Gefördert durch
DFG Deutsche Forschungsgemeinschaft

UNIVERSITÄT BAYREUTH

Exakte Verifizierung der starken BSD-Vermutung für einige absolut einfache abelsche Flächen

Timo Keller

mit Michael Stoll

Universität Bayreuth

9. März 2022

Inhalt

Elliptische Kurven

Algebraische Geometrie: elliptische Kurven

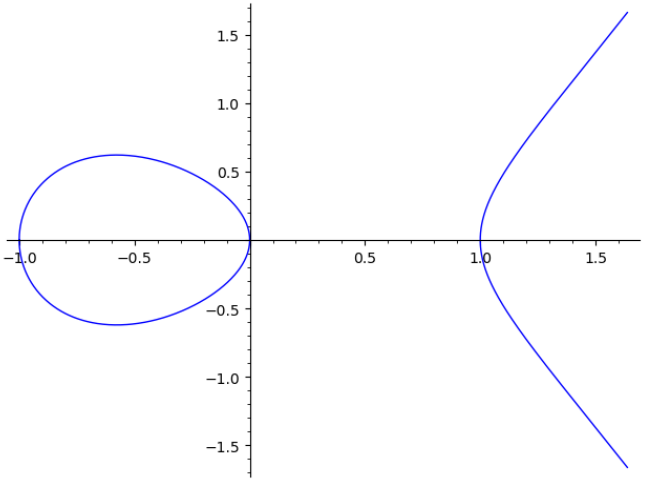
Polynomgleichungssysteme und ihre Nullstellengebilde:
(affine) Varietäten

Beispiel

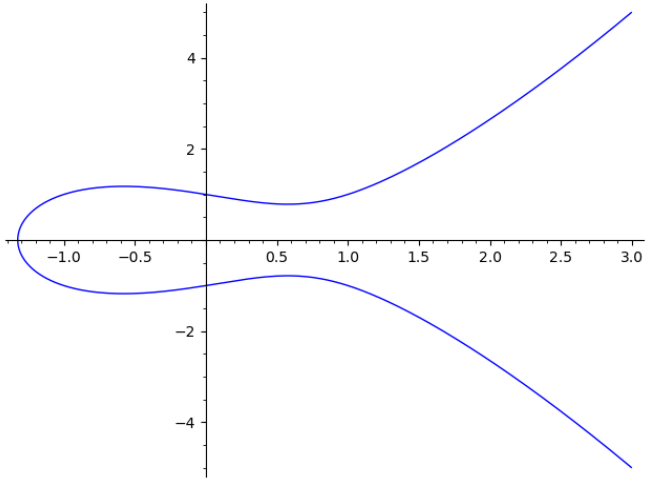
Elliptische Kurven gegeben durch Weierstraß-Gleichung

$$E : y^2 = x^3 + Ax + B$$

mit $A, B \in \mathbf{Q}$ so, dass $x^3 + Ax + B$ keine mehrfachen Nullstellen hat.



$y^2 = x^3 - x$



$y^2 = x^3 - x + 1$

Algebraische Geometrie: elliptische Kurven

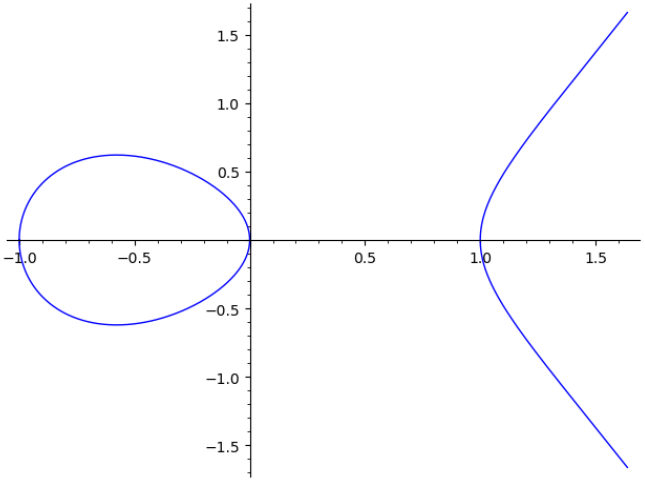
Polynomgleichungssysteme und ihre Nullstellengebilde:
(affine) Varietäten

Beispiel

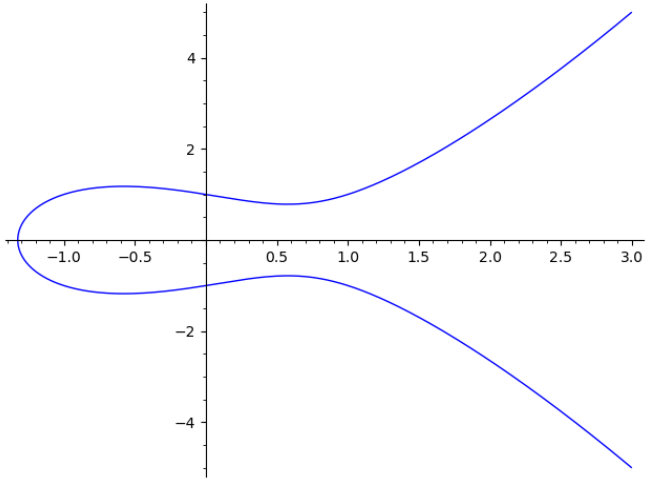
Elliptische Kurven gegeben durch Weierstraß-Gleichung

$$E : y^2 = x^3 + Ax + B$$

mit $A, B \in \mathbf{Q}$ so, dass $x^3 + Ax + B$ keine mehrfachen Nullstellen hat.



$y^2 = x^3 - x$



$y^2 = x^3 - x + 1$

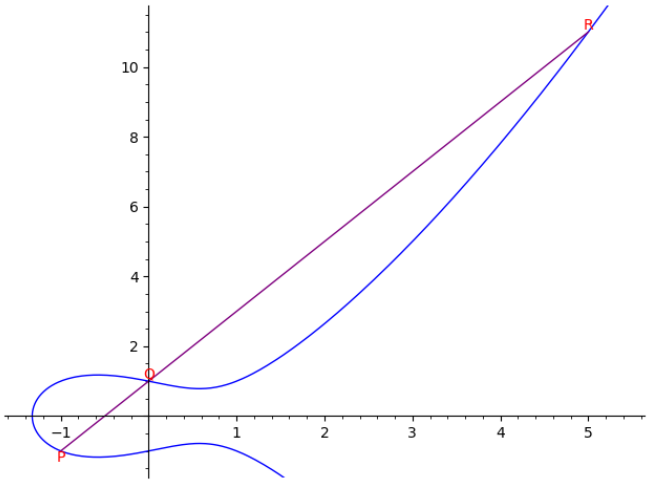
Die Gruppenstruktur

Betrachte eine elliptische Kurve

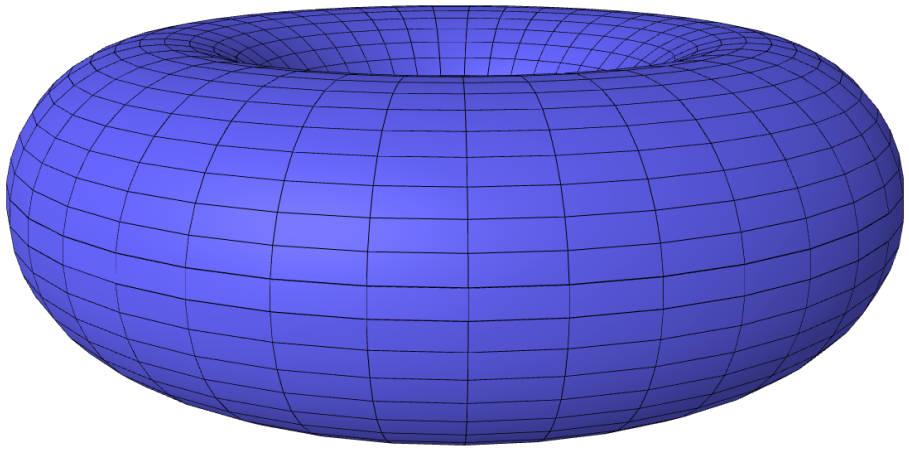
$$E : y^2 = x^3 + Ax + B.$$

$E(\mathbf{Q})$: Lösungen mit $x, y \in \mathbf{Q}$ zusammen mit Punkt im Unendlichen.

Gruppenstruktur auf $E(\mathbf{Q})$:



$P + Q + R = 0$



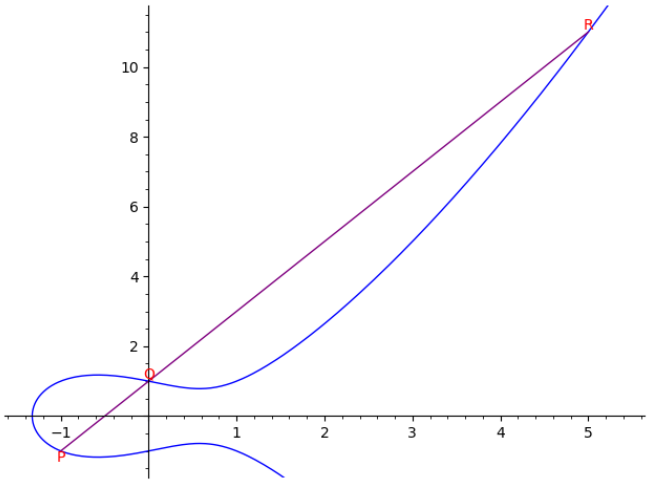
$E(\mathbf{C}) \cong \mathbf{C}/\Lambda$, $\Lambda \subset \mathbf{C}$ Gitter

Die Gruppenstruktur

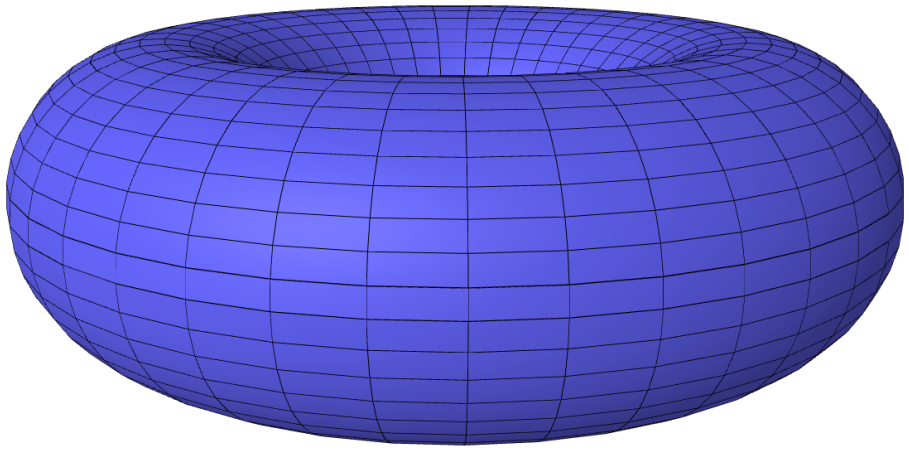
Betrachte eine elliptische Kurve

$$E : y^2 = x^3 + Ax + B.$$

$E(\mathbf{Q})$: Lösungen mit $x, y \in \mathbf{Q}$ zusammen mit Punkt im Unendlichen.
Gruppenstruktur auf $E(\mathbf{Q})$:



$P + Q + R = 0$



$E(\mathbf{C}) \cong \mathbf{C}/\Lambda$, $\Lambda \subset \mathbf{C}$ Gitter

Satz von Mordell (1922)

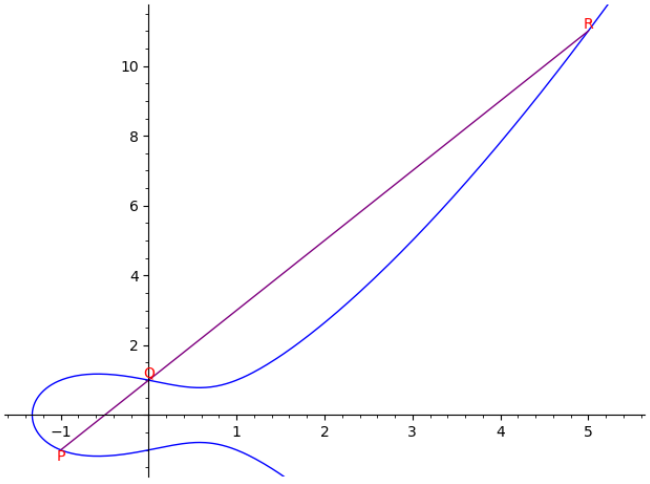
Die abelsche Gruppe $E(\mathbf{Q})$ ist endlich erzeugt:
$E(\mathbf{Q}) \cong \mathbf{Z}^r \oplus E(\mathbf{Q})_{\text{tors}}$ mit dem Rang $r \geq 0$ und $E(\mathbf{Q})_{\text{tors}}$ endlich.

Die Gruppenstruktur

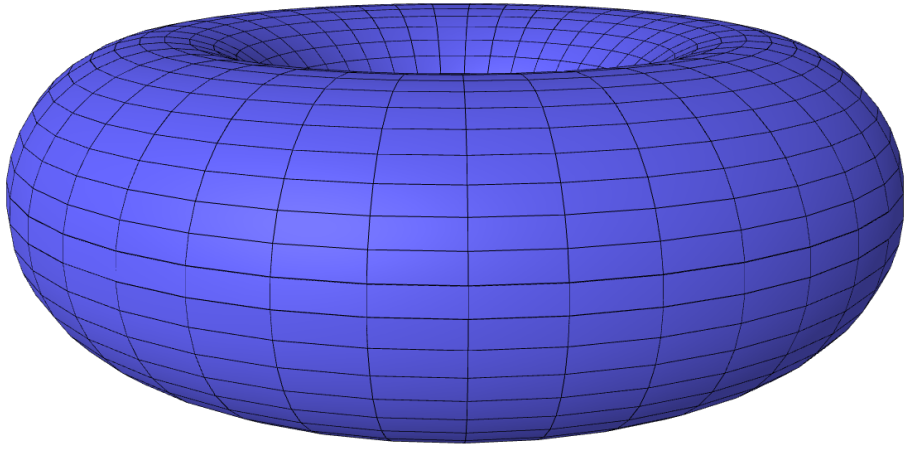
Betrachte eine elliptische Kurve

$$E : y^2 = x^3 + Ax + B.$$

$E(\mathbf{Q})$: Lösungen mit $x, y \in \mathbf{Q}$ zusammen mit Punkt im Unendlichen.
Gruppenstruktur auf $E(\mathbf{Q})$:



$P + Q + R = 0$



$E(\mathbf{C}) \cong \mathbf{C}/\Lambda$, $\Lambda \subset \mathbf{C}$ Gitter

Satz von Mordell (1922)

Die abelsche Gruppe $E(\mathbf{Q})$ ist endlich erzeugt:
$E(\mathbf{Q}) \cong \mathbf{Z}^r \oplus E(\mathbf{Q})_{\text{tors}}$ mit dem Rang $r \geq 0$ und $E(\mathbf{Q})_{\text{tors}}$ endlich.

Motivation für die und Aussage der BSD-Vermutung

Die Birch-Swinnerton-Dyer-Vermutung

L-Funktion von E:

$$L(E,s) = \prod_{p \in S_{\text{good}}} \frac{1}{1 - a_p p^{-s} + p^{1-2s}} \cdot \prod_{p \in S_{\text{bad}}} \frac{1}{1 - a_p p^{-s}}$$

mit $a_p = p + 1 - \#E(\mathbf{F}_p)$ für $p \in S_{\text{good}}$ (Spur des p-Frobenius).

Birch-Swinnerton-Dyer-Vermutung

$$r = r_{\text{an}} := \operatorname{ord}_{s=1} L(E,s)$$

- Aufgestellt in den 1960er Jahren nach Computerberechnungen.
- Gibt „Tag-Nacht-Algorithmus“ zur Berechnung von $E(\mathbf{Q})$.
- Bewiesen, wenn $\operatorname{ord}_{s=1} L(E,s) \leq 1$.

Die Birch-Swinnerton-Dyer-Vermutung

L-Funktion von E:

$$L(E,s) = \prod_{p \in S_{\text{good}}} \frac{1}{1 - a_p p^{-s} + p^{1-2s}} \cdot \prod_{p \in S_{\text{bad}}} \frac{1}{1 - a_p p^{-s}}$$

mit $a_p = p + 1 - \#E(\mathbf{F}_p)$ für $p \in S_{\text{good}}$ (Spur des p-Frobenius).

Birch-Swinnerton-Dyer-Vermutung

$$r = r_{\text{an}} := \operatorname{ord}_{s=1} L(E,s)$$

- Aufgestellt in den 1960er Jahren nach Computerberechnungen.
- Gibt „Tag-Nacht-Algorithmus“ zur Berechnung von $E(\mathbf{Q})$.
- Bewiesen, wenn $\operatorname{ord}_{s=1} L(E,s) \leq 1$.

Die Shafarevich-Tate-Gruppe

Die Shafarevich-Tate-Gruppe

$$Ш(E/\mathbb{Q}) := \ker\left(\mathrm{H}^1(\mathbf{Q}, E) \to \bigoplus_v \mathrm{H}^1(\mathbf{Q}_v, E)\right)$$

klassifiziert überall lokal triviale E-Torseure.

- $Ш(E/\mathbf{Q})$ ist Maß für Fehlschlagen des Lokal-global-Prinzips.
- Vermutung: endlich!
- Anwendung: Sei C Kurve vom Geschlecht 1.
  Entscheide: $C(\mathbf{Q}) = \emptyset$? $\#C(\mathbf{Q}) = \infty$?

Die Shafarevich-Tate-Gruppe

Die Shafarevich-Tate-Gruppe

$$Ш(E/\mathbb{Q}) := \ker\left(\mathrm{H}^1(\mathbf{Q}, E) \to \bigoplus_v \mathrm{H}^1(\mathbf{Q}_v, E)\right)$$

klassifiziert überall lokal triviale E-Torseure.

- $Ш(E/\mathbf{Q})$ ist Maß für Fehlschlagen des Lokal-global-Prinzips.
- Vermutung: endlich!
- Anwendung: Sei C Kurve vom Geschlecht 1.
  Entscheide: $C(\mathbf{Q}) = \emptyset$? $\#C(\mathbf{Q}) = \infty$?

starke BSD-Vermutung

$$\#Ш(E/\mathbf{Q}) = \#Ш(E/\mathbf{Q})_{\mathrm{an}} := \frac{(\#E(\mathbf{Q})_{\mathrm{tors}})^2}{\prod_p c_p} \cdot \frac{L^*(E,1)}{\Omega_E \,\mathrm{Reg}_E}$$

Vergleiche mit der analytischen Klassenzahlformel!

Die Shafarevich-Tate-Gruppe

Die Shafarevich-Tate-Gruppe

$$Ш(E/\mathbb{Q}) := \ker\left(\mathrm{H}^1(\mathbf{Q}, E) \to \bigoplus_v \mathrm{H}^1(\mathbf{Q}_v, E)\right)$$

klassifiziert überall lokal triviale E-Torseure.

- $Ш(E/\mathbf{Q})$ ist Maß für Fehlschlagen des Lokal-global-Prinzips.
- Vermutung: endlich!
- Anwendung: Sei C Kurve vom Geschlecht 1.
  Entscheide: $C(\mathbf{Q}) = \emptyset$? $\#C(\mathbf{Q}) = \infty$?

starke BSD-Vermutung

$$\#Ш(E/\mathbf{Q}) = \#Ш(E/\mathbf{Q})_{\mathrm{an}} := \frac{(\#E(\mathbf{Q})_{\mathrm{tors}})^2}{\prod_p c_p} \cdot \frac{L^*(E,1)}{\Omega_E \,\mathrm{Reg}_E}$$

Vergleiche mit der analytischen Klassenzahlformel!

Ein Beispiel für die Shafarevich-Tate-Gruppe

Die Selmer-Kubik

$$3x^3 + 4y^3 + 5z^3 = 0$$

ist ein nichttriviales Element von $Ш(E/\mathbf{Q})[3]$ mit der elliptischen Kurve

$$E : x^3 + y^3 + 3 \cdot 4 \cdot 5 \cdot z^3 = 0$$

mit $r = r_{\text{an}} = 0$.

Unter Annahme der starken Birch-Swinnerton-Dyer-Vermutung ist

$$Ш(E/\mathbf{Q}) \cong (\mathbf{Z}/3)^2.$$

Ein Beispiel für die Shafarevich-Tate-Gruppe

Die Selmer-Kubik

$$3x^3 + 4y^3 + 5z^3 = 0$$

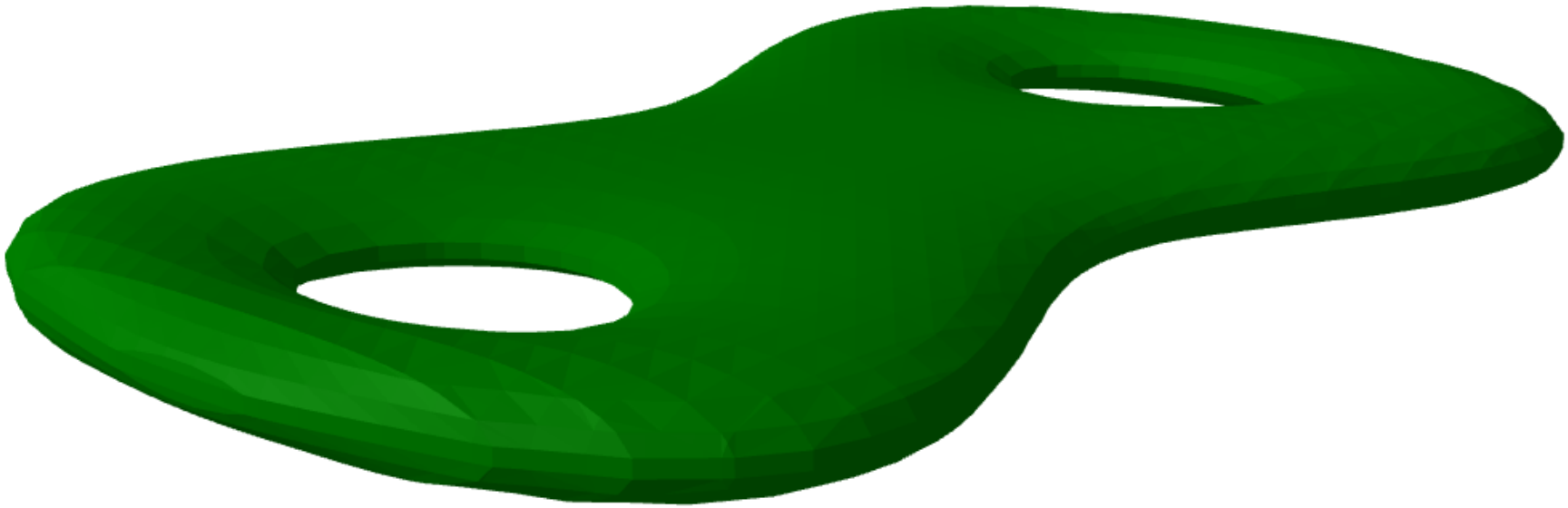
ist ein nichttriviales Element von $Ш(E/\mathbf{Q})[3]$ mit der elliptischen Kurve

$$E : x^3 + y^3 + 3 \cdot 4 \cdot 5 \cdot z^3 = 0$$

mit $r = r_{\text{an}} = 0$.
Unter Annahme der starken Birch-Swinnerton-Dyer-Vermutung ist

$$Ш(E/\mathbf{Q}) \cong (\mathbf{Z}/3)^2.$$

Es gibt Analogon für abelsche Varietäten höherer Dimension!



Kurve vom Geschlecht 2

Hier ist deutlich weniger bekannt!

Stand der Forschung zur (starken) BSD-Vermutung

- Wenn $\dim A = 1$, starke BSD verifiziert für Führer bis 5000.
- Vor allem Resultate für modulare abelsche Varietäten A.
- Nicht jede abelsche Varietät der Dimension > 1 ist modular.
- Aus Gross-Zagier und Kolyvagin-Logachëv kann man für diese $r = r_{\mathrm{an}}$ folgern, wenn $r_{\mathrm{an}} \leq \dim A$. (1980er Jahre)
- Außerdem gilt dann $\#Ш(A/\mathbf{Q})_{\mathrm{an}} \in \mathbf{Q}_{>0}$ und $\#Ш(A/\mathbf{Q}) < \infty$.

Stand der Forschung zur (starken) BSD-Vermutung

- Wenn $\dim A = 1$, starke BSD verifiziert für Führer bis 5000.
- Vor allem Resultate für modulare abelsche Varietäten A.
- Nicht jede abelsche Varietät der Dimension > 1 ist modular.
- Aus Gross-Zagier und Kolyvagin-Logachëv kann man für diese $r = r_{\mathrm{an}}$ folgern, wenn $r_{\mathrm{an}} \leq \dim A$. (1980er Jahre)
- Außerdem gilt dann $\#Ш(A/\mathbf{Q})_{\mathrm{an}} \in \mathbf{Q}_{>0}$ und $\#Ш(A/\mathbf{Q}) < \infty$.
- Offen: $\#Ш(A/\mathbf{Q}) \stackrel{?}{=} \#Ш(A/\mathbf{Q})_{\mathrm{an}}$ (starke BSD-Vermutung)

Stand der Forschung zur (starken) BSD-Vermutung

- Wenn $\dim A = 1$, starke BSD verifiziert für Führer bis 5000.
- Vor allem Resultate für modulare abelsche Varietäten A.
- Nicht jede abelsche Varietät der Dimension > 1 ist modular.
- Aus Gross-Zagier und Kolyvagin-Logachëv kann man für diese $r = r_{\mathrm{an}}$ folgern, wenn $r_{\mathrm{an}} \leq \dim A$. (1980er Jahre)
- Außerdem gilt dann $\#Ш(A/\mathbf{Q})_{\mathrm{an}} \in \mathbf{Q}_{>0}$ und $\#Ш(A/\mathbf{Q}) < \infty$.
- Offen: $\#Ш(A/\mathbf{Q}) \stackrel{?}{=} \#Ш(A/\mathbf{Q})_{\mathrm{an}}$ (starke BSD-Vermutung)

Probleme, wenn dim $A > 1$

Was ist nicht verfügbar?

- Für welche p gibt es p-Isogenien $A \to A'$?
- Das Eulersystem von Kolyvagin-Logachëv ist nicht explizit.

Starke BSD in Dimension > 1 bisher in keinem einzigen Fall verifiziert, der sich nicht auf Dimension 1 reduzieren lässt!

Ein explizites Eulersystem

Satz (K.): endlicher Träger von Ш

Sei A eine modulare abelsche Varietät über $\mathbf{Q}$.
Es ist $Ш(A/\mathbf{Q})[p] = 0$ für alle p mit

- $\rho_p : \mathrm{Gal}(\overline{\mathbf{Q}}|\mathbf{Q}) \to \mathrm{Aut}(A[p](\overline{\mathbf{Q}}))$ irreduzibel und
- $p \nmid 2 \cdot c \cdot \gcd_K(I_K)$ mit Heegnerindizes I_K und dem Tamagawaprodukt c.

Diese p sind explizit berechenbar.

Ein explizites Eulersystem

Satz (K.): endlicher Träger von Ш

Sei A eine modulare abelsche Varietät über $\mathbf{Q}$.
Es ist $Ш(A/\mathbf{Q})[p] = 0$ für alle p mit

- $\rho_p : \mathrm{Gal}(\overline{\mathbf{Q}}|\mathbf{Q}) \to \mathrm{Aut}(A[p](\overline{\mathbf{Q}}))$ irreduzibel und
- $p \nmid 2 \cdot c \cdot \gcd_K(I_K)$ mit Heegnerindizes I_K und dem Tamagawaprodukt c.

Diese p sind explizit berechenbar.

Berechnung von $\#Ш(A/\mathbf{Q})$ und $\#Ш(A/\mathbf{Q})_{\mathrm{an}}$

Für alle anderen p . . .

1. . . . berechne die p-adische L-Funktion, oder
2. . . . mache einen p-Abstieg,

. . . um $Ш(A/\mathbf{Q})[p]$ zu berechnen.

Berechne $\#Ш(A/\mathbf{Q})_{\mathrm{an}}$ mittels modularer Symbole und, wenn $r_{\mathrm{an}} = \dim A$, einem Heegnerindex.

Berechnung von $\#Ш(A/\mathbf{Q})$ und $\#Ш(A/\mathbf{Q})_{\mathrm{an}}$

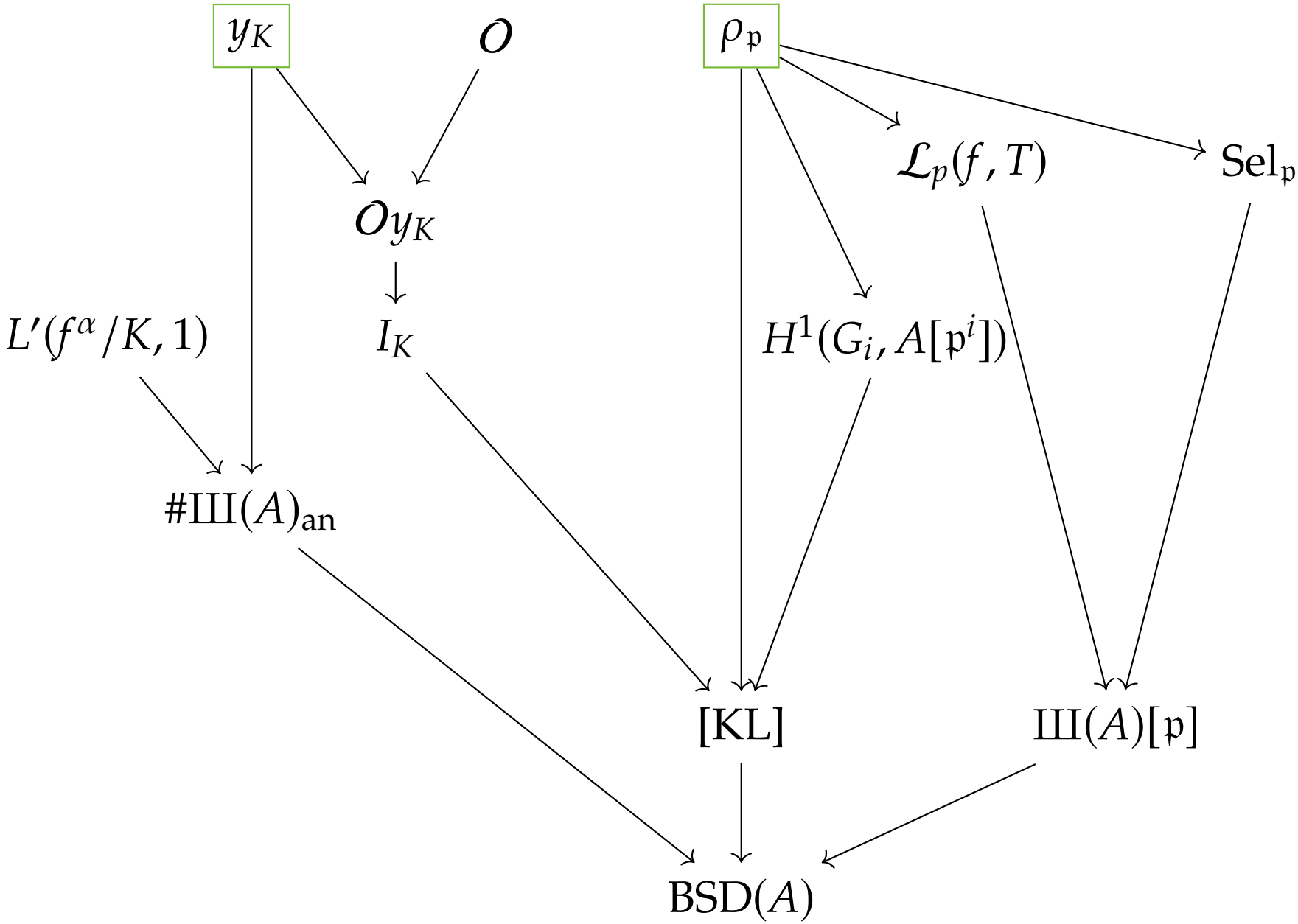
Für alle anderen p . . .

1. . . . berechne die p-adische L-Funktion, oder
2. . . . mache einen p-Abstieg,

. . . um $Ш(A/\mathbf{Q})[p]$ zu berechnen.

Berechne $\#Ш(A/\mathbf{Q})_{\mathrm{an}}$ mittels modularer Symbole und, wenn $r_{\mathrm{an}} = \dim A$, einem Heegnerindex.

Abhängigkeitsgraph des Projektes



Ein konkretes Beispiel

$A = \mathrm{Jac}(X_0(39)/w_{13})$

- $\mathcal{O} = \mathbf{Z}[\sqrt{2}]$
- $r = r_{\mathrm{an}} = 0$
- $A(\mathbf{Q}) = A(\mathbf{Q})_{\mathrm{tors}} = \mathbf{Z}/2 \times \mathbf{Z}/(2 \cdot 7)$
- $\rho_{\mathfrak{p}}$ ist reduzibel genau für $\mathfrak{p} = (\sqrt{2})$ und genau ein $\mathfrak{p}\bar{\mathfrak{p}} = 7$.
- $c = 7$

$A = \mathrm{Jac}(X_0(39)/w_{13})$

- $\mathcal{O} = \mathbf{Z}[\sqrt{2}]$
- $r = r_{\mathrm{an}} = 0$
- $A(\mathbf{Q}) = A(\mathbf{Q})_{\mathrm{tors}} = \mathbf{Z}/2 \times \mathbf{Z}/(2 \cdot 7)$
- $\rho_{\mathfrak{p}}$ ist reduzibel genau für $\mathfrak{p} = (\sqrt{2})$ und genau ein $\mathfrak{p}\bar{\mathfrak{p}} = 7$.
- $c = 7$
- $\mathrm{Sel}_2(A/\mathbf{Q}) \cong (\mathbf{Z}/2)^2 \cong A(\mathbf{Q})[2]$ impliziert $Ш(A/\mathbf{Q})[2] = 0$.

$A = \mathrm{Jac}(X_0(39)/w_{13})$

- $\mathcal{O} = \mathbf{Z}[\sqrt{2}]$
- $r = r_{\mathrm{an}} = 0$
- $A(\mathbf{Q}) = A(\mathbf{Q})_{\mathrm{tors}} = \mathbf{Z}/2 \times \mathbf{Z}/(2 \cdot 7)$
- $\rho_{\mathfrak{p}}$ ist reduzibel genau für $\mathfrak{p} = (\sqrt{2})$ und genau ein $\mathfrak{p}\bar{\mathfrak{p}} = 7$.
- $c = 7$
- $\mathrm{Sel}_2(A/\mathbf{Q}) \cong (\mathbf{Z}/2)^2 \cong A(\mathbf{Q})[2]$ impliziert $Ш(A/\mathbf{Q})[2] = 0$.
- [KL] mit $I_{\mathbf{Q}(\sqrt{-23})} = 7$ impliziert $\#Ш(A/\mathbf{Q})[\mathfrak{p}] = 0$ für $\mathfrak{p} \nmid (\sqrt{2}), 7$.
- $\#Ш(A/\mathbf{Q})_{\mathrm{an}} = 1$

$A = \mathrm{Jac}(X_0(39)/w_{13})$

- $\mathcal{O} = \mathbf{Z}[\sqrt{2}]$
- $r = r_{\mathrm{an}} = 0$
- $A(\mathbf{Q}) = A(\mathbf{Q})_{\mathrm{tors}} = \mathbf{Z}/2 \times \mathbf{Z}/(2 \cdot 7)$
- $\rho_{\mathfrak{p}}$ ist reduzibel genau für $\mathfrak{p} = (\sqrt{2})$ und genau ein $\mathfrak{p}\bar{\mathfrak{p}} = 7$.
- $c = 7$
- $\mathrm{Sel}_2(A/\mathbf{Q}) \cong (\mathbf{Z}/2)^2 \cong A(\mathbf{Q})[2]$ impliziert $Ш(A/\mathbf{Q})[2] = 0$.
- [KL] mit $I_{\mathbf{Q}(\sqrt{-23})} = 7$ impliziert $\#Ш(A/\mathbf{Q})[\mathfrak{p}] = 0$ für $\mathfrak{p} \nmid (\sqrt{2}), 7$.
- $\#Ш(A/\mathbf{Q})_{\mathrm{an}} = 1$
- $\rho_{\mathfrak{p}}$ ist reduzibel mit

$$0 \to \mathbf{Z}/7 \to A[\mathfrak{p}] \to \mu_7 \to 1$$

nicht-zerfallend exakt,
und $\mathrm{Sel}_{\mathfrak{p}}(A/\mathbf{Q}) \cong \mathbf{Z}/7 \cong A(\mathbf{Q})[7]$ folgt mit $\mathfrak{p}$-Abstieg.

$A = \mathrm{Jac}(X_0(39)/w_{13})$

- $\mathcal{O} = \mathbf{Z}[\sqrt{2}]$
- $r = r_{\mathrm{an}} = 0$
- $A(\mathbf{Q}) = A(\mathbf{Q})_{\mathrm{tors}} = \mathbf{Z}/2 \times \mathbf{Z}/(2 \cdot 7)$
- $\rho_{\mathfrak{p}}$ ist reduzibel genau für $\mathfrak{p} = (\sqrt{2})$ und genau ein $\mathfrak{p}\bar{\mathfrak{p}} = 7$.
- $c = 7$
- $\mathrm{Sel}_2(A/\mathbf{Q}) \cong (\mathbf{Z}/2)^2 \cong A(\mathbf{Q})[2]$ impliziert $Ш(A/\mathbf{Q})[2] = 0$.
- [KL] mit $I_{\mathbf{Q}(\sqrt{-23})} = 7$ impliziert $\#Ш(A/\mathbf{Q})[\mathfrak{p}] = 0$ für $\mathfrak{p} \nmid (\sqrt{2}), 7$.
- $\#Ш(A/\mathbf{Q})_{\mathrm{an}} = 1$
- $\rho_{\mathfrak{p}}$ ist reduzibel mit

$$0 \to \mathbf{Z}/7 \to A[\mathfrak{p}] \to \mu_7 \to 1$$

nicht-zerfallend exakt,
und $\mathrm{Sel}_{\mathfrak{p}}(A/\mathbf{Q}) \cong \mathbf{Z}/7 \cong A(\mathbf{Q})[7]$ folgt mit $\mathfrak{p}$-Abstieg.

- Die $\bar{\mathfrak{p}}$-adische L-Funktion hat konstanten Term eine Einheit in $\mathcal{O}_{\bar{\mathfrak{p}}} = \mathbf{Z}_7$, also zeigt die integrale GL_2-IMC $Ш(A/\mathbf{Q})[\bar{\mathfrak{p}}] = 0$, weil $\rho_{\bar{\mathfrak{p}}}$ irreduzibel ist.

$A = \mathrm{Jac}(X_0(39)/w_{13})$

- $\mathcal{O} = \mathbf{Z}[\sqrt{2}]$
- $r = r_{\mathrm{an}} = 0$
- $A(\mathbf{Q}) = A(\mathbf{Q})_{\mathrm{tors}} = \mathbf{Z}/2 \times \mathbf{Z}/(2 \cdot 7)$
- $\rho_{\mathfrak{p}}$ ist reduzibel genau für $\mathfrak{p} = (\sqrt{2})$ und genau ein $\mathfrak{p}\bar{\mathfrak{p}} = 7$.
- $c = 7$
- $\mathrm{Sel}_2(A/\mathbf{Q}) \cong (\mathbf{Z}/2)^2 \cong A(\mathbf{Q})[2]$ impliziert $Ш(A/\mathbf{Q})[2] = 0$.
- [KL] mit $I_{\mathbf{Q}(\sqrt{-23})} = 7$ impliziert $\#Ш(A/\mathbf{Q})[\mathfrak{p}] = 0$ für $\mathfrak{p} \nmid (\sqrt{2}), 7$.
- $\#Ш(A/\mathbf{Q})_{\mathrm{an}} = 1$
- $\rho_{\mathfrak{p}}$ ist reduzibel mit

$$0 \to \mathbf{Z}/7 \to A[\mathfrak{p}] \to \mu_7 \to 1$$

nicht-zerfallend exakt,
und $\mathrm{Sel}_{\mathfrak{p}}(A/\mathbf{Q}) \cong \mathbf{Z}/7 \cong A(\mathbf{Q})[7]$ folgt mit $\mathfrak{p}$-Abstieg.

- Die $\bar{\mathfrak{p}}$-adische L-Funktion hat konstanten Term eine Einheit in $\mathcal{O}_{\bar{\mathfrak{p}}} = \mathbf{Z}_7$, also zeigt die integrale GL_2-IMC $Ш(A/\mathbf{Q})[\bar{\mathfrak{p}}] = 0$, weil $\rho_{\bar{\mathfrak{p}}}$ irreduzibel ist.

Alle Atkin-Lehner-Quotienten von unserem Typ (I)

X	r	$\mathcal{O}$	$\#Ш_{an}$	$\rho_{\mathfrak{p}}$ red.	c	(D, I_D)	$\#Ш$
$X_0(23)$	0	$\sqrt{5}$	1	11_1	11	$(-7, 11)$	11^0
$X_0(29)$	0	$\sqrt{2}$	1	7_1	7	$(-7, 7)$	7^0
$X_0(31)$	0	$\sqrt{5}$	1	$\sqrt{5}$	5	$(-11, 5)$	5^0
$X_0(35)/w_7$	0	$\sqrt{17}$	1	2_1	1	$(-19, 1)$	1
$X_0(39)/w_{13}$	0	$\sqrt{2}$	1	$\sqrt{2}, 7_1$	7	$(-23, 7)$	7^0
$X_0(67)^+$	2	$\sqrt{5}$	1		1	$(-7, 1)$	1
$X_0(73)^+$	2	$\sqrt{5}$	1		1	$(-19, 1)$	1
$X_0(85)^*$	2	$\sqrt{2}$	1	$\sqrt{2}$	1	$(-19, 1)$	1
$X_0(87)/w_{29}$	0	$\sqrt{5}$	1	$\sqrt{5}$	5	$(-23, 5)$	5^0
$X_0(93)^*$	2	$\sqrt{5}$	1		1	$(-11, 1)$	1
$X_0(103)^+$	2	$\sqrt{5}$	1		1	$(-11, 1)$	1
$X_0(107)^+$	2	$\sqrt{5}$	1		1	$(-7, 1)$	1
$X_0(115)^*$	2	$\sqrt{5}$	1		1	$(-11, 1)$	1
$X_0(125)^+$	2	$\sqrt{5}$	1	$\sqrt{5}$	1	$(-11, 1)$	5^0

Alle Atkin-Lehner-Quotienten von unserem Typ (II)

X	r	$\mathcal{O}$	$\#Ш_{an}$	$\rho_{\mathfrak{p}}$ red.	c	(D, I_D)	$\#Ш$
$X_0(133)^*$	2	$\sqrt{5}$	1		1	$(-31, 1)$	1
$X_0(147)^*$	2	$\sqrt{2}$	1	$\sqrt{2}, 7_1$	1	$(-47, 1)$	7^0
$X_0(161)^*$	2	$\sqrt{5}$	1		1	$(-19, 1)$	1
$X_0(165)^*$	2	$\sqrt{2}$	1	$\sqrt{2}$	1	$(-131, 1)$	1
$X_0(167)^+$	2	$\sqrt{5}$	1		1	$(-15, 1)$	1
$X_0(177)^*$	2	$\sqrt{5}$	1		1	$(-11, 1)$	1
$X_0(191)^+$	2	$\sqrt{5}$	1		1	$(-7, 1)$	1
$X_0(205)^*$	2	$\sqrt{5}$	1		1	$(-31, 1)$	1
$X_0(209)^*$	2	$\sqrt{2}$	1		1	$(-51, 1)$	1
$X_0(213)^*$	2	$\sqrt{5}$	1		1	$(-11, 1)$	1
$X_0(221)^*$	2	$\sqrt{5}$	1		1	$(-35, 1)$	1
$X_0(287)^*$	2	$\sqrt{5}$	1		1	$(-31, 1)$	1
$X_0(299)^*$	2	$\sqrt{5}$	1		1	$(-43, 1)$	1
$X_0(357)^*$	2	$\sqrt{2}$	1		1	$(-47, 1)$	1

Ausblick

Herausforderung

Finde mittels Shnidman-Weiss[1] Beispiele von $A/\mathbf{Q}$ mit

$$\#Ш(A/\mathbf{Q}) = \#Ш(A/\mathbf{Q})_{\mathrm{an}} \neq 2^i!$$

[1] *Elements of prime order in Tate-Shafarevich groups of abelian varieties over $\mathbb{Q}$*, `arXiv:2106.14096`

Ausblick

Zukünftige Arbeit

- Verifikation für alle ~ 1200 Neuformen von Stufe ≤ 1000 mit reell-quadratischen Koeffizienten absehbar.
- Dimension 3: Eine generische Kurve vom Geschlecht 3 ist nicht hyperelliptisch, also brauchen wir eine explizite Theorie von Jacobischen und Höhen!
- Starke BSD-Vermutung über total reellen Zahlkörpern.

Ausblick

Zukünftige Arbeit

- Verifikation für alle ~ 1200 Neuformen von Stufe ≤ 1000 mit reell-quadratischen Koeffizienten absehbar.
- Dimension 3: Eine generische Kurve vom Geschlecht 3 ist nicht hyperelliptisch, also brauchen wir eine explizite Theorie von Jacobischen und Höhen!
- Starke BSD-Vermutung über total reellen Zahlkörpern.

Danke!

Mehr Details im nächsten Computeralgebra-Rundbrief.