

# Perfect Cuboids and the Box Variety

Ernst Kani  
Queen's University

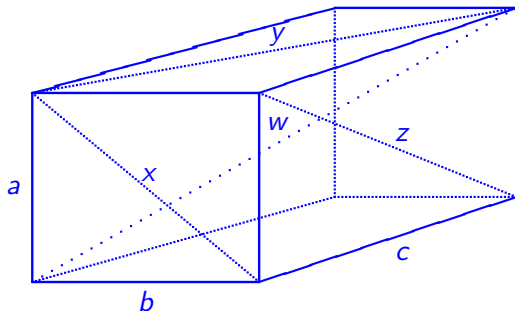
Québec-Maine Conference, Laval University  
27 Sept 2014

# Outline

1. Introduction
2. Early History
3. New Ideas (using Arithmetic Geometry)
4. The Bombieri-Lang Conjecture
5. Further Results
6. Diagonal Quotient Surfaces
7. Modular Correspondences
8. Mazur's Question

# 1. Introduction

- ▶ Consider a **rectangular box** (also known as **cuboid**):



- ▶ By **Pythagoras** we have the following relations:

$$(1) \quad a^2 + b^2 = x^2$$

$$(2) \quad b^2 + c^2 = y^2$$

$$(3) \quad a^2 + c^2 = z^2$$

$$(4) \quad a^2 + b^2 + c^2 = w^2$$

# 1. Introduction – 2

- ▶ A **rational cuboid** is a solution of (1) – (3) with  $a, b, c, x, y, z \in \mathbb{Q}^+$ .
- ▶ A **perfect cuboid** is a solution of (1) – (4) with  $a, \dots, w \in \mathbb{Q}^+$ .
- **Problem 1: (Sanderson, 1740, Euler 1770)** Find (parametric families of) rational cuboids.
- **Open Problem 2:** Are there **any** perfect cuboids?
- **Open Problem 3:** Are there at most **finitely many** perfect cuboids?

## 2. Early History

- **P. Halcke, 1719:** observed that  $(a, b, c) = (44, 240, 117)$  defines a rational cuboid. (This is the smallest one!)
- **Sanderson, 1740, Euler 1770:** Using **pythagorean triples**, Sanderson and Euler gave in their respective texts “Elements of Algebra” a systematic method for constructing rational cuboids. These are now called **Euler cuboids**; cf. Euler, *Elements of Algebra*, II, Art. 238 (p. 443).
- **A. Martin, 1894:** In *L'intermediaire des mathématiciens* vol. 1 (1894), p. 214, **Artemas Martin** (Washington) posed Problem 2 as **Question 361**. A solution was offered by **Brocard (1895)**, which was criticized by **Tannery (1896)**, as is mentioned in **L. Dickson's History of Number Theory**, vol. II, ch. XVII.

## 2. Early History - 2

- **H. Olsen, 1916:** Problem 254 of the *American Mathematical Monthly* **23** (1916) (proposed by H. Olsen, Chicago) requires you to find all perfect cuboids.
- **V. Spunar, 1917** submits a “solution” (which is published) that no such cuboids exist. (This solution is mentioned but is *not* criticized by Dickson, although it should be.)
- **M. Kraitchik, 1954:** establishes some congruence conditions for the sides  $a, b, c$  of a perfect cuboid.
- **J. Leech, 1977:** studies cuboids for which  $a, b, c$  and only 3 of  $x, y, z, w$  are rational (suggested by **M. Gardner, 1970**).
- **I. Korec, 1992:** Using his earlier results and a computer search, Korec shows that for a perfect cuboid  $\max(a, b, c) > 4 \times 10^9$ .

### 3. New Ideas (using Arithmetic Geometry)

- ▶ **Question:** Is there a **geometric reason** why it is easy to find lots of rational cuboids but difficult to find perfect ones?
- **A. Bremner, 1988:** studies the projective surface  $V \subset \mathbb{P}^5$  defined by equations (1) – (3). Thus, the rational points  $V(\mathbb{Q})$  of  $V$  (with  $abc \neq 0$ ) correspond to **rational cuboids**. He constructs another surface  $W$  which is birationally equivalent to  $V$ , and classifies all curves of degree  $\leq 3$  on  $W$ . He mentions that “the surface  $W$  has a superabundance of rational curves lying upon it.”
- **F. Beukers, van Geemen, < 2000:** In their (unpublished) preprint, they show that  $V$  is birationally equivalent to an **elliptic surface**  $V'$  fibered over  $\mathbb{P}^1$ . The sections of this fibration give rise to infinitely many rational curves on  $V'$  and hence on  $V$ .

### 3. New Ideas (using Arithmetic Geometry) - 2

- **R. van Luijk, 2000:** In his (unpublished) thesis, [vL] studies the **box variety** (the name is due to [FS])  $B \subset \mathbb{P}^6$  defined by equations (1) – (4), whose rational points  $B(\mathbb{Q})$  (with  $abc \neq 0$ ) correspond to **perfect cuboids**.  
He proves that  $B \otimes \mathbb{C}$  is a normal surface with 48 singularities, and that its desingularization  $\tilde{B}$  is **of general type**.  
He also finds a set  $\mathcal{L}$  of 92 curves of genus  $\leq 1$  on  $B \otimes \mathbb{C}$ :
  - 24 curves/ $\mathbb{Q}$  isomorphic to  $\mathbb{P}^1$  (the components of  $abc = 0$ ),
  - 8 curves/ $\mathbb{Q}(i)$ , isomorphic to  $\mathbb{P}^1$ ,
  - 60 elliptic curves/ $\mathbb{Q}(\sqrt{2}, i)$ , none defined over  $\mathbb{Q}$ .
- **Thus:** The geometry of the underlying surfaces  $V$  and  $B$  is radically different.



## 4. The Bombieri-Lang Conjecture

- ▶ **Question:** What special **diophantine properties** do varieties of **general type** have?
- **Theorem of Faltings, 1983:** If  $C/K$  is a curve of general type ( $\Leftrightarrow g_C \geq 2$ ) over a number field  $K$ , then  $C(K)$  is finite.
- **Bombieri-Lang Conjecture:** If  $X/K$  is a variety of general type, then  $X(K)$  is not Zariski-dense in  $X$ . ( $K$  a number field.)
- **Lang Conjecture (LC):** If  $X/K$  is a variety of general type, then there is a proper closed subset  $E(X) \subset X$  such that  $U(X) := X \setminus E(X)$  has finitely many  $K'$ -rational points for every number field  $K'/K$ .
- **Remark:** If (LC) is true for a surface  $X/K$ , then we must have:  $E(X) =$  union of all genus 0 and 1 curves on  $X \otimes \bar{K}$ . Since  $E(X)$  is supposed to be a closed set, this implies:

## 4. The Bombieri-Lang Conjecture - 2

- **Geometric Lang Conjecture (GLC):** A surface  $X/\overline{K}$  of general type contains at most finitely many curves of genus  $\leq 1$ .
- **Theorem of Bogomolov, 1977:** (GLC) is true for a smooth surface  $X/\mathbb{C}$ , provided that  $c_1^2(X) > c_2(X)$ .
- **Difficulties:** 1) How can we determine the exceptional set  $E(X)$ ? Even in the situation of **Bogomolov**, there is no algorithm for determining  $E(X)$ .  
2) The desingularization  $\tilde{B}_{\mathbb{C}}$  of the box variety does not satisfy Bogomolov's hypothesis. (Here  $c_1^2(\tilde{B}_{\mathbb{C}}) = 16$ ,  $c_2(\tilde{B}_{\mathbb{C}}) = 80$ .)

## 5. Further Results

- all unpublished, but available on [arXiv \[math.AG\]](#).
- **M. Stoll, D. Testa, 2010:** study the box variety  $B$  and its desingularization  $\tilde{B}$  in detail. For example:
  - they compute all the geometric invariants of  $\tilde{B}_{\mathbb{C}} = \tilde{B} \otimes \mathbb{C}$ ,
  - they determine  $\text{Aut}(\tilde{B}_{\mathbb{C}})$  (so  $|\text{Aut}(\tilde{B}_{\mathbb{C}})| = 1536 = 2^9 \cdot 3$ ),
  - they prove that the Picard group  $\text{Pic}(\tilde{B}_{\mathbb{C}}) = \text{NS}(\tilde{B}_{\mathbb{C}}) \simeq \mathbb{Z}^{64}$  and is generated by 140 curves: the 92 curves found by [vL], and the 48 exceptional curves which resolve the 48 singularities.
- **Question/Conjecture[ST]:** Is  $E(B_{\mathbb{C}}) = \mathcal{L}$ ? Is every curve of genus  $\leq 1$  on  $B_{\mathbb{C}}$  one of the 92 curves found by [vL]?
- **Note: Conjecture[ST] + Lang's Conjecture (LC) (+ [vL])** imply that **Problem 3** has a positive answer: there are only **finitely many** perfect cuboids.

## 5. Further Results - 2

- **A. Beauville, 2013:** gives a **more intrinsic** construction of the box variety  $B_{\mathbb{C}}$ . This implies:  
 $B_{\mathbb{C}}$  is a **diagonal quotient surface!**
- **E. Freitag, R. Salvati Manni, 2013:** give an analytic and a modular description of  $B_{\mathbb{C}}$ ,  $\text{Aut}(B_{\mathbb{C}})$  and of  $\mathcal{L}$ .
  - 1) They construct  $B_{\mathbb{C}}$  as an (explicit) quotient of  $\mathfrak{H}^* \times \mathfrak{H}^*$ ;
  - 2) They show that (an open part of)  $B \otimes \mathbb{Q}(i)$  has a **modular interpretation**;
  - 3) All  $\alpha \in \text{Aut}(B_{\mathbb{C}})$  are **modular** (i.e., induced by  $\Gamma(1) \times \Gamma(1)$ );
  - 4) All curves in  $\mathcal{L}$  are **modular** (or cuspidal).In particular:  $B \otimes \mathbb{Q}(i)$  is a (generalized) **modular diagonal quotient surface**.

## 6. Diagonal Quotient Surfaces

- ▶ **Let:**  $X$  be a smooth, projective curve over a field  $K$ ,  
 $G \leq \text{Aut}(X)$  a finite group of automorphisms of  $X$ ,  
 $\pi : X \rightarrow \bar{X} := G \backslash X$ , the quotient map,  
 $Y := X \times X$ , the product surface,  
 $\Delta_G = \{(g, g) : g \in G\} \leq G \times G$ , the diagonal subgroup,  
 $Z_G := \Delta_G \backslash Y$ , the **diagonal quotient surface** defined by  $G$ ,  
 $\phi = \phi_G : Y \rightarrow Z_G$ , the associated quotient map,  
 $\psi = \psi_G : Z_G \rightarrow \bar{Y} := \bar{X} \times \bar{X}$ , the induced map.
- ▶ **Remarks:** 1) We have that  $\psi \circ \phi = \pi \times \pi$  :

$$\pi \times \pi : Y = X \times X \xrightarrow{\phi} Z_G \xrightarrow{\psi} \bar{Y} = \bar{X} \times \bar{X}.$$

Thus,  $\phi$  and  $\psi$  are finite of degree  $\deg(\phi) = \deg(\psi) = |G|$ .

2) In general,  $Z_G$  has finitely many **quotient singularities**. The structure of  $Z_G$  and of its desingularization  $\tilde{Z}_G$  can be worked out; cf. **K.-Schanz, 1997**.

## 6. Diagonal Quotient Surfaces - 2

- **Application:** We apply this to:  
 $X := X(8) = \Gamma(8) \backslash \mathfrak{H}^*$ , the modular curve of level 8,  
 $G = \Gamma(4)/\Gamma(8) \simeq (\mathbb{Z}/2\mathbb{Z})^3$ , so  
 $\bar{X} = X(4) \simeq \mathbb{P}^1$ .

**Note:**  $g_X = 5$ , and  $X$  and  $G$  are defined over  $\mathbb{Q}$ .

- **Theorem 1:** ( $\sim$ [FS]) Let  $Z_G/\mathbb{Q}$  be the diagonal quotient surface of  $X = X(8)/\mathbb{Q}$  and  $G = \Gamma(4)/\Gamma(8)$ . Then

$$(5) \quad B \otimes \mathbb{Q}(i) \simeq Z_G \otimes \mathbb{Q}(i).$$

- **Key Idea:** [FS] use the fact that there is an isomorphism

$$X(8) \simeq \text{Proj}(A),$$

where  $A := \mathbb{C}[\vartheta_{00}(z), \vartheta_{10}(z), \vartheta_{01}(z), \vartheta_{00}(2z), \vartheta_{10}(2z)]$  is the graded ring generated by the classical **theta-functions**  $\vartheta_{a,b}$  (of weight  $\frac{1}{2}$ ).

## 6. Diagonal Quotient Surfaces - 3

- ▶ Recall that the **theta functions**  $\vartheta_{a,b}$  are defined by

$$\vartheta_{a,b}(z) = \sum_{n=-\infty}^{\infty} e^{\pi i((n+a/2)^2 z + b(n+a/2))}.$$

and satisfy the classical **theta-relations**

$$\vartheta_{00}^2(z) = \vartheta_{00}^2(2z) + \vartheta_{10}^2(2z)$$

$$\vartheta_{01}^2(z) = \vartheta_{00}^2(2z) - \vartheta_{10}^2(2z)$$

$$\vartheta_{10}^2(z) = 2\vartheta_{00}(2z)\vartheta_{10}(2z).$$

[FS] also work out the action of the generators

$$T = \begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix}, \quad T' = \begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix}, \quad R = \begin{pmatrix} 5 & 8 \\ 8 & 13 \end{pmatrix}$$

of  $G = \Gamma(4)/\Gamma(8)$  on the basis  $\vartheta_{00}(z), \vartheta_{10}(z), \dots, \vartheta_{10}(2z)$ . This allows them to compute the **ring of invariants** of  $A \otimes A$  with respect to  $\Delta_G$ . (They use instead a group  $\Delta(4,8)$ , but this leads to the same ring of invariants.)

## 7. Modular Correspondences

- ▶ **Question:** What is special about a product of modular curves?
- ▶ **Partial answer:** It comes equipped with a rich supply of curves, the **modular correspondences**. (→ **Hecke operators**.)
- **Construction:** Let  $\alpha \in \mathrm{GL}_2^+(\mathbb{Q}) \cap M_2(\mathbb{Z})$ , and let

$$T(\alpha) = \{(z, \alpha(z)) : z \in \mathfrak{H}^*\} \subset \mathfrak{H}^* \times \mathfrak{H}^*$$

be its graph. Then for any  $\Gamma = \Gamma(N)$ , its image

$$T_\Gamma(\alpha) \subset X(N) \times X(N) = \Gamma(N) \backslash \mathfrak{H}^* \times \Gamma(N) \backslash \mathfrak{H}^*$$

is an irreducible (algebraic) curve on  $X(N) \times X(N)$ .

- **Example:** For  $\Gamma = \Gamma(1)$ , each modular correspondence is of the form  $T_\Gamma(\alpha_n)$ , for some  $n \geq 1$ , where  $\alpha_n = \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix}$ . Moreover,  $T_\Gamma(\alpha_n) \sim X_0(n)$ .



## 7. Modular Correspondences - 2

- **Theorem 2: ([FS])** Via the isomorphism (5), each curve in  $\mathcal{L}$  is either the image of modular correspondence  $T(\alpha)$  (with  $\det(\alpha) = 1$ ) or the image of cuspidal curve  $\{c\} \times \mathfrak{H}^*$  or  $\mathfrak{H}^* \times \{c\}$ , where  $c \in \mathfrak{H}^* \setminus \mathfrak{H}$  is a cusp.

The following is a **partial converse**:

- **Theorem 3:** If  $C$  is curve of genus  $\leq 1$  on  $B_{\mathbb{C}} \simeq Z_G \otimes \mathbb{C}$  which is **modular** (i.e.,  $C = \phi(T_{\Gamma(8)}(\alpha))$ , for some  $\alpha$ ), then  $C \in \mathcal{L}$ .
- **Thus:** The **Conjecture [ST]** (i.e.,  $E(B) = \mathcal{L}$ )  $\Leftrightarrow$  (\*) every curve in  $E(B)$  is modular or cuspidal.

## 8. Mazur's Question

- **Mazur, 1978:** To what extent are the isogeny classes of elliptic curves  $E/\mathbb{Q}$  determined by their mod  $N$  Galois representations?
- **Frey (1985), Darmon (1994):** Formulated conjectures which make this question much more precise.
- **Remark:** To study isomorphisms of mod  $N$  Galois representations, one is naturally led to consider the **modular diagonal quotient surface**

$$Z_N = Z_{X(N), G_N}, \quad \text{where } G_N = \Gamma(1)/(\pm\Gamma(N)),$$

because the points of  $Z_N$  “classify” such isomorphisms.

- **Conjecture (1995):** If  $N = p$  is a prime with  $p \geq 23$ , then every curve  $C$  in  $E(Z_p)$  is modular.
- **Note:** This conjecture + (LC)  $\Rightarrow$  Darmon's Conjecture.

## 8. Mazur's Question - 2

- **Theorem 4 (Bakker/Tsimmerman, 2013):** The above conjecture is true for  $p \gg 0$ .
- **Remark:** Unfortunately, their proof does not give any estimate on how large  $p$  has to be.
- ▶ **But suppose:** that their methods **could be refined** to give a proof of the above conjecture. Then it might be possible to also prove a similar statement for  $Z_G \otimes \mathbb{C} = B_{\mathbb{C}}$ , i.e. to prove condition (\*). Then we would have:
- ▶ **(LC)  $\Rightarrow$   $\#(\text{perfect cuboids}) < \infty$  (Problem 3)**