Perfect Cuboids and the Box Variety

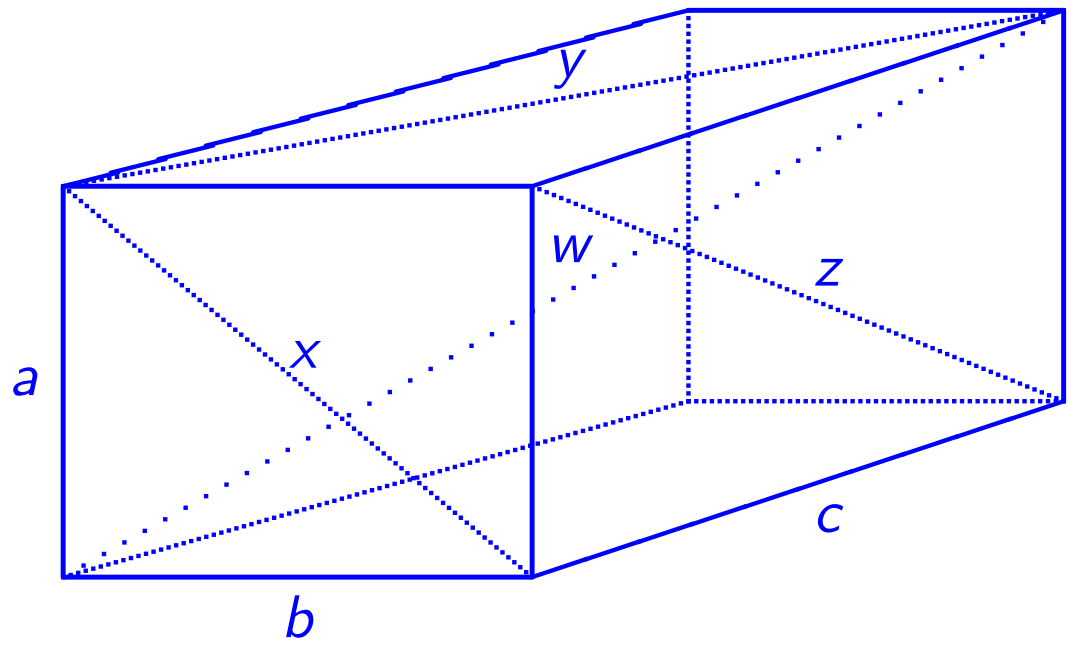
Ernst Kani
Queen's University

CMS Conference, McMaster University
7 December 2014

Outline

1. Introduction

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



- By Pythagoras we have the following relations:

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

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

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

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

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 $a, \ldots, w \in \mathbb{Q}^+$.

- 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 ≤ 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 ≤ 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 $X \otimes \overline{K}$. 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 ≤ 1.
- Theorem of Bogomolov, 1977: (GLC) is true for a smooth surface $X/\mathbb{C}$ of general type, 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 $\mathrm{Aut}(\tilde{B}_{\mathbb{C}})$ (so $|\mathrm{Aut}(\tilde{B}_{\mathbb{C}})| = 1536 = 2^9 \cdot 3$),
    – they prove that the Picard group $\mathrm{Pic}(\tilde{B}_{\mathbb{C}}) = \mathrm{NS}(\tilde{B}_{\mathbb{C}}) \simeq \mathbb{Z}^{64}$ 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 ≤ 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 $B_{\mathbb{C}}$, $\mathrm{Aut}(B_{\mathbb{C}})$ 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 $\alpha \in \mathrm{Aut}(B_{\mathbb{C}})$ are modular (i.e., they are induced by elements in $\langle \Gamma(1) \times \Gamma(1), \tau \rangle$, where τ is the automorphism which interchanges the two factors of the product)
  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,
  $G \leq \mathrm{Aut}(X)$ a finite group of automorphisms of X,
  $\pi : X \to \overline{X} := G\backslash X$, 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,
  $\phi = \phi_G : Y \to Z_G$, the associated quotient map,
  $\psi = \psi_G : Z_G \to \overline{Y} := \overline{X} \times \overline{X}$, the induced map.
- Remarks: 1) We have that $\psi \circ \phi = \pi \times \pi$:

$$\pi \times \pi : Y = X \times X \stackrel{\phi}{\to} Z_G \stackrel{\psi}{\to} \overline{Y} = \overline{X} \times \overline{X}.$$

  Thus, ϕ and ψ 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
  $\overline{X} = X(4) \simeq \mathbb{P}^1$.
  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) $$B \otimes \mathbb{Q}(i) \simeq Z_G \otimes \mathbb{Q}(i).$$

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

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

  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

$$\begin{aligned} \vartheta_{00}^2(z) &= \vartheta_{00}^2(2z) + \vartheta_{10}^2(2z) \\ \vartheta_{01}^2(z) &= \vartheta_{00}^2(2z) - \vartheta_{10}^2(2z) \\ \vartheta_{10}^2(z) &= 2\vartheta_{00}(2z)\vartheta_{10}(2z). \end{aligned}$$

[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 $\vartheta_{00}(z), \vartheta_{10}(z), \ldots, \vartheta_{10}(2z)$. This allows them them to compute the ring of invariants of $A \otimes A$ with respect to Δ_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. ($\longrightarrow$ 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 $\alpha_n = \left(\begin{smallmatrix} 1 & 0 \\ 0 & n \end{smallmatrix}\right)$. 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 ≤ 1 on $B_{\mathbb{C}} \simeq Z_G \otimes \mathbb{C}$ which is modular (i.e., $C = \phi(T_{\Gamma(8)}(\alpha))$, for some α), 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.

7. Modular Correspondences - 3

- Proof Sketch of Theorem 3: Recall the situation:

$$\begin{array}{c} X(8) \times X(8) \\ \phi \downarrow \\ B \\ \psi \downarrow \\ X(4) \times X(4) \end{array}$$

Suppose that $C := \phi(T_{\Gamma(8)}(\alpha)) \in E(B)$, i.e., $g_C \leq 1$ $\Rightarrow g_{\overline{C}} \leq 1$, where $\overline{C} := \psi(C) = T_{\Gamma(4)}(\alpha)$.

Step 1: $g_{\overline{C}} \geq 3$, if $\det(\alpha) \geq 3$.

Put $n = \det(\alpha)$. Then

$$\overline{C} \sim X_0(4, n) := \mathfrak{H}^*/(\Gamma(4) \cap \Gamma_0(4n)),$$

and one can derive an explicit formula for $g_{X_0(4,n)}$.

7. Modular Correspondences - 4

- Step 2: Analyze the cases $\det(\alpha) \leq 2$.

  Case 1: $\det(\alpha) = 1$.

  Then $\alpha \in \mathrm{SL}_2(\mathbb{Z}) = \Gamma(1)$, so

  $$C = \phi(\Gamma_{\overline{\alpha}}) \quad \text{with} \quad \overline{\alpha} \in G_8 = \Gamma(1)/(\pm\Gamma(8)).$$

  A careful analysis shows that

  $$g_C \leq 1 \Leftrightarrow \mathrm{ord}(\overline{\alpha}) | 8 \Rightarrow C \in \mathcal{L}.$$

  Case 2: $\det(\alpha) = 2$.

  Here $C \sim H\backslash X_0(8,2)$, where $|H| \mid 4$ and

  $$X_0(8,2) = (\Gamma(8) \cap \Gamma_0(2 \cdot 8))\backslash \mathfrak{H}^*,$$

  which has genus 17. A precise analysis shows that $g_C \geq 3$.

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/Tsimerman, 2013): The above conjecture is true for $p >> 0$.
- 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) $\Rightarrow$ #(perfect cuboids) $< \infty$ (Problem 3)