

Vom Satz des Pythagoras zu aktueller Algebraischer Geometrie

Dr. Oliver Labs

Universität des Saarlandes, Saarbrücken,
E-Mail: Labs@Math.Uni-Sb.de, mail@OliverLabs.net,
Web: www.OliverLabs.net

Saarbrücken, Otto–Hahn–Gymnasium, 16. März, 2009

Einführung

Der Satz des Pythagoras

Algebraische Flächen

Endliche Körper in der algebraischen Geometrie

Einführung

- ▶ **Satz des Pythagoras**
- ▶ der Kreis als algebraische Kurve
- ▶ einige algebraische Flächen
- ▶ endliche Körper in der algebraischen Geometrie
- ▶ Anwendungen auf Entschlüsselung geheimer Nachrichten und Zahlentheorie

Einführung

- ▶ Satz des Pythagoras
- ▶ der Kreis als algebraische Kurve
- ▶ einige algebraische Flächen
- ▶ endliche Körper in der algebraischen Geometrie
- ▶ Anwendungen auf Entschlüsselung geheimer Nachrichten und Zahlentheorie

Einführung

- ▶ Satz des Pythagoras
- ▶ der Kreis als algebraische Kurve
- ▶ einige algebraische Flächen
- ▶ endliche Körper in der algebraischen Geometrie
- ▶ Anwendungen auf Entschlüsselung geheimer Nachrichten und Zahlentheorie

Einführung

- ▶ Satz des Pythagoras
- ▶ der Kreis als algebraische Kurve
- ▶ einige algebraische Flächen
- ▶ endliche Körper in der algebraischen Geometrie
- ▶ Anwendungen auf Entschlüsselung geheimer Nachrichten und Zahlentheorie

Einführung

- ▶ Satz des Pythagoras
- ▶ der Kreis als algebraische Kurve
- ▶ einige algebraische Flächen
- ▶ endliche Körper in der algebraischen Geometrie
- ▶ Anwendungen auf Entschlüsselung geheimer Nachrichten und Zahlentheorie

Einführung

Der Satz des Pythagoras

Satz und Beweis

Kreis und Kugel

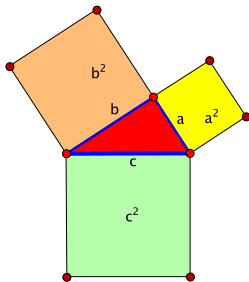
Algebraische Flächen

Endliche Körper in der algebraischen Geometrie

Der Satz des Pythagoras

Satz (des Pythagoras)

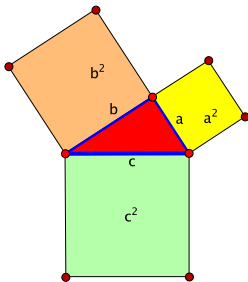
Ist ein Dreieck mit den Seitenlängen a, b, c mit einem rechtem Winkel gegenüber der Seite c gegeben, so gilt:
 $a^2 + b^2 = c^2$.



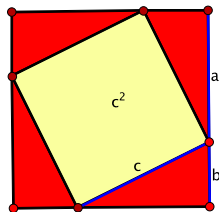
Der Satz des Pythagoras

Satz (des Pythagoras)

Ist ein Dreieck mit den Seitenlängen a, b, c mit einem rechtem Winkel gegenüber der Seite c gegeben, so gilt:
 $a^2 + b^2 = c^2$.



Beweis:



$$(a + b)^2 - c^2 = 4 \cdot \frac{1}{2} \cdot ab$$

$$\Leftrightarrow$$

$$a^2 + 2ab + b^2 - c^2 = 2ab$$

$$\Leftrightarrow$$

$$a^2 + b^2 = c^2.$$

(zum Satz des Pythagoras)

Das Schöne daran:

- ▶ Man kann die Aussage beweisen!

(zum Satz des Pythagoras)

Das Schöne daran:

- ▶ Man kann die Aussage beweisen!
- ▶ Der Beweis ist kurz und leicht verständlich.

(zum Satz des Pythagoras)

Das Schöne daran:

- ▶ Man kann die Aussage beweisen!
- ▶ Der Beweis ist kurz und leicht verständlich.
- ▶ Die Griechen kannten diesen Beweis schon vor mehr als 2000 Jahren.

(zum Satz des Pythagoras)

Das Schöne daran:

- ▶ Man kann die Aussage beweisen!
- ▶ Der Beweis ist kurz und leicht verständlich.
- ▶ Die Griechen kannten diesen Beweis schon vor mehr als 2000 Jahren.
- ▶ Die Aussage ist immer noch richtig.

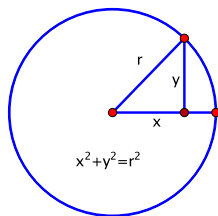
(zum Satz des Pythagoras)

Das Schöne daran:

- ▶ Man kann die Aussage beweisen!
- ▶ Der Beweis ist kurz und leicht verständlich.
- ▶ Die Griechen kannten diesen Beweis schon vor mehr als 2000 Jahren.
- ▶ Die Aussage ist immer noch richtig.
- ▶ Und wird auch immer richtig bleiben!

Kreis und Kugel

Der Satz des Pythagoras liefert auch einen Bezug zwischen Geometrie und Algebra:

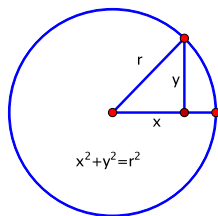


Die Punkte (x, y) auf dem Kreis um den Ursprung mit Radius r erfüllen: $x^2 + y^2 = r^2$ (eine algebraische Kurve).

Ähnlich erfüllen die Punkte einer Kugel: $x^2 + y^2 + z^2 = r^2$.

Kreis und Kugel

Der Satz des Pythagoras liefert auch einen Bezug zwischen Geometrie und Algebra:

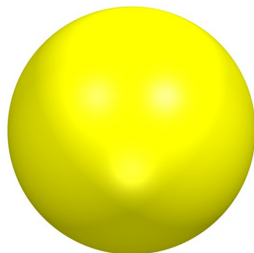
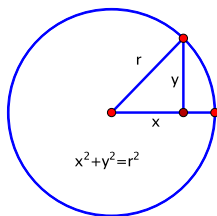


Die Punkte (x, y) auf dem Kreis um den Ursprung mit Radius r erfüllen: $x^2 + y^2 = r^2$ (eine algebraische Kurve).

Ähnlich erfüllen die Punkte einer Kugel: $x^2 + y^2 + z^2 = r^2$.

Kreis und Kugel

Der Satz des Pythagoras liefert auch einen Bezug zwischen Geometrie und Algebra:



Die Punkte (x, y) auf dem Kreis um den Ursprung mit Radius r erfüllen: $x^2 + y^2 = r^2$ (eine algebraische Kurve).

Ähnlich erfüllen die Punkte einer Kugel: $x^2 + y^2 + z^2 = r^2$.

Einführung

Der Satz des Pythagoras

Algebraische Flächen

Konstruktion komplizierterer Flächen

Flächen mit Singularitäten

Viele A_1 -Singularitäten

Endliche Körper in der algebraischen Geometrie

Definition

Definition

Eine **reelle algebraische Fläche** vom **Grad** d ist eine Menge von Punkten $(x, y, z) \in \mathbb{R}^3$ im Raum, die eine polynomielle Gleichung vom Grad d erfüllen.

Einige Beispiele:

Definition

Definition

Eine **reelle algebraische Fläche** vom **Grad** d ist eine Menge von Punkten $(x, y, z) \in \mathbb{R}^3$ im Raum, die eine polynomielle Gleichung vom Grad d erfüllen.

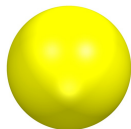
Einige Beispiele:

Definition

Definition

Eine **reelle algebraische Fläche** vom **Grad** d ist eine Menge von Punkten $(x, y, z) \in \mathbb{R}^3$ im Raum, die eine polynomielle Gleichung vom Grad d erfüllen.

Einige Beispiele:



$$x^2 + y^2 + z^2 = 1$$

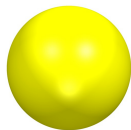
Grad 2

Definition

Definition

Eine **reelle algebraische Fläche** vom **Grad** d ist eine Menge von Punkten $(x, y, z) \in \mathbb{R}^3$ im Raum, die eine **polynomielle Gleichung vom Grad** d erfüllen.

Einige Beispiele:



$$x^2 + y^2 + z^2 = 1$$

Grad 2



$$x^2 + y \cdot z = 0$$

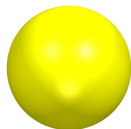
Grad 2

Definition

Definition

Eine **reelle algebraische Fläche** vom **Grad** d ist eine Menge von Punkten $(x, y, z) \in \mathbb{R}^3$ im Raum, die eine **polynomielle Gleichung vom Grad** d erfüllen.

Einige Beispiele:



$$x^2 + y^2 + z^2 = 1$$

Grad 2



$$x^2 + y \cdot z = 0$$

Grad 2



$$x^3 + y^2 = z^2$$

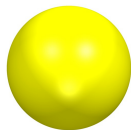
Grad 3

Definition

Definition

Eine **reelle algebraische Fläche** vom **Grad d** ist eine Menge von Punkten $(x, y, z) \in \mathbb{R}^3$ im Raum, die eine **polynomielle Gleichung vom Grad d** erfüllen.

Einige Beispiele:



$$x^2 + y^2 + z^2 = 1$$

Grad 2



$$x^2 + y \cdot z = 0$$

Grad 2



$$x^3 + y^2 = z^2$$

Grad 3



$$x^3 + y^2 \cdot z + x \cdot z^2 = x \cdot z$$

Grad 3

Konstruktion komplizierterer Flächen

Es gibt viele Methoden, kompliziertere Flächen zu konstruieren, deren Geometrie wir verstehen können. Erste basieren auf folgenden Eigenschaften:

- ▶ $x \mapsto 2 \cdot x$ staucht ein Objekt in x -Richtung um den Faktor 2.
- ▶ $y \mapsto \frac{1}{3} \cdot y$ streckt ein Objekt in y -Richtung um den Faktor 3. (mit SURFER zeigen)
- ▶ Gilt $a \cdot b = 0$ für zwei reelle Zahlen $a, b \in \mathbb{R}$, so folgt: $a = 0$ oder $b = 0$. (mit SURFER zeigen)

Konstruktion komplizierterer Flächen

Es gibt viele Methoden, kompliziertere Flächen zu konstruieren, deren Geometrie wir verstehen können. Erste basieren auf folgenden Eigenschaften:

- ▶ $x \mapsto 2 \cdot x$ staucht ein Objekt in x -Richtung um den Faktor 2.
- ▶ $y \mapsto \frac{1}{3} \cdot y$ streckt ein Objekt in y -Richtung um den Faktor 3. (mit SURFER zeigen)
- ▶ Gilt $a \cdot b = 0$ für zwei reelle Zahlen $a, b \in \mathbb{R}$, so folgt: $a = 0$ oder $b = 0$. (mit SURFER zeigen)

Konstruktion komplizierterer Flächen

Es gibt viele Methoden, kompliziertere Flächen zu konstruieren, deren Geometrie wir verstehen können. Erste basieren auf folgenden Eigenschaften:

- ▶ $x \mapsto 2 \cdot x$ staucht ein Objekt in x -Richtung um den Faktor 2.
- ▶ $y \mapsto \frac{1}{3} \cdot y$ streckt ein Objekt in y -Richtung um den Faktor 3. (mit SURFER zeigen)
- ▶ Gilt $a \cdot b = 0$ für zwei reelle Zahlen $a, b \in \mathbb{R}$, so folgt: $a = 0$ oder $b = 0$. (mit SURFER zeigen)

Konstruktion komplizierterer Flächen

Es gibt viele Methoden, kompliziertere Flächen zu konstruieren, deren Geometrie wir verstehen können. Erste basieren auf folgenden Eigenschaften:

- ▶ $x \mapsto 2 \cdot x$ staucht ein Objekt in x -Richtung um den Faktor 2.
- ▶ $y \mapsto \frac{1}{3} \cdot y$ streckt ein Objekt in y -Richtung um den Faktor 3. (mit SURFER zeigen)
- ▶ Gilt $a \cdot b = 0$ für zwei reelle Zahlen $a, b \in \mathbb{R}$, so folgt: $a = 0$ oder $b = 0$. (mit SURFER zeigen)

Konstruktion komplizierterer Flächen

Es gibt viele Methoden, kompliziertere Flächen zu konstruieren, deren Geometrie wir verstehen können. Erste basieren auf folgenden Eigenschaften:

- ▶ $x \mapsto 2 \cdot x$ staucht ein Objekt in x -Richtung um den Faktor 2.
- ▶ $y \mapsto \frac{1}{3} \cdot y$ streckt ein Objekt in y -Richtung um den Faktor 3. (mit SURFER zeigen)
- ▶ Gilt $a \cdot b = 0$ für zwei reelle Zahlen $a, b \in \mathbb{R}$, so folgt: $a = 0$ oder $b = 0$. (mit SURFER zeigen)

Konstruktion komplizierterer Flächen

Es gibt viele Methoden, kompliziertere Flächen zu konstruieren, deren Geometrie wir verstehen können. Erste basieren auf folgenden Eigenschaften:

- ▶ $x \mapsto 2 \cdot x$ staucht ein Objekt in x -Richtung um den Faktor 2.
- ▶ $y \mapsto \frac{1}{3} \cdot y$ streckt ein Objekt in y -Richtung um den Faktor 3. (mit SURFER zeigen)
- ▶ Gilt $a \cdot b = 0$ für zwei reelle Zahlen $a, b \in \mathbb{R}$, so folgt: $a = 0$ oder $b = 0$. (mit SURFER zeigen)

Flächen mit Singularitäten

Höhere Potenzen \Rightarrow wesentlich kompliziertere Gebilde.
Insbesondere können dabei auch Spitzen (genannt
Singularitäten) auftreten. Einige Beispiele:



$$x^2 + y^2 = z^2$$

Flächen mit Singularitäten

Höhere Potenzen \Rightarrow wesentlich kompliziertere Gebilde.
Insbesondere können dabei auch Spitzen (genannt
Singularitäten) auftreten. Einige Beispiele:



$$x^2 + y^2 = z^2$$



$$x^3 + y^2 = z^2$$

Flächen mit Singularitäten

Höhere Potenzen \Rightarrow wesentlich kompliziertere Gebilde.
Insbesondere können dabei auch Spitzen (genannt
Singularitäten) auftreten. Einige Beispiele:



$$x^2 + y^2 = z^2$$



$$x^3 + y^2 = z^2$$



$$x^3 + y^2z + \\ xz^2 = xz$$

Flächen mit Singularitäten

Höhere Potenzen \Rightarrow wesentlich kompliziertere Gebilde.
 Insbesondere können dabei auch Spitzen (genannt
 Singularitäten) auftreten. Einige Beispiele:



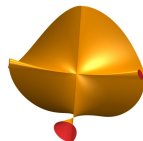
$$x^2 + y^2 = z^2$$



$$x^3 + y^2 = z^2$$



$$\begin{aligned} x^3 + y^2z + \\ xz^2 = xz \end{aligned}$$



$$\begin{aligned} x^2yz + x^2z^2 = \\ y^3z + y^3 \end{aligned}$$

Flächen mit Singularitäten

Höhere Potenzen \Rightarrow wesentlich kompliziertere Gebilde.
 Insbesondere können dabei auch Spitzen (genannt
 Singularitäten) auftreten. Einige Beispiele:



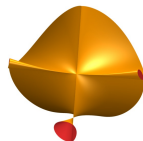
$$x^2 + y^2 = z^2$$



$$x^3 + y^2 = z^2$$



$$\begin{aligned} x^3 + y^2 z + \\ xz^2 = xz \end{aligned}$$



$$\begin{aligned} x^2 y z + x^2 z^2 = \\ y^3 z + y^3 \end{aligned}$$



$$\begin{aligned} (x^2 + y^2)^3 = \\ 4x^2 y^2 (z^2 + 1) \end{aligned}$$

Flächen mit Singularitäten

Höhere Potenzen \Rightarrow wesentlich kompliziertere Gebilde.
 Insbesondere können dabei auch Spitzen (genannt
 Singularitäten) auftreten. Einige Beispiele:



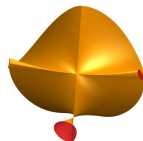
$$x^2 + y^2 = z^2$$



$$x^3 + y^2 = z^2$$



$$\begin{aligned} x^3 + y^2 z + \\ xz^2 = xz \end{aligned}$$



$$\begin{aligned} x^2 y z + x^2 z^2 = \\ y^3 z + y^3 \end{aligned}$$



$$\begin{aligned} (x^2 + y^2)^3 = \\ 4x^2 y^2 (z^2 + 1) \end{aligned}$$

Halten wir die höchste Potenz d der Gleichung fest, stellt sich
 die **Frage**: Was ist die größtmögliche Anzahl von Spitzen?

Flächen mit Singularitäten

Höhere Potenzen \Rightarrow wesentlich kompliziertere Gebilde.
 Insbesondere können dabei auch Spitzen (genannt
 Singularitäten) auftreten. Einige Beispiele:



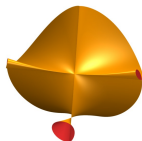
$$x^2 + y^2 = z^2$$



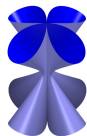
$$x^3 + y^2 = z^2$$



$$\begin{aligned} x^3 + y^2 z + \\ xz^2 = xz \end{aligned}$$



$$\begin{aligned} x^2 y z + x^2 z^2 = \\ y^3 z + y^3 \end{aligned}$$



$$\begin{aligned} (x^2 + y^2)^3 = \\ 4x^2 y^2 (z^2 + 1) \end{aligned}$$

Halten wir die höchste Potenz d der Gleichung fest, stellt sich
 die **Frage**: Was ist die größtmögliche Anzahl von Spitzen?

Antwort: $d = 1, 2, 3, 4, 5, 6$: bekannt. $d \geq 7$: bisher unbekannt.

Viele A_1 -Singularitäten

Grad d	3	4	5	6	7	8	9	10	11	12	d
$\mu_{A_1}^R(d) \geq$	4	16	31	65	99	168	226	345	425	600	$\approx \frac{5}{12}d^3$
$\mu_{A_1}^R(d) \leq$	4	16	31	65	104	174	246	360	480	645	$\approx \frac{4}{9}d^3$

- ▶ $\mu^3(3) = 4$: G. Salmon? A. Cayley? (ca. 1850), SURFER-Bilder
- ▶ $\mu^3(4) = 16$: E.E. Kummer (1864),
- ▶ $\mu^3(5) \geq 31$: E. G. Togliatti (1940),
 $\mu^3(5) \leq 31$: A. Beauville (1979),
- ▶ $\mu^3(6) \geq 65$: W. Barth (1996),
 $\mu^3(6) \leq 65$: Jaffe / Ruberman (1997),
- ▶ $\mu_{A_1}(7) \geq 99$: O. L. (2004) [math.AG/0409348](#): mit endlichen Körpern,
 $\mu_{A_1}(7) \leq 104$: A. Varchenko (1982): Formel für alle d .

Viele A_1 -Singularitäten

Grad d	3	4	5	6	7	8	9	10	11	12	d
$\mu_{A_1}^R(d) \geq$	4	16	31	65	99	168	226	345	425	600	$\approx \frac{5}{12}d^3$
$\mu_{A_1}^R(d) \leq$	4	16	31	65	104	174	246	360	480	645	$\approx \frac{4}{9}d^3$

- ▶ $\mu^3(3) = 4$: G. Salmon? A. Cayley? (ca. 1850), SURFER-Bilder
- ▶ $\mu^3(4) = 16$: E.E. Kummer (1864),
- ▶ $\mu^3(5) \geq 31$: E. G. Togliatti (1940),
 $\mu^3(5) \leq 31$: A. Beauville (1979),
- ▶ $\mu^3(6) \geq 65$: W. Barth (1996),
 $\mu^3(6) \leq 65$: Jaffe / Ruberman (1997),
- ▶ $\mu_{A_1}(7) \geq 99$: O. L. (2004) [math.AG/0409348](#): mit endlichen Körpern,
 $\mu_{A_1}(7) \leq 104$: A. Varchenko (1982): Formel für alle d .

Viele A_1 -Singularitäten

Grad d	3	4	5	6	7	8	9	10	11	12	d
$\mu_{A_1}^R(d) \geq$	4	16	31	65	99	168	226	345	425	600	$\approx \frac{5}{12}d^3$
$\mu_{A_1}^R(d) \leq$	4	16	31	65	104	174	246	360	480	645	$\approx \frac{4}{9}d^3$

- ▶ $\mu^3(3) = 4$: G. Salmon? A. Cayley? (ca. 1850), SURFER-Bilder
- ▶ $\mu^3(4) = 16$: E.E. Kummer (1864),
- ▶ $\mu^3(5) \geq 31$: E. G. Togliatti (1940),
 $\mu^3(5) \leq 31$: A. Beauville (1979),
- ▶ $\mu^3(6) \geq 65$: W. Barth (1996),
 $\mu^3(6) \leq 65$: Jaffe / Ruberman (1997),
- ▶ $\mu_{A_1}(7) \geq 99$: O. L. (2004) [math.AG/0409348](#): mit endlichen Körpern,
 $\mu_{A_1}(7) \leq 104$: A. Varchenko (1982): Formel für alle d .

Viele A_1 -Singularitäten

Grad d	3	4	5	6	7	8	9	10	11	12	d
$\mu_{A_1}^R(d) \geq$	4	16	31	65	99	168	226	345	425	600	$\approx \frac{5}{12}d^3$
$\mu_{A_1}^R(d) \leq$	4	16	31	65	104	174	246	360	480	645	$\approx \frac{4}{9}d^3$

- ▶ $\mu^3(3) = 4$: G. Salmon? A. Cayley? (ca. 1850), SURFER-Bilder
- ▶ $\mu^3(4) = 16$: E.E. Kummer (1864),
- ▶ $\mu^3(5) \geq 31$: E. G. Togliatti (1940),
 $\mu^3(5) \leq 31$: A. Beauville (1979),
- ▶ $\mu^3(6) \geq 65$: W. Barth (1996),
 $\mu^3(6) \leq 65$: Jaffe / Ruberman (1997),
- ▶ $\mu_{A_1}(7) \geq 99$: O. L. (2004) [math.AG/0409348](#): mit endlichen Körpern,
 $\mu_{A_1}(7) \leq 104$: A. Varchenko (1982): Formel für alle d .

Viele A_1 -Singularitäten

Grad d	3	4	5	6	7	8	9	10	11	12	d
$\mu_{A_1}^R(d) \geq$	4	16	31	65	99	168	226	345	425	600	$\approx \frac{5}{12}d^3$
$\mu_{A_1}^R(d) \leq$	4	16	31	65	104	174	246	360	480	645	$\approx \frac{4}{9}d^3$

- ▶ $\mu^3(3) = 4$: G. Salmon? A. Cayley? (ca. 1850), SURFER-Bilder
- ▶ $\mu^3(4) = 16$: E.E. Kummer (1864),
- ▶ $\mu^3(5) \geq 31$: E. G. Togliatti (1940),
 $\mu^3(5) \leq 31$: A. Beauville (1979),
- ▶ $\mu^3(6) \geq 65$: W. Barth (1996),
 $\mu^3(6) \leq 65$: Jaffe / Ruberman (1997),
- ▶ $\mu_{A_1}(7) \geq 99$: O. L. (2004) [math AG/0409348](#): mit endlichen Körpern,
 $\mu_{A_1}(7) \leq 104$: A. Varchenko (1982): Formel für alle d .

Viele A_1 -Singularitäten

Grad d	3	4	5	6	7	8	9	10	11	12	d
$\mu_{A_1}^R(d) \geq$	4	16	31	65	99	168	226	345	425	600	$\approx \frac{5}{12}d^3$
$\mu_{A_1}^R(d) \leq$	4	16	31	65	104	174	246	360	480	645	$\approx \frac{4}{9}d^3$

- ▶ $\mu^3(3) = 4$: G. Salmon? A. Cayley? (ca. 1850), SURFER-Bilder
- ▶ $\mu^3(4) = 16$: E.E. Kummer (1864),
- ▶ $\mu^3(5) \geq 31$: E. G. Togliatti (1940),
 $\mu^3(5) \leq 31$: A. Beauville (1979),
- ▶ $\mu^3(6) \geq 65$: W. Barth (1996),
 $\mu^3(6) \leq 65$: Jaffe / Ruberman (1997),
- ▶ $\mu_{A_1}(7) \geq 99$: O. L. (2004) [math AG/0409348](#): mit endlichen Körpern,
 $\mu_{A_1}(7) \leq 104$: A. Varchenko (1982): Formel für alle d .

Viele A_1 -Singularitäten

Grad d	3	4	5	6	7	8	9	10	11	12	d
$\mu_{A_1}^R(d) \geq$	4	16	31	65	99	168	226	345	425	600	$\approx \frac{5}{12}d^3$
$\mu_{A_1}^R(d) \leq$	4	16	31	65	104	174	246	360	480	645	$\approx \frac{4}{9}d^3$

- ▶ $\mu^3(3) = 4$: G. Salmon? A. Cayley? (ca. 1850), SURFER-Bilder
- ▶ $\mu^3(4) = 16$: E.E. Kummer (1864),
- ▶ $\mu^3(5) \geq 31$: E. G. Togliatti (1940),
 $\mu^3(5) \leq 31$: A. Beauville (1979),
- ▶ $\mu^3(6) \geq 65$: W. Barth (1996),
 $\mu^3(6) \leq 65$: Jaffe / Ruberman (1997),
- ▶ $\mu_{A_1}(7) \geq 99$: O. L. (2004) [▶ math.AG/0409348](https://mathoverflow.net/questions/409348): mit endlichen Körpern,
 $\mu_{A_1}(7) \leq 104$: A. Varchenko (1982): Formel für alle d .

Viele A_1 -Singularitäten

Grad d	3	4	5	6	7	8	9	10	11	12	d
$\mu_{A_1}^R(d) \geq$	4	16	31	65	99	168	226	345	425	600	$\approx \frac{5}{12}d^3$
$\mu_{A_1}^R(d) \leq$	4	16	31	65	104	174	246	360	480	645	$\approx \frac{4}{9}d^3$

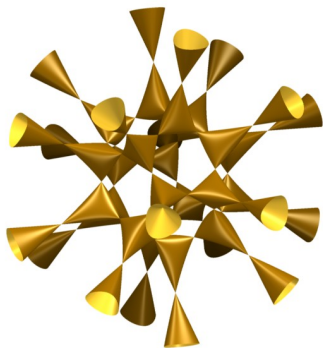
- ▶ $\mu^3(3) = 4$: G. Salmon? A. Cayley? (ca. 1850), SURFER-Bilder
- ▶ $\mu^3(4) = 16$: E.E. Kummer (1864),
- ▶ $\mu^3(5) \geq 31$: E. G. Togliatti (1940),
 $\mu^3(5) \leq 31$: A. Beauville (1979),
- ▶ $\mu^3(6) \geq 65$: W. Barth (1996),
 $\mu^3(6) \leq 65$: Jaffe / Ruberman (1997),
- ▶ $\mu_{A_1}(7) \geq 99$: O. L. (2004) [▶ math.AG/0409348](https://mathoverflow.net/questions/409348): mit endlichen Körpern,
 $\mu_{A_1}(7) \leq 104$: A. Varchenko (1982): Formel für alle d .

Viele A_1 -Singularitäten

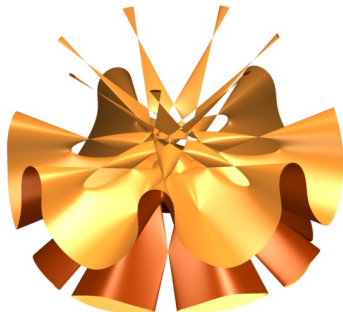
Grad d	3	4	5	6	7	8	9	10	11	12	d
$\mu_{A_1}^R(d) \geq$	4	16	31	65	99	168	226	345	425	600	$\approx \frac{5}{12}d^3$
$\mu_{A_1}^R(d) \leq$	4	16	31	65	104	174	246	360	480	645	$\approx \frac{4}{9}d^3$

- ▶ $\mu^3(3) = 4$: G. Salmon? A. Cayley? (ca. 1850), SURFER-Bilder
- ▶ $\mu^3(4) = 16$: E.E. Kummer (1864),
- ▶ $\mu^3(5) \geq 31$: E. G. Togliatti (1940),
 $\mu^3(5) \leq 31$: A. Beauville (1979),
- ▶ $\mu^3(6) \geq 65$: W. Barth (1996),
 $\mu^3(6) \leq 65$: Jaffe / Ruberman (1997),
- ▶ $\mu_{A_1}(7) \geq 99$: O. L. (2004) [▶ math.AG/0409348](https://mathoverflow.net/questions/409348): mit endlichen Körpern,
 $\mu_{A_1}(7) \leq 104$: A. Varchenko (1982): Formel für alle d .

Viele Spitzen — Schönheit durch Symmetrie



$d = 6$. 65 Spitzen. Gefunden von W. Barth (1996). Symmetrie des Ikosaeders. Gleichung involviert den Goldenen Schnitt.



$d = 7$. 99 Spitzen. Gefunden von O. Labs (2004). Symmetrie des regelmäßigen 7-Ecks. Vielleicht sind 104 möglich — unbekannt!!!

Einführung

Der Satz des Pythagoras

Algebraische Flächen

Endliche Körper in der algebraischen Geometrie

Rechnen auf der Zeiger-Uhr

Endliche Körper

Geometrie über endlichen Körpern

Rechnen auf elliptischen Kurven

Rechnen auf der Zeiger-Uhr

Rechnen mit 12 ganzen Stunden:
 $0, 1, 2, 3, \dots, 11$ ($12 \text{ Uhr} \equiv 0 \text{ Uhr}$).

- ▶ Addition: $3 + 8 = 11$
- ▶ Addition: $5 + 8 = 13 \equiv 1$
- ▶ Subtraktion: $5 - 8 = -3 \equiv 9$
- ▶ Multiplikation: $5 \cdot 3 = 15 \equiv 3$
- ▶ Multiplikation: $5 \cdot 7 = 35 \equiv 11$
- ▶ Multiplikation: $5 \cdot 11 = 55 \equiv 5 \cdot (-1) = -5 \equiv 7 \text{ Uhr}$
- ▶ Allgemein: normal rechnen, dann Rest bei Division durch 12 nehmen (oder auch schon vorher Rest nehmen).
- ▶ Division: $5 : 3 \equiv ?$

Rechnen auf der Zeiger-Uhr

Rechnen mit 12 ganzen Stunden:
 $0, 1, 2, 3, \dots, 11$ ($12 \text{ Uhr} \equiv 0 \text{ Uhr}$).

- ▶ Addition: $3 + 8 = 11$
- ▶ Addition: $5 + 8 = 13 \equiv 1$
- ▶ Subtraktion: $5 - 8 = -3 \equiv 9$
- ▶ Multiplikation: $5 \cdot 3 = 15 \equiv 3$
- ▶ Multiplikation: $5 \cdot 7 = 35 \equiv 11$
- ▶ Multiplikation: $5 \cdot 11 = 55 \equiv 5 \cdot (-1) = -5 \equiv 7 \text{ Uhr}$
- ▶ Allgemein: normal rechnen, dann Rest bei Division durch 12 nehmen (oder auch schon vorher Rest nehmen).
- ▶ Division: $5 : 3 \equiv ?$

Rechnen auf der Zeiger-Uhr

Rechnen mit 12 ganzen Stunden:
 $0, 1, 2, 3, \dots, 11$ ($12 \text{ Uhr} \equiv 0 \text{ Uhr}$).

- ▶ Addition: $3 + 8 = 11$
- ▶ Addition: $5 + 8 = 13 \equiv 1$
- ▶ Subtraktion: $5 - 8 = -3 \equiv 9$
- ▶ Multiplikation: $5 \cdot 3 = 15 \equiv 3$
- ▶ Multiplikation: $5 \cdot 7 = 35 \equiv 11$
- ▶ Multiplikation: $5 \cdot 11 = 55 \equiv 5 \cdot (-1) = -5 \equiv 7 \text{ Uhr}$
- ▶ Allgemein: normal rechnen, dann Rest bei Division durch 12 nehmen (oder auch schon vorher Rest nehmen).
- ▶ Division: $5 : 3 \equiv ?$

Rechnen auf der Zeiger-Uhr

Rechnen mit 12 ganzen Stunden:
 $0, 1, 2, 3, \dots, 11$ ($12 \text{ Uhr} \equiv 0 \text{ Uhr}$).

- ▶ Addition: $3 + 8 = 11$
- ▶ Addition: $5 + 8 = 13 \equiv 1$
- ▶ Subtraktion: $5 - 8 = -3 \equiv 9$
- ▶ Multiplikation: $5 \cdot 3 = 15 \equiv 3$
- ▶ Multiplikation: $5 \cdot 7 = 35 \equiv 11$
- ▶ Multiplikation: $5 \cdot 11 = 55 \equiv 5 \cdot (-1) = -5 \equiv 7 \text{ Uhr}$
- ▶ Allgemein: normal rechnen, dann Rest bei Division durch 12 nehmen (oder auch schon vorher Rest nehmen).
- ▶ Division: $5 : 3 \equiv ?$

Rechnen auf der Zeiger-Uhr

Rechnen mit 12 ganzen Stunden:
 $0, 1, 2, 3, \dots, 11$ ($12 \text{ Uhr} \equiv 0 \text{ Uhr}$).

- ▶ Addition: $3 + 8 = 11$
- ▶ Addition: $5 + 8 = 13 \equiv 1$
- ▶ Subtraktion: $5 - 8 = -3 \equiv 9$
- ▶ Multiplikation: $5 \cdot 3 = 15 \equiv 3$
- ▶ Multiplikation: $5 \cdot 7 = 35 \equiv 11$
- ▶ Multiplikation: $5 \cdot 11 = 55 \equiv 5 \cdot (-1) = -5 \equiv 7 \text{ Uhr}$
- ▶ Allgemein: normal rechnen, dann Rest bei Division durch 12 nehmen (oder auch schon vorher Rest nehmen).
- ▶ Division: $5 : 3 \equiv ?$

Rechnen auf der Zeiger-Uhr

Rechnen mit 12 ganzen Stunden:
 $0, 1, 2, 3, \dots, 11$ ($12 \text{ Uhr} \equiv 0 \text{ Uhr}$).

- ▶ Addition: $3 + 8 = 11$
- ▶ Addition: $5 + 8 = 13 \equiv 1$
- ▶ Subtraktion: $5 - 8 = -3 \equiv 9$
- ▶ Multiplikation: $5 \cdot 3 = 15 \equiv 3$
- ▶ Multiplikation: $5 \cdot 7 = 35 \equiv 11$
- ▶ Multiplikation: $5 \cdot 11 = 55 \equiv 5 \cdot (-1) = -5 \equiv 7 \text{ Uhr}$
- ▶ Allgemein: normal rechnen, dann Rest bei Division durch 12 nehmen (oder auch schon vorher Rest nehmen).
- ▶ Division: $5 : 3 \equiv ?$

Rechnen auf der Zeiger-Uhr

Rechnen mit 12 ganzen Stunden:
 $0, 1, 2, 3, \dots, 11$ ($12 \text{ Uhr} \equiv 0 \text{ Uhr}$).

- ▶ Addition: $3 + 8 = 11$
- ▶ Addition: $5 + 8 = 13 \equiv 1$
- ▶ Subtraktion: $5 - 8 = -3 \equiv 9$
- ▶ Multiplikation: $5 \cdot 3 = 15 \equiv 3$
- ▶ Multiplikation: $5 \cdot 7 = 35 \equiv 11$
- ▶ Multiplikation: $5 \cdot 11 = 55 \equiv 5 \cdot (-1) = -5 \equiv 7 \text{ Uhr}$
- ▶ Allgemein: normal rechnen, dann Rest bei Division durch 12 nehmen (oder auch schon vorher Rest nehmen).
- ▶ Division: $5 : 3 \equiv ?$

Rechnen auf der Zeiger-Uhr

Rechnen mit 12 ganzen Stunden:
 $0, 1, 2, 3, \dots, 11$ ($12 \text{ Uhr} \equiv 0 \text{ Uhr}$).

- ▶ Addition: $3 + 8 = 11$
- ▶ Addition: $5 + 8 = 13 \equiv 1$
- ▶ Subtraktion: $5 - 8 = -3 \equiv 9$
- ▶ Multiplikation: $5 \cdot 3 = 15 \equiv 3$
- ▶ Multiplikation: $5 \cdot 7 = 35 \equiv 11$
- ▶ Multiplikation: $5 \cdot 11 = 55 \equiv 5 \cdot (-1) = -5 \equiv 7 \text{ Uhr}$
- ▶ Allgemein: normal rechnen, dann Rest bei Division durch 12 nehmen (oder auch schon vorher Rest nehmen).
- ▶ Division: $5 : 3 \equiv ?$

Division

- ▶ Division: $5 : 3 \equiv ?$
- ▶ $\frac{5}{3}$ ist die Zahl aus $\{0, 1, 2, \dots, 11\}$, für die $\frac{5}{3} \cdot 3 \equiv 5$ gilt.

z	0	1	2	3
$z \cdot 3$	$0 \equiv 0$	$3 \equiv 3$	$6 \equiv 6$	$9 \equiv 9$
z	4	5	6	7
$z \cdot 3$	$12 \equiv 0$	$15 \equiv 3$	$18 \equiv 6$	$21 \equiv 9$
z	8	9	10	11
$z \cdot 3$	$24 \equiv 0$	$27 \equiv 3$	$30 \equiv 6$	$33 \equiv 9$

Also: Für jedes z ist $z \cdot 3$ ist teilbar durch 3 und $\frac{5}{3} \cdot 3 \equiv 5$ hat also keine Lösung.

Division

- ▶ Division: $5 : 3 \equiv ?$
- ▶ $\frac{5}{3}$ ist die Zahl aus $\{0, 1, 2, \dots, 11\}$, für die $\frac{5}{3} \cdot 3 \equiv 5$ gilt.

z	0	1	2	3
$z \cdot 3$	$0 \equiv 0$	$3 \equiv 3$	$6 \equiv 6$	$9 \equiv 9$
z	4	5	6	7
$z \cdot 3$	$12 \equiv 0$	$15 \equiv 3$	$18 \equiv 6$	$21 \equiv 9$
z	8	9	10	11
$z \cdot 3$	$24 \equiv 0$	$27 \equiv 3$	$30 \equiv 6$	$33 \equiv 9$

Also: Für jedes z ist $z \cdot 3$ ist teilbar durch 3 und $\frac{5}{3} \cdot 3 \equiv 5$ hat also keine Lösung.

Division

- ▶ Division: $5 : 3 \equiv ?$
- ▶ $\frac{5}{3}$ ist die Zahl aus $\{0, 1, 2, \dots, 11\}$, für die $\frac{5}{3} \cdot 3 \equiv 5$ gilt.

z	0	1	2	3
$z \cdot 3$	$0 \equiv 0$	$3 \equiv 3$	$6 \equiv 6$	$9 \equiv 9$
z	4	5	6	7
$z \cdot 3$	$12 \equiv 0$	$15 \equiv 3$	$18 \equiv 6$	$21 \equiv 9$
z	8	9	10	11
$z \cdot 3$	$24 \equiv 0$	$27 \equiv 3$	$30 \equiv 6$	$33 \equiv 9$

Also: Für jedes z ist $z \cdot 3$ ist teilbar durch 3 und $\frac{5}{3} \cdot 3 \equiv 5$ hat also keine Lösung.

Division

- ▶ Division: $5 : 3 \equiv ?$
- ▶ $\frac{5}{3}$ ist die Zahl aus $\{0, 1, 2, \dots, 11\}$, für die $\frac{5}{3} \cdot 3 \equiv 5$ gilt.

z	0	1	2	3
$z \cdot 3$	$0 \equiv 0$	$3 \equiv 3$	$6 \equiv 6$	$9 \equiv 9$
z	4	5	6	7
$z \cdot 3$	$12 \equiv 0$	$15 \equiv 3$	$18 \equiv 6$	$21 \equiv 9$
z	8	9	10	11
$z \cdot 3$	$24 \equiv 0$	$27 \equiv 3$	$30 \equiv 6$	$33 \equiv 9$

Also: Für jedes z ist $z \cdot 3$ teilbar durch 3 und $\frac{5}{3} \cdot 3 \equiv 5$ hat also keine Lösung.

Endliche Körper

Satz

In $\mathbb{F}_p = \{0, 1, 2, \dots, p-1\}$ ist Division immer möglich für Zahlen $\neq 0$. Man sagt: \mathbb{F}_p ist ein Körper.

Beispiel

Wir betrachten den Körper \mathbb{F}_7 :

z	0	1	2	3	4	5	6
$1 : z$	0	1	4, da $4 \cdot 2 = 8 \equiv 1$	5	2	3	6

Dann ist z.B.:

$$\frac{5}{3} \cdot 3 = 5 \cdot \frac{1}{3} \cdot 3 \equiv 5 \cdot 5 \cdot 3 = 75 = 70 + 5 = 10 \cdot 7 + 5 \equiv 5.$$

Endliche Körper

Satz

In $\mathbb{F}_p = \{0, 1, 2, \dots, p-1\}$ ist Division immer möglich für Zahlen $\neq 0$. Man sagt: \mathbb{F}_p ist ein Körper.

Beispiel

Wir betrachten den Körper \mathbb{F}_7 :

z	0	1	2	3	4	5	6
$1 : z$	0	1	4, da $4 \cdot 2 = 8 \equiv 1$	5	2	3	6

Dann ist z.B.:

$$\frac{5}{3} \cdot 3 = 5 \cdot \frac{1}{3} \cdot 3 \equiv 5 \cdot 5 \cdot 3 = 75 = 70 + 5 = 10 \cdot 7 + 5 \equiv 5.$$

Endliche Körper

Satz

In $\mathbb{F}_p = \{0, 1, 2, \dots, p-1\}$ ist Division immer möglich für Zahlen $\neq 0$. Man sagt: \mathbb{F}_p ist ein Körper.

Beispiel

Wir betrachten den Körper \mathbb{F}_7 :

z	0	1	2	3	4	5	6
$1 : z$	0	1	$4, \text{ da } 4 \cdot 2 = 8 \equiv 1$	5	2	3	6

Dann ist z.B.:

$$\frac{5}{3} \cdot 3 = 5 \cdot \frac{1}{3} \cdot 3 \equiv 5 \cdot 5 \cdot 3 = 75 = 70 + 5 = 10 \cdot 7 + 5 \equiv 5.$$

Endliche Körper

Satz

In $\mathbb{F}_p = \{0, 1, 2, \dots, p-1\}$ ist Division immer möglich für Zahlen $\neq 0$. Man sagt: \mathbb{F}_p ist ein Körper.

Beispiel

Wir betrachten den Körper \mathbb{F}_7 :

z	0	1	2	3	4	5	6
$1 : z$	0	1	4, da $4 \cdot 2 = 8 \equiv 1$	5	2	3	6

Dann ist z.B.:

$$\frac{5}{3} \cdot 3 = 5 \cdot \frac{1}{3} \cdot 3 \equiv 5 \cdot 5 \cdot 3 = 75 = 70 + 5 = 10 \cdot 7 + 5 \equiv 5.$$

Endliche Körper

Satz

In $\mathbb{F}_p = \{0, 1, 2, \dots, p-1\}$ ist Division immer möglich für Zahlen $\neq 0$. Man sagt: \mathbb{F}_p ist ein Körper.

Beispiel

Wir betrachten den Körper \mathbb{F}_7 :

z	0	1	2	3	4	5	6
$1 : z$	0	1	4, da $4 \cdot 2 = 8 \equiv 1$	5	2	3	6

Dann ist z.B.:

$$\frac{5}{3} \cdot 3 = 5 \cdot \frac{1}{3} \cdot 3 \equiv 5 \cdot 5 \cdot 3 = 75 = 70 + 5 = 10 \cdot 7 + 5 \equiv 5.$$

Endliche Körper

Satz

In $\mathbb{F}_p = \{0, 1, 2, \dots, p-1\}$ ist Division immer möglich für Zahlen $\neq 0$. Man sagt: \mathbb{F}_p ist ein Körper.

Beispiel

Wir betrachten den Körper \mathbb{F}_7 :

z	0	1	2	3	4	5	6
$1 : z$	0	1	4, da $4 \cdot 2 = 8 \equiv 1$	5	2	3	6

Dann ist z.B.:

$$\frac{5}{3} \cdot 3 = 5 \cdot \frac{1}{3} \cdot 3 \equiv 5 \cdot 5 \cdot 3 = 75 = 70 + 5 = 10 \cdot 7 + 5 \equiv 5.$$

Endliche Körper

Satz

In $\mathbb{F}_p = \{0, 1, 2, \dots, p-1\}$ ist Division immer möglich für Zahlen $\neq 0$. Man sagt: \mathbb{F}_p ist ein Körper.

Beispiel

Wir betrachten den Körper \mathbb{F}_7 :

z	0	1	2	3	4	5	6
$1 : z$	0	1	4, da $4 \cdot 2 = 8 \equiv 1$	5	2	3	6

Dann ist z.B.:

$$\frac{5}{3} \cdot 3 = 5 \cdot \frac{1}{3} \cdot 3 \equiv 5 \cdot 5 \cdot 3 = 75 = 70 + 5 = 10 \cdot 7 + 5 \equiv 5.$$

Endliche Körper

Satz

In $\mathbb{F}_p = \{0, 1, 2, \dots, p-1\}$ ist Division immer möglich für Zahlen $\neq 0$. Man sagt: \mathbb{F}_p ist ein Körper.

Beispiel

Wir betrachten den Körper \mathbb{F}_7 :

z	0	1	2	3	4	5	6
$1 : z$	0	1	4, da $4 \cdot 2 = 8 \equiv 1$	5	2	3	6

Dann ist z.B.:

$$\frac{5}{3} \cdot 3 = 5 \cdot \frac{1}{3} \cdot 3 \equiv 5 \cdot 5 \cdot 3 = 75 = 70 + 5 = 10 \cdot 7 + 5 \equiv 5.$$

Endliche Körper

Satz

In $\mathbb{F}_p = \{0, 1, 2, \dots, p-1\}$ ist Division immer möglich für Zahlen $\neq 0$. Man sagt: \mathbb{F}_p ist ein Körper.

Beispiel

Wir betrachten den Körper \mathbb{F}_7 :

z	0	1	2	3	4	5	6
$1 : z$	0	1	$4, \text{ da } 4 \cdot 2 = 8 \equiv 1$	5	2	3	6

Dann ist z.B.:

$$\frac{5}{3} \cdot 3 = 5 \cdot \frac{1}{3} \cdot 3 \equiv 5 \cdot 5 \cdot 3 = 75 = 70 + 5 = 10 \cdot 7 + 5 \equiv 5.$$

Endliche Körper

Satz

In $\mathbb{F}_p = \{0, 1, 2, \dots, p-1\}$ ist Division immer möglich für Zahlen $\neq 0$. Man sagt: \mathbb{F}_p ist ein Körper.

Beispiel

Wir betrachten den Körper \mathbb{F}_7 :

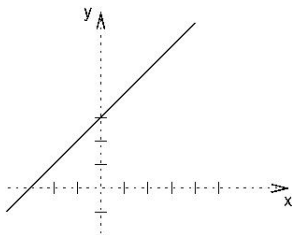
z	0	1	2	3	4	5	6
$1 : z$	0	1	4, da $4 \cdot 2 = 8 \equiv 1$	5	2	3	6

Dann ist z.B.:

$$\frac{5}{3} \cdot 3 = 5 \cdot \frac{1}{3} \cdot 3 \equiv 5 \cdot 5 \cdot 3 = 75 = 70 + 5 = 10 \cdot 7 + 5 \equiv 5.$$

Geometrie über endlichen Körpern

Die Geradengleichung $y = x + 3$ über \mathbb{F}_5 :



über \mathbb{R}

Die Ebene \mathbb{R}^2 : ∞ viele Punkte.

Die Gerade: ∞ viele Punkte.

	0	1	2	3	4
0			•		
1				•	
2					•
3	•				
4		•			

über \mathbb{F}_5

Die Ebene: 25 Punkte.

Die Gerade: 5 Punkte.

Rechnen auf elliptischen Kurven (über \mathbb{R})

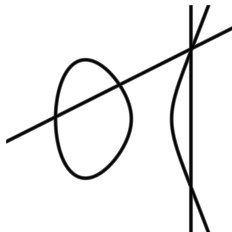


$$y^2 = x^3 + ax + b.$$

(mit $4a^3 - 27b^2 \neq 0$).

- ▶ 0 ist kein echter Punkt, sondern ein ∞ oben gedachter.
- ▶ $P = (x, y) \Rightarrow -P = (x, -y)$.
- ▶ Ist $Q \neq 0$, so schneidet \overline{PQ} die Kurve in einem weiteren Punkt $R = (s, t)$. Wir setzen: $P + Q = -R$.
- ▶ Z.B.: ist: $P + 0 = P$, $P + (-P) = 0$.

Rechnen auf elliptischen Kurven (über \mathbb{R})

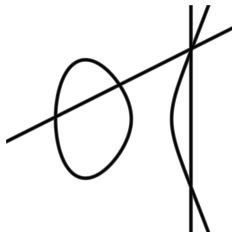


$$y^2 = x^3 + ax + b.$$

(mit $4a^3 - 27b^2 \neq 0$).

- ▶ 0 ist kein echter Punkt, sondern ein ∞ oben gedachter.
- ▶ $P = (x, y) \Rightarrow -P = (x, -y)$.
- ▶ Ist $Q \neq 0$, so schneidet \overline{PQ} die Kurve in einem weiteren Punkt $R = (s, t)$. Wir setzen: $P + Q = -R$.
- ▶ Z.B.: ist: $P + 0 = P$, $P + (-P) = 0$.

Rechnen auf elliptischen Kurven (über \mathbb{R})

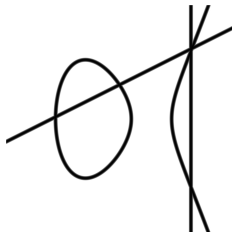


$$y^2 = x^3 + ax + b.$$

(mit $4a^3 - 27b^2 \neq 0$).

- ▶ 0 ist kein echter Punkt, sondern ein ∞ oben gedachter.
- ▶ $P = (x, y) \Rightarrow -P = (x, -y)$.
- ▶ Ist $Q \neq 0$, so schneidet \overline{PQ} die Kurve in einem weiteren Punkt $R = (s, t)$. Wir setzen: $P + Q = -R$.
- ▶ Z.B.: ist: $P + 0 = P$, $P + (-P) = 0$.

Rechnen auf elliptischen Kurven (über \mathbb{R})

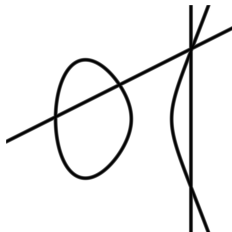


$$y^2 = x^3 + ax + b.$$

(mit $4a^3 - 27b^2 \neq 0$).

- ▶ 0 ist kein echter Punkt, sondern ein ∞ oben gedachter.
- ▶ $P = (x, y) \Rightarrow -P = (x, -y)$.
- ▶ Ist $Q \neq 0$, so schneidet \overline{PQ} die Kurve in einem weiteren Punkt $R = (s, t)$. Wir setzen: $P + Q = -R$.
- ▶ Z.B.: ist: $P + 0 = P$, $P + (-P) = 0$.

Rechnen auf elliptischen Kurven (über \mathbb{R})



$$y^2 = x^3 + ax + b.$$

(mit $4a^3 - 27b^2 \neq 0$).

- ▶ 0 ist kein echter Punkt, sondern ein ∞ oben gedachter.
- ▶ $P = (x, y) \Rightarrow -P = (x, -y)$.
- ▶ Ist $Q \neq 0$, so schneidet \overline{PQ} die Kurve in einem weiteren Punkt $R = (s, t)$. Wir setzen: $P + Q = -R$.
- ▶ Z.B.: ist: $P + 0 = P$, $P + (-P) = 0$.

Rechnen auf elliptischen Kurven (über \mathbb{F}_p)

Addition in Formeln

Sind $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, so setzen wir:

$$m = \frac{y_1 - y_2}{x_1 - x_2}, \quad \text{falls } x_1 \neq x_2.$$

Damit ist: $P_1 + P_2 = (m^2 - x_1 - x_2, -m(x_3 - x_1) - y_1)$.

Anwendung: Faktoren finden

$n \in \mathbb{N}$ große natürliche Zahl. Gibt es $p, q \neq 1$ mit $n = p \cdot q$?

Falls man über \mathbb{F}_n durch $x_1 - x_2$ nicht teilen kann, so hat man einen Faktor $\neq 1$ von n gefunden!

Bsp: $n = 12$ und $n = \text{RSA-200}$ (eine Fastprimzahl) im Jahr 2005 zerlegt, 2 Jahre auf mehreren Rechnern.

Anwendung: Entschlüsselung geheimer Nachrichten.

Rechnen auf elliptischen Kurven (über \mathbb{F}_p)

Addition in Formeln

Sind $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, so setzen wir:

$$m = \frac{y_1 - y_2}{x_1 - x_2}, \quad \text{falls } x_1 \neq x_2.$$

Damit ist: $P_1 + P_2 = (m^2 - x_1 - x_2, -m(x_3 - x_1) - y_1)$.

Anwendung: Faktoren finden

$n \in \mathbb{N}$ große natürliche Zahl. Gibt es $p, q \neq 1$ mit $n = p \cdot q$?

Falls man über \mathbb{F}_n durch $x_1 - x_2$ nicht teilen kann, so hat man einen Faktor $\neq 1$ von n gefunden!

Bsp: $n = 12$ und $n = \text{RSA-200}$ (eine Fastprimzahl) im Jahr 2005 zerlegt, 2 Jahre auf mehreren Rechnern.

Anwendung: Entschlüsselung geheimer Nachrichten.

Rechnen auf elliptischen Kurven (über \mathbb{F}_p)

Addition in Formeln

Sind $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, so setzen wir:

$$m = \frac{y_1 - y_2}{x_1 - x_2}, \quad \text{falls } x_1 \neq x_2.$$

Damit ist: $P_1 + P_2 = (m^2 - x_1 - x_2, -m(x_3 - x_1) - y_1)$.

Anwendung: Faktoren finden

$n \in \mathbb{N}$ große natürliche Zahl. Gibt es $p, q \neq 1$ mit $n = p \cdot q$?

Falls man über \mathbb{F}_n durch $x_1 - x_2$ nicht teilen kann, so hat man einen Faktor $\neq 1$ von n gefunden!

Bsp: $n = 12$ und $n = \text{RSA-200}$ (eine Fastprimzahl) im Jahr 2005 zerlegt, 2 Jahre auf mehreren Rechnern.

Anwendung: Entschlüsselung geheimer Nachrichten.

Rechnen auf elliptischen Kurven (über \mathbb{F}_p)

Addition in Formeln

Sind $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, so setzen wir:

$$m = \frac{y_1 - y_2}{x_1 - x_2}, \quad \text{falls } x_1 \neq x_2.$$

Damit ist: $P_1 + P_2 = (m^2 - x_1 - x_2, -m(x_3 - x_1) - y_1)$.

Anwendung: Faktoren finden

$n \in \mathbb{N}$ große natürliche Zahl. Gibt es $p, q \neq 1$ mit $n = p \cdot q$?

Falls man über \mathbb{F}_n durch $x_1 - x_2$ nicht teilen kann, so hat man einen Faktor $\neq 1$ von n gefunden!

Bsp: $n = 12$ und $n = \text{RSA-200}$ (eine Fastprimzahl) im Jahr 2005 zerlegt, 2 Jahre auf mehreren Rechnern.

Anwendung: Entschlüsselung geheimer Nachrichten.

Rechnen auf elliptischen Kurven (über \mathbb{F}_p)

Addition in Formeln

Sind $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, so setzen wir:

$$m = \frac{y_1 - y_2}{x_1 - x_2}, \quad \text{falls } x_1 \neq x_2.$$

Damit ist: $P_1 + P_2 = (m^2 - x_1 - x_2, -m(x_3 - x_1) - y_1)$.

Anwendung: Faktoren finden

$n \in \mathbb{N}$ große natürliche Zahl. Gibt es $p, q \neq 1$ mit $n = p \cdot q$?

Falls man über \mathbb{F}_n durch $x_1 - x_2$ nicht teilen kann, so hat man einen Faktor $\neq 1$ von n gefunden!

Bsp: $n = 12$ und $n = \text{RSA-200}$ (eine Fastprimzahl) im Jahr 2005 zerlegt, 2 Jahre auf mehreren Rechnern.

Anwendung: Entschlüsselung geheimer Nachrichten.

Rechnen auf elliptischen Kurven (über \mathbb{F}_p)

Addition in Formeln

Sind $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, so setzen wir:

$$m = \frac{y_1 - y_2}{x_1 - x_2}, \quad \text{falls } x_1 \neq x_2.$$

Damit ist: $P_1 + P_2 = (m^2 - x_1 - x_2, -m(x_3 - x_1) - y_1)$.

Anwendung: Faktoren finden

$n \in \mathbb{N}$ große natürliche Zahl. Gibt es $p, q \neq 1$ mit $n = p \cdot q$?

Falls man über \mathbb{F}_n durch $x_1 - x_2$ nicht teilen kann, so hat man einen Faktor $\neq 1$ von n gefunden!

Bsp: $n = 12$ und $n = \text{RSA-200}$ (eine Fastprimzahl) im Jahr 2005 zerlegt, 2 Jahre auf mehreren Rechnern.

Anwendung: Entschlüsselung geheimer Nachrichten.

Konstruktion interessanter Flächen

Endliche Körper kann man auch verwenden, um interessante Flächen zu finden:

- ▶ Eine Fläche vom Grad 7 mit 99 Singularitäten (O.L., 2004)
- ▶ Ein exzeptioneller Mechanismus (Geiß/Schreyer, 2008).
- ▶ ... noch vieles weitere möglich. . .

Konstruktion interessanter Flächen

Endliche Körper kann man auch verwenden, um interessante Flächen zu finden:

- ▶ Eine Fläche vom Grad 7 mit 99 Singularitäten (O.L., 2004)
- ▶ Ein exzeptioneller Mechanismus (Geiß/Schreyer, 2008).
- ▶ ... noch vieles weitere möglich. . .

Konstruktion interessanter Flächen

Endliche Körper kann man auch verwenden, um interessante Flächen zu finden:

- ▶ Eine Fläche vom Grad 7 mit 99 Singularitäten (O.L., 2004)
- ▶ Ein exzeptioneller Mechanismus (Geiß/Schreyer, 2008).
- ▶ ... noch vieles weitere möglich. . .

Konstruktion interessanter Flächen

Endliche Körper kann man auch verwenden, um interessante Flächen zu finden:

- ▶ Eine Fläche vom Grad 7 mit 99 Singularitäten (O.L., 2004)
- ▶ Ein exzeptioneller Mechanismus (Geiß/Schreyer, 2008).
- ▶ ... noch vieles weitere möglich. . .

Zusammenfassung

Wir haben erfahren:

- ▶ Schön kann nicht nur ein Bild, sondern auch ein Beweis oder eine Formel sein.
- ▶ Geometrie ist wesentlich mehr als nur Gerade, Kreis, Kugel und Ebene.
- ▶ Es existieren viele Zusammenhänge zwischen zunächst sehr unterschiedlich erscheinenden Gebieten, insbesondere zur Verschlüsselung und Zahlentheorie.
- ▶ Es gibt noch viele, viele offene Fragen in der Geometrie bzw. in der Mathematik.
- ▶ Es macht viel Spaß, sich damit zu beschäftigen und noch mehr, einige davon selbst zu beantworten.

Zusammenfassung

Wir haben erfahren:

- ▶ Schön kann nicht nur ein Bild, sondern auch ein Beweis oder eine Formel sein.
- ▶ Geometrie ist wesentlich mehr als nur Gerade, Kreis, Kugel und Ebene.
- ▶ Es existieren viele Zusammenhänge zwischen zunächst sehr unterschiedlich erscheinenden Gebieten, insbesondere zur Verschlüsselung und Zahlentheorie.
- ▶ Es gibt noch viele, viele offene Fragen in der Geometrie bzw. in der Mathematik.
- ▶ Es macht viel Spaß, sich damit zu beschäftigen und noch mehr, einige davon selbst zu beantworten.

Zusammenfassung

Wir haben erfahren:

- ▶ Schön kann nicht nur ein Bild, sondern auch ein Beweis oder eine Formel sein.
- ▶ Geometrie ist wesentlich mehr als nur Gerade, Kreis, Kugel und Ebene.
- ▶ Es existieren viele Zusammenhänge zwischen zunächst sehr unterschiedlich erscheinenden Gebieten, insbesondere zur Verschlüsselung und Zahlentheorie.
- ▶ Es gibt noch viele, viele offene Fragen in der Geometrie bzw. in der Mathematik.
- ▶ Es macht viel Spaß, sich damit zu beschäftigen und noch mehr, einige davon selbst zu beantworten.

Zusammenfassung

Wir haben erfahren:

- ▶ Schön kann nicht nur ein Bild, sondern auch ein Beweis oder eine Formel sein.
- ▶ Geometrie ist wesentlich mehr als nur Gerade, Kreis, Kugel und Ebene.
- ▶ Es existieren viele Zusammenhänge zwischen zunächst sehr unterschiedlich erscheinenden Gebieten, insbesondere zur Verschlüsselung und Zahlentheorie.
- ▶ Es gibt noch viele, viele offene Fragen in der Geometrie bzw. in der Mathematik.
- ▶ Es macht viel Spaß, sich damit zu beschäftigen und noch mehr, einige davon selbst zu beantworten.

Zusammenfassung

Wir haben erfahren:

- ▶ Schön kann nicht nur ein Bild, sondern auch ein Beweis oder eine Formel sein.
- ▶ Geometrie ist wesentlich mehr als nur Gerade, Kreis, Kugel und Ebene.
- ▶ Es existieren viele Zusammenhänge zwischen zunächst sehr unterschiedlich erscheinenden Gebieten, insbesondere zur Verschlüsselung und Zahlentheorie.
- ▶ Es gibt noch viele, viele offene Fragen in der Geometrie bzw. in der Mathematik.
- ▶ Es macht viel Spaß, sich damit zu beschäftigen und noch mehr, einige davon selbst zu beantworten.

Zusammenfassung

Wir haben erfahren:

- ▶ Schön kann nicht nur ein Bild, sondern auch ein Beweis oder eine Formel sein.
- ▶ Geometrie ist wesentlich mehr als nur Gerade, Kreis, Kugel und Ebene.
- ▶ Es existieren viele Zusammenhänge zwischen zunächst sehr unterschiedlich erscheinenden Gebieten, insbesondere zur Verschlüsselung und Zahlentheorie.
- ▶ Es gibt noch viele, viele offene Fragen in der Geometrie bzw. in der Mathematik.
- ▶ Es macht viel Spaß, sich damit zu beschäftigen und noch mehr, einige davon selbst zu beantworten.

Vielen Dank...

für Ihre Aufmerksamkeit!

Oliver Labs

Vortrag zum Nachlesen auf:

www.OliverLabs.net

Weitere Bilder, Hintergrund-Informationen und unsere
Visualisierungs-Software *surfer* auf:

www.Imaginary2008.de

Weitere Bilder / Filme / Software zu algebraischen Flächen auf:

www.AlgebraicSurface.net