Rationale Punkte auf algebraischen Kurven

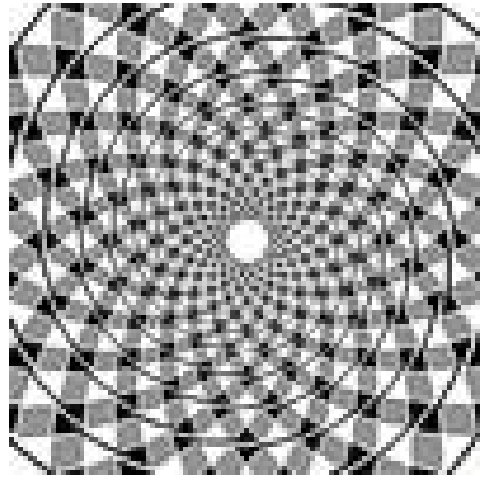
THOMAS CHRIST, JÖRN STEUDING (Uni Würzburg)

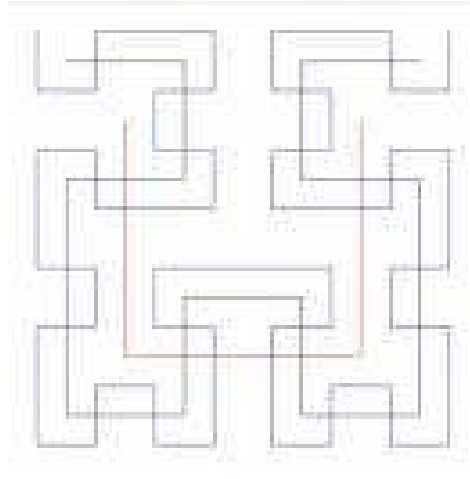
Würzburg, den 7. Oktober 2009

– W-Seminare –

Kurven

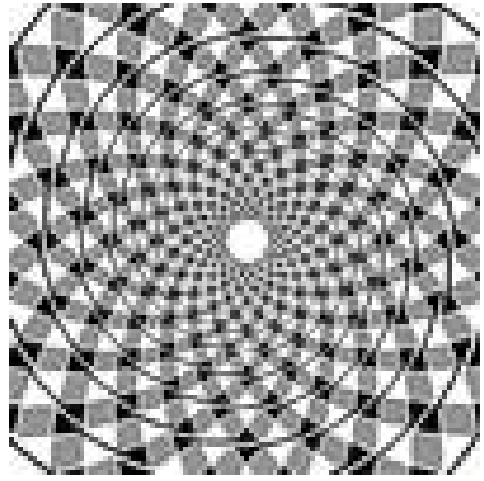
Kurven begegnen uns in allen Lebenslagen...

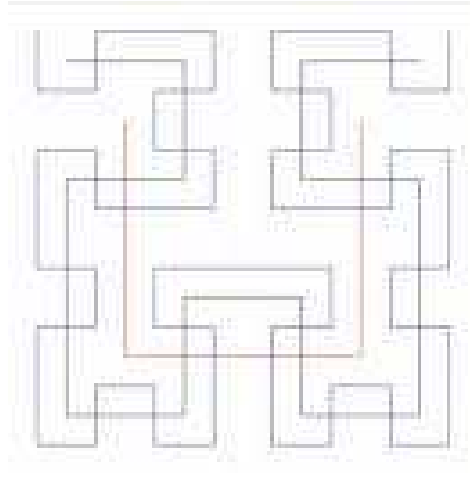




Kurven

Kurven begegnen uns in allen Lebenslagen...

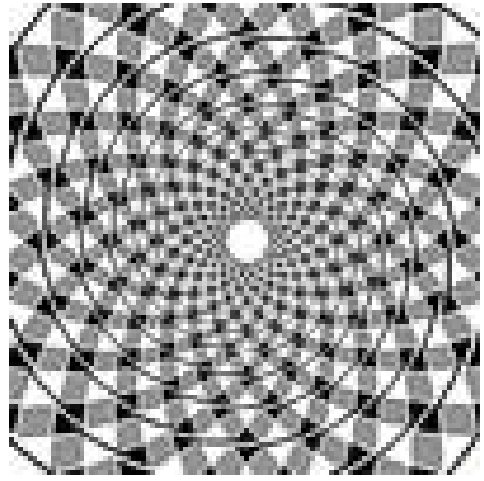


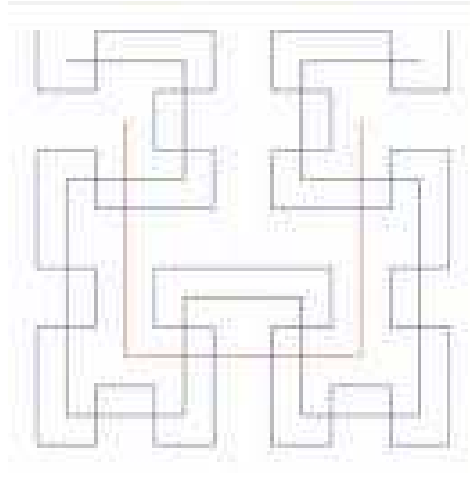


...aber nicht alle Kurven sind algebraisch!

Kurven

Kurven begegnen uns in allen Lebenslagen...



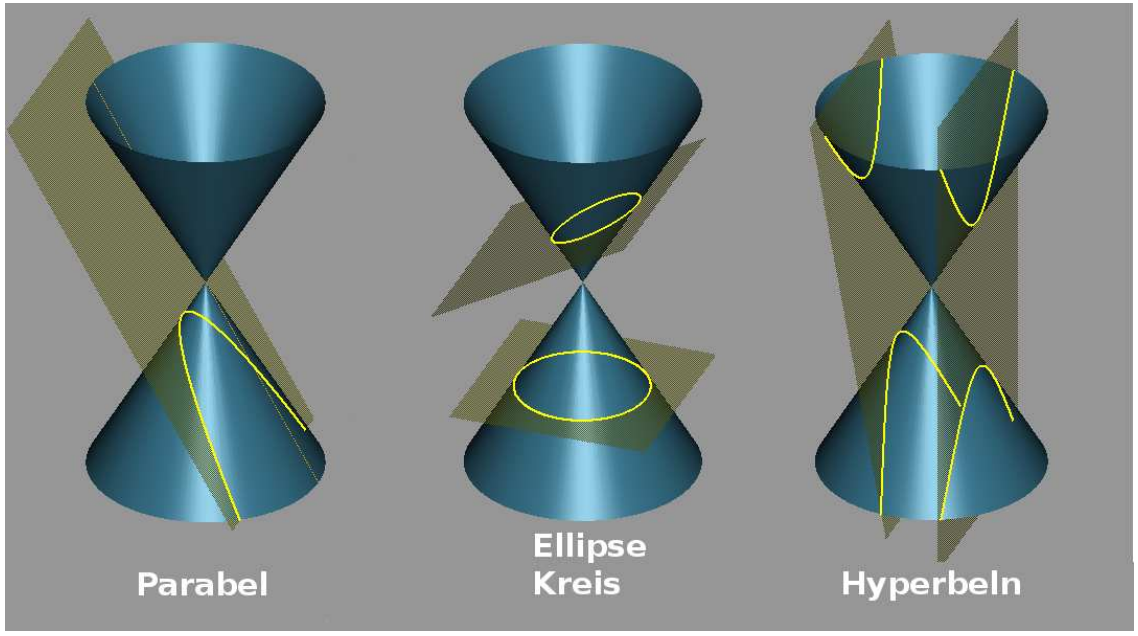


...aber nicht alle Kurven sind algebraisch!

Rechts: die ersten drei Generationen der Hilbert-Kurve (ein stetiges, den Raum füllendes Bild eines Intervalls); mehr über raumfüllende Kurven lernt man bei Michael Bader (http://www5.in.tum.de/lehre/vorlesungen/algowiss/ss04/vorlesung/rfk.pdf)

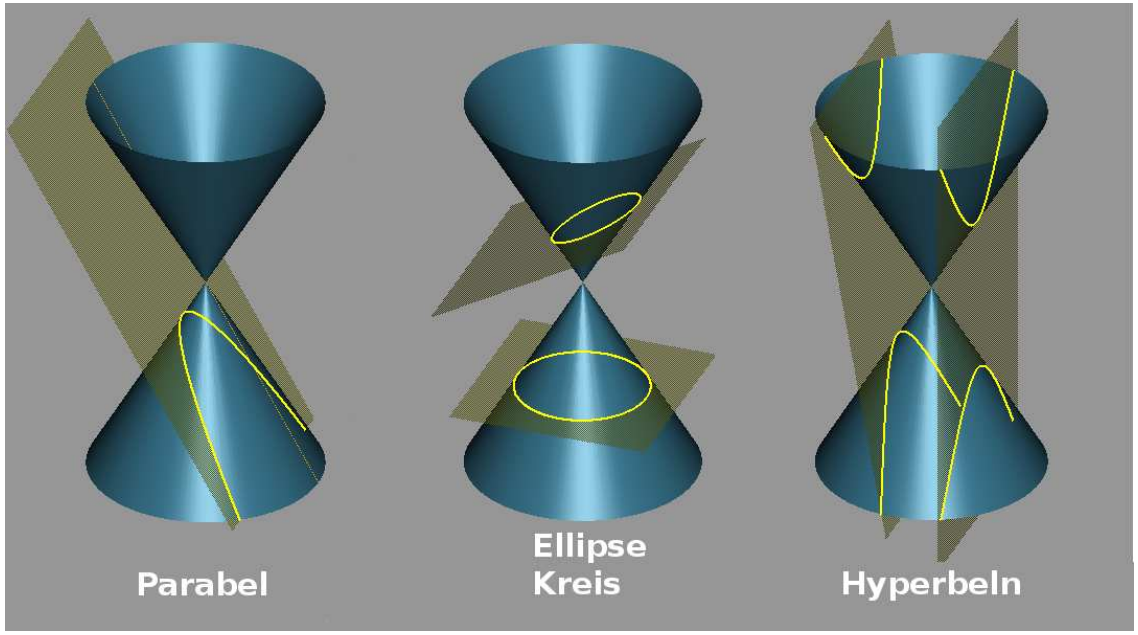
Algebraische Kurven

sind uns die liebsten! Sie lassen sich als **Nullstellengebilde von Polynomen** beschreiben:



Algebraische Kurven

sind uns die liebsten! Sie lassen sich als **Nullstellengebilde von Polynomen** beschreiben:



Ellipse: $(X/a)^2 + (Y/b)^2 = 1$ — Planeten bewegen sich auf elliptischen Bahnen **(Kepler)**.
Parabel: $Y = aX^2$ — Flanken im Fußball sind Parabeln **(Kaltz).**
Hyperbel: $X^2 - dY^2 = 1$ — Bögen in der Architektur **(Gaudí).**

All diese Beispiele treten als Kegelschnitte auf!

Dieser Vortrag ist im Internet erhältlich unter

http://www.mathematik.uni-wuerzburg.de/∼steuding/

Bei Fragen melden Sie sich bitte per email an

steuding@mathematik.uni-wuerzburg.de

1. Beispiel

Bereits mit den einfachsten algebraischen Kurven

— Gerade und Kreis —

lassen sich interessante rationale Punkte entdecken!

Pythagoräische Tripel

Rechtwinklige Dreiecke mit ganzzahligen Seitenlängen sind nützlich bei der **Konstruktion rechter Winkel**: Z.B.

$$3^2 + 4^2 = 5^2, \quad 5^2 + 12^2 = 13^2, \quad \ldots$$

Pythagoräische Tripel

Rechtwinklige Dreiecke mit ganzzahligen Seitenlängen sind nützlich bei der **Konstruktion rechter Winkel**: Z.B.

$$3^2 + 4^2 = 5^2, \quad 5^2 + 12^2 = 13^2, \quad \ldots$$

Euklid: Alle pythagoräischen Tripel (a, b, c) sind gegeben durch

$$a = k^2 - \ell^2, \quad b = 2k\ell, \quad c = k^2 + \ell^2 \qquad (k > \ell \text{ ganzzahlig}).$$

Z.B. $k = 2, \ell = 1$ gibt das Tripel $a = 3, b = 4, c = 5$.

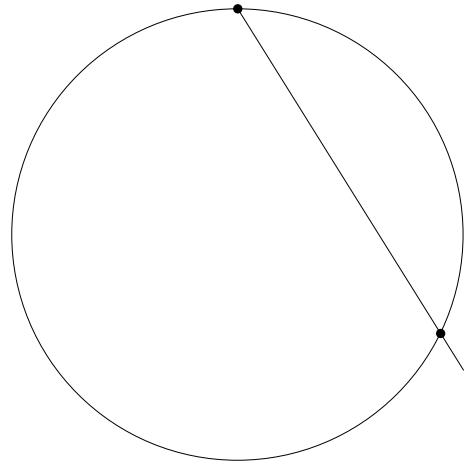
Insbesondere gibt es unendlich viele pythagoräische Tripel!

Pythagoräische Tripel – Beweis

Pythag. Tripel $(a, b, c) \leftrightarrow$ rationale Lösungen u, v von $U^2 + V^2 = 1$

Pythagoräische Tripel – Beweis

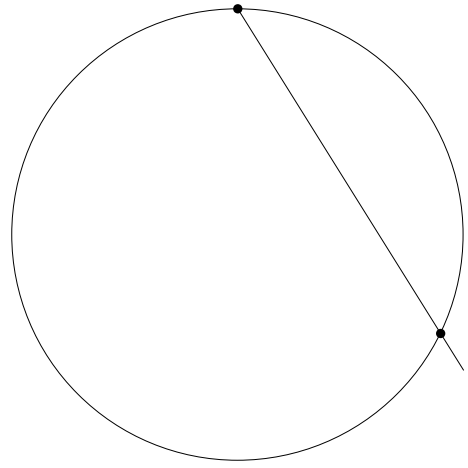
Pythag. Tripel $(a, b, c) \leftrightarrow$ rationale Lösungen u, v von $U^2 + V^2 = 1$



Die rationalen Lösungen entstehen alle durch Schnitt des **Kreises** $U^2 + V^2 = 1$ mit den Geraden $V = mU + 1$ mit Steigung $m \in \mathbb{Q}^*$.

Pythagoräische Tripel – Beweis

Pythag. Tripel (a, b, c) $\leftrightarrow$ rationale Lösungen u, v von $U^2 + V^2 = 1$



Die rationalen Lösungen entstehen alle durch Schnitt des **Kreises** $U^2 + V^2 = 1$ mit den Geraden $V = mU + 1$ mit Steigung $m \in \mathbb{Q}^*$.

Der Schnittpunkt hat die Koordinaten $(u, v) = (\frac{-2m}{m^2+1}, \frac{1-m^2}{m^2+1})$.

Mit $m = \frac{k}{\ell}$ ergeben sich die pythagoräischen Tripel.

Im Bild $(u, v) = (\frac{80}{89}, -\frac{39}{89}) \leftrightarrow (a, b, c) = (39, 80, 89)$.

Die Fermatsche Vermutung

Pierre de Fermat, $* 1607(?) - \dagger 1665$

Hobbymathematiker und Jurist in Toulouse

Die Fermatsche Vermutung

Pierre de Fermat, $* 1607(?) - \dagger 1665$

Hobbymathematiker und Jurist in Toulouse

Gibt es ganze Zahlen x, y, z mit

$$x^n + y^n = z^n \ , \qquad \text{wobei} \quad n \geq 3,$$

dann ist $xyz = 0$. Nur triviale Lösungen im Gegensatz zu den pythagoräischen Tripeln bei $n = 2$!

Die Fermatsche Vermutung

Pierre de Fermat, $* 1607(?) - \dagger 1665$

Hobbymathematiker und Jurist in Toulouse

Gibt es ganze Zahlen x, y, z mit

$$x^n + y^n = z^n \ , \qquad \text{wobei} \quad n \geq 3,$$

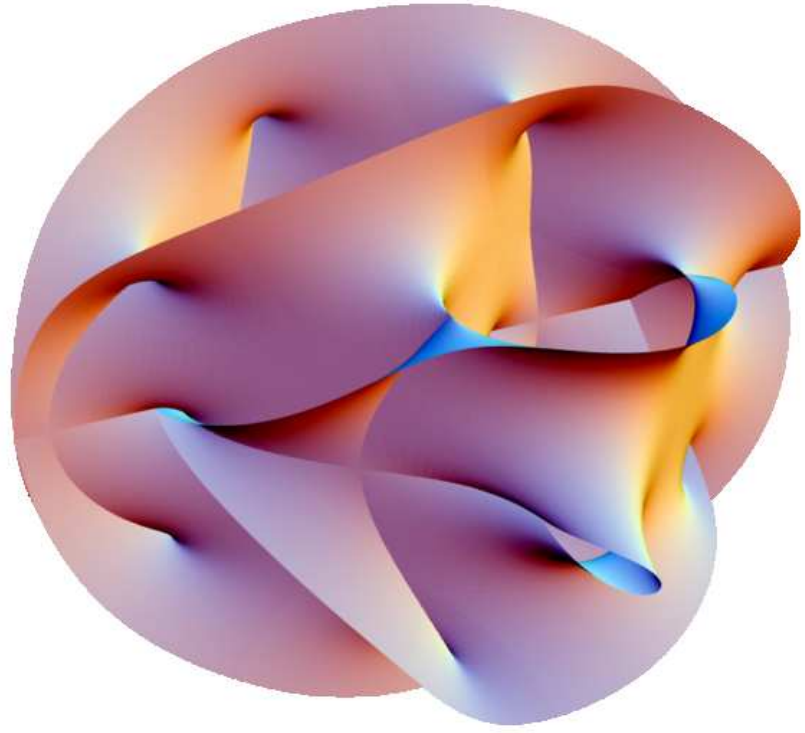
dann ist $xyz = 0$. Nur triviale Lösungen im Gegensatz zu den pythagoräischen Tripeln bei $n = 2$!

Leider hatte **Fermat** keinen Platz, seinen 'wunderbaren Beweis' aufzuschreiben...
Vermutlich glaubte er, dass sein Beweis für $n = 4$ allgemein gültig wäre.
Andrew Wiles bewies 1995 die Fermatsche Vermutung mit Hilfe von elliptischen Kurven!

Ästhetik

Die Fermat-Kurve für den Exponenten $n = 5$: Keine rationalen Punkte!

(Der Beweis ist schwierig!)



Wie macht man solche schönen Bilder? Computeralgebra: MATHEMATICA; Maple...

2. Beispiel

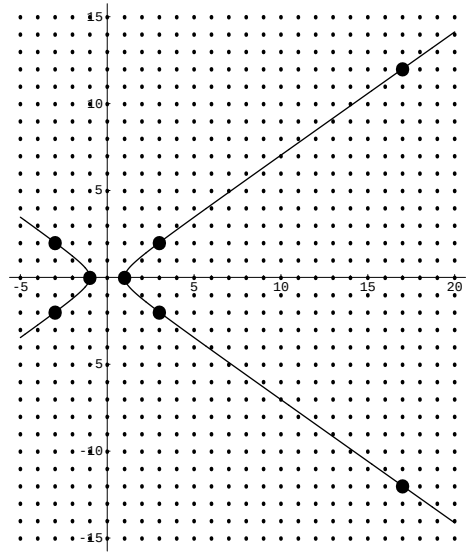
Etwas schwierigere Beispiele algebraischer Kurven sind

Hyperbeln

Besitzen auch diese rationale Punkte?

Die Pellsche Gleichung

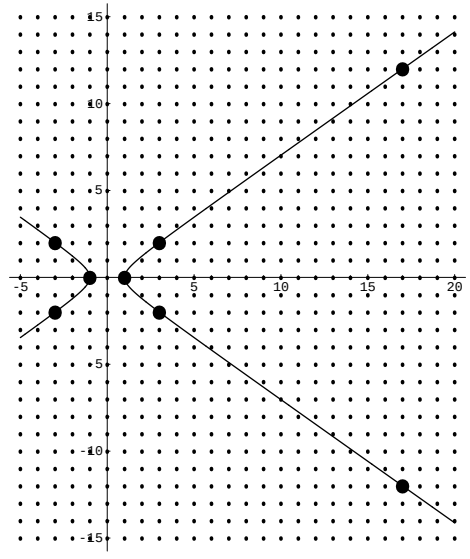
$X^2 - dY^2 = 1$ mit $d \in \mathbb{N}$ quadratfrei.



$X^2 - 2Y^2 = 1$ – geometrisch: eine Hyperbel!

Die Pellsche Gleichung

$X^2 - dY^2 = 1$ mit $d \in \mathbb{N}$ quadratfrei.

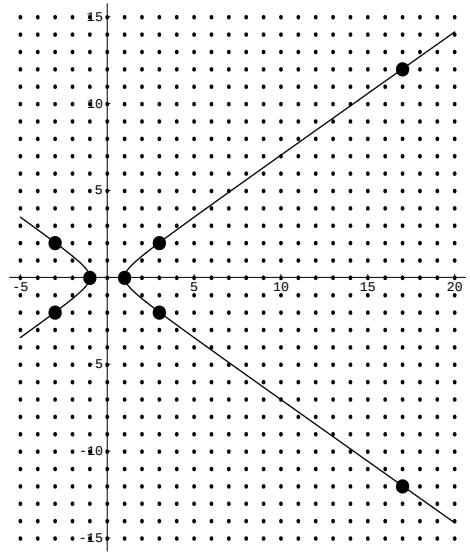


$X^2 - 2Y^2 = 1$ – geometrisch: eine Hyperbel!

Gesucht: Lösungen x, y in $\mathbb{Z}$ bzw. $\mathbb{N}$?

Die Pellsche Gleichung

$X^2 - dY^2 = 1$ mit $d \in \mathbb{N}$ quadratfrei.



$X^2 - 2Y^2 = 1$ – geometrisch: eine Hyperbel!

Gesucht: Lösungen x, y in $\mathbb{Z}$ bzw. $\mathbb{N}$?

Triviale Lösungen: $x = \pm 1, y = 0$;

Symmetrie: Mit (x, y) lösen auch $(\pm x, \pm y)$.

Einer für alle

Gegeben eine Lösung, z.B.

$$x = 3,\ y = 2 \qquad (3^2 - 2 \cdot 2^2 = 1),$$

entstehen weitere Lösungen durch Potenzieren:

$$(3 + 2\sqrt{2})^2 = 17 + 12\sqrt{2} \qquad \text{und} \qquad 17^2 - 2 \cdot 12^2 = 1.$$

Tatsächlich entstehen so alle Lösungen!

Einer für alle

Gegeben eine Lösung, z.B.

$$x = 3,\ y = 2 \qquad (3^2 - 2 \cdot 2^2 = 1),$$

entstehen weitere Lösungen durch Potenzieren:

$$(3 + 2\sqrt{2})^2 = 17 + 12\sqrt{2} \qquad \text{und} \qquad 17^2 - 2 \cdot 12^2 = 1.$$

Tatsächlich entstehen so alle Lösungen! U.a.

$$(3 + 2\sqrt{2})^3 = 99 + 70\sqrt{2} \qquad \text{und} \qquad 99^2 - 2 \cdot 70^2 = 1,$$

Es ist kein Zufall, dass $\frac{99}{70}$ das Länge–Breite-Verhältnis von **Din A4** ist! ($\approx \sqrt{2}$).

Einer für alle

Gegeben eine Lösung, z.B.

$$x = 3,\ y = 2 \qquad (3^2 - 2 \cdot 2^2 = 1),$$

entstehen weitere Lösungen durch Potenzieren:

$$(3 + 2\sqrt{2})^2 = 17 + 12\sqrt{2} \qquad \text{und} \qquad 17^2 - 2 \cdot 12^2 = 1.$$

Tatsächlich entstehen so alle Lösungen! U.a.

$$(3 + 2\sqrt{2})^3 = 99 + 70\sqrt{2} \qquad \text{und} \qquad 99^2 - 2 \cdot 70^2 = 1,$$

Es ist kein Zufall, dass $\frac{99}{70}$ das Länge–Breite-Verhältnis von **Din A4** ist! ($\approx \sqrt{2}$).

Aber wie findet man rationalen oder sogar ganzzahligen Punkt?

Die kleinste Lösung von $X^2 - 61Y^2 = 1$ in natürlichen Zahlen ist

$$x = 1\,766\,319\,049, \qquad y = 226\,153\,980.$$

3. Beispiel

Mit den rationalen Punkten auf

Elliptische Kurven

kann man addieren wie mit Zahlen!

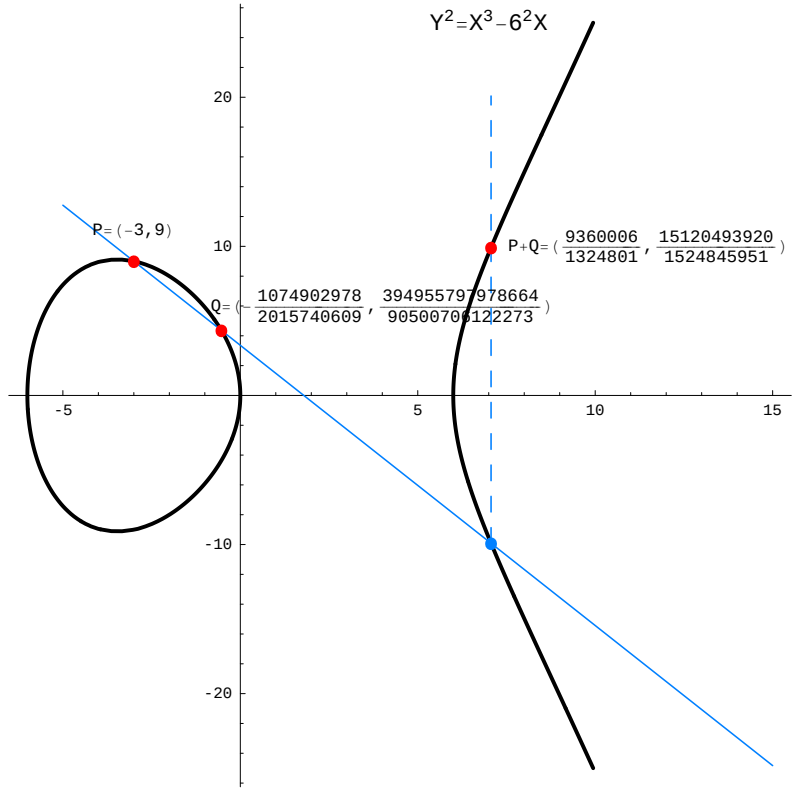
Was sind elliptische Kurven?

Topologisch: donuts!

Algebraisch definiert durch

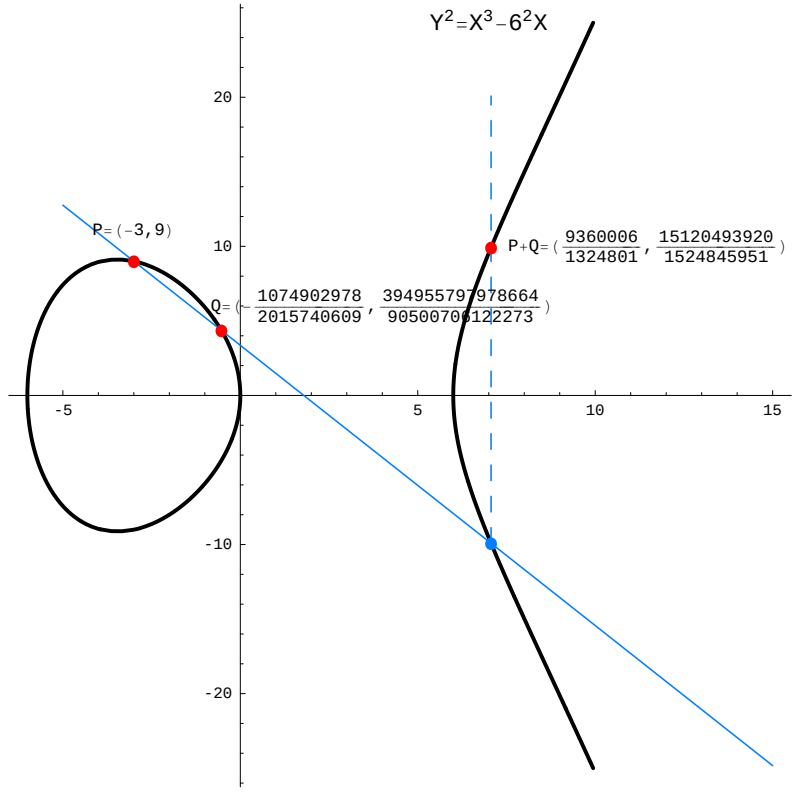
$$Y^2 = X^3 + aX + b \quad \text{für gewisse } a, b \in \mathbb{Q}.$$

Addition auf elliptischen Kurven



$$(-3,9) \oplus (\frac{1074902978}{2015740609}, \frac{394955797978664}{90500706122273}) = (\frac{9360006}{1324801}, \frac{15120493920}{1524845951})$$

Addition auf elliptischen Kurven



$$(-3,9) \oplus (\frac{1074902978}{2015740609}, \frac{394955797978664}{90500706122273}) = (\frac{9360006}{1324801}, \frac{15120493920}{1524845951})$$

Durch Addition rationaler Punkte gewinnt man neue rationale Punkte...

Dies hat Anwendungen in der Kryptographie!

Mögliche Struktur des Seminars

I. Grundlagen: Elementare Zahlentheorie (incl. modularer Arithmetik) / Die rationalen Zahlen und die reellen Irrationalzahlen $\mathbb{Q}$ vs. $\mathbb{R}$ / Wissenswertes über Polynome

Mögliche Struktur des Seminars

I. Grundlagen: Elementare Zahlentheorie (incl. modularer Arithmetik) / Die rationalen Zahlen und die reellen Irrationalzahlen $\mathbb{Q}$ vs. $\mathbb{R}$ / Wissenswertes über Polynome

II. Beispiele algebraischer Kurven: Lineare diophantische Gleichungen / analytische Geometrie und Kegelschnitte / Die Pellsche Gleichung / Pythagoräische Tripel und die Fermat-Gleichung

Mögliche Struktur des Seminars

I. Grundlagen: Elementare Zahlentheorie (incl. modularer Arithmetik) / Die rationalen Zahlen und die reellen Irrationalzahlen $\mathbb{Q}$ vs. $\mathbb{R}$ / Wissenswertes über Polynome

II. Beispiele algebraischer Kurven: Lineare diophantische Gleichungen / analytische Geometrie und Kegelschnitte / Die Pellsche Gleichung / Pythagoräische Tripel und die Fermat-Gleichung

III. Elliptische Kurven: Theorie über $\mathbb{Q}$ / Theorie über endlichen Körpern / Anwendungen: Faktorisieren, Primzahltests, Kryptographie (mit Computereinsatz)

Mögliche Struktur des Seminars

I. Grundlagen: Elementare Zahlentheorie (incl. modularer Arithmetik) / Die rationalen Zahlen und die reellen Irrationalzahlen $\mathbb{Q}$ vs. $\mathbb{R}$ / Wissenswertes über Polynome

II. Beispiele algebraischer Kurven: Lineare diophantische Gleichungen / analytische Geometrie und Kegelschnitte / Die Pellsche Gleichung / Pythagoräische Tripel und die Fermat-Gleichung

III. Elliptische Kurven: Theorie über $\mathbb{Q}$ / Theorie über endlichen Körpern / Anwendungen: Faktorisieren, Primzahltests, Kryptographie (mit Computereinsatz)

IV. Allgemeine Theorie algebraischer Kurven: Singularitäten / Hilbertscher Nullstellensatz(?) / Diskussion des Satzes von Faltings (ohne Beweis)

Mögliche Literatur

- **J. Steuding:** Elementare Zahlentheorie [Zahlbereiche / diophantische Gleichungen (incl. pythag. Tripel und die Fermat-Glg. / Pellsche Gleichung]
  www.mathematik.uni-wuerzburg.de/∼steuding/elemzahltheo.htm (ab Ende Oktober!)
- **St. Reith, J. Steuding:** Elliptische Kurven mit Anwendungen in der Kryptographie [Theorie (über $\mathbb{Q}$ und endlichen Körpern) und Praxis (Faktorisieren, Primzahltests, Kryptographie)]
  www.mathematik.uni-wuerzburg.de/∼steuding/Elliptic.htm (ab Ende Oktober!)
- **G. Fischer:** Ebene algebraische Kurven [Spezielle algebraische Kurven (Zykloiden) / Varietäten / Singularitäten / Satz von Bézout / allgemeine Theorie] Vieweg 1994
- **G. Fischer:** Analytische Geometrie [Elementargeometrie / Kegelschnitte] Vieweg 2001, 7. Auflage
- **W.P. Barth:** Ebene algebraische Kurven [Grundlagen / Singularitäten / Schnittzahlen und der Satz von Bézout / Kubiken] via www.mi.uni-erlangen.de/ barth/skripten.shtml

Notwendiges

Die Schüler benötigen **Begabung**, Motivation und Ausdauer!

Ohne Begeisterung besteht keine Disziplin, sich eingehend mit einem Problem zu beschäftigen **– die Mathematik des W-Seminars ist aber teilweise schwieriger als die übliche Schulmathematik!**

Notwendiges

Die Schüler benötigen **Begabung**, Motivation und Ausdauer!

Ohne Begeisterung besteht keine Disziplin, sich eingehend mit einem Problem zu beschäftigen **– die Mathematik des W-Seminars ist aber teilweise schwieriger als die übliche Schulmathematik!**

Kaum Vorkenntnisse!

Der kanonische Schulstoff ist ausreichend; schön wären Vorkenntnisse über analytische Geometrie und elementare Zahlentheorie und einige Beweiskonzepte (z.B. indirekter Beweis). Falls nicht bekannt, so könnte dies auch thematisiert werden!

Notwendiges

Die Schüler benötigen **Begabung**, Motivation und Ausdauer!

Ohne Begeisterung besteht keine Disziplin, sich eingehend mit einem Problem zu beschäftigen **– die Mathematik des W-Seminars ist aber teilweise schwieriger als die übliche Schulmathematik!**

Kaum Vorkenntnisse!

Der kanonische Schulstoff ist ausreichend; schön wären Vorkenntnisse über analytische Geometrie und elementare Zahlentheorie und einige Beweiskonzepte (z.B. indirekter Beweis). Falls nicht bekannt, so könnte dies auch thematisiert werden!

Beispiel eines Teilprojektes:

Ein**e** Schüler**in** beschäftigt sich mit pythagoräischen Tripeln und stellt dieses Thema der Gruppe vor: Beweis des Satzes von Euklid / Computerprogramm zur Erstellung pyth. Tripel / Anwendungen pyth. Tripel in und ausserhalb der Mathematik

Résumé

- Mathematik ist schwierig, aber gerade deshalb spannend!
- Mathematik ist unglaublich nützlich und universell einsetzbar!
- Mathematik ist Anwendung und Grundlagenforschung!

Résumé

- Mathematik ist schwierig, aber gerade deshalb spannend!

  Andrew Wiles löst 1995 nach über 350 Jahren die Fermatsche Vermutung.

- Mathematik ist unglaublich nützlich und universell einsetzbar!

- Mathematik ist Anwendung und Grundlagenforschung!

Résumé

- Mathematik ist schwierig, aber gerade deshalb spannend!

  Andrew Wiles löst 1995 nach über 350 Jahren die Fermatsche Vermutung.

- Mathematik ist unglaublich nützlich und universell einsetzbar!

  Kegelschnitte werden in Architektur und Ingenieurswissenschaften eingesetzt.

- Mathematik ist Anwendung und Grundlagenforschung!

Résumé

- Mathematik ist schwierig, aber gerade deshalb spannend!

  Andrew Wiles löst 1995 nach über 350 Jahren die Fermatsche Vermutung.

- Mathematik ist unglaublich nützlich und universell einsetzbar!

  Kegelschnitte werden in Architektur und Ingenieurswissenschaften eingesetzt.

- Mathematik ist Anwendung und Grundlagenforschung!

  In der modernen Kryptographie werden seit 1986 elliptische Kurven benutzt.

Dieser Vortrag ist im Internet erhältlich unter

http://www.mathematik.uni-wuerzburg.de/∼steuding/

Bei Fragen melden Sie sich bitte per email an

steuding@mathematik.uni-wuerzburg.de

Vielen Dank!