Perfekte Kuboide und die Kastenvarietät

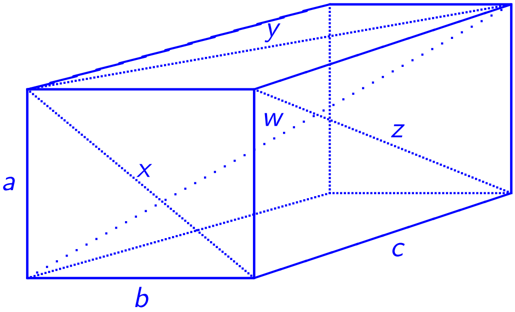
Ernst Kani
Queen's University

Tübinger Kolloquium, Universität Duisburg-Essen
21. Mai 2016

Outline

1. Einleitung

- Man betrachte einen recteckigen Kasten (oder Kuboid):



- Nach Pythagoras gelten die folgenden Relationen:

$$
\begin{array}{lrcl}
(1) & a^2 + b^2 & = & x^2 \\
(2) & b^2 + c^2 & = & y^2 \\
(3) & a^2 + c^2 & = & z^2 \\
(4) & a^2 + b^2 + c^2 & = & w^2
\end{array}
$$

1. Einleitung – 2

- Ein rationales Kuboid ist eine Lösung der Gleichungen (1) – (3) mit $a, b, c, x, y, z \in \mathbb{Q}^+$.
- Ein perfektes Kuboid ist eine Lösung der Gleichungen (1) – (4) with $a, b, c, x, y, z, w \in \mathbb{Q}^+$.

- Problem 1: **(Sanderson, 1740, Euler 1770)** Finde (parametrische Familien von) rationalen Kuboiden.
- Offenes Problem 2: Gibt es perfekte Kuboide?
- Offenes Problem 3: Gibt es höchstens endlich viele perfekte Kuboide?

2. Frühgeschichte

- P. Halcke, 1719: bemerkte, daß $(a, b, c) = (44, 240, 117)$ ein rationales Kuboid liefert. (Das ist das kleinste!)
- Sanderson, 1740, Euler 1770: Mithilfe der Pythagorischen Tripel, Sanderson und Euler geben in ihren jeweiligen Büchern "Elements of Algebra" eine systematische Methode um rationale Kuboide zu konstruieren. Diese heißen jetzt Eulersche Kuboide; vgl. Euler, *Elements of Algebra*, II, Art. 238 (S. 443).
- A. Martin, 1894: In *L'intermediaire des mathématiciens* vol. **1** (1894), p. 214, Artemas Martin (Washington) stellte Problem 2 als Question 361. Brocard (1895) bot eine Lösung an, die aber von Tannery (1896) kritisiert wurde; vgl. L. Dickson's History of Number Theory, vol. II, ch. XVII.

2. 2. Frühgeschichte - 2

- H. Olsen, 1916: Das Problem 254 des American Mathematical Monthly **23** (1916), welches von H. Olsen aus Chicago gestellt wurde, verlangt, daß man alle perfekten Kuboide findet.
  V. Spunar, 1917 reicht eine “Lösung” ein, die behauptet, daß es keine solche Kuboide gäbe. (Diese Lösung wird in Dicksons Buch erwähnt, wird aber *nicht* kritisiert, obwohl sie falsch ist.)
- M. Kraitchik, 1954: findet Kongruenzbedingungen für die Seiten a, b, c eines perfekten Kuboids.
- J. Leech, 1977: untersucht Kuboide mit der Eigenschaft, daß a, b, c und nur 3 der Zahlen x, y, z, w rational sind (Vorschlag von M. Gardner, 1970).
- I. Korec, 1992: Mithilfe seiner früheren Resultate und einem Computer zeigt Korec, daß $\max(a, b, c) > 4 \times 10^9$ ist, wenn a, b, c die Seiten eines perfekten Kuboids sind.

3. Neue Ideen (mithilfe der arithmetischen Geometrie)

- Frage: Gibt es einen geometrischen Grund dafür, daß es leicht ist, viele rationale Kuboide zu konstruieren, aber schwierig ist, perfekte Kuboide zu finden?

- A. Bremner, 1988: untersucht die projektive Fläche $V \subset \mathbb{P}^5$, die durch die Gleichungen (1) – (3) definiert wird. Daher: die rationalen Punkte $V(\mathbb{Q})$ auf V (mit $abc \neq 0$) entsprechen den rationalen Kuboiden.
  Er betrachtet eine weitere Fläche W, die birational äquivalent zu V ist, und klassifiziert alle Kurven vom Grad ≤ 3 auf W. Er erwähnt, daß W viele rationale Kurven besitzt. ("W has a superabundance of rational curves lying upon it.")

- F. Beukers, van Geemen, < 2000: In ihrem (unveröffentlichen) Preprint zeigen sie, daß V birational äquivalent zu einer elliptischen Fläche V' ist, die über $\mathbb{P}^1$ gefasert ist. Die Schnitte der Faserung liefern unendlich viele rationale Kurven auf V' und daher auch auf V.

3. Neue Ideen - 2

- R. van Luijk, 2000: In seiner (unveröffenlichen) Diplomarbeit untersucht [vL] die Kastenvarietät (box variety) $B \subset \mathbb{P}^6$. (Der Name stammt von [FS].) Diese wird durch die Gleichungen (1) – (4) definiert, und daher entprechen die rationalen Punkte $B(\mathbb{Q})$ (mit $abc \neq 0$) den perfekten Kuboiden.

  Er zeigt, daß $B \otimes \mathbb{C}$ eine normale Fläche ist, die 48 Singularitäten besitzt, und daß ihre Desingularisierung $\tilde{B}$ von allgemeinem Typ ist.

  Ferner findet er 92 Kurven vom Geschlecht ≤ 1 auf $B \otimes \mathbb{C}$:
  – 24 Kurven/$\mathbb{Q}$ isomorph zu $\mathbb{P}^1$ (Komponenten von $abc = 0$),
  – 8 Kurven/$\mathbb{Q}(i)$, isomorph zu $\mathbb{P}^1$,
  – 60 elliptische Kurven/$\mathbb{Q}(\sqrt{2}, i)$, keine über $\mathbb{Q}$ definiert.

- Bezeichnung: Sei $\mathcal{L}$ die Menge dieser 92 Kurven.

- Daher: Die Flächen V und B sind geometrisch vollkommen verschieden.

4. Die Bombieri-Lang Vermutung

- Frage: Welche spezielle diophantischen Eigenschaften besitzen die Varietäten von allgemeinem Typ?

- Satz von Faltings, 1983: Ist C/K eine Kurve von allgemeinem Typ ($\Leftrightarrow g_C \geq 2$) über einem Zahlkörper K, so ist $C(K)$ endlich.
- Bombieri-Lang Vermuting: Ist X/K von allgemeinem Typ, so ist $X(K)$ *nicht* Zariski-dicht in X. (K ein Zahlkörper.)
- Lang Vermutung (LC): Ist X/K von algemeinem Typ, so gibt es eine echte abgeschlossene Teilmenge $E(X) \subset X$ derart, daß $U(X) := X \setminus E(X)$ für jeden Zahlkörper K'/K endlich viele K'-rationale Punkte besitzt.
- Bemerkung: Gilt (LC) für eine Fläche X/K, so ist $E(X) =$ Vereinigung aller Geschlecht 0 oder 1 Kurven auf $X \otimes \overline{K}$.

  Da $E(X)$ abgeschlossen sein soll, so folgt:

4. Die Bombieri-Lang Vermutung - 2

- Geometrische Lang Vermutung (GLC): Eine Fläche $X/\overline{K}$ allgemeinen Typs enthält höchstens endlich viele Kurven vom Geschlecht ≤ 1.
- Satz (?) von Bogomolov, 1977: (GLC) gilt, wenn $X/\mathbb{C}$ eine glatte Fläche allgemeinen Typs ist, für die $c_1^2(X) > c_2(X)$ ist.
- Bemerkung/Frage: In dem Bourbaki-Artikel von M. Deschamps (1977) wird (ohne Beweis) behauptet, daß die obige Aussage aus den Resultaten von Bogomolov folgt. Stimmt das?
- Schwierigkeiten: 1) Wie kann man die Menge $E(X)$ bestimmen? Sogar in der Situation von Bogomolov gibt es keinen Algorithmus zur Bestimmung von $E(X)$.
  2) Für die Desingularisierung $\tilde{B}_{\mathbb{C}}$ der Kastenvarietät ist Bogomolovs Voraussetzung *nicht erfüllt.* (Es gilt hier, daß $c_1^2(\tilde{B}_{\mathbb{C}}) = 16$ und $c_2(\tilde{B}_{\mathbb{C}}) = 80$ ist.)

5. Weitere Resultate

- alle unveröffentlich, aber erhältlich bei arXiv [math.AG].

- M. Stoll, D. Testa, 2010: untersuchen die Kastenvarietät $B_{\mathbb{C}}$ und ihre Desingularisierung $\tilde{B}_{\mathbb{C}}$. Zum Beispiel:
  – sie berechnen alle geometrischen Invarianten von $\tilde{B}_{\mathbb{C}}$,
  – sie bestimmen $\mathrm{Aut}(\tilde{B}_{\mathbb{C}})$ (es gilt $|\mathrm{Aut}(\tilde{B}_{\mathbb{C}})| = 1536 = 2^9 \cdot 3$),
  – sie bewisen, daß die Picardgruppe $\mathrm{Pic}(\tilde{B}_{\mathbb{C}}) = \mathrm{NS}(\tilde{B}_{\mathbb{C}}) \simeq \mathbb{Z}^{64}$ und von 140 Kurven erzeugt wird: die 92 Kurven in $\mathcal{L}$, und die 48 exzeptionellen Kurven, die die 48 Singularitäten auflösen.
- Frage/Vermutung(ST): Ist $E(B_{\mathbb{C}}) = \mathcal{L}$? Ist jede Kurve vom Geschlecht ≤ 1 auf $B_{\mathbb{C}}$ eine der 92 Kurven, die [vL] gefunden hat?
- N.B.: Aus Vermutung (ST) + Langs Vermutung (LC) (+ [vL]) folgt, daß Problem 3 eine positive Antwort hat: es gibt nur endlich viele perfekte Kuboide.

5. Weitere Resultate - 2

- Bemerkung: Um (ST) zu motivieren, beweisen Stoll und Testa[ST]:

  • *Die Kurven in* $\mathcal{L}$ *sind genau diejenigen glatten Kurven* C *auf* $B_{\mathbb{C}}$*, die Geschlecht* $g_C \leq 1$ *und Grad* $\deg(C) \leq 4$ *haben.*

  Nach Bogomolov ist der Grad einer Kurve beschränkt, wenn ihr Geschlecht beschränkt ist. [FS] beweisen genauer:

  • *Ist* $C \subset B_{\mathbb{C}}$ *glatt (oder, allgemeiner, ist die Normalisierung* $\tilde{C} \to C$ *von* C *bijektiv), so gilt, daß*

$$\deg(C) \leq 16 g_{\tilde{C}} + 176.$$

  Natalia García-Fritz[GF] (2015) hat in ihrer Doktorarbeit das folgende Resultat bewiesen:

  • *Ist* $C \subset B_{\mathbb{C}}$ *glatt an jeder Singularität von* $B_{\mathbb{C}}$*, so gilt, daß*

$$\deg(C) \leq 4 g_{\tilde{C}} + 44.$$

5. Weitere Resultate - 3

- A. Beauville, 2013: gibt eine Konstruktion der Kastenvarietät $B_{\mathbb{C}}$, die etwas mehr intrinsisch ist. Daraus folgt:

  $B_{\mathbb{C}}$ ist eine Diagonalquotientenfläche!

- E. Freitag, R. Salvati Manni, 2013: geben eine analytische und eine modulare Beschreibung von $B_{\mathbb{C}}$, $\mathrm{Aut}(B_{\mathbb{C}})$ und von $\mathcal{L}$.
  1) Sie konstruieren $B_{\mathbb{C}}$ als einen Quotient von $\mathfrak{H}^* \times \mathfrak{H}^*$;
  2) Sie zeigen, daß (ein offener Teil von) $B \otimes \mathbb{Q}(i)$ eine modulare Interpretation besitzt.
  3) Jedes $\alpha \in \mathrm{Aut}(B_{\mathbb{C}})$ ist modular (d.h., wird induziert von Elementen in $\langle \Gamma(1) \times \Gamma(1), \tau \rangle$, wobei τ der Automorphismus ist, der die zwei Faktoren des Produkts vertauscht).
  4) Alle Kurven in $\mathcal{L}$ sind modular (oder kuspidal).

  Insbesondere folgt aus 1): $B \otimes \mathbb{Q}(i)$ ist eine (verallgemeinerte) modulare Diagonalquotientenfläche.

6. Diagonalquotientenflächen

- **Sei:** X eine glatte projektive Kurve über einem Körper K, $G \leq \mathrm{Aut}(X)$ eine endliche Gruppe von Automorphismen, $\pi : X \to \overline{X} := G\backslash X$, der Quotientenmorphismus, $Y := X \times X$, die Produktfläche, $\Delta_G = \{(g,g) : g \in G\} \leq G \times G$, die diagonale Untergruppe, $Z_G := \Delta_G \backslash Y$, die Diagonalquotientenfläche bezüglich G, $\phi = \phi_G : Y \to Z_G$, der zugehörige Quotientenmorphismus, $\psi = \psi_G : Z_G \to \overline{Y} := \overline{X} \times \overline{X}$, der induzierte Morphismus.
- Bemerkungen: 1) Es ist $\psi \circ \phi = \pi \times \pi$:

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

  Daher sind ϕ und ψ endliche Morphismen vom Grad $\deg(\phi) = \deg(\psi) = |G|$.

  2) Die Fläche Z_G hat höchstens endlich viele Quotienten-singularitäten. Die Struktur von Z_G und die ihrer Desingularisierung $\tilde{Z}_G$ kann man explizit beschreiben; vgl. K.-Schanz, 1997.

6. Diagonalquotientenflächen - 2

- Anwendung: Betrachte die folgende Situation:
  $X := X(8) = \Gamma(8)\backslash\mathfrak{H}^*$, die Modulkurve der Stufe 8,
  $G = \Gamma(4)/\Gamma(8) \simeq (\mathbb{Z}/2\mathbb{Z})^3$, also ist
  $\overline{X} = X(4) \simeq \mathbb{P}^1$.
  N.B.: $g_X = 5$, und X und G sind über $\mathbb{Q}$ definiert.
- Satz 1: ($\sim$[FS]) Sei $Z_G/\mathbb{Q}$ die Diagonalquotienfläche von $X = X(8)_{/\mathbb{Q}}$ bzgl. $G = \Gamma(4)/\Gamma(8)$. Dann gilt:

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

- Grundidee: [FS] benützen die Existenz einer Isomorphie

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

wobei $A := \mathbb{C}[\vartheta_{00}(z), \vartheta_{10}(z), \vartheta_{01}(z), \vartheta_{00}(2z), \vartheta_{10}(2z)]])$ der graduierte Ring ist, der von den klassischen Thetafunktionen $\vartheta_{a,b}$ (vom Gewicht $\frac{1}{2}$) erzeugt wird.

6. Diagonalquotientenflächen - 3

- Erinnerung: Die Thetafunktionen $\vartheta_{a,b}$ sind durch

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

definiert und erfüllen die klassischen Thetarelationen

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

[FS] bestimmen auch die Wirkung der Erzeugenen

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

von $G = \Gamma(4)/\Gamma(8)$ auf der Basis $\vartheta_{00}(z), \vartheta_{10}(z), \ldots, \vartheta_{10}(2z)$. Dadurch können sie den Ring der Invarianten von $A \otimes A$ bzgl. Δ_G bestimmen. (Eigentlich benützen sie hierzu eine Gruppe $\Delta(4,8)$, aber diese führt zum gleichen Invariantenring.)

7. Modularkorrespondenzen

- Frage: Inwiefern ist ein Produkt von Modulkurven etwas Besonderes?
- Teilantwort: Es besitzt einen reichen Vorrat von Kurven, nämlich die Modularkorrespondenzen. ($\to$ Heckeoperatoren.)

- Konstruktion: Sei $\alpha \in \mathrm{GL}_2^+(\mathbb{Q}) \cap M_2(\mathbb{Z})$, und sei

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

  sein Graph. Ist $\Gamma = \Gamma(N)$, so ist das Bild

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

  eine irreduzible (algebraische) Kurve auf $X(N) \times X(N)$.

- Beispiel: Ist $\Gamma = \Gamma(1)$, so ist jede Modularkorrespondenz von der Gestalt $T_\Gamma(\alpha_n)$, mit $n \geq 1$, wobei $\alpha_n = \left(\begin{smallmatrix} 1 & 0 \\ 0 & n \end{smallmatrix}\right)$. Ferner ist $T_\Gamma(\alpha_n)$ birational äquivalent zu $X_0(n)$: $T_\Gamma(\alpha_n) \sim X_0(n)$.

7. Modularkorrespondenzen - 2

- Satz 2: **([FS])** Via der Isomorphie (5) ist jede Kurve in $\mathcal{L}$ entweder das Bild einer Modularkorrespondenz $T(\alpha)$ (mit $\det(\alpha) = 1$) oder das Bild einer Spitzenkurve $\{c\} \times \mathfrak{H}^*$ oder $\mathfrak{H}^* \times \{c\}$, wobei $c \in \mathfrak{H}^* \setminus \mathfrak{H}$ eine Spitze ist.

  Der folgende Satz beinhaltet eine Teilumkehrung:

- Satz 3: Ist C eine Kurve vom Geschlecht ≤ 1 auf $B_{\mathbb{C}} \simeq Z_G \otimes \mathbb{C}$, die modular ist, (d.h., $C = \phi(T_{\Gamma(8)}(\alpha))$, für ein α), so ist $C \in \mathcal{L}$.
- Daher: Die Vermutung (ST) (d.h., $E(B) = \mathcal{L}$) $\Leftrightarrow$
  (*) *Jede Kurve in $E(B)$ ist modular oder eine Spitzenkurve.*

7. Modularkorrespondenzen - 3

- Beweiskizze von Satz 3: Wir haben die folgende Situation:

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

Sei $C := \phi(T_{\Gamma(8)}(\alpha)) \in E(B)$, d.h., $g_C \leq 1$
$\Rightarrow g_{\overline{C}} \leq 1$, wobei $\overline{C} := \psi(C) = T_{\Gamma(4)}(\alpha)$.

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

Setze $n = \det(\alpha)$. Dann gilt

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

und man kann eine explizite Formel für $g_{X_0(4,n)}$ herleiten.

7. Modularkorrespondenzen - 4

- **2. Schritt:** Analyse der Fälle $\det(\alpha) \leq 2$.

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

  Dann ist $\alpha \in SL_2(\mathbb{Z}) = \Gamma(1)$, also ist

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

  Eine etwas penible Analyse zeigt, daß

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

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

  Hier gilt, daß $C \sim H\backslash X_0(8,2)$, wobei $|H| \mid 4$ und

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

  Geschlecht 17 hat. Eine genaue Analyse zeigt, daß $g_C \geq 3$.

8. Die Frage von Mazur

- Mazur, 1978: Inwieweit sind die Isogenieklassen elliptischer Kurven $E/\mathbb{Q}$ durch ihre mod N Galoisdarstellungen bestimmt?
- Frey (1985), Darmon (1994): Formulierten Vermutungen, die diese vage Frage präzisieren.
- Remark: Die Studie der Isomorphismen der mod N Galoisdarstellungen führt ganz natürlich zu den modularen Diagonalquotientflächen

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

  da die Punkte von Z_N solche Isomorphismen "klassifizieren".
- Vermutung (1995): Ist $N = p$ eine Primzahl mit $p \geq 23$, so ist jede Kurve C in $E(Z_p)$ modular.
- N.B.: Diese Vermutung + (LC) $\Rightarrow$ Darmon's Conjecture.

8. Frage von Mazur - 2

- Satz 4 (Bakker/Tsimerman, 2013): Die obige Vermutung ist richtig, wenn $p >> 0$.
- Bemerkung: Leider liefert der Beweis von [BT] keine Abschätzung über die Größe von p.
- Aber man könnte hoffen, daß die Methode von [BT] sich derart verfeinern lässt, um einen Beweis der obigen Vermutung zu liefern. Dann ist es vielleicht auch möglich, daß man eine ähnliche Aussage für $Z_G \otimes \mathbb{C} = B_{\mathbb{C}}$ beweisen kann, d.h., daß man Bedingung (*) beweist.
  Dann würden wir erhalten:
- (LC) $\Rightarrow$ #(perfekten Kuboide) $< \infty$ (Problem 3)

Literatur

- [BT] Bakker, Tsimerman, On the Frey-Mazur Conjecture over low genus curves. ArXiv, 2013.
- [Be] A. Beauville, A tale of two surfaces. ArXiv, 2013.
- [FS] E. Freitag, R. Salvati Manni, A parametrization of the box variety by theta functions. ArXiv, 2013.
- [Ga] N. García-Fritz, Curves of low genus on surfaces and applications to Diophantine problems. Ph.D. Thesis, Queen's University at Kingston, 2015.
- [ST] M. Stoll, D. Testa, The surface parametrizing cuboids. ArXiv, 2010.
- [vL] R. van Luijk, On perfect cuboids. Doktoraalskriptie, 2000.