Mathematisch-Physikalische Kolloquium der Fakultät für Mathematik und Physik der Leibniz Universität Hannover
6. Juni 2023

Das Lokal-Global-Prinzip in der diophantischen Geometrie – nach hundert Jahren

Jean-Louis Colliot-Thélène
CNRS et Université Paris-Saclay
z. Z. Leibniz Universität Hannover


ALEXANDER
VON
HUMBOLDT

Im Zentrum des heutigen Vortrages steht :

Helmut Hasse, mit mehreren Artikeln zum Thema “Quadratische Formen” im Crelles Journal (1923, 1924)

Wir werden früher anfangen, und später enden.

Diophantische Gleichungen (Diophantus von Alexandria, circa 260 nach Chr.)
$f(x_1, \ldots, x_n)$ ein Polynom mit ganzen Koeffizienten.

Das Problem heute : Entscheiden, ob die Gleichung
$f(x_1, \ldots, x_n) = 0$ Lösungen hat mit
(a) $x_1, \ldots, x_n$ ganzen Zahlen, d.h. im Ring $\mathbb{Z}$
oder
(b) $x_1, \ldots, x_n$ rationalen Zahlen, d.h. im Körper $\mathbb{Q}$

Dann : "alle Lösungen finden" (werden wir heute nicht besprechen)

Nach Matiyasevich (Fields medal 1964) kann man Problem (a) nicht systematisch lösen (zehntes Hilbertsches Problem).

Euklid (300 v. Chr.)
Die Gleichung $x^2 = 2y^2$ *mit* x, y *ganzen Zahlen hat die einzige Lösung* $x = y = 0$.
Beweis.
Wenn andere Lösung, dann $x^2 = 2y^2 \neq 0$, und kleinste Lösung hat $x \neq 0$ und $y \neq 0$ nicht beide gerade.
Aber $x^2 = 2y^2$ impliziert x gerade, also $x = 2m$, also $x^2 = 4m^2$, also $4m^2 = 2y^2$, also $2m^2 = y^2$ also y gerade. Wiederspruch.

Das ist ein frühes Beispiel von Benutzung der 2-adischen Bewertung im Sinne von Hensel (1861-1941).

Anderes Beispiel.
Betrachten wir die Gleichung in ganzen Zahlen

$$x^3 + 5y^3 + 25z^3 = 0$$

Wenn es eine Lösung mit $(x, y, z) \neq (0, 0, 0)$ gibt, dann gibt es solch'eine Lösung, so dass 5 nicht alle ganze Zahlen (x, y, z) teilt. Aus der Gleichung folgt : 5 teilt x^3 alors 5 teilt x also 5^2 teilt $5y^3$ alors 5 teilt y und x also 5^3 teilt $25z^3$ alors 5 teilt z. Wiederspruch. Also gibt es nur die "triviale" Lösung $(0, 0, 0)$.

Kongruenzen

Sei $m > 1$ eine ganze Zahl. Man sagt, zwei Zahlen a, b sind kongruent modulo eine ganze Zahl m when m teilt $a - b$, anders gesagt, die haben gleichen Rest nach Teilung durch m :
$a = Am + r$, $b = Bm + r$, $0 \leq r < m$.

Sei $m > 1$ gegeben. Kongruenzen mod m haben folgende Eigenschaften

Wenn a kongruent a' und b kongruent b' dann ist $a - b$ kongruent $a' - b'$, und ab ist kongruent $a'b'$.

Die Kongruenzklassen bilden also einen Ring $\mathbb{Z}/m$.

Spezieller Fall, $m = 9$: die Neunerprobe mittels der Quersumme.

Denn $1, 10, 100, 1000...$ sind alle kongruent 1 mod 9.

Sei m eine ganze Zahl. Wenn $m = 2n$ dann ist $m^2 = 4n^2$ kongruent 0 modulo 4. Wenn $m = 2n + 1$ dann ist $(2n + 1)^2 = 4n^2 + 4n + 1$ kongruent 1 mod 4. Alors ist eine ganze Zahl der Gestalt $a = x^2 + y^2$ kongruent $0, 1$ oder 2 mod 4, aber nicht kongruent 3 mod 4.

In der anderen Richtung, schwerer (..., Fermat, Euler 1750) :
Wenn eine Primzahl p nicht kongruent 3 mod. 4 ist, dann kann man $p = x^2 + y^2$ in ganzen Zahlen (x, y) lösen.
Das könnte man als erstes Beispiel vom lokal-global Prinzip betrachten.

Seien $a, b, c \in \mathbb{Z},\ abc \neq 0$. Gleichung der Gestalt

$$ax^2 + by^2 + cz^2 = 0,$$

Legendre (1830) zeigte :
Wenn es $r, s, t \in \mathbb{Z}$ ohne gemeinsamen Teiler gibt, so dass $ar^2 + bs^2 + ct^2$ durch $4abc$ teilbar ist, dann hat die obige Gleichung eine nichttriviale Lösung mit $x, y, z \in \mathbb{Z}$.

Aus der Kongruenzannahme folgt erstaunlicherweise, dass a, b, c nicht gleichzeitig positiv oder gleichzeitig negativ sind.
Mehr darüber unten.

Wenn man eine Primzahl p wählt und m durch die Potenzen p^t von p laufen läßt, und Kongruenzen modulo alle p^t betrachtet, definiert man nach Kurt Hensel (1861-1941) einen Ring $\mathbb{Z}_p$, der alle $\mathbb{Z}/p^t$ kontrolliert : eine Polynomialgleichung $f(x_1, \ldots, x_n)$ mit ganzen Koeffizienten hat eine Lösung in $\mathbb{Z}_p$ dann und nur dann, wann es eine Lösung modulo alle p^t hat.
Der Ring $\mathbb{Z}_p$, Ring der p-adischen Zahlen, ist "besser" als alle $\mathbb{Z}/p^t$: genau wie $\mathbb{Z}$ hat er keinen Nullteiler, also kann man den Fraktionskörper $\mathbb{Q}_p$ von $\mathbb{Z}_p$ betrachten, genau wie $\mathbb{Q}$ der Fraktionskörper von $\mathbb{Z}$ ist. Der Körper $\mathbb{Q}_p$ ist eine Komplettierung von $\mathbb{Q}$, genau wie $\mathbb{R}$ eine Komplettierung von $\mathbb{Q}$ ist.
Der Körper $\mathbb{Q}$ liegt also in jedem "lokalen" Körper $\mathbb{Q}_p$ (und in $\mathbb{R}$).

Eine notwendige Bedingung, die alle möglichen Kongruenzen und Positivitätsbedingungen enthält :
Wenn eine Polynomalgleichung mit Koeffizienten in $\mathbb{Z}$ eine Lösung mit Koordinaten in $\mathbb{Z}$ hat, dann auch im Körper $\mathbb{R}$ der Reellen and in jedem Ring $\mathbb{Z}_p$.

Wenn eine Polynomalgleichung mit Koeffizienten in $\mathbb{Q}$ eine Lösung mit Koordinaten in $\mathbb{Q}$ hat, in jedem Köper $\mathbb{Q}_p$ und im Körper $\mathbb{R}$ der Reellen.

Die lokalen Bedingungen kann man algorithmisch entscheiden.

Die Gleichung $pz^2 - x^2 - y^2 = 0$ mit p einer ungeraden Primzahl (Fermat, Euler) besitzt Lösungen in allen Komplettierungen von $\mathbb{Q}$ bis auf möglicherweise $\mathbb{Q}_p$ und $\mathbb{Q}_2$, und dann :

- weder in $\mathbb{Q}_p$ und $\mathbb{Q}_2$ (falls p kongruent 3 mod 4)

oder

- auch in $\mathbb{Q}_p$ und $\mathbb{Q}_2$, (falls p kongruent 1 mod 4) und dann hat eine Lösung in $\mathbb{Q}$.

Den Satz von Legendre (1830) kann man auch so lesen :
Seien a, b, c rationale Zahlen, $abc \neq 0$.
Wenn die Gleichung $ax^2 + by^2 + c = 0$ Lösungen in allen Körpern $\mathbb{Q}_p$ und in $\mathbb{R}$ hat, dann auch in $\mathbb{Q}$.
Ausserdem hat man den folgenden Satz, der den berühmten quadratischen Reziprozitätssatz von Gauss (1801) (vermutet von Euler) enthält :
Die Anzahl der Komplettierungen (p-adisch oder reel) von $\mathbb{Q}$ für welche eine gegebene Gleichung $ax^2 + by^2 + c = 0$ keine Lösung hat, ist immer **gerade**.

Vor hundert Jahren

Der Satz von Legendre wurde in verschieden Richtungen verallgemeinert (Hilbert, Minkowski, Hasse).
Hasse, Marburger Dissertation, 1921 – damals war er 22 Jahre alt) ; Vier Artikel zum Thema "Quadratische Formen" im Crelles Journal (1923, 1924)
Diese Reihe von Artikeln hat zur folgenden Definition geführt.
Man sagt, das Hassesche Prinzip, oder das Lokal-Global Prinzip, gilt für eine Klasse von Gleichungen über $\mathbb{Q}$, oder allgemeiner über einem Zahlkörper k, wenn eine Gleichung in dieser Klasse eine Lösung hat, sobald es "lokale" Lösungen in jeder Komplettierung k_v von k hat.
Falls $k = \mathbb{Q}$, dann laufen die k_v durch die $\mathbb{Q}_p$ und $\mathbb{R}$.

Man hat also den Satz, den wir hier nur für $k = \mathbb{Q}$ zitieren.
Für das Bestehen von (nichttrivialen) Nullstellen von einer beliebigen quadratischen Form über $\mathbb{Q}$

$$\sum_{i=1}^{n} a_i x_i^2$$

gilt das Lokal-Global Prinzip.
Der Beweis in dem Falle $n = 4$, den Hasse fand, beruht auf
• dem Falle $n = 3$ (Legendre),
• dem Dirichletschen Primzahlsatz (1837/1841), wonach jede arithmetische Progression $an + b$ mit $a > 0$, a und b ganz und prim zueindander (unendlich viele) Primzahlen enthält, und
• dem verallgemeinerten Reziprozitätssatz von Gauss (1801) (Hilbert, Furtwängler)

zusammenziehen, wo A eine durch die rechten Seiten von (22.) bestimmte, zu $2 \prod_i p_i$ prime ganze Zahl ist. Bestimmt man dann, was nach dem *Dirichlet*schen Satz sicher möglich, eine positive Primzahl $P \equiv (-1)^\delta A \bmod. 2^3 \prod_i p_i$, so genügt die ganze Zahl $m = (-1)^\delta 2^\alpha \prod_i p_i^{\alpha_i} P$ beiden Bedingungen (23.), ist also in $K(2)$, $K(p_\infty)$ und den $K(p_i)$ durch die beiden binären Formen in (21.) darstellbar. Dasselbe gilt auch für alle übrigen $K(p)$. Denn die nach Satz 5 (S. 135) für die Darstellbarkeit von m in $K(p)$ notwendigen und hinreichenden Bedingungen:

$$\left(\frac{m, a_1 a_2}{p}\right) = \left(\frac{a_1, -a_1 a_2}{p}\right) \text{ und } \left(\frac{m, -a_3 a_4}{p}\right) = \left(\frac{-a_3, -a_3 a_4}{p}\right)$$

sind für alle übrigen p außer P von selbst erfüllt, da diese p nicht in m und den a_i aufgehen, müssen also nach dem Produktsatz für das *Hilbert*sche Symbol auch für die allein noch übrige Primzahl P bestehen. Dann ist aber m nach Satz 7 (S. 137) durch die beiden binären Formen in (21.) rational darstellbar, und damit Satz 14 bewiesen.

Für die Darstellbarkeit der Null in $K(1)$ durch quaternäre Formen erhält man somit folgendes Kriterium:

Satz 15: Eine quaternäre Form der Invariante d stellt die Null dann und nur

Darstellbarkeit von Zahlen durch quadratische Formen in einem beliebigen algebraischen Zahlkörper.

Von Herrn *Helmut Hasse* in Kiel.

Inhalt.

Einleitung.

In drei früheren Arbeiten [1]) habe ich das Darstellbarkeits- und Äquivalenzproblem für quadratische Formen im Körper der rationalen Zahlen vollständig und systematisch behandelt. Die Resultate waren deshalb alle sehr einfach zu gewinnen, weil als Bereich für die auftretenden Größen (Koeffizienten, Variable und dargestellte Zahlen) ein Körper zugrundegelegt wurde. Daß dieser Körper gerade der rationale Zahlkörper war, ist für die Anwendbarkeit der dort eingeschlagenen Methoden von keinerlei Bedeutung. Ich zeige in dieser sowie in einer weiteren Arbeit, daß sich alle a. a. O. ausgeführten Untersuchungen in ganz analoger Weise für einen beliebigen algebraischen Zahlkörper k als Grundkörper durchführen lassen.

Das charakteristische meiner Methode in den genannten Arbeiten besteht darin, daß die Möglichkeit einer Darstellbarkeits- oder Äquivalenzbeziehung für den Körper K allen rationalen Zahlen aus der Möglichkeit dieser Beziehung für alle *Hensel*schen

[1]) Über die Darstellbarkeit von Zahlen durch quadratische Formen im Körper der rationalen Zahlen, Über die Äquivalenz quadratischer Formen im Körper der rationalen Zahlen, Symmetrische Matrizen im Körper der rationalen Zahlen, dieses Journal Bd. 152. S. 129 ff., S. 205 ff., Bd. 153, S. 12 ff., im folgenden zitiert mit H I, H II, H III.

Erweiterungskörper $K(p)$ erschlossen wird, für die sich die betr. Kriterien leichter finden lassen, als für den Körper K, hauptsächlich deshalb, weil in einem $K(p)$ nur die einzige Primzahl p vorkommt. Wie sich herausstellte, liegt dieser Methode das allgemeine Prinzip zugrunde:

Für das Bestehen einer Darstellbarkeits- oder Äquivalenzbeziehung im rationalen Körper K ist notwendig und hinreichend, daß dieselbe in allen $K(p)$ besteht [1]).

Für einen algebraischen Grundkörper k führt diese und die genannte folgende Arbeit zu dem entsprechenden Prinzip:

(I.) *Für das Bestehen einer Darstellbarkeits- oder Äquivalenzbeziehung in einem algebraischen Körper k ist notwendig und hinreichend, daß dieselbe in jedem Henselschen Erweiterungskörper $k(\mathfrak{p})$ besteht.*

Ich will in dieser Arbeit, parallel zu H I, das Darstellbarkeitsproblem für einen beliebigen algebraischen Grundkörper k vollständig behandeln, in der weiteren, parallel zu H II und H III, das Äquivalenzproblem und die höheren Darstellbarkeitsprobleme.

Meine Entwicklungen fußen vor allem auf den Sätzen über das quadratische *Hilbert*sche Normenrestsymbol $\left(\frac{\alpha, \beta}{\mathfrak{p}}\right)$, die von *Hilbert-Furtwängler* in deren Arbeiten über die Reziprozitätsgesetze und Klassenkörper erhalten sind und neuerdings von Herrn *Hensel* und mir auf Grund der *Hensel*schen Methoden in der algebraischen Zahlentheorie von anderen Grundlagen ausgehend behandelt und erweitert werden. Insbesondere lege ich das allgemeine quadratische Reziprozitätsgesetz in der *Hilbert*schen Fassung $\prod_{\mathfrak{p}} \left(\frac{\alpha, \beta}{\mathfrak{p}}\right) = +1$ zugrunde, das zum Beweis meines Prinzips (I.) verwendet wird, ebenso zu demselben Zweck den auf algebraische Körper vorallgemeinerten Satz von den Primzahlen in einer arithmetischen Reihe, also die Tatsache, daß in jeder Idealklasse im allgemeinsten Sinne eines algebraischen Zahlkörpers unendlich viele Primideale vorhanden sind. Die Notwendigkeit der Verwendung der in diesen beiden Sätzen steckenden transzendenten Methoden zum Beweis des Prinzips (I.) im Gegensatz zu allen übrigen, rein arithmetischen Entwicklungen dieser Arbeit scheint mir in der Natur der Sache zu liegen. Es soll aus der Möglichkeit gewisser Beziehungen für jeden einzelnen Primteiler $\mathfrak{p}$ von k auf das Bestehen dieser Beziehungen in k selbst, d. h. für die *Gesamtheit* aller $\mathfrak{p}$ geschlossen werden. Es ist daher natürlich, daß hierbei Betrachtungen über die „Dichtigkeit" von Primteilern $\mathfrak{p}$ gewisser Eigenschaften hineinspielen, wie sie doch den genannten transzendenten Beweisen eigentümlich sind.

In neuerer Zeit hat sich Herr *Siegel* [2]) mit speziellen Darstellbarkeitsproblemen durch quadratische Formen beschäftigt. Die von ihm gewonnenen Sätze über die Darstellbarkeit von algebraischen Zahl

Nach 1923 wurde von Hasse und anderen das Lokal-Global Prinzip und die Klassenkörpertheorie weiter entwickelt.
Als Verallgemeinerung vom Satz von Legendre und Hilbert hat man :
(Hassesche Normensatz) *Sei K/k eine zyklische Erweiterung eines Zahlkörpers k. Wenn $c \in k$ in alle Komplettierungen von k eine lokale Norm von K/k ist, dann auch global.*
Ähnliche Sätze wurden von Albert, Brauer-Hasse-Noether (1933), später Eichler, Kneser, Harder, bewiesen, im Besonderen bei der Entwicklung der arithmetischen Theorie der linearen algebraischen Gruppen.

Dass das Hassesche Prinzip für beliebige Gleichungen nicht gilt, auch bei relativ einfachen Gleichungen, wurde früh erkannt.
Fälle, wo Hassesche Prinzip nicht gilt :
Hasse : Der Normensatz gilt nicht allgemein wenn die Erweiterung nicht zyklisch ist.
Lind (1940) und Reichardt (1942) $x^4 - 17 = 2z^2$
Selmer (1951) $3x^3 + 4y^3 + 5z^3 = 0$.
Cassels und Guy (1966) $5x^3 + 9y^3 + 10z^3 + 12t^3 = 0$.

Vor fünfzig Jahren

Um weiter zu gehen, muss man sich fragen : in diesen Beispielen, was ist das Hindernis zum Hasseschen Prinzip ?
Im ICM 1970 zeigte Yuri I. Manin, dass fast alle Gegenbeispiele, die man zu dieser Zeit hatte, könnten mit einem gemeinsamen Formalismus erklärt werden, der seine Ursprung in dem Reziprozitätssatz hat.

Nämlich, man kombiniert den Reziprozitätssatz der Klassenkörpertheorie für die Brauergruppe von Zahlkörpern (1930) mit der globalen Brauergruppe von algebraischen Varietäten, die von Grothendieck definiert und studiert wurde (1968).

Das Brauer-Maninsche Hindernis kann man knapp mit Formeln definieren

$$X(k) \subset [\prod_v X(k_v)]^{Br} \subset \prod_v X(k_v).$$

Auf der linken Seite haben wir die Menge der Lösungen der Gleichung X mit Koordinaten in k, auf der rechten Seite haben wir das Produkt für alle Komplettierung k_v der Lösungen in k_v
Hassesche Prinzip hieße : rechte Seite nicht leer impliziert linke Seite nicht leer.
Brauer-Maninsche Hindernis : wenn die Brauer-Maninsche Menge $[\prod_v X(k_v)]^{Br}$ in der Mitte leer ist.

Aus verschiedenen Gründen (darunter die Bombieri-Lang Vermutung), hat kein Mensch daran geglaubt, dass das Brauer-Maninsche Hindernis für alle Arte von Gleichungen das endgültige Hindernis zum Hasseschen Prinzip sein könnte.

Das erste bedingungsloses Gegenbeispiel einer neuen Art wurde aber erst 30 Jahren später gefunden (Skorobogatov). Man kann auch dieses neue Hindernis formal definieren und sogar raffinieren. Es gibt eine Reihe von Arbeiten in dieser Richtung.

Es bleiben aber viele Gleichungen, für die man kein ähnliches Hindernis bauen kann.
Zum Beispiel, für einfach aussehenden Hyperflächen der Gestalt

$$\sum_{i=0}^{n} a_i x_i^d = 0$$

when $n \geq 4$ und $d > n$ (das sind Varietäten "vom allgemeinen Typ") hat man keine Methode, um bedingungslose Gegenbeispiele zum Hasseschen Prinzip zu bauen, obwohl wir glauben, dass es viele gibt.
Also scheint es vernünftig, sich auf Gleichungen, deren Komplexität, also deren algebraischen Geometrie nicht zu wild ist, zu beschränken.

Eine gute Klasse von Gleichungen, sagen wir ab jetzt algebraischen Varietäten, oder kurz Varietäten, wurde von den komplexen algebraischen Geometern in den 90. Jahren entdeckt. Das entstand bei der Entwicklung der birationalen Klassifikation Varietäten höherer Dimension (MMP).

Es ist die Klasse der "rational zusammenhängenden" Varietäten. Das sind die Varietäten, die über dem komplexen Körper $\mathbb{C}$ die Eigenschaft haben, dass man zwei beliebige Punkte durch eine Kurve vom Geschlecht Null (also eine parametrisierbare Kurve) verbinden kann.

Beispiele von “rational zusammenhängenden” Varietäten.

- Hyperflächen der Gestalt $\sum_{i=0}^{n} a_i x_i^d = 0$ mit $n \geq 2$ und $d \leq n$.
- Unirationale Varietäten, die man über den komplexen Zahlen $\mathbb{C}$ (nicht unbedingt eindeutig) parametrisieren kann, wie kubische Hyperflächen $\sum_{i=0}^{n} a_i x_i^3 = 0, n \geq 3$.
- Varietäten, welche einen Schar von Kegelschnitten besitzen, also Gleichungen der Gestalt $a(t)x^2 + b(t)y^2 + c(t) = 0$ mit $a(t), b(t), c(t)$ Polynomen.
- Homogene Räume von zusammenhängen linearen algebraischen Gruppen, wie Quadriken (Gleichung $\sum_{i=0}^{n} a_i x_i^2 = 0$).

Für Varietäten der Dimension 2 (Flächen) wurde die folgende Vermutung von J.-J. Sansuc und mir in 1979 hervorgehoben und untersucht.

Hauptvermutung (1999). Sei X eine Varietät über einem Zahlkörper $k \subset \mathbb{C}$. Wenn die Varietät $X_{\mathbb{C}}$ rational zusammenhängend ist, dann ist das Brauer-Maninsche Hindernis zum Hasseschen Prinzip für X/k das einzige Hindernis.

Also, bei solchen Varietäten hofft man :

$$[\prod_{v} X(k_v)]^{Br} \neq \emptyset \Longrightarrow X(k) \neq \emptyset.$$

Einige Klassen von rational zusammenhängenen Varietäten, für welche die Hauptvermutung bewiesen ist.

Homogene Räume

Varietäten X/k mit einer geometrisch transitiven Aktion einer einer linearen zusammenhängenden algebraischen Gruppe G, so dass geometrisch $X = G/H$ mit H zusammenhängend (Sansuc 1981, Borovoi 1996)

Methoden : Anwendungen der Klassenkörpertheorie zusammen mit Galoiskohomologie (Serre, Tate) und der früheren Ergebnissen von Albert, Brauer-Hasse-Noether (1933), Eichler, Kneser, Harder.

Anwendungen der Zirkelmethode (Hardy, Littlewood, Davenport, Birch, Hooley, Heath-Brown)

Satz (Birch, 1961/1962) *Sei* $F(x_0, \ldots, x_n) = 0$ *eine nichtsinguläre Hyperfläche vom Grad* d *mit Koeffizienten in* $\mathbb{Q}$. *Wenn* $n \geq (d-1)2^d$ *dann gilt das Hassesche Prinzip.*

Nach der Hauptvermutung, wenn $n \geq 4$, sollte das Hassesche Prinzip gelten, sobald $n \geq d$.

Für $d = 3$, Birch gibt $n \geq 16$. Das Hassesche Prinzip wurde für $n \geq 9$ (Heath-Brown 1983) und dann für $n = 8$ (Hooley 1988) bewiesen. Nach der Hauptvermutung, sollte es für $n \geq 4$ gelten.

Faserung und Abstieg

In den Jahren 1980-1987 (CT, Sansuc, Coray, Swinnerton-Dyer) wurde die Hauptvermutung für eine Klasse von Gleichungen, die man mit den vorigen Methoden nicht behandeln kann, bewiesen :
Für Châtelet Gleichungen

$$y^2 - az^2 = P(t)$$

mit $a \in \mathbb{Q}$ *und* $P(t)$ *Polynom mit Koeffizienten in* $\mathbb{Q}$ *und vom Grad* 4 *gilt die Hauptvermutung* .
In dem Fall $P(t)$ *irreduzibel erhält man das Hassesche Prinzip.*

Es werden folgende Methoden benutzt.

Faserung Durch Abschnitten mit Hyperebenen versucht man sich auf Varietäten von kleiner Dimension zu reduzieren, wie Hasse als er den Fall von quadratischen Formen in 5 Variablen aus dem Fall mit 4 Variablen bewies.
Da muss man sich spezielle Varietäten benutzen, die man mittels der Klassenkörpertheorie produziert, wie etwa del Pezzo Flächen vom Grad 6.

Abstieg (Descente). Ein Analog von einer Methode, die bei Kurven der Gestalt $y^2 = P(t)$ seit langem benutzt ist.
Die Abstiegsvarietäten in unserem Fall sind Durchschnitte von zwei Quadriken, also definiert durch ein System

$$f(x_1, \ldots, x_8) = 0, \; g(x_1, \ldots, x_8) = 0$$

mit f und g homogen vom Grade 2. Die Suche von Punkten (Lösungen) auf einer Fläche wird auf die Suche von Punkten (Lösungen) auf einer 5-dimensionaler Varietät, die irgendwie einfacher zu behandeln ist, zurückgeführt.

Die Beweise laufen gegenseitig, von Châtelet Flächen zu Durchschnitte von zwei Quadriken und umgekehrt.
Was letzere Durchschnitte betrifft, jetzt wissen wir :

Für (vernünftige) Durschschnitte von zwei Quadriken in wenigstens 8 *Variablen gilt das Hassesche Prinzip.*
(CT-Sansuc-Swinnerton-Dyer 1987, Heath-Brown 2018, CT 2022, Molyakov 2023)
Nach der Hauptvermutung sollte das Hassesche Prinzip schon mit 7 Variablen gelten, und schon mit 6 Variablen im "glatten" Fall.

Rund um die Schinzelsche Vermutung

Bemerkung (1979, ... ,1994) : *Unter Annahme der Schinzelschen Vermutung kann man die Hauptvermutung für alle Gleichungen der Gestalt*

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

beweisen. Nämlich, man braucht nur den Hasseschen Beweis für quadratische Formen in 4 Variablen nachzuahmen.

Die Schinzelsche Vermutung (1958) ist eine gewagte aber wohl bekannte Vermutung, die den Satz von Dirichlet für ein lineares Polynom $P(x) = ax + b$ auf alle vernünftige endliche Systeme von Polynomen $P_i(x)$ ausdehnt. Sie geht auf Bouniakowsky (1857) und auf Arbeiten von Hardy und Littlewood (20ger Jahren) zurück.

"Arithmetic statistics"
Green, Tao, Ziegler (2010-2012) haben einen Satz in dieser Richtung, aber mit zwei Variablen, bewiesen.
Für ein vernünftiges System von einer beliebigen Anzahl von linearen Polynomen in zwei Variablen $a_i x + b_i y + c_i$ $(i = 1, \ldots, N$ *kann man ganze Zahlen* (n, m) *finden, so dass alle* $a_i n + b_i m + c$ $(i = 1, \ldots, N)$, *prim sind.*
Jetzt liefert das Argument mit der Schinzelschen Vermutung :

Satz. *Für Gleichungen der Gestalt* $a(t)x^2 + b(t)y^2 + c(t) = 0$ *mit Koeffizienten in* $\mathbb{Q}$*, wenn alle Polynome alle ihre Wurzeln in* $\mathbb{Q}$ *haben, dann gilt eine starke Version der Hauptvermutung, nämlich die Lösungen liegen dicht in der Brauer-Maninschen Menge* $[\prod_v X(k_v)]^{Br}$.
(Browning, Harpaz, Mathiesen, Skorobogatov, Wittenberg, 2014-2016)
Für fast alle Gleichungen dieser Art wusste man vorher nicht, ob Lösungen "dicht" in der Varietät waren, i. B. ob es unendlich viele gab.

Skorobogatov und Sofos (2022) “Schinzel on average”
Betrachten wir die Menge der irreduziblen Polynomen $P(t)$ vom Grad d mit einer offensichtlichen, arithmetischen extra Bedingung.

Wenn man die Polynomen nach dem maximum der Größe der Koeffizienten ordnet, als dieses Maximum wächst, für 100 % dieser Polynomen $P(t)$ gibt es wenigstens eine ganze Zahl m, so dass $P(m)$ eine Primzahl ist.
Dies reicht, um zu zeigen : *Für eine positive Proportion der Gleichungen der Gestalt $y^2 - az^2 = P(t)$ mit Koeffizienten in $\mathbb{Q}$, und $P(t)$ irreduzibel vom Grad d, gilt das Hassesche Prinzip.*

Geometrie der Zahlen (à la Minkowski)

The Hasse principle for random Fano hypersurfaces
Browning, Le Boudec, Sawin (2023)

Wenn $n \geq 4$ *und* $d \leq n$*, dann gilt das Hassesche Prinzip für* **fast alle** *Hyperflächen.*
(Man weiß aber nicht welche !)

Fast alle : Die Hyperflächen werden nach Höhe ihrer Koeffizienten geordnet, und dann werden sie gezählt als die Höhe wächst.

Ähnliche Ergebnisse für kubische Flächen ($d = 3, n = 3$).
Entspricht der experimentalen Tatsache, dass Brauer-Maninsche Hindernis kann in diesem Fall vorkommen, aber sehr selten.

Leider, und zum Schluss :

Die folgende Frage bleibt offen.

Kann man entscheiden, ob eine gegebene Gleichung

$$ax^3 + by^3 + cz^3 + dt^3 = 0$$

mit ganzzahligen Koeffizienten eine nichttriviale Lösung in (x, y, z, t) *ganzen Zahlen hat ?*