A_{2,1}$$

if and only if

(i) $(L, M) \simeq ([a, b, a], [a, 2b, 4a])$, where $a \equiv 1 \pmod 2$ and $b \equiv 0 \pmod 2$ or;

(ii) $L_2 \simeq \mathbb{H}_2$ and M is the unique primitive sublattice of L with index 2.

Corollaries

Corollaries

- Let p be a prime greater than 13 and let $\gcd(k, p) = 1$. For two binary lattices L and M,

$$Q(L) \cap A_{p,k} = Q(M) \cap A_{p,k}$$

if and only if $L \simeq M$ or $(L, M) \simeq ([1, 1, 1], [1, 0, 3])$.

Corollaries

- Let p be a prime greater than 13 and let $\gcd(k, p) = 1$. For two binary lattices L and M,

$$Q(L) \cap A_{p,k} = Q(M) \cap A_{p,k}$$

  if and only if $L \simeq M$ or $(L, M) \simeq ([1, 1, 1], [1, 0, 3])$.

- For two binary lattices L and M such that $Q(L) \cap A_{p,k} \neq \emptyset$,

$$r(pn + k, L) = r(pn + k, M) \quad \text{for any non-negative integer } n$$

  if and only if $(p, k) = (2, 1), (3, 1), (3, 2)$, $L_p \simeq \mathbb{H}_p$ and M is the unique primitive sublattice of L with index p such that $u_p(M) = \left(\frac{k}{p}\right)$ only when $p = 3$.

Necessary conditions for $k = 0$

Necessary conditions for $k = 0$

- Let L and M be non-isometric binary lattices such that

$$\boxed{Q(L) \cap p\mathbb{Z} = Q(M) \cap p\mathbb{Z}.}$$

Then we have

Necessary conditions for $k = 0$

- Let L and M be non-isometric binary lattices such that

$$\boxed{Q(L) \cap p\mathbb{Z} = Q(M) \cap p\mathbb{Z}.}$$

Then we have

- $L_q \simeq M_q$ for any $q \neq 2, p$;

Necessary conditions for $k = 0$

- Let L and M be non-isometric binary lattices such that

$$\boxed{Q(L) \cap p\mathbb{Z} = Q(M) \cap p\mathbb{Z}.}$$

Then we have

- $L_q \simeq M_q$ for any $q \neq 2, p$;
- If $p \neq 2$, then $L_2 \simeq M_2$ or $(L_2, M_2) \simeq ([1,1,1],[1,0,3])$;

Necessary conditions for $k = 0$

- Let L and M be non-isometric binary lattices such that

$$\boxed{Q(L) \cap p\mathbb{Z} = Q(M) \cap p\mathbb{Z}.}$$

Then we have

- $L_q \simeq M_q$ for any $q \neq 2, p$;
- If $p \neq 2$, then $L_2 \simeq M_2$ or $(L_2, M_2) \simeq ([1, 1, 1], [1, 0, 3])$;
- $L_p \simeq \mathbb{H}$ if and only if $M_p \simeq \mathbb{H}$.

Necessary conditions for $k = 0$

- Let L and M be non-isometric binary lattices such that

$$\boxed{Q(L) \cap p\mathbb{Z} = Q(M) \cap p\mathbb{Z}.}$$

Then we have

- $L_q \simeq M_q$ for any $q \neq 2, p$;
- If $p \neq 2$, then $L_2 \simeq M_2$ or $(L_2, M_2) \simeq ([1,1,1],[1,0,3])$;
- $L_p \simeq \mathbb{H}$ if and only if $M_p \simeq \mathbb{H}$.
- If $L_p \not\simeq \mathbb{H}$, then $Q(\Lambda_p(L)) = Q(\Lambda_p(M))$.

Necessary conditions for $k = 0$

- Let L and M be non-isometric binary lattices such that

$$\boxed{Q(L) \cap p\mathbb{Z} = Q(M) \cap p\mathbb{Z}.}$$

  Then we have

- $L_q \simeq M_q$ for any $q \neq 2, p$;
- If $p \neq 2$, then $L_2 \simeq M_2$ or $(L_2, M_2) \simeq ([1,1,1],[1,0,3])$;
- $L_p \simeq \mathbb{H}$ if and only if $M_p \simeq \mathbb{H}$.
- If $L_p \not\simeq \mathbb{H}$, then $Q(\Lambda_p(L)) = Q(\Lambda_p(M))$.
- Conversely, if neither L_p nor M_p is isometric to $\mathbb{H}$ and $Q(\Lambda_p(L)) = Q(\Lambda_p(M))$, then $Q(L) \cap p\mathbb{Z} = Q(M) \cap p\mathbb{Z}$.

When $L_2 \simeq M_2$

When $L_2 \simeq M_2$

- For two non-isometric binary lattices L and M, assume that $L_p \simeq M_p \simeq \mathbb{H}$ and $L_2 \simeq M_2$ if $p \neq 2$.

When $L_2 \simeq M_2$

- For two non-isometric binary lattices L and M, assume that $L_p \simeq M_p \simeq \mathbb{H}$ and $L_2 \simeq M_2$ if $p \neq 2$.
- Let T be the binary lattice s.t. $r(p, T) > 0$ and $d_T = d_L$.

When $L_2 \simeq M_2$

- For two non-isometric binary lattices L and M, assume that $L_p \simeq M_p \simeq \mathbb{H}$ and $L_2 \simeq M_2$ if $p \neq 2$.
- Let T be the binary lattice s.t. $r(p, T) > 0$ and $d_T = d_L$.
- (Main result for $k = 0$, $L_2 \simeq M_2$) Under the above assumptions,

$$Q(L) \cap p\mathbb{Z} = Q(M) \cap p\mathbb{Z} \text{ if and only if } |f_T| = 4 \text{ and } f_L \sim f_M \cdot f_T^2.$$

Furthermore, if the above holds, then $-4p^4 + 1 \leq d_L < 0$.

When $L_2 \simeq M_2$

- For two non-isometric binary lattices L and M, assume that $L_p \simeq M_p \simeq \mathbb{H}$ and $L_2 \simeq M_2$ if $p \neq 2$.
- Let T be the binary lattice s.t. $r(p, T) > 0$ and $d_T = d_L$.
- (Main result for $k = 0$, $L_2 \simeq M_2$) Under the above assumptions,

  $$Q(L) \cap p\mathbb{Z} = Q(M) \cap p\mathbb{Z} \text{ if and only if } |f_T| = 4 \text{ and } f_L \sim f_M \cdot f_T^2.$$

  Furthermore, if the above holds, then $-4p^4 + 1 \leq d_L < 0$.
- Since f_T^2 is contained in the ambiguous class, $f_M \cdot f_T^2$ is well defined up to equivalence.

When $L_2 \simeq M_2$

- For two non-isometric binary lattices L and M, assume that $L_p \simeq M_p \simeq \mathbb{H}$ and $L_2 \simeq M_2$ if $p \neq 2$.
- Let T be the binary lattice s.t. $r(p, T) > 0$ and $d_T = d_L$.
- (Main result for $k = 0$, $L_2 \simeq M_2$) Under the above assumptions,

  $$Q(L) \cap p\mathbb{Z} = Q(M) \cap p\mathbb{Z} \text{ if and only if } |f_T| = 4 \text{ and } f_L \sim f_M \cdot f_T^2.$$

  Furthermore, if the above holds, then $-4p^4 + 1 \leq d_L < 0$.
- Since f_T^2 is contained in the ambiguous class, $f_M \cdot f_T^2$ is well defined up to equivalence.
- The above lower bound for d_L is extremal. In fact, $(L, M) = ([1, 1, p^4], [p^2, 1, p^2])$ satisfies the above condition.

Sketch of proof

Sketch of proof

- Assume that $Q(L) \cap p\mathbb{Z} = Q(M) \cap p\mathbb{Z}$.

Sketch of proof

- Assume that $Q(L) \cap p\mathbb{Z} = Q(M) \cap p\mathbb{Z}$.
- Note that for any integer n,

$$\begin{aligned} r(pn, f_L) &= r(n, f_L \cdot f_T) + r(n, f_L \cdot f_T^{-1}) - r\left(\tfrac{n}{p}, L\right) \qquad \text{and} \\ r(pn, f_M) &= r(n, f_M \cdot f_T) + r(n, f_M \cdot f_T^{-1}) - r\left(\tfrac{n}{p}, M\right). \end{aligned}$$

Sketch of proof

- Assume that $Q(L) \cap p\mathbb{Z} = Q(M) \cap p\mathbb{Z}$.
- Note that for any integer n,

$$\begin{aligned} r(pn, f_L) &= r(n, f_L \cdot f_T) + r(n, f_L \cdot f_T^{-1}) - r\left(\tfrac{n}{p}, L\right) \qquad \text{and} \\ r(pn, f_M) &= r(n, f_M \cdot f_T) + r(n, f_M \cdot f_T^{-1}) - r\left(\tfrac{n}{p}, M\right). \end{aligned}$$

- Using Weber's Theorem, one may prove that $(f_L \cdot f_T, f_L \cdot f_T^{-1})$ is properly equivalent to

$$(f_M \cdot f_T, f_M \cdot f_T^{-1}),\ \ (f_M \cdot f_T, f_M^{-1} \cdot f_T),\ \ (f_M^{-1} \cdot f_T^{-1}, f_M \cdot f_T^{-1}) \ \text{ or}$$

$$(f_M^{-1} \cdot f_T^{-1}, f_M^{-1} \cdot f_T).$$

Sketch of proof

- Assume that $Q(L) \cap p\mathbb{Z} = Q(M) \cap p\mathbb{Z}$.
- Note that for any integer n,

$$\begin{aligned} r(pn, f_L) &= r(n, f_L \cdot f_T) + r(n, f_L \cdot f_T^{-1}) - r\left(\tfrac{n}{p}, L\right) \qquad \text{and} \\ r(pn, f_M) &= r(n, f_M \cdot f_T) + r(n, f_M \cdot f_T^{-1}) - r\left(\tfrac{n}{p}, M\right). \end{aligned}$$

- Using Weber's Theorem, one may prove that $(f_L \cdot f_T, f_L \cdot f_T^{-1})$ is properly equivalent to

$$(f_M \cdot f_T, f_M \cdot f_T^{-1}), \;\; (f_M \cdot f_T, f_M^{-1} \cdot f_T), \;\; (f_M^{-1} \cdot f_T^{-1}, f_M \cdot f_T^{-1}) \;\; \text{or}$$

$$(f_M^{-1} \cdot f_T^{-1}, f_M^{-1} \cdot f_T).$$

- Therefore we have

$$f_L \simeq f_M \cdot f_T^{-2} \simeq f_M \cdot f_T^2 \quad \text{or} \quad f_L \simeq f_M^{-1} \cdot f_T^{-2} \simeq f_M^{-1} \cdot f_T^2.$$

When $L_2 \not\simeq M_2$

When $L_2 \not\simeq M_2$

- Assume that $L_p \simeq M_p \simeq \mathbb{H}$ and $L_2 \simeq [1,1,1]$, $M_2 \simeq [1,0,3]$.

When $L_2 \not\simeq M_2$

- Assume that $L_p \simeq M_p \simeq \mathbb{H}$ and $L_2 \simeq [1,1,1]$, $M_2 \simeq [1,0,3]$.
- (Main result for $k = 0$, $L_2 \not\simeq M_2$) Under the above assumptions, $Q(L) \cap p\mathbb{Z} = Q(M) \cap p\mathbb{Z}$ if and only if there are odd integers a, b such that

$$L \simeq [a, b, a],\ \ M \simeq [a, 2b, 4a] \ \text{ and } r\left(p^2, \left[4, 2, \frac{1-d_L}{4}\right]\right) > 0.$$

Furthermore, if the above holds, then $-4p^2 + 1 \leq d_L < 0$.

When $L_2 \not\simeq M_2$

- Assume that $L_p \simeq M_p \simeq \mathbb{H}$ and $L_2 \simeq [1,1,1]$, $M_2 \simeq [1,0,3]$.
- (Main result for $k = 0$, $L_2 \not\simeq M_2$) Under the above assumptions, $Q(L) \cap p\mathbb{Z} = Q(M) \cap p\mathbb{Z}$ if and only if there are odd integers a, b such that

$$L \simeq [a,b,a],\ M \simeq [a,2b,4a] \text{ and } r\left(p^2, \left[4, 2, \frac{1-d_L}{4}\right]\right) > 0.$$

  Furthermore, if the above holds, then $-4p^2 + 1 \leq d_L < 0$.
- The above lower bound for d_L is extremal. In fact, $L = [p,1,p]$ and $M = [p,2,4p]$ satisfies the above condition.

When $p = 3$

	$f_L,\ f_M$	$f_L,\ f_M$	$f_L,\ f_M$
$L_3 \simeq M_3 \simeq \mathbb{H}_3,\ L_2 \simeq M_2$	$[1,0,17],[2,2,9]$	$[1,0,32],[4,4,9]$	$[1,0,56],[8,8,9]$
$L_3 \simeq M_3 \simeq \mathbb{H}_3,\ L_2 \simeq M_2$	$[7,0,8],[4,4,15]$	$[1,0,65],[9,8,9]$	$[5,0,13],[2,2,33]$
$L_3 \simeq M_3 \simeq \mathbb{H}_3,\ L_2 \simeq M_2$	$[1,0,77],[9,4,9]$	$[7,0,11],[2,2,39]$	$[1,0,80],[9,2,9]$
$L_3 \simeq M_3 \simeq \mathbb{H}_3,\ L_2 \simeq M_2$	$[5,0,16],[4,4,21]$	$[1,1,39],[5,5,9]$	$[1,1,51],[7,7,9]$
$L_3 \simeq M_3 \simeq \mathbb{H}_3,\ L_2 \simeq M_2$	$[1,1,69],[9,7,9]$	$[1,1,81],[9,1,9]$	$[5,1,15],[7,3,11]$
$L_3 \simeq M_3 \simeq \mathbb{H}_3,\ L_2 \simeq M_2$	$[1,1,75],[9,5,9]$		
$L_3 \simeq M_3 \simeq \mathbb{H}_3,\ L_2 \not\simeq M_2$	$[3,1,3],[3,2,12]$	$[1,1,9],[4,2,9]$	$[1,1,7],[4,2,7]$
$L_3 \simeq M_3 \simeq \mathbb{H}_3,\ L_2 \not\simeq M_2$	$[1,1,3],[4,2,3]$		

Table $Q(L) \cap 3\mathbb{Z} = Q(M) \cap 3\mathbb{Z}$

Corollaries

Corollaries

- (Corollary) Let p be a prime and let L, M be non isometric binary lattices. Then $r(pn, L) = r(pn, M)$ for any integer n if and only if neither L_p nor M_p is isometric to $\mathbb{H}$ and $\Lambda_p(L) \simeq \Lambda_p(M)$.

Corollaries

- (Corollary) Let p be a prime and let L, M be non isometric binary lattices. Then $r(pn, L) = r(pn, M)$ for any integer n if and only if neither L_p nor M_p is isometric to $\mathbb{H}$ and $\Lambda_p(L) \simeq \Lambda_p(M)$.
- (Corollary) If $Q(L) \cap A_{p,k} \neq Q(M) \cap A_{p,k}$, then $(Q(L) - Q(M)) \cap A_{p,k}$ is an infinite set.

Kaplansky's conjecture

Kaplansky's conjecture

Let L and M be (positive definite integral) ternary $\mathbb{Z}$-lattices.

Kaplansky's conjecture

Let L and M be (positive definite integral) ternary $\mathbb{Z}$-lattices.

- (Schiemann) $L \simeq M$ if and only if $r(a, L) = r(a, M)$ for any integer a.

Kaplansky's conjecture

Let L and M be (positive definite integral) ternary $\mathbb{Z}$-lattices.

- (Schiemann) $L \simeq M$ if and only if $r(a, L) = r(a, M)$ for any integer a.
- (Cerviño-Hein) There are infinitely many counterexamples for the quaternary case.

Kaplansky's conjecture

Let L and M be (positive definite integral) ternary $\mathbb{Z}$-lattices.

- (Schiemann) $L \simeq M$ if and only if $r(a, L) = r(a, M)$ for any integer a.
- (Cerviño-Hein) There are infinitely many counterexamples for the quaternary case.
- What happens if $Q(L) = Q(M)$?

Kaplansky's conjecture

Let L and M be (positive definite integral) ternary $\mathbb{Z}$-lattices.

- (Schiemann) $L \simeq M$ if and only if $r(a, L) = r(a, M)$ for any integer a.
- (Cerviño-Hein) There are infinitely many counterexamples for the quaternary case.
- What happens if $Q(L) = Q(M)$?
- (Kaplansky's conjecture) $Q(L) = Q(M)$ if and only if either
  - (i) both L and M are regular and $L \in \text{gen}(M)$, or
  - (ii) $(L, M) \simeq (\langle a \rangle \perp [b, b, b], \langle a, b, 3b \rangle)$, or
  - (iii) $(L, M) \simeq \left(\begin{pmatrix} a & \frac{b}{2} & \frac{b}{2} \\ \frac{b}{2} & a & \frac{b}{2} \\ \frac{b}{2} & \frac{b}{2} & a \end{pmatrix}, [a, 2b, 2a + b] \perp \langle 2a - b \rangle \right)$.