Berechnungen zur Geometrie und Arithmetik algebraischer Flächen

Andreas-Stephan Elsenhans

Universität Paderborn

5. Mai 2017

Gemeinsame Arbeit mit J. Jahnel.

Algebraische Varietäten

Definition
Eine algebraische Varietät ist die Lösungsmenge eines polynomiellen Gleichungssystems im affinen oder projektiven Raum.

Beispiele

- Der affine Raum K^n.
- Der projektive Raum

$$\mathbf{P}^n(K) = \{[x_0 : x_1 : \ldots : x_n] : (x_0, \ldots, x_n) \in K^n \setminus \{0\}\}.$$

- Eine Quadrik im $\mathbf{P}^2$, etwa $X^2 + Y^2 = Z^2$.
- Eine kubische Kurve in K^2, etwa $Y^2 = X^3 + X + 3$.

Punktanzahlen
In den reellen oder komplexen Zahlen haben obige Mengen unendlich viele Punkte.

Endliche Körper

Satz
Der Restklassenring $\mathbb{Z}/n\mathbb{Z}$ ist genau dann ein Körper, wenn n eine Primzahl ist.

Satz
Ist q die Potenz einer Primzahl, so gibt es genau einen Körper mit q Elementen. Sonst gibt es keinen Körper mit q Elementen.

Notation
$\mathbb{F}_q$ der Körper mit $q = p^d$ Elementen. $\mathrm{Frob}_p \colon x \mapsto x^p$ erzeugt $\mathrm{Aut}(\mathbb{F}_q)$.

Bemerkung
Über endlichen Körpern haben algebraische Varietäten nur endlich viele Punkte.

Punktanzahlen I

Satz
Der affine Raum $\mathbb{F}_q^n$ hat q^n Punkte.

Satz
Der projektive Raum $\mathbf{P}^n(\mathbb{F}_q)$ hat $q^n + q^{n-1} + \cdots + q + 1$ Punkte.

Beweis:

$$\begin{aligned}\mathbf{P}^n(\mathbb{F}_q) = \quad & \{[1 : a_1 : a_2 : \cdots : a_n] \mid a_i \in \mathbb{F}_q\} \\ & \cup \{[0 : 1 : a_2 : \cdots : a_n] \mid a_i \in \mathbb{F}_q\} \\ & \vdots \\ & \cup \{[0 : \ldots : 0 : 1 : a_n] \mid a_i \in \mathbb{F}_q\} \\ & \cup \{[0 : \ldots : 0 : 1]\}.\end{aligned}$$

□

Quadratische Flächen

Definition
Eine quadratische Fläche ist die Nullstellenmenge einer quaternären quadratischen Form in $\mathbf{P}^3(K)$.

Satz
Ist $2 \neq 0$ in K, so kann jede quadratische Form über K durch lineare Transformationen diagonalisiert werden.

Ergebnis
Wir müssen nur Diagonalformen $aX^2 + bY^2 + cZ^2 + dW^2 = 0$ betrachten.
Die Fläche ist glatt, wenn kein Koeffizient null ist.
Die Koeffizienten können beliebig um Quadrate abgeändert werden.

Satz
Es gibt genau 2 Klassen glatter quadratischer Flächen über einem endlichen Körper mit $2 \neq 0$. Diese sind durch $abcd = \square$ und $abcd \neq \square$ gegeben. $16abcd$ ist die *Diskriminante* der quadratischen Form.

Punktanzahlen quadratischer Flächen

Satz
Es gilt

$$\#V(\mathbb{F}_p) = p^2 + 2p + 1 \text{ oder } p^2 + 1\,,$$

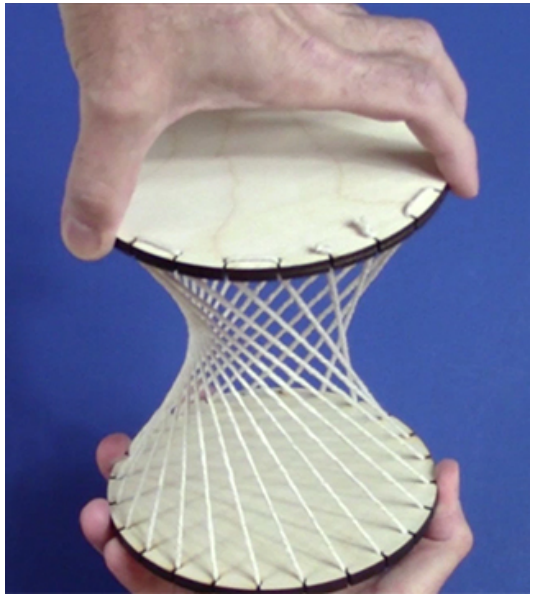
je nachdem ob die Diskriminante ein Quadrat bzw. kein Quadrat ist.

Beweis:
Durch Rechnen mit Charaktersummen oder unter Verwendung der Theorie quadratischer Formen.

Satz
Eine glatte quadratische Fläche hat zwei Familien von Geraden.

Satz
Sei V eine glatte quadratische Fläche über einem endlichen Körper K mit $2 \neq 0$. Die Geraden sind genau dann über K definiert, wenn die Diskriminante ein Quadrat ist.

Geraden auf quadratischen Flächen



Beispiel

Gleichung
$E_1 : Y^2 = X^3 + X + 3$

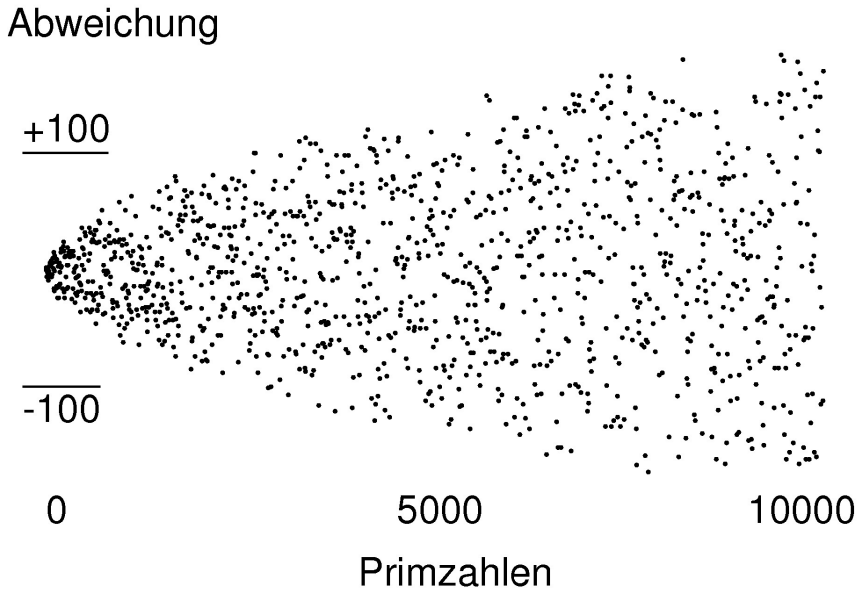
Experiment
Zähle die Punkte $E_1(\mathbb{Z}/p\mathbb{Z})$:

p	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$\#E_1$	2	3	3	5	17	14	16	20	26	35	40	38	38	46	53

Beobachtung
Modulo p hat die Gleichung etwa p Lösungen.

Heuristische Erklärung
Wir nehmen die Werte von $x^3 + x + 3$ als gleichverteilt in K an. Trifft man ein Quadrat, so hat man 2 Punkte auf der Kurve, sonst keinen. Die Hälfte der Elemente von $K^\times$ sind Quadrate.

$E_1 : Y^2 = X^3 + X + 3$ – Abweichungen der Anzahlen



Streuung der Punktanzahl

Satz (Hasse)
Es gilt

$$|q - \#E(\mathbb{F}_q)| \leq 2\sqrt{q}$$

für jede glatte affine Kurve E der Form $Y^2 = X^3 + aX^2 + bX + c$ und jeden Körper $\mathbb{F}_q$.

Experiment

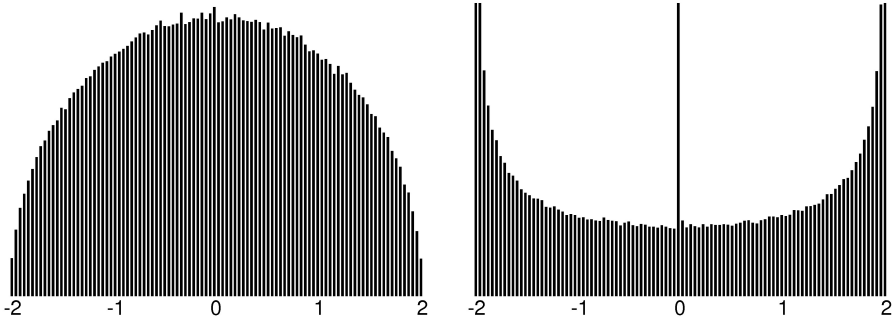
$$E_1 : y^2 = x^3 + x + 3$$
$$E_2 : y^2 = x^3 - 17$$

Experiment:
Verteilung von

$$\frac{p - \#E_i(\mathbb{F}_p)}{\sqrt{p}}$$

für alle Primzahlen $p < 10^7$, $i = 1, 2$.

Histogramm $\frac{p-\#E_i(\mathbb{F}_q)}{\sqrt{p}}$



$$E_1 : y^2 = x^3 + x + 3$$
$$j(E_1) = \frac{55296}{275}$$

$$E_2 : y^2 = x^3 - 17$$
$$j(E_2) = 0$$

(664579 Primzahlen, 100 Gruppen)

Die Kurve $Y^2 = X^3 - C$

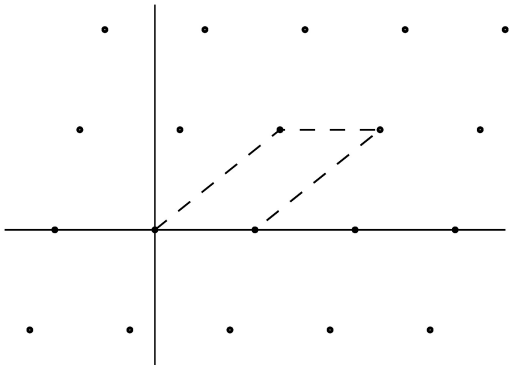
Gleichung
E_C: $Y^2 = X^3 - C$

Dritte Einheitswurzeln
$\zeta_3 := \exp\left(\frac{2\pi i}{3}\right)$, $\zeta_3^3 = 1$

Automorphismus
$(X, Y) \mapsto (\zeta_3 X, Y)$ ist Automorphismus von E_C.

Punktanzahl
Ist $p \equiv 2 \bmod 3$, so hat jede Zahl modulo p eine eindeutig bestimmte Kubikwurzel modulo p. D.h., zu jedem Wert von Y gibt es genau einen Wert von X, sodass (X, Y) auf E_C liegt.
Folglich hat E genau p Punkte, wenn $p \equiv 2 \bmod 3$ ist.

Kubische Kurven und Gitter in $\mathbb{C}$



Doppelt-periodische Funktionen
$f(z) = f(z+\lambda)$ für alle $\lambda \in \Lambda$.

Beispiel
Weierstrass-$\wp$-Funktion $\wp(z) = \frac{1}{z^2} + \sum_{\lambda \in \Lambda \setminus \{0\}} \frac{1}{(z+\lambda)^2} - \frac{1}{\lambda^2}$.

Struktur doppelt-periodischer Funktionen

Satz

- Jede Λ-periodische, meromorphe Funktion ist eine rationale Funktion in $\wp(z), \wp'(z)$.
- $\wp'(z)^2 = \wp(z)^3 - g_2\wp(z) - g_3$, mit g_2, g_3 abhängig von Λ.

Beobachtung
Doppelt-periodische Funktionen sind das gleiche wie die Funktionen auf einer algebraischen Kurve der Form $Y^2 = X^3 + aX + b$.

Analytischer Ansatz
Eigenschaften der Kurven entsprechen Eigenschaften der Gitter.

Definition
$\Lambda \subset \mathbb{C}$ hat *komplexe Multiplikation mit* $\tau \in \mathbb{C} \setminus \mathbb{Z}$ falls $\tau\Lambda \subset \Lambda$.

Beispiel
Das Gitter zu $Y^2 = X^3 - C$ hat komplexe Multiplikation mit $\mathbb{Q}(\zeta_3)$ für $\zeta_3 = \exp(\frac{2\pi i}{3})$.

Philosophie

Punktanzahlen als Messreihe

- Ist eine Gleichung gegeben, so kann ihre Lösungsanzahl modulo p bestimmt werden.
- Dieses liefert eine Folge von *Messwerten*, die der Gleichung zugeordnet sind.
- Diese spiegelt Eigenschaften der Gleichung wider.

Bisherige Beispiele

- Quadratische Flächen $\rightsquigarrow$ Definitionskörper der Geraden.
- Kubische Kurve $\rightsquigarrow$ Endomorphismus (komplexe Multiplikation).

Frage
Welche Phänomene treten bei anderen Gleichungstypen auf?

Verbindungen zur Kohomologie

Theorem (Lefschetzsche Spurformel)
Sei V eine n-dimensionale glatte, projektive Varietät über $\mathbb{F}_p$. Dann gilt

$$\#V(\mathbb{F}_p) = \sum_{i=0}^{2n} (-1)^i \mathrm{Tr}(\mathrm{Frob}_p \mid \mathrm{H}^i_{et}(V, \mathbb{Q}_\ell)) .$$

Erinnerung
Die Spur einer linearen Abbildung ist die Summe ihrer Eigenwerte.

Interpretation
Die Punktanzahlen enthalten Information über die Kohomologie inklusive der Galois-Modulstruktur dieser Vektorräume.

Satz (Deligne-Weil)
Alle Eigenwerte des Frobenius auf H^i_{et} sind ganze algebraische Zahlen vom Betrag $p^{i/2}$.

Punktanzahlen auf quadratischen Flächen

Beispiel
Im Fall einer glatten quadratischen Fläche ist H^2 zweidimensional. Erzeuger der Kohomologie sind durch jeweils eine Gerade der beiden Familien gegeben.
Sind die Geraden erst über $\mathbb{F}_{p^2}$ definiert, so permutiert der Frobenius die beiden Kohomologieklassen. Der Frobenius hat daher die Darstellungsmatrix

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Sind die Geraden bereits über $\mathbb{F}_p$ definiert, so ist die Darstellungsmatrix die Einheitsmatrix. Beim Übergang zur Kohomologie sind alle Eigenwerte mit p zu multiplizieren.

Ergebnis
Punktanzahl p^2+1 oder p^2+2p+1.

Allgemeiner Ansatz: p-adisches Punktezählen

Idee
Bestimme die Punktanzahl von $V(\mathbb{F}_{p^d})$ modulo Potenzen von p. Dies wird als p-adisches Zählen bezeichnet.

Kleiner Fermatscher Satz
$x \in \mathbb{F}_p \Rightarrow x^{p-1} \in \{0,1\}$.

Beispiel-Fläche
$V = \{[X:Y:Z:W] \in \mathbf{P}^3 \mid f(X,Y,Z,W) = 0\}$.

Punktanzahl

$$\#V(\mathbb{F}_p)(p-1) \equiv \left(p^4 - 1 - \sum_{x,y,z,w \in \mathbb{F}_p} f^{p-1}(x,y,z,w)\right) \bmod p\,.$$

Summenberechnung

Potenzen
f^{p-1} ist ein Polynom vom Grad $(p-1)\deg(f)$. Es besteht aus sehr vielen Monomen.

Summation für ein Monom
$$\sum_{x,y,z,w \in \mathbb{F}_p} M(x,y,z,w)$$

- Ist eine Variable in M nicht enthalten, so ist die Summe $\equiv 0 \bmod p$.
- Hat eine Variable in M nicht durch $p-1$ teilbaren Exponenten, so ist die Summe $\equiv 0 \bmod p$.

D.h., viele Terme liefern keinen Beitrag.

Folgerungen

Folgerung
Ist der Grad von f kleiner als die Anzahl der Variablen, so liefert kein Monom einen Beitrag. Es ergibt sich $\#V(\mathbb{F}_p) \cdot (p-1) \equiv -1 \bmod p$. D.h., $\#V(\mathbb{F}_p) \equiv 1 \bmod p$.

Folgerung
Jede quadratische und jede kubische Fläche über einem endlichen Körper hat mindestens einen Punkt.

Folgerung
Für eine Fläche 4. Grades hängt die Punktanzahl modulo p nur vom Koeffizienten von $(XYZW)^{p-1}$ in f^{p-1} ab.

Fehlerextrapolation

Idee
Obige Rechnung kann auch mit $f^{k\cdot(p-1)}$ statt f^{p-1} durchgeführt werden. Beides liefert die Punktanzahl von $V\colon f = 0$ modulo p, aber nicht modulo p^2. Dies sind jeweils p-adische Approximationen mit Genauigkeit 1.

Fehlerextrapolation
Bilde eine Linearkombination mehrerer Appoximationen mit dem Ziel, den Fehler möglichst weitgehend zu eliminieren.

$$\begin{aligned} f(x_0,y_0,z_0,w_0)^{p-1} &= 1+ep \\ f(x_0,y_0,z_0,w_0)^{2(p-1)} &= 1+2ep+e^2p^2 \\ \Rightarrow 2f(x_0,y_0,z_0,w_0)^{p-1} - f(x_0,y_0,z_0,w_0)^{2(p-1)} &\equiv 1 \bmod p^2 \end{aligned}$$

Öffentliche Implementation

Magma-Implementation
In `magma` steht unsere Implementation eines Verfahrens von David Harvey (UNSW) zur allgemeinen Verfügung.

```
WeilPolynomialOfDegree2K3Surface
```

Performance
Berechnet die Punktanzahl im Fall einer Fläche über Körpern wie $\mathbb{F}_{101^{10}}$ in wenigen Minuten.

K3 Flächen

Definition Eine K3-Fläche ist eine einfach zusammenhängende algebraische Fläche mit trivialem kanonischen Bündel.

Modelle von K3-Flächen

Grad-2-Modell: Zweiblättrige Überlagerung des $\mathbf{P}^2$ verzweigt an einer Kurve 6. Grades z.B. $W^2 = X^6 + Y^6 + Z^6$.

Grad-4-Modell: Fläche 4. Grades im $\mathbf{P}^3$ z.B. $X^4 + Y^4 + Z^4 = W^4$.

Grad-6-Modell: Vollständiger Durchschnitt einer Quadrik und einer Kubik in $\mathbf{P}^4$.

Grad-8-Modell: Vollständiger Durchschnitt dreier Quadriken in $\mathbf{P}^5$.

Bemerkungen
Zu jedem positiven, geraden Grad gibt es Modelle.
K3-Flächen sind eine Verallgemeinerung von elliptischen Kurven.

Geometrie von K3-Flächen

Hodge-Diamant

$$\begin{array}{ccccc} & & 1 & & \\ & 0 & & 0 & \\ 1 & & 20 & & 1 \\ & 0 & & 0 & \\ & & 1 & & \end{array}$$

Definition
Es gibt einen 22-dimensionalen Vektorraum von 2-dimensionalen Zykeln. Ein Zykel heißt *algebraisch*, wenn er durch algebraische Kurven repräsentiert werden kann. Sonst heißt er *transzendent*.

Fragen
Kann man die algebraischen Zykel verstehen oder berechnen?
Trägt die Kohomologie weitere berechenbare Strukturen?

Algebraische Zykel

Definitionskörper
Jeder algebraische Zykel kann über einer endlichen Körpererweiterung realisiert werden.
Die absolute Galoisgruppe des Grundkörpers ($\mathbb{Q}$ oder $\mathbb{F}_p$) operiert daher nur über einen endlichen Quotienten auf dem Raum der algebraischen Zykel. D.h. alle Eigenwerte sind Einheitswurzeln.

Idee
Bestimme eine Oberschranke für die Dimension des Raums der algebraischen Zykel, indem man die Anzahl der Einheitswurzel-Eigenwerte bestimmt.

Gute Reduktion

$$\begin{aligned} rk\mathrm{Pic}V_{\overline{K}} &= \text{Dimension des Raums der algebraischen Zykel} \\ &\leq \text{Dimension des Raums der algebraischen Zykel} \\ &\quad \text{nach Reduktion modulo } p \end{aligned}$$

Schranken für den Picard-Rang

Algorithmus
Eingabe: K3-Fläche V, definiert über $\mathbb{Q}$ mit guter Reduktion an p.

- Berechne die Punktanzahl von $V(\mathbb{F}_p), V(\mathbb{F}_{p^2}), \ldots$.
- Bestimme mit den Newton-Identitäten das charakteristische Polynom Φ des Frobenius.
- Bestimme die Anzahl der Einheitswurzel-Eigenwerte des Frobenius auf $\mathrm{H}^2_{\mathrm{et}}(V, \mathbb{Q}_\ell(1))$.
- Gebe diese Anzahl als Oberschranke für den Picard-Rang zurück.

Artin-Tate Formel

$$|\Delta| = \frac{\lim_{T\to q} \frac{\Phi(T)}{(T-q)^\rho}}{q^{21-\rho} \# \mathrm{Br}(V)}$$

$\# \mathrm{Br}(V)$ ist immer ein Quadrat.

Schranken für den Picard-Rang II

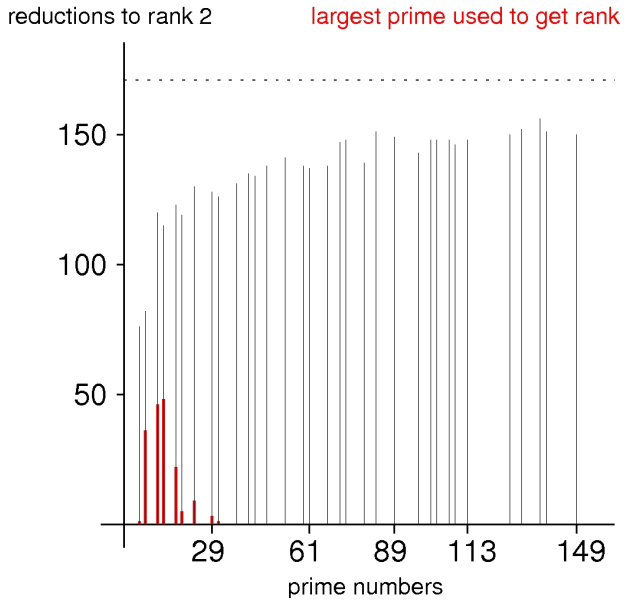
Algorithmus
Eingabe: K3-Fläche V

- Bestimme einige Primzahlen guter Reduktion.
- Berechne zu jeder Primzahl obige Rangschranke und Δ.
- Bilde das Minimum der Rangschranken.
- Im Fall inkompatibler Werte von Δ, verschärfe die Schranke um 1.

(van Luijk, Kloosterman)

Test
Erzeuge zufällige K3-Flächen vom Grad 2 und versuche den Rang zu berechnen.

Test des Picard-Rang Algorithmus



Ergebnis

Beobachtung
Die Methode findet eine scharfe Oberschranke in allen Testbeispielen.

Theorem (F. Charles)
Hat die K3-Fläche V keine reelle Multiplikation, so haben die Primzahlen, die auf scharfe Rangschranken führen, positive Dirichlet-Dichte.

Reelle Multiplikation
Reelle Multiplikation bedeutet, dass die Kohomologie der Fläche als Hodge-Struktur zusätzliche Endomorphismen hat.

Aufgabe
Finde K3-Flächen mit zusätzlichen Endomorphismen.

K3-Flächen mit Automorphismen

Flächen als Überlagerungen

$$V_1 \colon w^4 = f_4(x,y,z)$$
$$V_2 \colon f_2(x,y,z,w) = 0, u^3 = f_3(x,y,z,w)$$

- V_1 ist glatte Quartik. (Grad 4 Modell)
  V_1 ist 4-blättige Überlagerung des $\mathbf{P}^2$.
  V_1 hat den Automorphismus $w \mapsto iw$.
- V_2 ist K3-Fläche als Grad-6-Modell.
  V_2 ist 3-blättige Überlagerung von $Q \colon f_2(x,y,z,w) = 0$.
  V_2 hat den Automorphismus $u \mapsto \zeta_3 u$.
- $p \equiv 3 \bmod 4 \Rightarrow \#V_1(\mathbb{F}_p) = \#\{w^2 = f_4(x,y,z)\} \equiv 1 \bmod p$
- $p \equiv 2 \bmod 3 \Rightarrow \#V_2(\mathbb{F}_p) = \#Q(\mathbb{F}_p) \equiv 1 \bmod p$

Nicht-ordinäre Primzahlen

Definition
Für eine K3-Fläche V heißt die Primzahl p nicht-ordinär, wenn $\#V(\mathbb{F}_p) \equiv 1 \bmod p$ gilt.

Experiment
Eine zufällige K3-Fläche hat nur sehr wenige nicht-ordinäre Primzahlen.

Beobachtung
In den obigen Beispielen sind alle Primzahlen $p \equiv 3 \bmod 4$ bzw. $p \equiv 2 \bmod 3$ nicht-ordinär.

Frage
Können wir weitere Beispiele mit vielen nicht-ordinären Primzahlen finden?

Suche nach Beispielen

Suchraum
Betrachte K3-Flächen der Form

$$w^2 = f(x,y,z)g(x,y,z)\,.$$

Der Suchraum ist das kartesische Produkt zweier Listen von Formen.

Idee
Berechne soviele Daten wie irgend möglich für jede einzelne Form.

Punkte zählen mit Bit-Operationen

Initialisierung

- Liste alle Punkte von $\mathbf{P}^2(\mathbb{F}_p)$ auf.
- Werte alle Formen in allen Punkten aus.
- Codiere $f = 0$ oder $f \neq 0$ für jede Form f in Bit-Vektoren.
- Codiere $f = \square$ oder $f \neq \square$ für jede Form f in Bit-Vektoren.

Zählen

Für jedes Paar f_i, g_j:

- Wende Bit-Operationen auf die Bit-Vektoren an und bestimme
- Bitvektor, der $f_i g_j = 0$ oder $\neq 0$ codiert.
- Bitvektor, der $f_i g_j = \square$ oder $\neq \square$ kodiert.
- Benutze `popcount` um die Lösungszahl zu bestimmen.

Geschwindigkeit

Mehr als 10^6 Flächen pro Sekunde.

Ergebnis

Rohdaten

Einzeln auffällige Flächen.

Familien

Diese können mit *viel Gefühl* zu Familien zusammengesetzt werden.

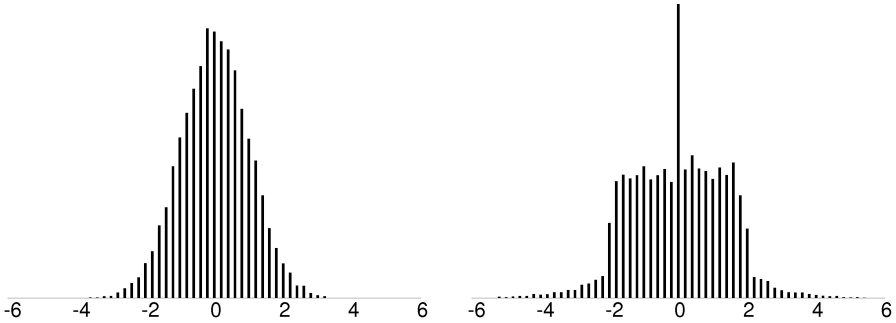
Beispiel

$$\begin{aligned} w^2 = &[(\tfrac{1}{8}t^2-\tfrac{1}{2}t+\tfrac{1}{4})y^2 + (t^2-2t+2)yz + (t^2-4t+2)z^2] \\ &[(\tfrac{1}{8}t^2+\tfrac{1}{2}t+\tfrac{1}{4})x^2 + (t^2+2t+2)xz + (t^2+4t+2)z^2] \\ &[2x^2 + (t^2+2)xy + t^2y^2]\,. \end{aligned}$$

Beobachtung

Alle gefundenen Familien sind rationale Kurven im Gleichungsraum.

Verteilung der normalisierten Abweichung



$V_1 : w^2 = xyz(x+y+z)(3x+5y+7z)(-5x+11y-2z)$

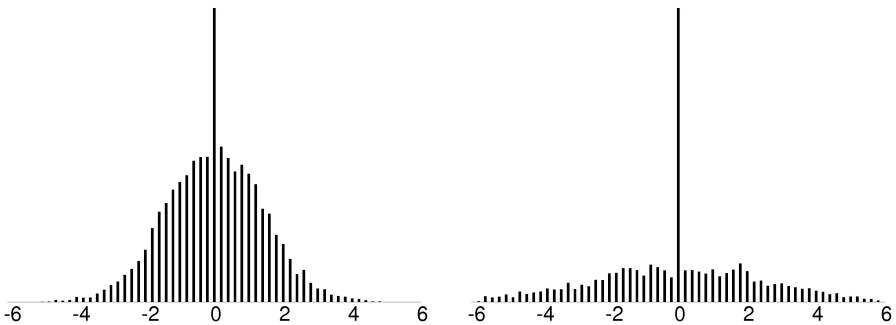
$V_2 : w^2 = xyz(x^3+3x^2y-2x^2z+5xy^2-xz^2+3y^3-2y^2z-3yz^2+2z^3)$

$M_1 = [0.0153, 0.9894, 0.0291, 2.9546, 0.1504]$ $(B = 175000)$

$M_2 = [-0.0039, 0.9705, -0.0865, 5.6756, -1.4465]$ $(B = 250000)$

V_1 generisch, V_2 nicht-ordinär an allen Primzahlen mit $\left(\frac{3}{p}\right) = -1$

Verteilung der normalisierten Abweichung II



$V_3 : w^2 = xyz(x+y+z)(1x+2y+3z)(5x+8y+20z)$

$V_4 : w^2 = xyz(x^3-3x^2z-3xy^2-3xyz+y^3+9y^2z+6yz^2+z^3)$

$M_3 = [-0.0004, 0.992, -0.0248, 5.9371, -0.4236]$ $(B = 300000)$

$M_4 = [-0.0017, 0.9892, -0.0974, 14.3608, -3.38]$ $(B = 300000)$

V_3, V_4 komplexe Multiplikation mit $\mathbb{Q}(i), \mathbb{Q}(i, \zeta_9 + \zeta_9^{-1})$

Gittertheoretische Erklärung

Kohomologie als Gitter
Die Kohomologie H^2 mit Koeffizienten in $\mathbb{Z}$ ist ein 22-dimensionales Gitter. Das transzendente Gitter Λ ist das orthogonale Komplement zum Erzeugnis aller algebraischen Kurven in H^2.

Endomorphismen
Ein Endomorphismus ist eine lineare Abbildung ϕ mit $\phi(\Lambda) \subset \Lambda$.

Erklärung
Im obigen Fall hat Λ einen nicht-trivialen Automorphismus mit Minimalpolynom $X^2 - 3$.

Bemerkung
Dies wird als reelle Multiplikation bezeichnet.

Zusammenfassung

Startpunkt
Berechnung der Punktanzahlen algebraischer Varietäten über endlichen Körpern.

Lefschetz-Spurformel
Punktanzahlen stehen in enger Verbindung zur Kohomologie der Varietät.

Öffentlicher Code
`magma`-Implementation von Punktzählalgorithmen für K3-Flächen.

Gefundene Beispiele
K3-Flächen mit vielen nicht-ordinären Primstellen und verschiedenen Endomorphismenkörpern.

Vielen Dank!