K3 surfaces

lecture 13: Quadratic lattices and Pelle's equation

Misha Verbitsky

IMPA, sala 236

October 14, 2024, 17:00

Summary from the last lecture

Let $(V_{\mathbb Z}, q)$ be a non-degenerate quadratic lattice of signature (a,b) with $a\geqslant 3, b\geqslant 1$, and $g\in \mathbb Z$ a number such that there exists $x\in V_{\mathbb Z}$ such that $q(x,x)\neq 0$. Denote by $V_{\mathbb R}$ the tensor product $V_{\mathbb R}:=V_{\mathbb Z}\otimes_{\mathbb Z}\mathbb R$. As usual, we denote the Grassmannian of positive, oriented 2-planes by $\operatorname{Gr}_{+,+}(V_{\mathbb R})$ and the null-quadriv $\{l\in \mathbb P(V_{\mathbb R})\ \ |\ \ q(l,l)=0\}$ by $\operatorname{Null}(V_{\mathbb R})$.

In lecture 12, **we reduced density of the quartics in the Teichmüller space of K3 surfaces to the following statement.**

Theorem 1: Let $\mathfrak R\subset V_{\mathbb Z}$ the set of all vectors η such that $(\eta,\eta)=g$, and $Z(\mathfrak R)\subset \operatorname{Gr}_{+,+}(V_{\mathbb R})$ the set of all 2-planes orthogonal to some $\eta\in\mathfrak R$. **Then $Z(\mathfrak R)$ is dense in $\operatorname{Gr}_{+,+}(V_{\mathbb R})$.**

and reduced it further to
Theorem 3: Let $\mathfrak R\subset V_{\mathbb Z}$ the set of all vectors η such that $(\eta,\eta)=g$. **Then the closure of $\mathbb P\mathfrak R\subset \mathbb P V_{\mathbb R}$ contains $\operatorname{Null}(V_{\mathbb R})$.**

Also, **the following result was used implicitly.** We will deduce it from Meyers' theorem today.

THEOREM: Let $V_{\mathbb Z}=H^2(M,\mathbb Z)$ be the intersection lattice of a K3 surface. **Then there exists $x\in V_{\mathbb Z}$ such that $(x,x)=4$.**

Quadratic form representing 0

REMARK: Recall that an element of a lattice $\Lambda = \mathbb{Z}^n$ is called **primitive** if it is not divisible by an integer. For any primitive element $x \in \Lambda$, the quotient lattice $\Lambda/\langle x\rangle$ is torsion-free. Therefore, we can find a basis in Λ starting from x, and **there exists $\eta \in \Lambda^*$ such that $\langle \eta, x\rangle = 1$.**

DEFINITION: Let (Λ, q) be a quadratic lattice. We say that Λ (or q) **represents** $n \in \mathbb{Z}$ if there exists $x \in V_{\mathbb{Z}}$ such that $(x, x) = n$.

THEOREM: (Meyer)
Let q be an indefinite rational quadratic form on a space $V = \mathbb{Q}^r$, $r \geqslant 5$. **Then q represents 0.**

Proof: *A. Meyer, Ueber einen Satz von Dirichlet, Journal für Mathematik vol. 103 (1888) p. 98.* ■

REMARK: In the modern literature, Meyer's theorem is deduced from the Hasse-Minkowski theorem,

https://mathoverflow.net/questions/384352/a-list-of-proofs-of-the-hasse-minkowski-theorem

Quadratic form representing 4

EXAMPLE: Let $U_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ be the hyperbolic lattice 2x2. **Then it represents 4.** Indeed, $(2x+y, 2x+y) = 4(x,y) = 4$.

Claim 0: Let (Λ, q) be a unimodular even quadratic lattice which represents 0. **Then Λ contains U_2** (and hence represents 4).

Proof: Since Λ is unimodular, the natural map $q: \Lambda \longrightarrow \Lambda^*$ is an isomorphism. Then for any primitive $x \in \Lambda$ there exists $y \in \Lambda$ such that $q(x,y) = 1$. Assume that $q(x,x) = 0$. Then $q(y+kx, y+kx) = q(y,y) + 2kq(y,x)$; **choosing $k = -\frac{q(y,y)}{2}$, we obtain an element $y' := y + kx$ such that the $q(x,x) = 0, q(y', y') = 0$, and $q(x, y') = 1$.** ■

THEOREM: Let $V_{\mathbb{Z}} = H^2(M, \mathbb{Z})$ be the intersection lattice of a K3 surface. **Then there $V_{\mathbb{Z}}$ represents 4.**

Proof: From the classification of even unimodular form it follows that $V_{\mathbb{Z}}$ is a product of 2 E_{-8} and three U_2, and the latter represents 4. Even without using the classification, we can apply Meyer's theorem. Indeed, $\operatorname{rk} V_{\mathbb{Z}} = 22$, and the intersection form is even and indefinite. Together with Claim 0, Meyer's theorem implies that $V_{\mathbb{Z}}$ represents 4. ■

Discriminant of a quadratic lattice

DEFINITION: Let $(V_{\mathbb Z}, q)$ be a quadratic lattice, and $V_{\mathbb Q} := V_{\mathbb Z} \otimes_{\mathbb Z} \mathbb Q$. **The dual lattice** $V_{\mathbb Z}^*$ the set of all $x \in V_{\mathbb Q}$ such that $q(x, V_{\mathbb Z}) \subset \mathbb Z$.

REMARK: Let $e_1, ..., e_n$ be a basis in $V_{\mathbb Z}$, and $e_i^* \in V_{\mathbb Q}^*$ be **the dual basis in** $V_{\mathbb Q}^*$, that is, 1-forms which satisfy $\langle e_i, e_j^* \rangle = \delta_{ij}$. Using q to identify $V_{\mathbb Q}$ and $V_{\mathbb Q}^*$, we obtain that $\{e_i^*\}$ is a basis in $V_{\mathbb Z}^*$, hence **$V_{\mathbb Z}^*$ is a lattice of the same rank as $V_{\mathbb Z}$.**

REMARK: **Clearly, $V_{\mathbb Z}^* \supset V_{\mathbb Z}$.**

DEFINITION: **The discriminant group** of $V_{\mathbb Z}$ is $\operatorname{Disc}_{V_{\mathbb Z}} := V_{\mathbb Z}^*/V_{\mathbb Z}$.

REMARK: Let $\Lambda_1 \subset \Lambda$ be a sublattice in a quadratic lattice (Λ, q), $\operatorname{rk}\Lambda = \operatorname{rk}\Lambda_1$. We have the following family of sublattices $\Lambda_1^* \supset \Lambda^* \supset \Lambda \supset \Lambda_1$. **This defines a natural map $\Lambda_1 \xrightarrow{a} \operatorname{Disc}(\Lambda_1)$.**

Claim 1: Let $\Gamma_1 = SO(\Lambda_1)$ and $\Gamma_2 \subset \Gamma_1$ be its subgroup consisting of all maps preserving $\Lambda \supset \Lambda_1$. **Then Γ_2 is a group of all $\gamma \in SO(\Lambda_1)$ such that γ preserves the image of Λ in $\operatorname{Disc}(\Lambda_1)$.**

Proof: It is clear that any element of Γ_2 preserves $a(\Lambda)$. Conversely, any $\gamma \in SO(\Lambda_1)$ which preserves $a(\Lambda)$ also preserves $\Lambda := a^{-1}(a(\Lambda))$ ∎

Commensurability

DEFINITION: Two subgroups $G_1, G_2 \subset GL(n, \mathbb{R})$ are called **commensurable** if $G_1 \cap G_2$ has finite index in G_1 and in G_2.

PROPOSITION: Let $\Lambda_1 \subset \Lambda$ be quadratic lattices of the same rank. **Then $SO(\Lambda_1)$ and $SO(\Lambda)$ are commensurable.**

Proof: By Claim 1, $\Gamma_2 := SO(\Lambda_1) \cap SO(\Lambda)$ has finite index in $SO(\Lambda_1)$; indeed, the discriminant group is finite, and Γ_2 is a subgroup of $SO(\Lambda_1)$ which preserves a finite subset of $\operatorname{Disc}(\Lambda_1)$. To see that Γ_2 is commensurable with $SO(\Lambda)$, we consider a lattice $N\Lambda$, for N a sufficiently big integer, such that $\Lambda_1 \subset N\Lambda$. Then $SO(\Lambda) = SO(N\Lambda)$ has finite index in $\Gamma_2 = SO(\Lambda_1) \cap SO(N\Lambda)$.
■

Extending isometries of a lattice

Corollary 2: Let (B, q) be a non-degenerate quadratic lattice, and $A \subset B$ a non-degenerate sublatice of smaller rank. Denote by $\Gamma_A \subset SO(A)$ the group of all isometries of A which can be extended to an isometry of B. **Then Γ_A is of finite index in $SO(A)$.**

Proof: Consider the lattice $B_1 := A \oplus A^\perp \subset B$; clearly, it has finite index, hence $SO(B_1)$ is commensurable to $SO(B)$. This implies that the group $\mathrm{St}_A(SO(B)) \subset SO(B)$ of all elements preserving A is commensurable with $\mathrm{St}_A(SO(B_1)) \subset SO(B_1)$. However, any element of $SO(A)$ is extended to an element of $SO(B_1)$, hence the natural map $\mathrm{St}_A(SO(B_1)) \longrightarrow SO(A)$ is surjective. **Then the restriction map $\mathrm{St}_A(SO(B_1)) \cap \mathrm{St}_A(SO(B)) \longrightarrow SO(A)$ has finite index.** ■

Pell's equation

DEFINITION: Let $w \in \mathbb{Z}^{>0}$ be a integer which is not divisible by a square of an integer > 1. We say that w is **square-free.**

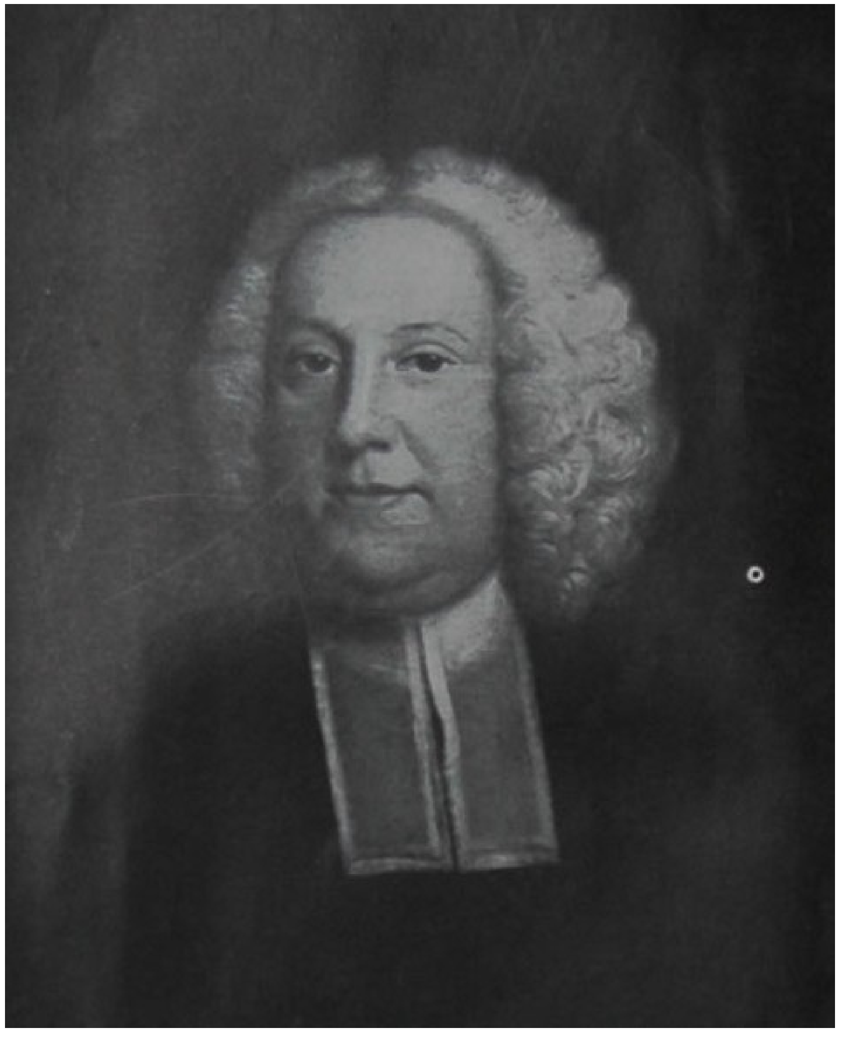
Let $w > 1$ be a square-free integer, and K the set of numbers $a + b\sqrt{w}$, where a, b are rational. Since the norm $N(a + b\sqrt{w}) := a^2 - wb^2$ is multiplicative on K, **the solutions of an equation $N(a + b\sqrt{w}) = 1$ form a multiplicative group.** Denote by Γ its quotient by ± 1.

THEOREM: (Legendre, Pell, Dirichlet) This group is isomorphic to $\mathbb{Z}$.
Proof: Next slide.

REMARK: Let $\sigma : K \longrightarrow K$ be the automorphism of K given as $a + b\sqrt{w} \mapsto a - b\sqrt{w}$. Since $N(x) = x\sigma(x)$, we have $x^{-1} = xN(x)^{-1}$. Therefore, x is invertible in $\mathcal{O}_K := \mathbb{Z} + Z\sqrt{w}$ if and only if $N(x) = \pm 1$. If $N(x) = -1$ has a solution, **the group of solutions of the Pell equation $a^2 - wb^2 = 1$ is an index 2 subgroup in the group $\mathcal{O}_K^*$ of invertible elements in the ring $\mathcal{O}_K$, otherwise it coincides with $\mathcal{O}_K^*$.**

REMARK: Consider $\mathcal{O}_K$ as a lattice equipped with the quadratic form $q(z) = N(z)$, and let $\xi \in \mathcal{O}_K$ be a solution of the Pell equation $N(\xi) = 1$. **Then the map $z \mapsto \xi z$ induces an isometry on the lattice $(\mathcal{O}_K, q)$.** In other words, **solutions of Pell's equation are identified with integer points in $SO(q)$.**

John Pell (1611-1685)



John Pell (1611-1685)

John Pell's connection with the equation is that he revised Thomas Branker's translation of Johann Rahn's 1659 book "Teutsche Algebra" into English, with a discussion of Brouncker's solution of the equation. Leonhard Euler mistakenly thought that this solution was due to Pell, as a result of which he named the equation after Pell.

Lagrange theorem (1)

REMARK: To prove that the group of solutions of $N(x + y\sqrt{w}) = 1$ is isomorphic to $\mathbb{Z}$ it suffices to produce a single non-trivial solution. Indeed, the set of solution is the set of all matrices $\begin{pmatrix} x & y\sqrt{w} \\ y\sqrt{w} & x \end{pmatrix}$ with determinant 1 and (x, y) integer. **Such points form a discrete subgroup in the connected component of $SO(1,1,\mathbb{R})$ which is isomorphic to $\mathbb{R}$.**

THEOREM: (Lagrange)
Let $w > 1$ be a square-free integer. **Then the equation $x^2 - y^2 w = 1$ has non-trivial integer solutions.**

We use the following lemma.

Lemma 1: There exists infinitely many $y > 0$ such that $|x - y\sqrt{w}| < \frac{1}{y}$.

Proof: Consider the interval $[0, 1[$ as the union of m intervals

$$[0, 1/m[,\ \ [1/m, 2/m[,\ \ \dots,\ \ [m - 1/m, 1[.$$

By the pigeonhole principle, there exist integers $a, b \in [0, m]$ such that the fractional parts of $a\sqrt{w}$ and $b\sqrt{w}$ belong to the same interval, giving $|(a - b)\sqrt{w} - c| < \frac{1}{m}$, where $|a - b| < m$. ■

Lagrange theorem (2)

THEOREM: (Lagrange)
Let $w > 1$ be a square-free integer. **Then the equation $x^2 - y^2 w = 1$ has non-trivial integer solutions.**

Proof. Step 1: Lemma 1 implies that **for some integer $M > 0$, the equation $x^2 - y^2 w = M$ has infinitely many solutions.** Indeed, consider a solution of $|x - y\sqrt{w}| < \frac{1}{y}$. Then $x = x - y\sqrt{w} + y\sqrt{w} \leqslant y\sqrt{w} + 1$, hence $x \leqslant y\sqrt{w} + 1$. Then

$$|x^2 - wy^2| = |x - y\sqrt{w}|(x + y\sqrt{w}) < \frac{1}{y}(y\sqrt{w} + 1 + y\sqrt{w}) \leqslant 2\sqrt{w} + 1.$$

Therefore, **there are infinitely many solutions of $|x^2 - y^2 w| < 2\sqrt{w} + 1$.**

Step 2: Let $M > 0$ be an integer such that there are infinitely many $z \in \mathbb{Z} + \mathbb{Z}\sqrt{w}$ with $N(z) = M$. Then **there are numbers $z_1, z_2 \in \mathbb{Z} + \mathbb{Z}\sqrt{w}$ such that $z_1 \equiv z_2 \mod M$ and $N(z_1) = N(z_2) = M$.** This gives $z_1 = Mz_3 + z_2$, for some $z_3 \in \mathbb{Z} + \mathbb{Z}\sqrt{w}$. Let $\sigma(a + b\sqrt{w}) := a - b\sqrt{w}$. Then

$$z_1 = z_2\sigma(z_2)z_3 + z_2 = z_2(z_3\sigma(z_2) + 1) = z_2 z, \quad (*)$$

where $z = z_3\sigma(z_2) + 1$. **Applying the norm to both sides of (*), we obtain $M = N(z_1) = N(z_2)N(z)$, hence $N(z) = 1$.** ■