Algorithmische Aspekte der Vermutung von Birch und Swinnerton-Dyer

Jan Steffen Müller

15.6.2011

Rang

Notation.

- Sei $E/\mathbb{Q}$ eine elliptische Kurve, gegeben durch eine minimale Weierstraß-Gleichung

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in \mathbb{Z}.$$

- Sei $E(\mathbb{Q})$ die Gruppe der $\mathbb{Q}$-rationalen Punkte auf E.

Satz 1. (Mordell)
Es gilt

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{tors}}$$

mit $r \geq 0$ und $|E(\mathbb{Q})_{\text{tors}}| < \infty$.
Wir nennen r den (Mordell-Weil) Rang von E.

Reduktion

Für eine Primzahl p seien

- $\widetilde{E}/\mathbb{F}_p$ die Reduktion von E modulo p,
- $N_p = |\widetilde{E}(\mathbb{F}_p)|$,
- $a_p = p + 1 - N_p$.

Satz 2. (Hasse)
Es gilt $|a_p| \leq 2\sqrt{p}$.

- Birch und Swinnerton-Dyer fanden in Experimenten einen überraschenden Zusammenhang zwischen r und den Zahlen N_p.
- Dieser lässt sich am besten durch die L-Funktion von E beschreiben.

L-Funktion

Definition.
Sei Δ die Diskriminante der gegebenen Gleichung von E. Die komplexe L-Funktion von E ist definiert durch

$$L(E,s) = \prod_{p|\Delta} \frac{1}{1 - a_p p^{-s}} \prod_{p\nmid\Delta} \frac{1}{1 - a_p p^{-s} + p^{1-2s}}.$$

Die L-Funktion konvergiert a priori nur für $\Re(s) > 3/2$.

Außerdem sei N der Führer von E und

$$\Lambda(E,s) = N^{-s/2} \cdot \Gamma(s) \cdot L(E,s) \cdot (2\pi)^{-s}.$$

Satz 3 (Hecke, Shimura, Wiles et al.)
Die L-Funktion lässt sich analytisch auf ganz $\mathbb{C}$ fortsetzen und es gilt

$$\Lambda(E, 2-s) = \varepsilon \Lambda(E,s) \text{ mit } \varepsilon \in \{\pm 1\}.$$

BSD-Rangvermutung

Sei $r_{\mathrm{an}} := \mathrm{ord}_{s=1} L(E,s)$ der analytische Rang von E.

Vermutung 4. (BSD-Rangvermutung, Birch und Swinnerton-Dyer)
Es gilt $r = r_{\mathrm{an}}$.

- Vermutung 4 gilt für $r_{\mathrm{an}} \leq 1$ (Kolyvagin, Gross-Zagier, Wiles et al.)
- Für $r_{\mathrm{an}} \geq 2$ ist nichts allgemeines bekannt.

Die Vermutung kann aber numerisch in Beispielen überprüft werden. Man kann $L(E,s)$ und damit r_{an} folgendermaßen berechnen:

- durch numerische Approximierung mithilfe der Funktionalgleichung (Dokchitser);
- als $L(f_E, s)$, wobei $f_E \in S_2(\Gamma_0(N))$ die zu E gehörende Modulform ist (Cremona, Stein).

Rangberechnung I

Wie kann man den Rang r berechnen?

- Suche nach unabhängigen Punkten auf E liefert eine untere Schranke.
- Obere Schranken sind deutlich schwieriger.

Sei

- $n \in \mathbb{Z} \setminus \{0, \pm 1\}$,
- $[n] : E \to E$ Multiplikation mit n,
- $E[n] = \ker([n])$.

Dann ist die Sequenz

$$0 \longrightarrow E[n] \longrightarrow E \xrightarrow{[n]} E \longrightarrow 0$$

exakt.

Galois-Kohomologie

Notation.

- K: Körper mit algebraischem Abschluss $\overline{K}$,
- M: $\mathrm{Gal}\left(\overline{K}/K\right)$-Modul,
- Für $i \geq 1$ sei $H^i(K, M) = H^i\left(\mathrm{Gal}\left(\overline{K}/K\right), M\right)$.
- E und $E[n]$ sind $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$-Moduln.

Wir erhalten eine lange exakte Galois-Kohomologiesequenz

$$0 \longrightarrow E(\mathbb{Q})[n] \longrightarrow E(\mathbb{Q}) \xrightarrow{[n]} E(\mathbb{Q}) \xrightarrow{\delta} H^1(\mathbb{Q}, E[n]) \longrightarrow H^1(\mathbb{Q}, E)$$

$$\longrightarrow H^1(\mathbb{Q}, E).$$

Lokalisierung

Hieraus folgt die Exaktheit der kurzen Sequenz

$$0 \longrightarrow E(\mathbb{Q})/nE(\mathbb{Q}) \xrightarrow{\delta} H^1(\mathbb{Q}, E[n]) \longrightarrow H^1(\mathbb{Q}, E) \longrightarrow 0. \quad (1)$$

- Die Gruppe $E(\mathbb{Q})/nE(\mathbb{Q})$ ist endlich und Kenntnis ihrer Ordnung liefert uns den Rang.
- Es genügt, das Bild $\delta(E(\mathbb{Q})/nE(\mathbb{Q}))$ zu finden.
- Wir können (1) mittels Inflations-Restriktions-Sequenzen lokalisieren.

Lokalisierung

Hieraus folgt die Exaktheit der kurzen Sequenz

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(\mathbb{Q})/nE(\mathbb{Q}) & \xrightarrow{\delta} & H^1(\mathbb{Q}, E[n]) & \longrightarrow & H^1(\mathbb{Q}, E)[n] & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{res}_v} & & \downarrow{\scriptstyle \mathrm{res}_v} & & \downarrow{\scriptstyle \mathrm{res}_v} & & \\ 0 & \longrightarrow & E(\mathbb{Q}_v)/nE(\mathbb{Q}_v) & \xrightarrow{\delta_v} & H^1(\mathbb{Q}_v, E[n]) & \longrightarrow & H^1(\mathbb{Q}_v, E)[n] & \longrightarrow & 0. \end{array} \quad (1)$$

- Die Gruppe $E(\mathbb{Q})/nE(\mathbb{Q})$ ist endlich und Kenntnis ihrer Ordnung liefert uns den Rang.
- Es genügt, das Bild $\delta(E(\mathbb{Q})/nE(\mathbb{Q}))$ zu finden.
- Wir können (1) mittels Inflations-Restriktions-Sequenzen lokalisieren.

Lokalisierung

Hieraus folgt die Exaktheit der kurzen Sequenz

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(\mathbb{Q})/nE(\mathbb{Q}) & \xrightarrow{\delta} & H^1(\mathbb{Q}, E[n]) & \longrightarrow & H^1(\mathbb{Q}, E)[n] & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \prod_v \mathrm{res}_v} & & \downarrow{\scriptstyle \prod_v \mathrm{res}_v} & & \downarrow{\scriptstyle \prod_v \mathrm{res}_v} & & \\ 0 & \longrightarrow & \prod_v E(\mathbb{Q}_v)/nE(\mathbb{Q}_v) & \longrightarrow & \prod_v H^1(\mathbb{Q}_v, E[n]) & \longrightarrow & \prod_v H^1(\mathbb{Q}_v, E)[n] & \longrightarrow & 0. \end{array} \quad (1)$$

- Die Gruppe $E(\mathbb{Q})/nE(\mathbb{Q})$ ist endlich und Kenntnis ihrer Ordnung liefert uns den Rang.
- Es genügt, das Bild $\delta(E(\mathbb{Q})/nE(\mathbb{Q}))$ zu finden.
- Wir können (1) mittels Inflations-Restriktions-Sequenzen lokalisieren.

Selmer Gruppe

- $S^n(E) = \ker\left(H^1(\mathbb{Q}, E[n]) \to \bigcap_v H^1(\mathbb{Q}_v, E)[n]\right)$ heißt n-Selmer Gruppe von E.
- $Ш(E) = \ker\left(H^1(\mathbb{Q}, E)) \to \bigcap_v H^1(\mathbb{Q}_v, E)\right)$ heißt Shafarevich-Tate Gruppe von E.

Satz 5.

- Es gibt eine exakte Sequenz

$$0 \to E(\mathbb{Q})/nE(\mathbb{Q}) \to S^n(E) \to Ш(E)[n] \to 0.$$

- Die Gruppe $S^n(E)$ ist endlich.
- Wir erhalten eine obere Schranke für r, wenn wir $|S^n(E)|$ nach oben abschätzen können.

Prinzipale homogene Räume

- $H^1(\mathbb{Q}, E)$ ist isomorph zur Gruppe $WC(E)$ der Isomorphieklassen prinzipaler homogener Räume über E.
- Ein prinzipaler homogener Raum ist insbesondere ein Twist von E, d.h. eine Kurve $C/\mathbb{Q}$ vom Geschlecht 1, die über $\overline{\mathbb{Q}}$ zu E isomorph ist.
- Wir können die Elemente von $WC(E)$, die von $S^n(E)$ kommen, in der Praxis oft explizit berechnen. Falls wir $Ш(E)[n]$ kennen, so erhalten wir den Rang.
- Diese Technik heißt n-Abstieg und ist nicht effektiv.

Sei $[C] \in WC(E)$.

- $[C] \in Ш(E) \Leftrightarrow C(\mathbb{Q}_v) \neq \emptyset$ für alle v.
- Ist $[C] \in Ш(E)$ so gilt $[C] \neq 0 \Leftrightarrow C(\mathbb{Q}) = \emptyset$.

Shafarevich-Tate Gruppe

Vermutung 6. (Shafarevich-Tate)
Die Gruppe $Ш(E)$ ist endlich.

Satz 7. (Kolyvagin, et al.)
Vermutung 6 gilt für $r_{\mathrm{an}} \leq 1$.

Satz 8. (Cassels)
Aus $|Ш(E)| < \infty$ folgt $|Ш(E)| \in \mathbb{Z}^2$.

Weitere Invarianten

- Für p prim sei $E^0(\mathbb{Q}_p) = \{P \in E(\mathbb{Q}_p) : \widetilde{P} \text{ ist nichtsingulär}\}$.
- $c_p = |E(\mathbb{Q}_p)/E^0(\mathbb{Q}_p)|$ heißt Tamagawa-Zahl.
- $\Omega_E = \int_{E(\mathbb{R})} \frac{dx}{2y+a_1x+a_3}$ heißt reelle Periode.
- Für $P = (\frac{a}{b}, \frac{c}{d}) \in E(\mathbb{Q})$ sei $h(P) = \log \max\{|a|, |b|\}$.
- $\hat{h}(P) = \lim_{n\to\infty} \frac{h(2^n P)}{4^n}$ heißt kanonische Höhe.
- Erzeugen $P_1, \ldots, P_r$ den freien Anteil von $E(\mathbb{Q})$, so nennen wir $\mathrm{Reg}(E) = \det\left(\frac{1}{2}\left(\hat{h}(P_i + P_j) - \hat{h}(P_i) - \hat{h}(P_j)\right)_{i,j}\right)$ den Regulator.

BSD-Formel

Vermutung 9. (BSD-Formel, Birch und Swinnerton-Dyer)
Es gilt

$$\frac{L^{(r)}(E,1)}{r!} = \frac{\Omega_E \cdot \mathrm{Reg}(E) \cdot |Ш(E)| \cdot \prod_p c_p}{|E(\mathbb{Q})_{\mathrm{tors}}|^2}.$$

- Die Vermutung gilt bis auf eine rationale Konstante für $r_{\mathrm{an}} \leq 1$ (Kolyvagin et al.).
- Die Vermutung gilt für Führer $N < 5000$ (Miller et al.).

Berechnungsmethoden

- $|E(\mathbb{Q})_{\mathrm{tors}}|$: Nagell-Lutz, Reduktion $\mathrm{mod}\ p$ für gute Primzahlen;
- Ω_E: Arithmetisch-Geometrisches Mittel (Mestre);
- c_p: Algorithmus von Tate;
- $\mathrm{Reg}(E)$:
  - Zerlegung von $\hat{h}$ in lokale Höhen λ_v,
  - λ_p: explizite Formeln (Silverman, Cremona et al.),
  - λ_∞: Arithmetisch-Geometrisches Mittel (Bost-Mestre).

Jacobische Varietäten

- $C/\mathbb{Q}$: glatte projektive Kurve vom Geschlecht $g \geq 1$;
- $J = \mathrm{Jac}(C)$: Jacobische Varietät von C.
- Die Vermutungen und Resultate in diesem Abschnitt lassen sich auf beliebige abelsche Varietäten über Zahlkörpern verallgemeinern.

Satz 10. (Mordell-Weil)
Es gilt

$$J(\mathbb{Q}) \cong \mathbb{Z}^r \oplus J(\mathbb{Q})_{\mathrm{tors}}$$

mit $r \geq 0$ und $|J(\mathbb{Q})_{\mathrm{tors}}| < \infty$.

- Die L-Funktion $L(J, s) = L(C, s)$ lässt sich ähnlich wie im Fall $g = 1$ definieren.
- Sei $\Lambda(J, s) = N^{-s/2}\Gamma(s)^g L(J, s)(2\pi)^{-sg}$, wobei N der Führer von J ist.

BSD-Rangvermutung II

Vermutung 11. (Hasse-Weil)
Die L-Funktion lässt sich analytisch auf ganz $\mathbb{C}$ fortsetzen und es gilt

$$\Lambda(J, 2-s) = \varepsilon\Lambda(J, s) \text{ mit } \varepsilon \in \{\pm 1\}.$$

- Vermutung 11 gilt für J modular (Shimura) oder J mit komplexer Multiplikation (Shimura-Taniyama).

Sei $r_{\mathrm{an}} := \mathrm{ord}_{s=1} L(J, s)$ der analytische Rang von J.

Vermutung 12. (BSD-Rangvermutung, Tate)
Es gilt $r = r_{\mathrm{an}}$.

- Vermutung 12 gilt für $r_{\mathrm{an}} \leq 1$ und J modular (Kolyvagin).

BSD-Formel II

- Wir definieren $S^n(J)$ und $Ш(J)$ analog zum Fall $g = 1$.
- Für p prim sei die Tamagawa-Zahl c_p die Ordnung der $\mathbb{F}_p$-rationalen Punkte der Komponentengruppe des Néron-Modells von J.
- $\Omega_J = \int_{J(\mathbb{R})} \eta$ heißt reelle Periode, wobei η ein Néron-Differential ist.
- Erzeugen $P_1, \ldots, P_r$ den freien Anteil von $J(\mathbb{Q})$, so nennen wir $\mathrm{Reg}(J) = \det\left(\frac{1}{2}\left(\hat{h}(P_i + P_j) - \hat{h}(P_i) - \hat{h}(P_j)\right)_{i,j}\right)$ den Regulator, wobei $\hat{h}$ die kanonische Höhe auf J ist.

Vermutung 13. (BSD-Formel, Tate)
Es gilt

$$\frac{L^{(r)}(J,1)}{r!} = \frac{\Omega_J \cdot \mathrm{Reg}(J) \cdot |Ш(J)| \cdot \prod_p c_p}{|J(\mathbb{Q})_{\mathrm{tors}}|^2}.$$

Berechnungsmethoden II

- r: obere Schranke durch $|S^n(J)|$, untere Schranke durch Suchen nach unabhängigen Punkten;
- r_{an}:
  - numerische Approximierung mithilfe der Funktionalgleichung (Dokchitser),
  - für modulare J: mittels $L(f_J, s)$, wobei f_J die zu J gehörende Modulform ist (Stein,...);
- $|J(\mathbb{Q})_{\mathrm{tors}}|$: Reduktion $\mathrm{mod}\ p$ für gute Primzahlen;
- Ω_J: Explizite Integration auf $C(\mathbb{C})$ (Wetherell);
- c_p: Berechnung eines regulären Modells von C über $\mathrm{Spec}(\mathbb{Z}_p)$ (Raynaud).

Kanonische Höhe

- $K = J/\{\pm 1\}$: Kummersche Varietät zu J,
- $K \hookrightarrow \mathbb{P}^{2^g-1}$: explizite Einbettung von K,
- $\kappa : J \longrightarrow\!\!\!\!\!\rightarrow K \hookrightarrow \mathbb{P}^{2^g-1}$,
- $h : J \to \mathbb{R}$: Höhe auf J, definiert durch $h(P) = h(\kappa(P))$,
- $\hat{h}(P) = \lim_{n\to\infty} \frac{h(2^n P)}{4^n}$ heißt kanonische Höhe.
- Kann man $\hat{h}$ explizit berechnen und hat man eine Untergruppe G des freien Anteils von $J(\mathbb{Q})$ von endlichem Index, so kann man $\mathrm{Reg}(J)$ bis auf ein ganzzahliges Quadrat berechnen.

Berechnung der kanonischen Höhe

- Sei $g = 2$.
  - $\kappa(J)$ quartische Hyperfläche in $\mathbb{P}^3$;
  - $\exists$ Zerlegung von $\hat{h}$ in lokale Höhen $\lambda_v : K(\mathbb{Q}_v) \to \mathbb{R}$.
  - $\Rightarrow \exists$ explizite Formeln für λ_p (Flynn-Smart, Stoll, M.).
  - λ_∞ kann durch Teleskopreihen approximiert werden (Flynn-Smart).
- Sei $g \geq 3$. Hier ist die explizite Arithmetik von K zu kompliziert.
  - $\hat{h}(P) = -\sum_v \langle D, E \rangle_v$ für alle $D, E \in \mathrm{Div}^0(C)(\mathbb{Q})$ mit $[D] = [E] = P$ (Faltings-Hriljac); es gilt:
  - $\langle D, E \rangle_p$ ist durch arithmetische Schnitttheorie auf einem regulären Modell von C über $\mathrm{Spec}(\mathbb{Z}_p)$ gegeben und kann durch Gröbnerbasen (M.) oder Resultanten (Holmes) berechnet werden.
  - $\langle D, E \rangle_\infty$ kann durch die Riemannsche Thetafunktion ausgdrückt werden (Holmes, M.).

Numerische Evidenz

Satz 14. (Poonen-Stoll)
Aus $|Ш(J)| < \infty$ folgt $|Ш(J)| \in \mathbb{Z}^2$ oder $|Ш(J)| \in 2\mathbb{Z}^2$.

Ansatz um numerische Evidenz für die BSD-Formel zu erhalten: Wir berechnen

$$\mathrm{sha}_{\mathrm{conj}} = \frac{L^{(r)}(J,1) \cdot |J(\mathbb{Q})_{\mathrm{tors}}|^2}{r! \cdot \Omega_J \cdot \mathrm{Reg}(J) \cdot \prod_p c_p}$$

und überprüfen $\mathrm{sha}_{\mathrm{conj}} \in \mathbb{Z}^2$ oder $\mathrm{sha}_{\mathrm{conj}} \in 2\mathbb{Z}^2$.

- erfolgreich durchgeführt für 16 modulare Jacobische Flächen (Yoshida, Flynn-Leprevost-Schaefer-Stein-Stoll-Wetherell);
- für $g \geq 3$ bisher nicht möglich wegen fehlendem Algorithmus zur Regulatorenberechnung;
- Projekt: Überprüfung für modulare Jacobische zu hyperelliptischen Kurven (mit Balakrishnan und Stein).

p-adische L-Funktion

Notation.

- $J/\mathbb{Q}$: modular mit Modulform $f_J(z) = \sum_{n=1}^{\infty} a_n \exp(2\pi i n z)$,
- p: Primstelle gewöhnlicher guter Reduktion für J,
- $h(x) = x^2 - a_p x + p$.
- $L_p(J, u)$: die p-adische L-Funktion von J.

Satz 15.
$L_p(J, u)$ ist eine p-adisch analytische Funktion auf $D = \{z \in \mathbb{C}_p : |z - 1|_p < 1\}$. Ihre Taylor-Reihe $\mathcal{L}_p(J, T) \in \mathbb{C}_p[[T]]$ um $u = 1$ konvergiert auf $\{z \in \mathbb{C}_p : |z|_p < 1\}$.

Vermutung 16. (Mazur-Tate-Teitelbaum)
Es gilt $\operatorname{ord}_T \mathcal{L}_p(J,T) = r$.

- Für $g = 1$ und $\operatorname{ord}_T \mathcal{L}_p(J,T) \leq 1$ gilt die Vermutung (Perrin-Riou, Kolyvagin et al.).
- Es gilt $r \leq \operatorname{ord}_T \mathcal{L}_p(J,T)$ (Kato).
- Für $g = 1$ gilt $\mathcal{L}_p(J,0) = (1-\alpha^{-1})^2 \cdot L(J,1)/\Omega_J$, wobei $\alpha \in \mathbb{Z}_p^*$ Nullstelle von $h(x)$ ist.

$\Rightarrow$ Die BSD-Formel ist im Fall $g = 1, r = 0$ äquivalent zu

$$\mathcal{L}_p(J,0) = \left(1-\alpha^{-1}\right)^2 \frac{\operatorname{Reg}(J) \cdot |Ш(J)| \cdot \prod_p c_p}{|J(\mathbb{Q})_{\text{tors}}|^2}.$$

Können wir diese Formel auf beliebigen Rang verallgemeinern?

p-adische Höhe

Die BSD-Formel ist im Fall $g = 1, r = 0$ äquivalent zu

$$\mathcal{L}_p(J,0) = \left(1-\alpha^{-1}\right)^2 \frac{\mathrm{Reg}(J)\cdot|Ш(J)|\cdot\prod_p c_p}{|J(\mathbb{Q})_{\mathrm{tors}}|^2}.$$

Können wir diese Formel auf beliebigen Rang verallgemeinern?

- Sei $\mathcal{L}_p^*(J,0)$ der Leitkoeffizient der Potenzreihe $\mathcal{L}_p^*(J,T)$.
- Problem: $\alpha, \mathcal{L}_p^*(J,0) \in \mathbb{Q}_p$, aber $\mathrm{Reg}(J) \in \mathbb{R}$;
- Lösung: p-adische Höhe $h_p : J \to \mathbb{Q}_p$, eingeführt von Schneider, Néron, Mazur-Tate, Coleman-Gross, Nekovàř.
- Erzeugen $P_1, \ldots, P_r$ den freien Anteil von $J(\mathbb{Q})$, so heißt $\mathrm{Reg_p}(J) = \det\left(\frac{1}{2}\left(h_p(P_i+P_j) - h_p(P_i) - h_p(P_j)\right)_{i,j}\right)$ der p-adische Regulator.

p-adische BSD-Formel

Vermutung 17. (Mazur-Tate-Teitelbaum)
Ist E eine elliptische Kurve, so gilt

$$\mathcal{L}_p^*(E,0) = \frac{(1-\alpha^{-1})^2}{\log_p^r(1+p)} \cdot \frac{\mathrm{Reg}_p(E) \cdot |Ш(E)| \cdot \prod_p c_p}{|E(\mathbb{Q})_{\mathrm{tors}}|^2}.$$

- Der Normalisierungsfaktor $\frac{(1-\alpha^{-1})^2}{\log_p^r(1+p)}$ wurde durch numerische Experimente bestimmt und untermauert.
- $\mathcal{L}_p^*(E,0)$ kann mittels Riemannscher Summen approximiert werden (Stein).
- $\mathrm{Reg}_p(E)$ kann mithilfe von p-adischen σ-Funktionen berechnet werden (Mazur-Stein-Tate, Harvey).

Berechnung der p-adischen Höhe

Frage. Kann Vermutung 17 auf beliebige Jacobische verallgemeinert werden?

Problem.
Zur experimentiellen Untersuchung fehlte bisher eine Methode zur Berechnung des Regulators $\mathrm{Reg}_p(J)$.

Satz 18. (Coleman-Gross)
Es gilt $h_p(P) = -\sum_v (D,E)_v$ für alle $D, E \in \mathrm{Div}^0(C)(\mathbb{Q})$ mit $[D] = [E] = P$. Hierbei gilt:

- $(D,E)_\infty = 0$.
- Für Primzahlen $\ell \neq p$ ist $(D,E)_\ell$ durch arithmetische Schnitttheorie auf einem regulären Modell von C über $\mathrm{Spec}(\mathbb{Z}_\ell)$ gegeben und kann durch Gröbnerbasen (M.) oder Resultanten (Holmes) berechnet werden.
- Zur Berechnung von $(D,E)_p$ gibt es einen Algorithmus von Balakrishnan, der explizite Coleman-Integration benutzt.

p-adische BSD-Formel II

Für 16 modulare Jacobische Flächen und alle Primzahlen $p < 100$ guter, gewöhnlicher Reduktion ist die folgende Vermutung (bis auf $|Ш(J)|$) numerisch nachgewiesen worden:

Vermutung 19. (Balakrishnan-Stein-M.)
Angenommen der Hecke-Eigenwert a_p liegt in einem reell-quadratischen Zahlkörper K. Sei $\mathfrak{p} = p\mathcal{O}_K$.
Falls p in $\mathcal{O}_K$ träge ist, sei $\alpha \in K_{\mathfrak{p}}^*$ mit $h(\alpha) = 0$. Dann gilt

$$\mathcal{L}_p^*(J,0) = \pm \frac{\left(1-\alpha^{-1}\right)^2 \cdot \left(1-\overline{\alpha}^{-1}\right)^2}{\log_p^r(1+p)} \cdot \frac{\mathrm{Reg}_p(J) \cdot |Ш(J)| \cdot \prod_p c_p}{|J(\mathbb{Q})_{\mathrm{tors}}|^2}.$$

Ansonsten ist $\mathfrak{p} = \mathfrak{p}_1\mathfrak{p}_2$. Seien $\alpha_i \in K_{\mathfrak{p}_i}^*$ mit $h(\alpha_i) = 0$. Dann gilt

$$\mathcal{L}_p^*(J,0) = \pm \frac{\left(1-\alpha_1^{-1}\right)^2 \cdot \left(1-\alpha_2^{-1}\right)^2}{\log_p^r(1+p)} \cdot \frac{\mathrm{Reg}_p(J) \cdot |Ш(J)| \cdot \prod_p c_p}{|J(\mathbb{Q})_{\mathrm{tors}}|^2}.$$