Reziprozitätsgesetze und ganzzahlige Lösungen von Polynomialgleichungen

Jean-Louis Colliot-Thélène
CNRS
Université Paris-Sud

Mathematisches Kolloquium, Regensburg
8. Dezember 2005

Kongruenzen, Lokale Körper

Sei $f(x_1, \cdots, x_n)$ ein Polynom mit ganzzahligen Koeffizienten. Seit eh und je haben die Menschen Interesse für (primitive) ganzzahlige Lösungen der Gleichung

$$f(x_1, \cdots, x_n) = 0$$

gehabt.

Manchmal kann man schnell entscheiden, daß es keine Lösung gibt.
Die Gleichung $x^2 + y^2 + 1 = 0$ kann man schon im Körper $\mathbf{R}$ der reellen Zahlen nicht lösen.
Mittels Kongruenzen kann man auch oft entscheiden, daß es keine Lösung gibt.
Daß die Gleichung $x^2 + y^2 - 3z^2 = 0$ keine nicht-triviale Lösung hat, kann man sehen, indem man Kongruenzen modulo 9 benutzt – oder auch Kongruenzen modulo 4.
Sei p eine Primzahl. Mittels Kongruenzen modulo p^3 zeigt man, daß die Gleichung

$$x^3 + py^3 + p^2z^3 = 0$$

keine nicht-triviale Lösung hat.

Kurt Hensel verdankt man die Einführung der lokalen Körper. Zu jeder Primzahl p wird ein kommutativer Integritätbereich $\mathbf{Z}_p$ assoziiert. Der Quotientenkörper $\mathbf{Q}_p$ von $\mathbf{Z}_p$ ist die Komplettierung von $\mathbf{Q}$ bezüglich der p-adischen Metrik

$$|p^n \cdot a/b|_p = 1/p^n$$

($a, b \in \mathbf{Z}$, a und b prim zu p.)
Eine Gleichung $f(x_1, \cdots, x_n) = 0$ wie oben hat dann und nur dann eine (primitive) Lösung in $\mathbf{Z}_p$, wenn sie eine (primitive) Lösung modulo einer beliebigen Potenz von p hat.

Mit $X(R)$ bezeichnen wir die Menge aller Lösungen von $f(x_1, \cdots, x_n) = 0$ mit Koordinaten in einem kommutativen Ring R. Dann hat man natürliche Einbettungen

$$X(\mathbf{Z}) \subset \prod_p X(\mathbf{Z}_p)$$

$$X(\mathbf{Q}) \subset \prod_p X(\mathbf{Q}_p)$$

Dabei ist p entweder eine Primzahl oder $p = \infty$, im letzten Fall wird $\mathbf{Z}_\infty = \mathbf{Q}_\infty = \mathbf{R}$ gesetzt.
Eigentlich hat man eine präzisere Einbettung

$$X(\mathbf{Q}) \subset X(A_\mathbf{Q}),$$

wo $X(A_\mathbf{Q}) \subset \prod_p X(\mathbf{Q}_p)$ die Menge der Adele von X bezeichnet.

Der Satz von Legendre

Satz (Legendre, 1785) *Sei $q(x, y, z)$ eine ganzzahlige quadratische Form. Wenn die Gleichung $q(x, y, z) = 0$ nicht-triviale Lösungen in allen $\mathbf{Z}_p$, einschließlich $\mathbf{R}$, besitzt, dann hat sie eine nicht-triviale Lösung in $\mathbf{Z}$.*

Der Beweis gehört der Geometrie der Zahlen an. Er liefert eine obere Schranke für die Höhe der kleinsten Lösung.

Die üblichen Beweise benutzen nicht die volle Voraussetzung: man kann auf die reelle Annahme $X(\mathbf{R}) \neq \emptyset$ verzichten. Insbesondere wird diese Bedingung von den anderen Annahmen $X(\mathbf{Z}_p) \neq \emptyset$, p endlich, erzwungen.

Das quadratische Reciprozitätgesetz (theorema fundamentale)

Sei $p \neq 2$ eine Primzahl, $a \in \mathbf{Z}$ prim zu p,
Legendre Symbol $(a/p) = \pm 1$
$(a/p) = 1$ dann und nur dann, wenn a ein Quadrat mod. p ist.

p, q ungerade Primzahlen. Dann hat man

$$(p/q)(q/p) = (-1)^{(p-1)/2.(q-1)/2}$$

Dies wurde von Euler und Legendre (1785) unabhängig vermutet.
Erster Beweis, Gauß, 18. April 1796.

Sei p eine ungerade Primzahl.
Erster Ergänzungssatz

$$(-1/p) = (-1)^{(p-1)/2}$$

Also : -1 ist ein Quadrat modulo p dann und nur dann, wenn $p \equiv 1(4)$.

Zweiter Ergänzungssatz

$$(2/p) = (-1)^{(p^2-1)/8}$$

Also : 2 ist ein Quadrat modulo p dann und nur dann, wenn $p \equiv \pm 1(8)$.

Das Hasse-Prinzip für quadratische Formen

Satz (Minkowski, Hasse 1920) *Sei $n \geq 2$. Sei $q(x_1, \cdots, x_n)$ eine ganzzahlige quadratische Form. Wenn die Gleichung*

$$q(x_1, \cdots, x_n) = 0$$

nicht-triviale Lösungen in allen $\mathbf{Z}_p$ einschließlich $\mathbf{R}$ hat, dann hat sie auch eine nicht-triviale Lösung in $\mathbf{Z}$.
Der Hauptpunkt im Beweis von Hasse liegt bei dem Übergang von 3 Variablen (Satz von Legendre) zu 4 Variablen. Dabei benutzt Hasse den Dirichletschen Satz über Primzahlen in einer arithmetischen Progression.

Hauptfrage : **Gilt solch ein Lokal-Global Satz, oder wenigstens ein Ersatz, für andere Familien von Gleichungen ?**

Daß das Hasse-Prinzip im ursprünglichen Sinne allgemein nicht gilt, zeigen viele Beispiele.

Ein Beispiel von Lind (1940)
Es handelt sich um eine Kurve von Geschlecht 1, mit Punkten in allen $\mathbf{Q}_p$ und $\mathbf{R}$, die keinen Punkt in $\mathbf{Q}$ besitzt.

$$2y^2 = x^4 - 17, \quad x, y \in \mathbf{Q}$$

$$2u^2 = v^4 - 17w^4 \neq 0, \quad u, v, w \in \mathbf{Z}, \quad (v, w) = 1$$

Modulo 17^2 sieht man daß u durch 17 nicht teilbar ist. Da 2 keine vierte Potenz modulo 17 ist, folgt : *u ist kein Quadrat modulo 17.* p ungerade Primzahl, p teilt u (also $p \neq 17$) $\Longrightarrow$ 17 Quadrat modulo $p \Longrightarrow$(quadratisches Reziprozitätsgesetz) p Quadrat modulo 17. Also, ist 2 ein Quadrat modulo 17. Also *u ist ein Quadrat modulo 17.*
Widerspruch, $X(\mathbf{Q}) = \emptyset$.

Ein Beispiel von Iskovskikh (1971)

Es handelt sich um eine "rationale" Fläche, die Punkte in allen $\mathbf{Q}_p$ und $\mathbf{R}$ besitzt, in $\mathbf{Q}$ aber keine.

$$y^2 + z^2 = (3 - x^2)(x^2 - 2)$$

Lösung mit $x, y, z \in \mathbf{Q}$? $u^2 + v^2 = (3y^2 - x^2)(x^2 - 2y^2) \neq 0$, mit $u, v, x, y \in \mathbf{Z}, (x, y) = 1$

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

Modulo 4 nimmt $(3y^2 - x^2, x^2 - 2y^2)$ eine von den folgenden Werten :

$$(2, -1), (-1, 1), (3, 2)$$

Auf $\mathbf{R}$ hat man $3y^2 - x^2 > 0$, $x^2 - 2y^2 > 0$.

Sei p eine Primzahl. Wenn p^{2n+1} entweder $3y^2 - x^2$ oder $x^2 - 2y^2$ genau teilt, dann wird $u^2 + v^2$ genau von p^{2n+1}geteilt, also ist -1 ein Quadrat mod. p, also (erster Ergänzungssatz) $p \equiv 1$ mod. 4. Also nimmt $(3y^2 - x^2, x^2 - 2y^2)$ eine von den folgenden Werten modulo 4 :

$$(1,1), (2,1), (1,2)$$

also keine von den Werten

$$(2,-1), (-1,1), (3,2)$$

Widerspruch, $X(\mathbf{Q}) = \emptyset$.

Ein Beispiel von Borovoi und Rudnick (1995)

$$q(x, y, z) = -9x^2 + 2xy + 7y^2 + 2z^2$$

d.h.

$$-9x^2 + 2xy + 7y^2 + 2z^2 = 1$$

d.h.

$$(x - y)^2 + 8(x - y)(x + y) = 2z^2 - 1$$

Lösung auf $\mathbf{Q}$

$$q(-1/2, 1/2, 1) = 1$$

also Lösungen in allen $\mathbf{Z}_p$ für $p \neq 2$.

Lösung auf $\mathbf{Z}_2$, $q(4, 1, 1) = -127 \equiv 1(8)$.

Lösung mit $(x, y, z) \in \mathbf{Z}$?

Betrachtet man die Gleichung modulo Potenzen von 2, so erhält man

$$x - y \equiv \pm 3(8)$$

Sei p eine Primzahl.
Wenn $x - y$ durch p teilbar ist, dann auch $2z^2 - 1$
$\Longrightarrow$ p ungerade und 2 Quadrat mod. p
(zweiter Ergänzungssatz) $\Longrightarrow$ $p \equiv \pm 1(8)$.
Also $x - y \equiv \pm 1(8)$.
Widerspruch, $X(\mathbf{Z}) = \emptyset$.

Brauergruppe eines Körpers

Sei k ein Körper der Charakteristik Null, $\overline{k}$ ein algebraischer Abschluß.

Seien $a, b \in k^*$. Die k-Algebra $A = (a, b)_k$, die durch die Relationen

$$i^2 = a, j^2 = b, ij = -ji$$

definiert ist, hat die Dimension 4 über k, für sie gilt

$$A \otimes \overline{k} \simeq M_2(\overline{k}).$$

Das klassische Beispiel geht auf Hamilton zurück : $k = \mathbf{R}$, $a = b = -1$.

Allgemein wird eine k-Algebra A eine zentrale einfache Algebra (früher Hyperkomplexensystem) genannt, wenn es eine ganze Zahl $n \geq 1$ gibt, so daß $A \otimes_k \overline{k} \simeq M_n(\overline{k})$.
Der Tensorprodukt zweier zentraler einfacher k-Algebren ist wieder eine solche.
Wenn man zwei solche k-Algebren als äquivalent betrachtet, wenn es ganze Zahlen $r, s \geq 1$ gibt, so daß $M_r(A) \simeq M_s(B)$, dann definiert das Tensorprodukt eine Gruppenstruktur auf der Menge der Äquivalenzklassen. Dies ist die Brauergruppe von k. Sie wird $\mathrm{Br}(k)$ bezeichnet.

Klassenkörpertheorie

Lokale Klassenkörpertheorie

$$\mathrm{Br}(\mathbf{Q}_p) \simeq \mathbf{Q}/\mathbf{Z}.$$

$$\mathrm{Br}(\mathbf{R}) = \mathbf{Z}/2$$

Die fundamentale exakte Folge der globalen Klassenkörpertheorie

$$0 \to \mathrm{Br}(\mathbf{Q}) \to \bigoplus_{p \cup \infty} \mathrm{Br}(\mathbf{Q}_p) \to \mathbf{Q}/\mathbf{Z} \to 0.$$

Der Kegelschnitt $x^2 - ay^2 - bt^2 = 0$ über dem Körper k (Char.(k) $\neq 2$) besitzt einen rationalen Punkt (mit Koordinaten in k) dann und nur dann, wenn die Klasse der Quaternionenalgebra $(a, b)_k \in \mathrm{Br}(k)$ Null ist.
Die Summenformel $\sum_p (a, b)_p = 0$ enthält das quadratische Reziprozitätsgesetz so wie auch die beiden Ergänzungssätze.
Den Satz von Legendre kann man so umformulieren : Wenn $(a, b)_p \in \mathbf{Z}/2 \subset \mathrm{Br}(\mathbf{Q}_p)$ für alle Primzahlen p (endlich und unendlich) verschwindet , dann folgt $(a, b) = 0 \in \mathrm{Br}(\mathbf{Q})$.
Da $\sum_p (a, b)_p = 0$ braucht man nur das Verschwinden von $(a, b)_p$ bei allen p (endlich und unendlich) *bis auf eins* vorauszusetzen.

Die Brauergruppe eines Schemas

Auf einer algebraischen Mannigfaltigkeit, oder allgemeiner auf einem Schema, sind die Vektorbündel die natürlichen Analoga von Vektorräumen über einem Körper.
Azumaya Algebren über einem Schema sind die natürlichen Analoga von zentralen einfachen Algebren über einem Körper.
Man kann eine Äquivalenzrelation unter den Azumaya Algebren auf einem Schema X einführen, ähnlich wie bei Körpern. Die Menge der Äquivalenzklassen ist eine Gruppe, die Brauergruppe $\mathrm{Br}(X)$ von X.
Wenn X ein $\mathbf{Z}$-Schema ist, dann hat man für einen beliebigen kommutativen Ring R eine Paarung $X(R) \times \mathrm{Br}(X) \to \mathrm{Br}(R)$.

Die Brauer-Maninsche Bedingungen

Satz (Manin, 1970). *Sei X eine projektive Mannigfaltigkeit über $\mathbf{Q}$. Das Bild von $X(\mathbf{Q})$ in $X(A_{\mathbf{Q}}) = \prod_p X(\mathbf{Q}_p)$ liegt im Linkskern der (wohldefinierten) Paarung*

$$X(A_{\mathbf{Q}}) \times \mathrm{Br}(X) \to \mathbf{Q}/\mathbf{Z}$$

$$(\{M_p\}, \alpha) \mapsto \sum_p \mathrm{ev}_A(M_p).$$

Diesen Kern bezeichnet man mit $X(A_{\mathbf{Q}})^{\mathrm{Br}(X)}$.

Ganzzahlige Variante :

Satz *Sei X ein $\mathbf{Z}$-Schema von endlichem Typ. Das Bild von $X(\mathbf{Z})$ in $\prod_p X(\mathbf{Z}_p)$ liegt im Linkskern der (wohldefinierten) Paarung*

$$\prod_p X(\mathbf{Z}_p) \times \mathrm{Br}(X_{\mathbf{Q}}) \to \mathbf{Q}/\mathbf{Z}$$

$$(\{M_p\}, \alpha) \mapsto \sum_p \mathrm{ev}_A(M_p).$$

Diesen Kern bezeichnet man mit $(\prod_p X(\mathbf{Z}_p))^{\mathrm{Br}(X_{\mathbf{Q}})}$.
Wir paaren mit $\mathrm{Br}(X_{\mathbf{Q}})$. Die etwas natürlichere Paarung mit $\mathrm{Br}(X)$ würde weniger Information liefern.

Brauer-Maninsche Erklärung des Lindschen Beispiels
Durch die Gleichung

$$2y^2 = x^4 - 17 \neq 0$$

wird eine offene Menge U einer glatten projektiven Kurve $X/\mathbf{Q}$ definiert.
Es gilt $\prod_{p\cup\infty} X(\mathbf{Q}_p) \neq \emptyset$.
Die Azumaya Algebra $(y, 17) \in \mathrm{Br}(U)$ wird durch ein $A \in \mathrm{Br}(X)$ induziert.
Das Bild von

$$ev_A : X(\mathbf{Q}_p) \to \mathrm{Br}(\mathbf{Q}_p) \subset \mathbf{Q}/\mathbf{Z}$$

ist gleich Null wenn $p \neq 17$. Falls $p = 17$ so ist dieses Bild $\{1/2\} \subset \mathbf{Q}/\mathbf{Z}$.
Also $X(\mathbf{Q}) = \emptyset$.

Brauer-Maninsche Erklärung des Beispiels von Iskovskikh
Sei $c \in \mathbf{Z}, c > 0, c$ ungerade. Die Gleichung

$$y^2 + z^2 = (c - x^2)(x^2 - c + 1) \neq 0$$

definiert eine offene Menge U_c in einer glatten projektiven Fläche $X_c/\mathbf{Q}$.
Es gilt $\prod_{p \cup \infty} X_c(\mathbf{Q}_p) \neq \emptyset$.
Die Azumaya Algebra $(c - x^2, -1) \in \mathrm{Br}(U_c)$ wird durch ein $A \in \mathrm{Br}(X_c)$ induziert.

Wenn $p \neq 2$, dann ist das Bild von

$$ev_A : X_c(\mathbf{Q}_p) \to \mathrm{Br}(\mathbf{Q}_p) \subset \mathbf{Q}/\mathbf{Z}$$

gleich Null.
Wenn $p = 2$, stimmt dieses Bild mit $\{1/2\} \subset \mathbf{Q}/\mathbf{Z}$ überein dann und nur dann, wenn $c \equiv 3(4)$.
Also : *Wenn* $c \equiv 3(4)$, *dann ist* $X_c(A_{\mathbf{Q}})^{\mathrm{Br}(X)} = \emptyset$, *also auch* $X_c(\mathbf{Q}) = \emptyset$.
Mit der obigen Berechnung kann man zeigen : *Wenn* $c \equiv 1(4)$, *dann ist* $X_c(A_{\mathbf{Q}})^{\mathrm{Br}(X)} \neq \emptyset$.
Satz *Wenn* $c \equiv 1(4)$ *dann ist* $X_c(\mathbf{Q}) \neq \emptyset$.
(spezieller Fall eines Satzes von CT, Coray und Sansuc, 1981)

Brauer-Maninsche Bedingung und ganzahlige Lösungen : mehr Beispiele

Seien n, m, k positive ganze Zahlen, $(n, m) = 1$. Die Gleichung

$$m^2x^2 + n^{2k}y^2 - nz^2 = 1$$

kann man auch

$$(1 + n^k y)(1 - n^k y) = m^2x^2 - nz^2$$

umschreiben. Deren Lösung mit $(x, y, z) \in \mathbf{Z}$ wurde von F. Xu und R. Schulze-Pillot analysiert. Sei $X/\mathbf{Z}$ das Schema, das diese Gleichung definiert.

Es gilt $\prod_{p \cup \infty} X(\mathbf{Z}_p) \neq \emptyset$. Sei $U_{\mathbf{Q}} \subset X_{\mathbf{Q}}$ die offene Menge, die durch $1 + n^k y \neq 0$ definiert ist. Die Azumaya Algebra $(1 + n^k y, n) \in \mathrm{Br}(U_{\mathbf{Q}})$ wird von einem Element $A \in \mathrm{Br}(X_{\mathbf{Q}})$ induziert.

Wenn $p \neq 2$, das Bild

$$ev_A : X(\mathbf{Z}_p) \to \mathrm{Br}(\mathbf{Q}_p) \subset \mathbf{Q}/\mathbf{Z}$$

ist gleich Null.
Wenn $p = 2$, dann stimmt dieses Bild mit $\{1/2\} \subset \mathbf{Q}/\mathbf{Z}$ überein dann und nur dann, wenn
(i) 2 teilt m genau und $n \equiv 5\ (8)$ oder (ii) 4 teilt m und $n \equiv 3 \ \text{oder} \ 5\ (8)$
Also $X(\mathbf{Z}) = \emptyset$ in den beiden obigen Fällen.

Satz (F. Xu und R. Schulze-Pillot, 2004). *In allen anderen Fällen ist* $X(\mathbf{Z}) \neq \emptyset$.
Einen anderen Beweis liefert der folgende, allgemeine Satz.

Satz *Sei $q(x_1, \cdots, x_n)$ eine quadratische Form vom Rang n, mit ganzzahligen Koeffizienten, indefinit über $\mathbf{R}$, und sei $a \in \mathbf{Z}$, $a \neq 0$. Sei $X/\mathbf{Z}$ das $\mathbf{Z}$-Schema, das durch die Gleichung $q(x_1, \cdots, x_n) = a$ definiert ist. Nehmen wir an, $\prod_p X(\mathbf{Z}_p) \neq \emptyset$.*
(a) Wenn $n \geq 4$, dann ist $X(\mathbf{Z}) \neq \emptyset$: man kann $q(x_1, \cdots, x_n) = a$ in $\mathbf{Z}$ lösen.
(b) Sei $n = 3$ und $-a \cdot det(q)$ kein Quadrat. Dann ist $\mathrm{Br}(X_{\mathbf{Q}})/\mathrm{Br}(\mathbf{Q}) = \mathbf{Z}/2$, von einem $A \in \mathrm{Br}(X_{\mathbf{Q}})$ erzeugt. Es ist $X(\mathbf{Z}) \neq \emptyset$ dann und nur dann, wenn die Abbildung

$$\prod_p X(\mathbf{Z}_p) \to \mathbf{Q}/\mathbf{Z}$$

$$\{M_p\} \mapsto \sum_p \mathrm{ev}_A(M_p)$$

die Null in ihrem Bild enthält .

Der Satz (a) wurde in den fünfziger Jahren bewiesen (Eichler; Kneser, Watson).
Der Satz (b) ist eine Variante (CT/F.Xu, 2005) eines Satzes von Borovoi und Rudnick (1995).
Schwerpunkte des Beweises sind :
der starke Approximationssatz für die Spinorgruppe einer indefiniten quadratischen Form
die Darstellung von der affinen Quadrik $q = a$ über $\mathbf{Q}$, sobald sie einen rationalen Punkt besitzt, als ein Raum G/T, wo $G/\mathbf{Q}$ die Spinorgruppe von q ist, und T ein 1-dimensionaler algebraischer $\mathbf{Q}$-Torus ist.

Eine explizite Algebra A berechnet man folgenderweise. Sei M ein $\mathbf{Q}$-rationaler Punkt auf $q(x, y, z) = a$. Sei $l(x, y, z) = 0$ die Gleichung der tangentialen Ebene zur affiner Quadrik $X_{\mathbf{Q}}$ im Punkte M.
Dann nimmt man

$$A = (l(x, y, z), -a \cdot det(q)).$$

Homogene Räume von linearen algebraischen Gruppen

Das Hasse-Prinzip für prinzipalhomogene Räume von halbeinfachen einfach zusammenhängenden algebraischen Gruppen wurde im 20en Jahrhundert bewiesen (Hasse, Landherr, Eichler, Kneser, Harder, Chernousov).
Eine Folgerung ist die folgende Verallgemeinerung des Satzes von Minkowski und Hasse :
Satz (Harder, 1970) *Sei $X/\mathbf{Q}$ eine projektive Mannigfaltigkeit, die ein homogener Raum einer zusammenhängenden linearen Gruppe ist. Dann gilt das Hasse-Prinzip für X.*

Eine andere Folgerung ist der

Satz *Sei $X/\mathbf{Q}$ eine glatte projektive Mannigfaltigkeit, die eine offene Menge U enthält, die ihrerseits ein homogener Raum einer zusammenhängenden linearen Gruppe ist. Nehmen wir an, daß die geometrischen Isotropiegruppen von U zusammenhängend sind. Dann liegt $X(\mathbf{Q})$ dicht in $X(A_{\mathbf{Q}})^{\mathrm{Br}(X)}$.*
Insbesondere folgt aus $X(A_{\mathbf{Q}})^{\mathrm{Br}(X)} \neq \emptyset$ daß $X(\mathbf{Q}) \neq \emptyset$.
(Sansuc 1981, Borovoi, 1996)

Kurven vom Geschlecht 1

Beispiele : nichtsinguläre kubische Kurven in der Ebene $\mathbf{P}^2$, nichtsinguläre Durchschnitte zweier Quadriken im Raum $\mathbf{P}^3$.
Eine elliptische Kurve über $\mathbf{Q}$ ist eine Kurve vom Geschlecht 1 mit einer Gruppenstruktur, im Besonderen mit einem speziellen rationalen Punkt.

Zu jeder nichtsingulären projektiven Kurve $X/\mathbf{Q}$ vom Geschlecht 1 wird eine elliptische Kurve $J = J_X$ über $\mathbf{Q}$, die Jacobische Varietät von X, assoziiert. Die Kurve X ist ein prinzipalhomogener Raum unter J.

Die Menge aller Isomorphieklassen von Kurven $X/\mathbf{Q}$ vom Geschlecht 1 mit derselben Jacobischen Varietät $J_X = J$ hat eine natürliche abelsche Gruppenstruktur, es ist die Weil-Châtelet Gruppe $WC(J)$. Die Klasse von X in $WC(J)$ ist dann und nur dann Null, wenn $X(\mathbf{Q}) \neq \emptyset$.
Die Tate-Shafarevich Untergruppe

$$Ш(J) \subset WC(J)$$

besteht aus den Klassen von Kurven, die rationale Punkte in allen $\mathbf{Q}_p$ besitzen.

Hauptvermutung *Jede Gruppe* $Ш(J)$ *ist endlich.*

Satz (Manin 1970). *Sei* $Ш(J_X)$ *endlich. Wenn* $X(A_{\mathbf{Q}})^{\mathrm{Br}(X)} \neq \emptyset$, *dann ist* $X(\mathbf{Q}) \neq \emptyset$.

Dies folgt aus Ergebnissen von Cassels. Cassels hat auf der Gruppe $Ш(J)$ eine alternierende Form definiert, mit Werten in $\mathbf{Q}/\mathbf{Z}$. Ist $Ш(J)$ endlich, so ist diese Form nicht entartet.
Daraus folgt dann, daß für $r \geq 1$, die Untergruppe ${}_rШ(J)$ der Elemente von $Ш(J)$, die von r annulliert sind, eine direkte Summe von Gruppen der Gestalt $(\mathbf{Z}/n)^2$ ist. Insbesondere ist die Ordnung dieser Untergruppe ein Quadrat.

Es folgt ein bescheidenes Hasse-Prinzip :

Satz

Sei $X/\mathbf{Q}$ eine Kurve vom Geschlecht 1 und ℓ eine Primzahl. Angenommen es gelten die folgenden Bedingungen

(i) $Ш(J_X)$ ist endlich.

(ii) Für alle p ist $X(\mathbf{Q}_p) \neq \emptyset$.

(iii) Die Gruppe ${}_\ell Ш(J)$ hat höchstens ℓ Elemente.

(iv) Die Klasse von X in $Ш(J)$ wird von ℓ annulliert.

Dann ist $X(\mathbf{Q}) \neq \emptyset$.

Flächen, die eine Schar von Kurven vom Geschlecht Null besitzen

Satz *Seien* $a(t), b(t), c(t) \in \mathbf{Q}[t]$, $abc \neq 0$. *Sei* $X/\mathbf{Q}$ *eine nichtsinguläre projektive Fäche, die birational der Fläche mit affiner Gleichung*

$$a(t)x^2 + b(t)y^2 + c(t) = 0$$

ist. Gilt die Schinzelsche Vermutung, so liegt $X(\mathbf{Q})$ *dicht in* $X(A_{\mathbf{Q}})^{\mathrm{Br}(X)}$.
(CT/Sansuc 1978, Serre 1992, CT/Swinnerton-Dyer 1994)

Die Schinzelsche Vermutung

Seien $P_1(t), \cdots, P_m(t)$ irreduzible Polynome mit ganzzahligen Koeffizienten und positiven Leitkoeffizienten. Angenommen es gibt keine Primzahl, die alle $\prod_i P_i(n)$, $n \in \mathbf{Z}$, teilt. Dann gibt es unendlich viele $n \in \mathbf{N}$ so daß jedes $P_i(n)$ eine Primzahl ist.

Der einzige bewiesene Fall ist der Fall $m = 1$, $P_1(t) = at + b$ (Dirichlet).
Ein spezieller Fall der Vermutung ist der "Satz" über Primzahlzwillinge.
Allgemeinere spezielle Fälle dieser Vermutung gehen auf Bouniakowsky und Dickson zurück.

Wenn die Anzahl der $t \in \overline{\mathbf{Q}}$ mit $a(t)b(t)c(t) = 0$ sehr klein ist (höchstens 5), dann kann man den obigen Satz beweisen, ohne die Schinzelsche Vermutung zu benutzen
(CT/Sansuc/Swinnerton-Dyer 1984; CT 1990;
Salberger/Skorobogatov 1991).
Darauf aufbauend kann man den folgenden Satz beweisen (CT/Sansuc/SwD 1987) :

Satz *Sei $n \geq 8$. Wenn ein nichtsingulärer Durchschnitt zweier Quadriken im $\mathbf{P}^n_{\mathbf{Q}}$ einen reellen Punkt besitzt, dann besitzt er auch einen rationalen Punkt.*

Frühere Ergebnisse : Mordell ($n \geq 12$); Swinnerton-Dyer ($n \geq 10$).

Flächen, die eine Schar von Kurven vom Geschlecht 1 besitzen

Wir haben einen sehr speziellen Fall eines Hasse-Prinzips für besondere Kurven vom Geschlecht 1 erwähnt. Swinnerton-Dyer hat sich auf diese winzige Krücke gestützt, um eine Methode zu entwickeln, die die Existenz rationaler Punkte auf bestimmten Flächen, die eine Schar von Kurven vom Geschlecht 1 besitzen, voraussagt.

Die erste, spezielle, Arbeit ist 1995 erschienen. Andere Arbeiten sind gefolgt (CT/Skorobogatov/SwD, Bender/SwD, SwD, CT, Skorobogatov/SwD, Wittenberg). Hier werde ich die Technik überhaupt nicht beschreiben, sondern einige markante Sätze zitieren.

Satz (Swinnerton-Dyer, 2001) *Seien* $a_i \in \mathbf{Z}, i = 0, \cdots, 3$ *ganze kubikfreie Zahlen die keinen gemeinsamen Teiler besitzen. Sei* $X \subset \mathbf{P}^3_{\mathbf{Q}}$ *die kubische Fläche*

$$\sum_{i=0}^{3} a_i T_i^3 = 0.$$

Sei eine der folgenden Bedingungen erfüllt: (i) Es gibt eine Primzahl $p \neq 3$*, die* a_0 *teilt und keines der anderen* a_i*, und es gibt eine Primzahl* $q \neq 3$*, die* a_1 *teilt und keines der anderen* a_i*.*
(ii) Es gibt eine Primzahl $p \neq 3$*, die* a_0 *teilt und keines der anderen* a_i*, und die Klassen von* a_1, a_2, a_3 *in* $\mathbf{F}_p^*/\mathbf{F}_p^{*3}$ *sind nicht alle gleich. Nehmen wir an, Tate-Shafarevich Gruppen sind endlich. Dann gilt das Hasse-Prinzip für* X*.*

Satz (Swinnerton-Dyer 2001)
Nehmen wir an, Tate-Shafarevich Gruppen sind endlich. Dann gilt das Hasse-Prinzip für eine beliebige diagonale kubische Hyperfläche

$$\sum_{i=0}^{n} a_i T_i^3 = 0$$

über $\mathbf{Q}$, *sobald* $n \geq 4$.

Die zwei folgenden Sätze stellen die Krönung einer Reihe von Arbeiten dar (CT/Skorobogatov/Swinnerton-Dyer, Swinnerton-Dyer/Bender, CT, Harari).

Satz (Wittenberg, 2005)
Seien $q_1(x_0, \cdots, x_4)$ *und* $q_2(x_0, \cdots, x_4)$ *zwei quadratische Formen mit Koeffizienten in* $\mathbf{Q}$. *Die Gleichungen*

$$q_1(x_0, \cdots, x_4) = 0, q_2(x_0, \cdots, x_4) = 0$$

mögen eine nichtsinguläre Fläche $X \subset \mathbf{P}^4_{\mathbf{Q}}$ *definieren.*
Ist die Galoisgruppe der Gleichung $\det(\lambda q_1 + \mu q_2)$ *die symmetrische Gruppe* S_5, *gilt die Schinzelsche Vermutung und sind Tate-Shafarevich-Gruppen stets endlich, dann gilt das Hasse-Prinzip für* X.

Satz (Wittenberg, 2005)
Sei $X \subset \mathbf{P}^n_{\mathbf{Q}}$, $n \geq 5$ *ein nichtsingulärer Durchschnitt zweier Quadriken. Die Schinzelsche Vermutung und die Endlichkeit von Tate-Shafarevich Gruppen angenommen, gilt das Hasse-Prinzip für* X.

Vielen Dank für Ihre Aufmerksamkeit!

Die sogenannte Zirkelmethode (Hardy, Littlewood) ist sehr mächtig.
Die Ergebnisse, die sie liefert, gelten für homogene Formen von Grad d in n Variabeln, die Methode verlangt aber, daß n ziemlich groß im Bezug auf d ist.
Typisch ist ein Satz von Hooley (nach einer Arbeit von Heath-Brown im Fall von 10 Variablen):
Satz *Für nichtsinguläre kubische Formen in wenigstens 9 Variablen über* $\mathbf{Q}$ *gilt das Hasse-Prinzip.*
Es wird aber vermutet, daß dieser Satz schon ab 5 Variablen gilt.

Kurven vom Geschlecht ≥ 2

Sei $X/\mathbf{Q}$ eine glatte projektive Kurve mit Geschlecht $g \geq 2$. Zu solch einer Kurve wird ihre Jacobische Varietät $J_X/\mathbf{Q}$ assoziiert. Dies ist eine abelsche Varietät der Dimension g.

Die Menge $X(\mathbf{Q})$ ist endlich (Faltings).

Satz

Sei $X(A_{\mathbf{Q}})^{\mathrm{Br}(X)} \neq \emptyset$, *und* $Ш(J_X)$ *endlich.*
(a) Dann kann man X *in* J_X *einbetten.*
(b) Bei solch einer Einbettung liegt $X(A_{\mathbf{Q}})^{\mathrm{Br}(X)} \subset J(A_{\mathbf{Q}})$ *im topologischen Abschluß von* $J(\mathbf{Q})$ *in* $J(A_{\mathbf{Q}})$.
(c) (Scharaschkin) Wenn $J(\mathbf{Q})$ *endlich ist, dann ist* $X(\mathbf{Q}) = X(A_{\mathbf{Q}})^{\mathrm{Br}(X)}$; *insbesondere folgt aus*

$$X(A_{\mathbf{Q}})^{\mathrm{Br}(X)} \neq \emptyset$$

daß $X(\mathbf{Q}) \neq \emptyset$.

Frage (Skorobogatov) *Sei X eine beliebige glatte projektive Kurve mit Geschlecht $g \geq 2$. Ist $X(\mathbf{Q}) = \emptyset$, folgt dann $X(A_{\mathbf{Q}})^{\mathrm{Br}(X)} = \emptyset$?*

Diese Frage hat in letzter Zeit zu Arbeiten in drei Richtungen geführt.

Untersuchung bestimmter Shimura-Kurven (Skorobogatov, Siksek, Rotger, Yafaev).

Experimentelle Mathematik mit hyperelliptischen Kurven vom Geschlecht 2 mit kleinen Koeffizienten (Flynn, 2004)

Satz (Stoll, 2005) *Sei $E/\mathbf{Q}$ eine elliptische Kurve, X eine glatte projektive Kurve und $f : X \to E$ endlich. Nehmen wir an, daß $E(\mathbf{Q})$ endlich ist und daß die endliche Menge $X(\mathbf{Q}) \cap f^{-1}(E(\mathbf{Q}))$ leer ist.*
(i) Dann ist $X(\mathbf{Q}) = \emptyset$ (trivial).
(ii) Ist $Ш(E)$ endlich, dann ist $X(A_{\mathbf{Q}})^{\mathrm{Br}(X)} = \emptyset$.