Universitätsbibliothek
Heidelberg

Heidelberger Akademie
der Wissenschaften

Altes und Neues aus der Diophantischen Geometrie

Vortrag von

Peter Roquette

gehalten am 10. November 1979 in der Sitzung der
Mathematisch-Naturwissenschaftlichen Klasse der

Heidelberger Akademie der Wissenschaften

Erschienen in:
Jahrbuch der Heidelberger Akademie der Wissenschaften
für das Jahr 1979, S.111–128

Mit Genehmigung des Autors neu herausgegeben von

Gabriele Dörflinger
Universitätsbibliothek Heidelberg
2010

//ub-fachinfo.uni-hd.de/math/akademie/roquette2.pdf

§ 1. Problemstellung.

Unter *Diophantischer Geometrie* versteht man *ganzzahlige* Geometrie. Wir denken uns in der Ebene ein rechtwinkliges Koordinatensystem festgelegt, und wir markieren die Punkte mit ganzzahligen (positiven oder negativen) Koordinaten. Es entsteht ein diskretes Punktgitter, das die Ebene überzieht. Betrachten wir nun eine in der Ebene liegende geometrische Figur, beispielsweise eine Kurve. Die folgenden Fragen gehören zu den Grundproblemen der Diophantischen Geometrie:

(1) Gibt es ganzzahlige Gitterpunkte auf der Kurve?

(2) Wenn ja, wieviele?

(3) Gibt es einen Algorithmus zu ihrer Berechnung?

Diese Problemstellungen lassen sich physikalisch interpretieren. Geht man von der Hypothese aus, daß der physikalische Raum eine diskrete Struktur besitzt, so erscheint das ganzzahlige Punktgitter als das einfachste dieser Hypothese entsprechende ebene Modell. Betrachtet man die Bahnkurve eines sich bewegenden Teilchens, so wird man demgemäß nur denjenigen Punkten der Kurve eine reale Bedeutung beimessen, die gleichzeitig in dem Modell liegen, d. h. Gitterpunkte sind. Das Teilchen „springt“ also von einem Gitterpunkt der Bahnkurve zum nächsten und ist an den übrigen Punkten der Kurve nicht nachweisbar. Dabei ist die Kurve durch die physikalischen Gegebenheiten als bekannt anzusehen, etwa als Lösung der einschlägigen Differentialgleichung. In dem genannten Modell lassen sich nun die obigen geometrischen Fragen wie folgt physikalisch interpretieren:

(1) Ist das Teilchen auf seiner Bahnkurve überhaupt nachweisbar? (2) Wenn ja, an wievielen Punkten ist eine Messung oder Beobachtung möglich? (3) Lassen sich die in Frage kommenden Meßpunkte auf der Bahnkurve durch einen Algorithmus vorausberechnen?

Diese physikalische Interpretationsmöglichkeit hat zwar in der geschichtlichen Entwicklung der Diophantischen Geometrie keine Rolle gespielt, weder bei Diophant selbst noch bei den Mathematikern der Neuzeit, die sich mit diesen Problemstellungen befaßt haben. Wir erwähnen die physikalische Interpretation hier lediglich als Mittel zur Veranschaulichung. Andererseits sollte nicht übersehen werden, daß die mathematischen Untersuchungen über ganzzahlige, also diskrete Geometrie derselben erkenntnistheoretischen Wurzel entstammen wie die physikalischen Versuche der Naturerklärung durch Heranziehung diskreter Strukturen.

§ 2. Kreisbahn.

Als erstes Beispiel betrachten wir eine Kreisbewegung. Das Teilchen bewegt sich also auf einer Kreislinie, von der wir annehmen wollen, daß ihr Mittelpunkt im Ursprung des Koordinatensystems liegt. Es sei $r = \sqrt{c}$ der Radius des Kreises; die Kreisgleichung besitzt die Form

$$x^2 + y^2 = c.$$

Zeichnet man für verschiedene Werte $c = 1, 2, 3, \ldots$ die zugehörigen Kreislinien, so findet man, daß darauf in vielen Fällen Gitterpunkte liegen, in manchen Fällen jedoch

nicht. Es gibt keine Gitterpunkte für $c = 3, 6, 7, 11, 14, 15$. Testet man Kreise mit etwas größerem Radius, so findet man keine Gitterpunkte z. B. für $c = 161$; dagegen gibt es Gitterpunkte auf dem Kreis für $c = 98$ und auch für $c = 153$. Wie lautet das allgemeine Gesetz? Welche Eigenschaften der Zahl c sind dafür verantwortlich, daß die zugehörige Kreisbahn mindestens einen Gitterpunkt enthält?

Dies Problem hat eine lange Geschichte. Es erlangte eine gewisse Berühmtheit, da es in der *Arithmetik* des Diophant behandelt worden war; die endgültige Lösung wird schließlich Fermat zugeschrieben. Für uns ist die Fermatsche Lösung deshalb interessant, weil sie in besonders durchsichtiger Weise auf die *Spektralstruktur* der Diophantischen Geometrie Bezug nimmt; daher wollen wir kurz darauf eingehen.

Wir zerlegen die ganze, positive Zahl c in ein Produkt von Primzahlen. Man nennt dies die Spektralzerlegung von c; die dabei auftretenden Primzahlen bilden das *Spektrum* der Zahl c. Eine Primzahl p kann im Spektrum von c mehrfach vorkommen, z. B. kommt $p = 2$ im Spektrum von $c = 40$ mit der Vielfachheit 3 vor, denn $40 = 2^3 \cdot 5$. Dagegen erscheint die Primzahl $p = 5$ im Spektrum von 40 mit der Vielfachheit 1.

Um die Lösung des Kreisproblems zu formulieren, teilt Fermat das Spektrum aller Primzahlen p in drei Klassen ein, und zwar wie folgt:

I. Die erste Klasse enthält diejenigen Primzahlen p, welche durch 4 geteilt den Rest 1 lassen; man schreibt dafür $p \equiv 1 \bmod 4$. Dies sind die Primzahlen $p = 5, 13, 17, 29, 37, 41, 53, 61, \ldots$

II. Die zweite Klasse enthält diejenigen Primzahlen p, welche durch 4 geteilt den Rest 3 lassen, $p \equiv 3 \bmod 4$. Diese Klasse enthält die Primzahlen $p = 3, 7, 11, 19, 23, 31, 43, 47, 59, 67, \ldots$

III. Die dritte Klasse enthält nur eine einzige Primzahl, nämlich $p = 2$. Man bezeichnet dies als die Ausnahmeklasse des in Rede stehenden Problems.

Nun kann der Fermatsche Satz wie folgt ausgesprochen werden: *Wenn im Spektrum von c jede etwa vorhandene Primzahl der Klasse II mit einer geraden Vielfachheit erscheint, dann geht die Kreislinie* $x^2 + y^2 = c$ *durch mindestens einen Gitterpunkt. Andernfalls, wenn also mindestens eine Primzahl der Klasse II im Spektrum von c mit einer ungeraden Vielfachheit erscheint, dann geht die Kreislinie durch keinen einzigen Gitterpunkt.*

Was an diesem Ergebnis auffällt, im Vergleich zu den Ergebnissen der Euklidischen Geometrie, ist das besondere Begriffsvokabular der Spektraltheorie, das in der Formulierung verwendet wird. In der Tat ist das zusätzliche Auftreten der Spektralstruktur eines der wesentlichen Merkmale, durch das sich die diskrete Diophantische Geometrie von der kontinuierlichen Euklidischen Geometrie unterscheidet. In jedem Satz der Diophantischen Geometrie spielt die Spektralstruktur explizit oder implizit eine wesentliche Rolle; der obige Satz von Fermat ist ein besonders schönes Beispiel dafür.

Die angeführten numerischen Beispiele lassen sich nun ohne weiteres unter den Fermatschen Satz durch Berechnung der Spektralzerlegung von c unterordnen: Wir finden

$$161 = 7 \cdot 23,$$

also kommt sowohl die Primzahl 7 als auch 23, die beide der Klasse II angehören, im Spektrum von 161 mit der Vielfachheit 1 vor, d. h. mit ungerader Vielfachheit, und somit gibt es auf der Kreislinie $x^2 + y^2 = 161$ keinen Gitterpunkt. Andererseits ist

$$153 = 3^2 \cdot 17;$$

die im Spektrum von 153 vorkommenden Primzahlen sind 3 und 17, von denen 3 der Klasse II und 17 der Klasse I angehört. Da nun 3 die gerade Vielfachheit 2 besitzt, so ist die Bedingung des Fermatschen Satzes erfüllt und folglich gibt es mindestens einen Gitterpunkt auf der Kreislinie $x^2 + y^2 = 153$. Damit wissen wir allerdings noch nicht, wie wir einen solchen Gitterpunkt finden können; immerhin können wir in diesem Beispiel durch Ausprobieren leicht feststellen, daß $3^2 + 12^2 = 153$, und somit ist der Punkt $P = (3, 12)$ ein Gitterpunkt auf unserer Kreislinie. Für größeres c führt Ausprobieren nicht sehr schnell zum Ziel; daher ist es wichtig zu wissen, daß bereits Fermat selbst einen gut funktionierenden Algorithmus zur Berechnung der Gitterpunkte auf der Kreislinie $x^2 + y^2 = c$ angegeben hat. Wir gehen darauf nicht näher ein und stellen hier lediglich fest, daß für eine Kreislinie die in § 1 gestellten Probleme (1)–(3) erschöpfend gelöst sind. Was dabei die Frage (2) anbetrifft, also die Anzahl der Gitterpunkte auf der Kreislinie, so stellt sich heraus, daß diese Anzahl von der Reichhaltigkeit des Spektrums von c abhängt. Und zwar wächst die Anzahl der Gitterpunkte auf der Kreislinie $x^2 + y^2 = c$ ziemlich schnell, nämlich exponentiell, mit der Anzahl der im Spektrum von c vorkommenden Primzahlen der Klasse I. Andererseits gibt es beliebig große Kreislinien $x^2 + y^2 = c$, deren Gitterpunktanzahl gleich 8 ist, nämlich wenn $c = p$ eine Primzahl aus der Klasse I ist. Wenn $c = 2^h$ eine Potenz von 2 ist, so ist die Gitterpunktanzahl gleich 4; dies ist die Minimalzahl angesichts der Symmetrien des Problems. Merkwürdig an dem Fermatschen Satz ist die Klasseneinteilung auf dem Spektrum der Primzahlen. Dabei spielt die Zahl 4 eine Sonderrolle, und somit ist 4 als eine Diophantische Invariante der Kreislinie anzusehen. Betrachtet man statt Kreisbahnen Ellipsenbahnen (und auch für diesen Fall liegen vollständige Ergebnisse vor), so ist die Zahl 4 durch eine andere Invariante zu ersetzen, die durch die Gestalt der jeweiligen Ellipse bestimmt ist. Die Verfolgung dieses Sachverhalts mündet schließlich in die moderne *Klassenkörpertheorie*, so genannt nach den damit verbundenen Klasseneinteilungen im Spektrum der Primzahlen.

§ 3. Hyperbel.

Als nächstes Beispiel wollen wir Hyperbelbahnen untersuchen, wie sie etwa von Kometen beschrieben werden. Wir nehmen die zu betrachtenden Hyperbelbahnen in der Form an:

$$x^2 - dy^2 = 1,$$

wobei d eine ganze positive Zahl bedeutet. Jede solche Hyperbel besteht aus zwei getrennten Ästen, die spiegelbildlich zur y-Achse liegen. Der Einfachheit halber beschränken wir die folgende Diskussion auf einen der beiden Äste, und zwar auf den in der rechten Halbebene, für welchen $x > 0$. Wenn wir also von der Hyperbel $x^2 - dy^2 = 1$ sprechen, so ist damit genauer der in der rechten Halbebene liegende Ast dieser Hyperbel gemeint.

Es geht nun wieder um die drei in § 1 formulierten Fundamentalfragen der Diophantischen Geometrie. Zunächst sieht man sofort, daß die Hyperbel $x^2 - dy^2 = 1$ stets durch mindestens einen Gitterpunkt geht, nämlich durch das Perihel $x = 1, y = 0$. Wir bezeichnen diesen als den trivialen Gitterpunkt der Hyperbel und modifizieren die Fundamentalfragen (1)–(3) aus § 1 dahingehend, daß wir nach den *nichttrivialen* Gitterpunkten suchen.

Die im folgenden zu berichtenden Sätze wurden ebenfalls von Fermat entdeckt, unabhängig davon auch von Euler. Der letztere prägte für die Gleichung $x^2 - dy^2 = 1$ die Bezeichnung *Pellsche Gleichung*, unter welchem Namen sie heute bekannt ist, obwohl diese Bezeichnung offenbar auf einem historischen Irrtum beruht. Der englische Mathematiker Pell hat sich, entgegen der Meinung Eulers, wohl nicht sehr mit den nach ihm benannten Gleichungen beschäftigt.

Das erste Ergebnis lautet: *Wenn in dem Spektrum von d mindestens eine Primzahl mit einer ungeraden Vielfachheit vorkommt* (gleichgültig zu welcher Klasse diese Primzahl gehört), *dann gibt es einen nichttrivialen Gitterpunkt auf der Hyperbel* $x^2 - dy^2 = 1$. *Und zwar gibt es dann sogar unendlich viele solche Gitterpunkte. Andernfalls, wenn jede Primzahl des Spektrums von d eine gerade Vielfachheit besitzt, wenn also d eine Quadratzahl ist, dann besitzt die Hyperbel nur einen einzigen Gitterpunkt, nämlich den trivialen.*

Demnach besitzt die gleichseitige Hyperbel $x^2 - y^2 = 1$ keinen nichttrivialen Gitterpunkt, weil $d = 1$ eine Quadratzahl ist. $d = 2$ ist keine Quadratzahl, und daher liegen auf der Hyperbel $x^2 - 2y^2 = 1$ unendlich viele nichttriviale Gitterpunkte. Einer davon ist der Punkt P mit den Koordinaten $x = 3$, $y = 2$, wie man durch Einsetzen bestätigt. Wie findet man nun die weiteren Gitterpunkte auf der Hyperbel? Dazu stellen wir den Punkt mit Koordinaten x, y in der Form $x + y \cdot \sqrt{2}$ dar (es ist dies eine analoge Darstellung wie man sie von der gewöhnlichen komplexen Ebene her kennt, wobei nur $i = \sqrt{-1}$ durch $\sqrt{2}$ zu ersetzen ist). Insbesondere ist $P = 3 + 2 \cdot \sqrt{2}$. Quadrieren liefert $P^2 = 17 + 12 \cdot \sqrt{2}$, und man verifiziert durch Einsetzen in die Hyperbelgleichung, daß auch der Punkt P^2 mit den Koordinaten $x = 17$, $y = 12$ ein Hyperbelpunkt ist. Dasselbe gilt für $P^3 = 99 + 70 \cdot \sqrt{2}$, $P^4 = 577 + 408 \cdot \sqrt{2}$ usw. Wir erhalten also, ausgehend von unserem Grundpunkt P, unendlich viele weitere Gitterpunkte $P^2, P^3, P^4, \ldots$ auf der Hyperbel. Spiegelbildlich zu diesen in Bezug auf die x-Achse liegen $P^{-1} = 3 - 2 \cdot \sqrt{2}$, $P^{-2} = 17 - 12 \cdot \sqrt{2}$, usw. Es stellt sich nun heraus, daß man auf diese Weise *alle* Gitterpunkte der Hyperbel $x^2 - 2y^2 = 1$ erhält. Und zwar ist das ein allgemeiner Sachverhalt:

Betrachten wir irgendeine unserer Hyperbeln $x^2 - dy^2 = 1$, wobei wir voraussetzen, daß d keine Quadratzahl ist, so daß also die Existenz eines nichttrivialen Gitterpunktes gesichert ist. Nehmen wir an, wir kennen denjenigen nichttrivialen Gitterpunkt P der Hyperbel, der dem Perihel am nächsten liegt; es seien x, y die Koordinaten von P. (Nach evtl. Spiegelung an der x-Achse können wir voraussetzen, daß $y > 0$). Wir nennen P den *Grundpunkt*. Wir schreiben nun $P = x + y \cdot \sqrt{d}$ und bilden nach obigem Rezept die Potenzen

$$\ldots, P^{-2}, P^{-1}, P^0 = 1, P, P^2, P^3, \ldots.$$

Diese Potenzen des Grundpunktes sind dann genau alle Gitterpunkte auf der Hyperbel $x^2 - dy^2 = 1$. Mit anderen Worten: die Gitterpunkte auf der Hyperbel bilden bei der angegebenen Multiplikation eine zyklische unendliche Gruppe, mit dem Grundpunkt P als erzeugendem, und dem Perihel als neutralem Element.

In unserem physikalischen Bild, der diskreten Bewegung eines Kometen auf der Hyperbel, bedeutet dieses Ergebnis folgendes. Nehmen wir an, der Komet sei in einer gewissen Position X beobachtet worden. X ist also (nach unserem Modell) ein *Gitterpunkt* auf der Bahnhyperbel. Folglich ist $X = P^n$ mit gewissem ganzzahligen Exponenten n. Der nächste Punkt, an dem der Komet beobachtet werden kann, ist

dann P^{n+1} oder P^{n-1} (je nach der Bewegungsrichtung), der darauffolgende ist P^{n+2} bzw. P^{n-2} usw. Mit anderen Worten: die Multiplikation der Hyperbelpunkte liefert einen Algorithmus zur Vorausberechnung der nächsten Bahnpunkte — vorausgesetzt, daß der Grundpunkt P bekannt ist.

Zur Berechnung des Grundpunktes P gibt es nun einen einfachen Algorithmus, der an die Kettenbruchentwicklung von $\sqrt{d}$ anknüpft. Wir können hier nicht darauf eingehen und begnügen uns mit dem Hinweis, daß es sich um eine der schönsten und weitreichendsten Anwendungen der klassischen Lehre der Kettenbruchentwicklungen handelt, wobei mannigfache Beziehungen der Diophantischen Geometrie zu anderen Gebieten der Mathematik zutage treten.

Die drei Grundfragen (1)-(3) aus § 1 lassen sich somit auch für Hyperbeln $x^2 - dy^2 = 1$ erschöpfend beantworten.

Auf der Basis seiner Theorie behandelte Fermat eine Reihe numerischer Spezialfälle; der interessanteste für ihn war wohl $d = 109$, wobei der Grundpunkt die y-Koordinate $y = 15140424455100$ besitzt. Übrigens war Fermat nicht der erste, der sich mit dem Hyperbelproblem befaßt hat; wie das Kreisproblem hat auch das Hyperbelproblem eine lange Geschichte. Diophant diskutierte das Problem u. a. für $d = 26$ und fand dazu den Grundpunkt P mit den Koordinaten $x = 51$, $y = 10$. Im 12. Jahrhundert wurde von dem indischen Mathematiker Bháscara Achárya eine Theorie dieser Hyperbeln entwickelt; er gelangte für $d = 61$ zu dem Grundpunkt $x = 1766319049$, $y = 226153980$. Als Kuriosität sei noch das berühmte Rinderproblem von Archimedes erwähnt, das sich in einem Brief an Eratosthenes findet und offenbar gedacht war als eine Art Denksportaufgabe. Aus gewissen Angaben soll auf die Größe und Zusammensetzung einer Rinderherde geschlossen werden; analysiert man diese Aufgabe, so stellt sich heraus, daß es sich um die Aufsuchung des Grundpunktes für die Hyperbel $x^2 - dy^2 = 1$ mit $d = 43850508116$ handelt. Angesichts der Größe der Diskriminante d ist es nicht verwunderlich, daß diese Aufgabe erst in neuerer Zeit vollständig gelöst werden konnte; erst vor wenigen Jahren gelang es, ein Computerprogramm so zu schreiben, daß die Aufgabe in zumutbarer Zeit gelöst werden konnte. Die Koordinaten des Grundpunktes besitzen dabei mehr als 200000 Dezimalstellen.

§ 4. Gerade.

In den vorangegangenen Abschnitten haben wir Kreise und Hyperbeln besprochen; diese dienten uns als Beispiele für Kurven 2. Ordnung. Der Fall einer allgemeinen Kurve 2. Ordnung mit ganzzahligen Koeffizienten, in beliebiger Lage, läßt sich daran anschließend in derselben Weise erschöpfend behandeln, nur sind die Ergebnisse etwas komplizierter. Es entsteht nun die Frage, ob ähnliches auch für Kurven höherer Ordnung gilt. Dieser Frage wollen wir uns in den folgenden Abschnitten zuwenden, zunächst jedoch, der Vollständigkeit halber, auf die Kurven erster Ordnung eingehen, also die Geraden. Eine Gerade wird gegeben durch eine Gleichung der Form

$$ax + by = c.$$

Wir nehmen an, daß a, b, c ganze Zahlen sind (nicht notwendig positiv). Die Erörterung der Grundfragen (1)–(3) aus § 1 im Falle einer Geraden gehört sozusagen zu

den klassischen Anfängen der Mathematik; sie findet sich im VII. Buch von Euklid. Die Ergebnisse sind wie folgt:

Wenn die Spektren von a und b zueinander fremd sind, also keine gemeinsame Primzahl besitzen, dann gibt es stets einen Gitterpunkt auf der Geraden $ax + by = c$, *bei beliebigem Wert von c.* Die Berechnung eines solchen Gitterpunktes erfolgt mit Hilfe des *Euklidischen Algorithmus*, der im Laufe der Mathematikgeschichte zu dem Musterbeispiel aller Algorithmen geworden ist. Zwar liefert die direkte Anwendung des Euklidischen Algorithmus zunächst nur einen Gitterpunkt auf einer anderen Geraden, nämlich der Geraden $ax + by = 1$, die zur gegebenen Geraden $ax + by = c$ parallel ist. Jedoch erhält man dann durch Multiplikation mit der Konstanten c einen Gitterpunkt auf der Geraden $ax + by = c$. Ausgehend von dem so gewonnenen Gitterpunkt auf dieser Geraden gewinnt man weitere Gitterpunkte durch mehrfache Addition oder Subtraktion des Vektors $(b, -a)$. Und zwar ergeben sich auf diese Weise *alle* Gitterpunkte auf der Geraden. Insbesondere sehen wir, daß es auf der Geraden unendlich viele Gitterpunkte gibt, die insgesamt eine äquidistante Punktreihe bilden.

Wenn die Spektren von a und b nicht zueinander fremd sind, d. h. wenn a und b einen gemeinsamen Primteiler besitzen, dann liegt auf der Geraden $ax + by = c$ nicht immer ein Gitterpunkt, d. h. nicht für beliebige Wahl von c. Die Bedingung an c ist, daß c ein Vielfaches des größten gemeinsamen Teilers d von a und b sein muß. Ist das der Fall, so kann man die Koeffizienten der Geradengleichung durch d dividieren und erhält dann den oben diskutierten Fall zurück.

§ 5. Kubische Kurven.

Als einfachste Kurven dritter Ordnung bieten sich die Kurven der Form

$$y^2 = x^3 + k$$

zur Untersuchung an. Dabei bedeutet k eine beliebige ganze Zahl. Zunächst erkennt man, daß die Kurve für $k = 0$ in geometrischer Hinsicht eine Sonderrolle spielt. Denn die Kurve $y^2 = x^3$ besitzt im Koordinatenursprung eine Spitze, an welcher die Kurve keine Tangente besitzt. Die anderen Kurven $y^2 = x^3 + k$ mit $k \neq 0$ sind dagegen überall glatt, haben keine Spitze und auch keine andere Singularität. Es zeigt sich nun, daß die Kurve $y^2 = x^3$ auch im Hinblick auf die Diophantischen Grundprobleme (l)–(3) eine Sonderrolle spielt. Es kann unmittelbar verifiziert werden, daß diese Kurve unendlich viele Gitterpunkte trifft, und daß man diese in einfacher Weise mittels der Parameterdarstellung $x = t^2, y = t^3$ für t = 0,1,2,3,... darstellen kann. Andererseits werden wir sehen, daß für $k \neq 0$ die Kurve $y^2 = x^3 + k$ höchstens endlich viele Gitterpunkte trifft (wenn überhaupt einen).

Im folgenden wird $k \neq 0$ vorausgesetzt. Für spezielle Werte von k kennt man eine Liste der Gitterpunkte schon seit längerer Zeit. Zum Beispiel gibt es für $k = 1$ genau drei Gitterpunkte auf der Kurve $y^2 = x^3 + 1$, nämlich die Punkte (l, 0), (0,1), (2, 3). (Eigentlich gibt es noch zwei weitere Gitterpunkte, nämlich die sich daraus durch Spiegelsymmetrie ergebenden (0, -1) und (2, -3); der Einfachheit halber zählt man jedoch von jedem bezüglich der x-Achse spiegelsymmetrischen Punktepaar nur einen, um triviale Verdoppelungen zu vermeiden.)

Für $k = -1$ und $k = 2$ gibt es je nur einen einzigen Gitterpunkt auf der zugehörigen Kurve $y^2 = x^3 - 1$ bzw. $y^2 = x^3 + 2$, und zwar den Punkt (1,0) bzw. (-1,1). Für $k = \pm 6$ gibt es überhaupt keinen Gitterpunkt, und für $k = 17$ gibt es 8 Gitterpunkte; der am weitesten vom Nullpunkt entfernte Gitterpunkt auf $y^2 = x^3 + 17$ besitzt die Koordinaten $x = 5234$, $y = 378661$. Im Jahre 1953 veröffentlichte Hemer eine Liste der bekannten Gitterpunkte für $|k| \leq 100$, und diese Liste ist später mit Hilfe von Computern auf größere Werte von k ausgedehnt worden. Das Gemeinsame an all diesen Untersuchungen ist, daß bisher keine allgemeine Methode gefunden wurde, die gleichmäßig für alle k funktioniert. Für jeden Wert von k muß die Diskussion gesondert geführt werden, unter Ausnutzung der speziellen, individuellen Spektraleigenschaften von k. Für $k = -7$ sind zwar zwei Gitterpunkte bekannt, nämlich (2,1) und (32,181), aber man weiß heute immer noch nicht, ob dies alle sind. Jedenfalls hat man auf der Kurve $y^2 = x^3 - 7$ in dem Bereich, der mit heutigen Computern zugänglich ist, keine weiteren Gitterpunkte gefunden. Aber vielleicht gibt es doch noch Gitterpunkte mit sehr viel größeren Koordinaten? Ähnlich unvollkommen ist unser Kenntnisstand z. B. für $k = -15$ oder $k = -87$.

Jedenfalls zeigt eine Inspektion der Anzahl der bekannten Gitterpunkte auch für große Werte von $|k|$, daß diese Anzahl relativ klein bleibt; für kein $|k| < 10^4$ sind auf der Kurve mehr als 12 Gitterpunkte bekannt. Es entsteht daraus der Eindruck, daß es vielleicht stets nur *endlich viele* Gitterpunkte auf der Kurve $y^2 = x^3 + k$ gibt. Diese rein numerische Evidenz ist natürlich keineswegs überzeugend, denn da sich die kubischen Kurven ins Unendliche erstrecken, so ist es zumindest nicht ausgeschlossen, daß vielleicht doch unendlich viele Gitterpunkte auf der Kurve $y^2 = x^3 + k$ liegen. Im Jahre 1909 bewies nun Thue das erste allgemeine Resultat über kubische Kurven; *danach gibt es in der Tat nur endlich viele Gitterpunkte auf der Kurve* $y^2 = x^3 + k$ *für* $k \neq 0$. Später bewies Baker im Jahre 1968, daß die Koordinaten x, y eines Gitterpunktes auf dieser Kurve nicht größer sind als durch die folgende Abschätzung angegeben:

$$|x|, |y| < \exp(10^{10} \cdot |k|^{10000})$$

wobei exp die Exponentialfunktion bedeutet. Im Prinzip hat damit Baker einen „Algorithmus“ angegeben, um die Existenz eines Gitterpunktes auf der Kurve $y^2 = x^3 + k$ zu testen, und auch gegebenenfalls alle Gitterpunkte zu berechnen: man braucht dazu „nur“ für x und y die Werte $0, \pm 1, \pm 2, \pm 3, \ldots$ bis hin zu der angegebenen Schranke in die Kurvengleichung einzusetzen und nachzuprüfen, ob die Gleichung erfüllt ist. Da jedoch die Bakersche Schranke sehr groß ist, so ist dies Verfahren auch mit den schnellsten heute verfügbaren Computern nicht durchführbar; der Bakersche Algorithmus ist nur von theoretischem Interesse und nicht von praktischem Wert. Es verwundert daher auch nicht, daß zum Beispiel der Fall $k = -7$ nicht auf diese Weise entschieden werden konnte.

Immerhin sind die angegebenen Resultate von Thue und Baker von großem theoretischen Interesse, und es entsteht die Frage, ob sie nicht auch für beliebige kubische Kurven gelten, auch wenn diese Kurven nicht von der speziellen Form $y^2 = x^3 + k$ sind. Eine beliebige kubische Kurve wird gegeben durch eine Gleichung der Form

$$f(x, y) = 0$$

wobei $f(x, y)$ ein Polynom dritten Grades bedeutet, also:

$$f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + k.$$

Wir nehmen an, daß die Koeffizienten $a, b, \ldots, k$ ganze Zahlen sind. Die ersten 4 Koeffizienten a, b, c, d sind nicht alle $= 0$, weil es sich sonst nicht um eine kubische Kurve, sondern um eine Kurve vom Grad < 3 handeln würde. Wenn das Polynom $f(x, y)$ in ein Produkt von Polynomen kleineren Grades zerlegbar ist, dann zerfällt die Kurve entsprechend in eine Gerade und eine Kurve zweiter Ordnung, oder in drei Geraden; es handelt sich dann um eine *reduzible* Kurve. In diesem Falle läuft unser Gitterpunktproblem auf Kurven 2. Ordnung und Geraden zurück. Daher nehmen wir jetzt an, daß die zu untersuchende kubische Kurve *irreduzibel* ist. Weiterhin nehmen wir an, daß die Kurve überall glatt ist, also keine Singularitäten besitzt (wir haben schon am Beispiel $y^2 - x^3$ gesehen, daß kubische Kurven mit Singularitäten Ausnahmen in Bezug auf das Gitterpunktproblem bilden). Für solche irreduziblen, glatten kubischen Kurven bewies Siegel im Jahre 1929 den *Endlichkeitssatz: es gibt nur endlich viele Gitterpunkte auf der Kurve. Und Baker ergänzte dies 1968 durch Angabe einer expliziten Schranke für die Koordinaten x, y der Gitterpunkte auf der Kurve:*

$$|x|, |y| < \exp\exp\exp(10^{10} \cdot H^{10000})$$

wobei H das Maximum der Beträge der Gleichungskoeffizienten a, b, c, . . . , k bedeutet.

Die Bakersche Schranke ist in diesem allgemeinen Fall also noch viel größer als für die oben diskutierten speziellen kubischen Kurven $y^2 = x^3 + k$. Jedoch ist es bei Schranken dieser geradezu astronomischen Größe ziemlich unerheblich, ob sie noch ein wenig vergrößert oder verkleinert werden können. Was uns die Bakersche Schranke zeigt, ist lediglich, daß die Grundprobleme (l)–(3) der Diophantischen Geometrie im Falle von kubischen Kurven wenigstens *im Prinzip* gelöst sind, wenn auch im Einzelfalle eine rechnerisch durchführbare Lösung bisher nicht gefunden ist. Angesichts der Tatsache, daß bei höheren Diophantischen Problemen nicht einmal eine solche prinzipielle Lösung möglich ist, ist das Bakersche Resultat durchaus bemerkenswert; es gehört zu den tiefliegendsten Resultaten der Diophantischen Geometrie überhaupt. Im Jahre 1974 ist Baker für seine Arbeiten mit der Fields Medaille ausgezeichnet worden, dem mathematischen Äquivalent des Nobelpreises.

§ 6. Kurven höherer Ordnung.

Wir betrachten jetzt ebene algebraische Kurven höherer Ordnung. Eine solche Kurve wird gegeben durch eine Gleichung der Form

$$f(x, y) = 0$$

wobei $f(x, y)$ ein Polynom höheren Grades bedeutet. Wir nehmen an, daß die Koeffizienten des Polynoms ganze Zahlen sind. Es wird vorausgesetzt, daß die Kurve irreduzibel ist, also nicht in Teilkurven kleinerer Ordnung zerfällt; das bedeutet, daß das Polynom $f(x, y)$ nicht in ein Produkt von Polynomen kleineren Grades zerlegt werden kann.

Wie bereits in § 5 bei den kubischen Kurven bemerkt, spielen die Singularitäten einer Kurve für das Gitterpunktproblem eine besondere Rolle. Eine Singularität ist ein solcher Kurvenpunkt, in welchem die Kurve keine Tangente im üblichen Sinne besitzt, in welchem die Kurve also nicht glatt ist. Zum Beispiel kann eine *einfache*

Spitze vorliegen, vom Typus der Kurve

$$y^2 = x^3$$

im Nullpunkt. Ein *einfacher Doppelpunkt* ist vom Typus der Kurve

$$(x^2 + y^2)^2 = 2(x^2 - y^2),$$

die sich im Nullpunkt einmal überkreuzt. Es gibt auch kompliziertere Singularitäten, zum Beispiel der dreifache Punkt der Kurve

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

im Nullpunkt.

Unsere gegebene Kurve besitzt jedenfalls nur endlich viele Singularitäten. Wir zählen diese durch den sogenannten *Singularitätsgrad* d. Genau genommen ist jedoch d nicht die Anzahl der Singularitäten, sondern es wird dabei jede Singularität mit einer gewissen Vielfachheit gezählt, die um so größer ist, je komplizierter die geometrische Struktur der Singularität ist. Eine einfache Spitze wird dabei mit der Vielfachheit 1 gezählt; ebenso ein einfacher Doppelpunkt. Eine Singularität vom Typus des obengenannten dreifachen Punktes muß mit der Vielfachheit 3 gezählt werden. Wir können und wollen hier nicht auf die etwas komplizierte Vorschrift zur Zählung der Vielfachheiten der Singularitäten eingehen; wir erwähnen lediglich, daß es sich um ein rein geometrisches Problem handelt, das nichts mit Gitterpunkten zu tun hat. Übrigens sind im Singularitätsgrad d auch die im Unendlichen liegenden und auch die komplexen Singularitäten der Kurve mitzuzählen.

Ein Satz aus der algebraischen Geometrie besagt, daß

$$d \leq \frac{(n-1)(n-2)}{2},$$

wobei n die Ordnung der vorgelegten irreduziblen Kurve $f(x, y) = 0$ bezeichnet. Insbesondere wird durch diese Ungleichung in Evidenz gesetzt, daß die Kurve nur endlich viele Singularitäten besitzt, wie bereits oben gesagt. Die Differenz

$$g = \frac{(n-1)(n-2)}{2} - d$$

heißt das *Geschlecht* der Kurve. Nach Definition ist das Geschlecht eine gewisse ganze Zahl ≥ 0. Für eine Gerade ist $g = 0$, ebenso für eine Kurve 2. Ordnung, z. B. Kreis oder Hyperbel. Für eine Kurve dritter Ordnung ist $g = 0$ oder $g = 1$, je nachdem ob die Kurve eine Singularität besitzt oder nicht.

Das Geschlecht g ist eine wichtige geometrische Invariante der Kurve. Und zwar ist sie von *birationalem Charakter;* das bedeutet, daß sich das Geschlecht nicht ändert, wenn man die Kurve einer birationalen Koordinatentransformation unterwirft, d. h. einer Koordinatentransformation, bei denen die Transformationsformeln durch rationale Funktionen gegeben werden. Die Bedeutung der Geschlechtszahl für die Geometrie der Kurven höherer Ordnung wurde erst im vergangenen Jahrhundert richtig erkannt, im Zuge der Entwicklung der algebraischen Geometrie. Damals handelte es sich jedoch bei den diesbezüglichen Untersuchungen um die gewöhnliche Geometrie; um so erstaunlicher ist es, daß nunmehr das Geschlecht auch in der Diophantischen

Geometrie eine Rolle spielt. Der *Siegelsche Endlichkeitssatz*, der in § 5 für kubische Kurven formuliert war, gilt nämlich auch für Kurven höherer Ordnung in der folgenden Form: *Jede Kurve vom Geschlecht* $g > 0$ *besitzt höchstens endlich viele Gitterpunkte*. Die Kurve windet sich also dergestalt durch das Zahlengitter, daß sie nur endlich viele Gitterpunkte trifft. Angesichts der Vielfalt der geometrischen Gestalten algebraischer Kurven ist dies in der Tat eine bemerkenswerte Entdeckung. Es handelt sich um einen der *Fundamentalsätze der ebenen Diophantischen Geometrie*.

In § 3 hatten wir bei gewissen Hyperbeln $x^2 - dy^2 = 1$ festgestellt, daß sie durch unendlich viele Gitterpunkte gehen. In § 4 ergab sich dasselbe für gewisse Geraden $ax + by = c$, und in § 5 für die singuläre Kubik $y^2 = x^3$. Im Hinblick auf den allgemeinen Endlichkeitssatz sehen wir nun, daß es sich bei den erwähnten Beispielen um *Ausnahmekurven* handelt, die in der Mannigfaltigkeit aller Kurven relativ selten vorkommen. Übrigens sind diese Beispiele in einem gewissen Sinne bereits als typisch für den Ausnahmefall anzusehen. Man kann nämlich zeigen: Jede algebraische Kurve, auf der es unendlich viele Gitterpunkte gibt, die also das Geschlecht 0 besitzt, ist *birational äquivalent zu einer Geraden.*

Durch den Siegelschen Endlichkeitssatz sind die Fundamentalprobleme (1), (2), (3) aus § 1 nicht vollständig gelöst. Was noch benötigt wird, ist ein *Algorithmus*, der zu entscheiden gestattet, ob es überhaupt einen Gitterpunkt auf der Kurve gibt, und mit dem dann auch alle vorhandenen Gitterpunkte berechnet werden können. Im Prinzip würde dazu ein Analogon zu der Bakerschen Abschätzung in § 5 ausreichen, wenn das allerdings wie gesagt auch nicht viel für die explizite rechnerische Durchführung bringen würde.

Bisher hat man für die Gitterpunkte auf Kurven vom Geschlecht $g > 1$ jedoch keine allgemeingültige Abschätzung vom Bakerschen Typus finden können. Nur für spezielle Klassen von Kurven ist das gelungen, z. B. für die hyperelliptischen Kurven:

$$y^2 = g(x),$$

$g(x)$ ein Polynom mindestens 3. Grades ohne mehrfache Nullstellen, sowie für die Thueschen Kurven:

$$h(x, y) = c,$$

$h(x, y)$ ein homogenes Polynom ohne mehrfache Faktoren, vom Grad ≥ 3. Der allgemeine Fall steht, wie gesagt, noch aus. Man zweifelt heute nicht mehr daran, daß das Problem lösbar ist, d. h. daß es effektive Schranken für die Gitterpunkte auf beliebigen Kurven vom Geschlecht > 0 gibt. Das Problem dürfte zu den interessantesten und schwierigsten der heutigen Mathematik gehören.

Abraham Robinson hat gezeigt, daß es wenigstens *relativ effektive* Schranken gibt, relativ zu dem bekannten Satz von Roth über die Approximation algebraischer Zahlen durch rationale Zahlen. Mit anderen Worten: könnte man eines Tages den Approximationssatz von Roth durch Angabe von effektiven Schranken ergänzen, so hätte man damit auch einen Weg zur Auffindung von effektiven Schranken für die Gitterpunkte auf Kurven. Mit denselben Methoden wie Robinson konnte der Berichterstatter nachweisen, daß es wenigstens für die *Anzahl* der Gitterpunkte auf einer Kurve eine effektive Abschätzung gibt.

§ 7. Rationale Punkte.

Halbiert man die Längeneinheit, so entsteht aus dem ganzzahligen Punktgitter das Gitter der halbzahligen Punkte. Statt zu halbieren können wir auch durch eine beliebige natürliche Zahl s teilen; die Koordinaten der Punkte des entstehenden Gitters sind rationale Zahlen, deren Nenner in s aufgeht. Wir sprechen kurz von dem $\frac{1}{s}$-zahligen Gitter. Alle Ergebnisse aus den früheren Abschnitten, die für das ganzzahlige Gitter formuliert waren, übertragen sich entsprechend auch auf das $\frac{1}{s}$-zahlige Gitter. Denn dieses entsteht ja durch eine einfache Koordinatentransformation (nämlich durch Division mit s) aus dem ganzzahligen Punktgitter. Insbesondere folgt: *Eine algebraische Kurve vom Geschlecht $g > 0$ trifft das $\frac{1}{s}$-zahlige Gitter nur endlich oft.*

Anders wird die Situation, wenn man alle diese $\frac{1}{s}$-zahligen Gitter gleichzeitig betrachtet, für $s = 2, 3, 4, 5, \ldots$ Die Vereinigungsmenge dieser Gitter ist selbst kein Punktgitter mehr, sondern sie liegt *dicht* in der Euklidischen Ebene. Es handelt sich um die Menge aller Punkte $P = (x, y)$, deren Koordinaten x, y rationale Zahlen sind. Wir sprechen kurz von *rationalen* Punkten. Die Grundprobleme (1)–(3) aus § 1 sind jetzt dahingehend abzuändern, daß nicht nur ganzzahlige Punkte sondern auch beliebige rationale Punkte zugelassen werden. (Übrigens entspricht das genau dem Standpunkt von Diophant selbst, der ebenfalls auch rationale Lösungen Diophantischer Gleichungen betrachtete.) Insbesondere fragen wir: Gibt es algebraische Kurven vom Geschlecht $g > 0$, die unendlich viele rationale Punkte enthalten?

Für das Geschlecht $g = 1$ war eine solche Kurve schon Fermat bekannt, nämlich

.

$$y^2 = x^3 - 2.$$

Man sieht zunächst sofort, daß der Punkt $x = 3$, $y = 5$ auf der Kurve liegt. Und zwar kann man zeigen, daß dies der einzige ganzzahlige Punkt auf der Kurve ist. Fermat fand jedoch einen zweiten rationalen Punkt, nämlich $x = \frac{129}{100}$, $y = \frac{-383}{1000}$, und weiter noch einen dritten: $x = \frac{164323}{29241}$, $y = \frac{66234835}{5000211}$. Allgemein gab Fermat ein Verfahren an, um aus gegebenen rationalen Kurvenpunkten neue zu berechnen; dieses Verfahren liefert, ausgehend von $P = (3, 5)$, unendlich viele weitere rationale Kurvenpunkte.

Bei dem in Rede stehenden Verfahren handelt es sich um das Additionstheorem der kubischen Kurven. Durch zwei rationale Kurvenpunkte P, Q ziehen wir eine Gerade; diese schneidet die kubische Kurve $y^2 = x^3 - 2$ in einem weiteren Punkt R', der ebenfalls rational ist. Spiegeln wir nun R' an der x-Achse, so erhalten wir einen rationalen Punkt R. Diese geometrische Konstruktion, welche von P und Q zu R führt, wird üblicherweise als Addition bezeichnet: $R = P + Q$. Es stellt sich heraus, daß man dadurch eine *Gruppenoperation* für die rationalen Punkte der Kurve $y^2 = x^3 - 2$ erhält; dabei muß allerdings auch der unendlich ferne Wendepunkt dieser Kurve als rationaler Punkt gezählt werden, er ist nämlich das neutrale Element dieser Gruppenoperation.

Ausgehend von dem Punkt $P = (3, 5)$ kann man also die Punkte $2P$, $3P$, $4P, \ldots$ bilden und es zeigt sich, daß diese alle verschieden sind. Für die Punkte $2P$ und $3P$ sind die Koordinaten oben explizit angegeben. Die Rekursionsformel zur Berechnung der Punkte $nP = (x_n, y_n)$ lautet etwa für die 1. Koordinate wie folgt:

$$x_{n+1} = -(x_n + x_1) + (\frac{y_n - y_1)}{x_n - x_1})^2 \quad (n \geq 2)$$

wobei $x_1 = 3$, $y_1 = 5$. Man nennt diese Formel das *Additionstheorem* der kubischen Kurve.

Entsprechend findet man ein Additionstheorem und demgemäß eine Gruppenstruktur für die rationalen Punkte einer beliebigen irreduziblen, glatten kubischen Kurve. (Die Koeffizienten der Kurvengleichung werden wie bisher stets als ganze Zahlen angenommen.) Mordell hat 1921 gezeigt, daß diese Gruppe stets *endlich viele Grundpunkte* $P_1, \ldots, P_r$ besitzt, aus denen man alle anderen durch fortgesetzte Addition und Subtraktion erhält. Die Situation ist also ähnlich wie bei dem Grundpunkt der in § 3 behandelten Hyperbeln, wo die Gruppenoperation als Multiplikation geschrieben wurde; nur handelt es sich jetzt um die *rationalen Punkte*, während es sich in § 3 um ganzzahlige Punkte gehandelt hat. Die ganzzahligen Punkte auf einer kubischen Kurve bilden keineswegs eine Gruppe, denn bei Addition treten im allgemeinen Nenner auf. Das zeigt bereits das obige Beispiel, in dem wir ausgehend von dem ganzzahligen Punkt $P = (3, 5)$ durch Addition schon nach wenigen Schritten ziemlich große Nenner erhielten.

Bis heute kennt man keinen Algorithmus, der es gestattet, die Grundpunkte einer kubischen Kurve explizit zu berechnen. Nicht einmal der Rang der Kurve (d. h. die maximale Anzahl linear unabhängiger unter den Grundpunkten) läßt sich algorithmisch berechnen. Zwar sind Einzelberechnungen an numerischen Beispielen durchgeführt worden, jedoch erweisen sich diese Rechnungen in der Regel als schwierig und ein allgemeines Gesetz ist bis heute nicht gefunden worden, obwohl Swinnerton-Dyer schon seit längerer Zeit Vermutungen in dieser Richtung aufgestellt und durch Computer nachgeprüft hat. Man weiß nach Néron, daß es kubische Kurven beliebig großen Ranges gibt, jedoch sind explizite Beispiele für Kurven großen Ranges schwer zu erhalten. Kürzlich haben Grunewald und Zimmert folgendes Beispiel für eine kubische Kurve vom Rang $\geq = 8$ angegeben:

$$\begin{aligned} y^2 &= x^3 + ax^2 + bx + c, \\ a &= -3^2 \cdot 1487 \cdot 1873 \\ b &= 2^5 \cdot 3^2 \cdot 5 \cdot 151 \cdot 14551 \cdot 33353 \\ c &= 2^8 \cdot 3^4 \cdot 5^2 \cdot 7 \cdot 15l^2 \cdot 193 \cdot 277 \cdot 156307. \end{aligned}$$

Wir haben es dabei vorgezogen, die Koeffizienten nicht in Dezimalschreibweise anzugeben, sondern in ihrer Spektralzerlegung, so wie es dem Diophantischen Problem angemessen ist.

Die kubischen Kurven spielen für das Problem der rationalen Punkte in ähnlicher Weise eine Sonderrolle wie die Hyperbeln sie für das Problem der ganzzahligen Gitterpunkte spielen. Das liegt daran, daß sich in jedem dieser Fälle eine dem Problem angepaßte *Gruppenstruktur* für die ganzzahligen bzw. rationalen Punkte nachweisen läßt. Für Kurven vom Geschlecht $g > 1$ gibt es keine solche, geometrisch konstruierbare Gruppenstruktur mehr. Es ist daher zu erwarten, daß sich Kurven vom Geschlecht $g > 1$ auch im Hinblick auf das Problem der rationalen Punkte anders verhalten als die kubischen Kurven vom Geschlecht $g = 1$. Seit vielen Jahren gibt es in dieser Richtung die folgende *Vermutung von Mordell: Eine algebraische Kurve vom Geschlecht* $g > 1$ *trifft höchstens endlich viele rationale Punkte.* Obwohl also die rationalen Punkte in der Ebene dicht liegen, windet sich die Kurve vermutlich dergestalt durch sie hindurch, daß sie nur endlich viele rationale Punkte trifft.

Bisher konnte die Mordellsche Vermutung nicht allgemein bewiesen werden.

Würde sie sich als richtig erweisen, so hätte das Konsequenzen zum Beispiel auch für die bekannte Vermutung von Fermat. Die Vermutung von Fermat besagt, daß es für $n > 2$ keine ganzen Zahlen a, b, c gibt mit $a^n + b^n = c^n$, außer den trivialen Lösungen, für welche $a = 0$ oder $b = 0$ ist. Setzt man $x = \frac{a}{c}$, $y = \frac{b}{c}$, so bedeutet das, daß es vermutlich keine rationalen Punkte auf der Kurve $x^n + y^n = 1$ gibt, außer den trivialen Punkten auf den Koordinatenachsen (für welche $x = 0$ oder $y = 0$). Bekanntlich ist die Fermatsche Vermutung bisher noch nicht bewiesen; lediglich für kleine Exponenten n ist sie verifiziert, nämlich für $n < 125000$ (Wagstaff 1978). Würde sich die Mordellsche Vermutung als richtig erweisen, so wäre wenigstens für alle $n > 3$ gezeigt, daß es nur endlich viele teilerfremde Lösungen von $a^n + b^n = c^n$ gibt, was in der Tat einen Fortschritt in Richtung auf die Fermatsche Vermutung bedeuten würde. Man beachte dazu, daß die Fermatsche Kurve $x^n + y^n = 1$ das Geschlecht $g = \frac{(n-1)(n-2)}{2}$besitzt, also $g > 1$ für $n > 3$.

Bisher konnte die Vermutung von Mordell nur für gewisse Teilklassen von Kurven bestätigt werden (noch nicht für die Fermatschen Kurven). Unabhängig von der speziellen Gestalt der Kurven sind lediglich die folgenden beiden Resultate in Richtung der Mordellschen Vermutung bekannt.

In diesen Untersuchungen wird angenommen, daß es entgegen der Mordellschen Vermutung doch unendlich viele rationale Punkte

$$P_n = (x_n, y_n) \qquad n = 1, 2, 3, \ldots$$

auf der zu untersuchenden Kurve vom Geschlecht > 1 gibt. Es wird dann gezeigt, daß diese Punkte relativ selten sind, also schnell wachsen, wobei das „Wachstum“ jeweils in einem bestimmten Sinne gemessen wird. Nämlich wie folgt:

(i) Der Satz von Mahler. Es sei q_n der größte Primteiler, der im Spektrum des Nenners von x_n oder y_n vorkommt. Dann gilt

$$q_n \to \infty.$$

(ii) Der Satz von Mumford. Es sei H_n das Maximum der Beträge der Zähler und Nenner von x_n und y_n. Man nennt H_n die *Höhe* von P_n. Wir denken uns die Punkte nach wachsender Höhe durchgezählt, also $H_1 \leq H_2 \leq H_3 = \ldots$ Dann gilt: ,

$$H_n \geq a \cdot e^{bn}$$

mit gewissen Konstanten $a, b \neq 0$. Die Höhen wachsen demnach exponentiell an.

§ 8. Höhere Dimension.

Alle bisherigen Bemerkungen beziehen sich auf die Diophantische Geometrie der Ebene. Die Problemstellungen (1)–(3) in § 1 lassen sich jedoch auch für den Raum oder allgemeiner für den r-dimensionalen Raum, $r \geq 2$ formulieren. Dabei hat man statt Kurven beliebige algebraische Mannigfaltigkeiten zu betrachten, die sich durch Gleichungen mit ganzzahligen Koeffizienten definieren lassen, und es entsteht die Frage nach Gitterpunkten auf diesen Mannigfaltigkeiten, bzw. nach rationalen Punkten.

Diese Frage ist im Raum oder in höheren Dimensionen ungleich schwerer zu behandeln als in der Ebene. Es gibt zwar eine Vielzahl von Einzeluntersuchungen über Mannigfaltigkeiten von speziellem Typus, z. B. über Quadriken, jedoch gibt es

kaum Resultate von ähnlich allgemeiner Bedeutung wie die oben diskutierten Sätze von Siegel, Mahler und Baker in der Ebene. Wahrscheinlich herrschen in höherer Dimension tatsächlich andere Verhältnisse als in der Ebene, und es treten Phänomene auf, die man in der Ebene noch nicht sieht. Ich will hier zwei Sätze erwähnen, die in diese Richtung weisen.

Der erste Satz stammt von Birch und betrifft Hyperflächen in Räumen von sehr großer Dimension. Eine Hyperfläche im r-dimensionalen Raum wird gegeben durch eine Gleichung der Form

$$f(x_1, \ldots, x_r) = 0,$$

wobei f ein Polynom in r Unbestimmten bedeutet. Wir setzen voraus, daß die Koeffizienten von f ganze Zahlen sind. Ferner werde angenommen, daß es sich um ein homogenes Polynom handelt. Die Hyperfläche $f = 0$ stellt dann einen Kegel mit der Spitze im Nullpunkt dar. Insbesondere gibt es stets einen Gitterpunkt auf der Fläche, nämlich den Nullpunkt. Gibt es noch weitere, nichttriviale Gitterpunkte auf der Hyperfläche? Der Satz von Birch besagt, daß das der Fall ist, *vorausgesetzt daß die Dimension r hinreichend groß ist im Vergleich zum Grad n des Polynoms.* Ferner muß selbstverständlich vorausgesetzt werden, daß die Gleichung $f = 0$ wenigstens irgendwelche reellen nichttrivialen Lösungen besitzt, d. h. daß die Hyperfläche nicht nur aus dem Nullpunkt besteht, weil sonst schon die Quadrik $x_1^2 + \ldots + x_r^2 = 0$ vom Grad 2 ein Gegenbeispiel wäre.

Wenn die Hyperfläche singularitätenfrei ist, so läßt sich genauer spezifizieren, was im Satz von Birch unter „hinreichend groß“ zu verstehen ist; es bedeutet

$$r > (n-1) \cdot 2^n.$$

Für Quadriken ist $n = 2$ und daher besagt dies, daß $r > 4$; das ist ein klassisches Ergebnis von Hasse. Für Quadriken weiß man auch, daß diese Ungleichung scharf ist, denn es gibt Quadriken im 4-dimensionalen Raum ohne nichttriviale Gitterpunkte. Bei Hyperflächen großen Grades n wird vermutet, daß die angegebene, exponentiell wachsende Schranke $(n-1)2^n$ zu groß ist; vielleicht gibt es eine polynomial wachsende Schranke. Doch ist darüber bisher nichts Genaueres bekannt.

Das zweite Resultat, das wir besprechen wollen, betrifft die Frage der algorithmischen Entscheidbarkeit der Diophantischen Geometrie. Im ebenen Fall sind wir auf diese Frage in den vorangegangenen Abschnitten des öfteren eingegangen. Im allgemeinen Falle stammt die Frage von Hilbert; sie kommt als 10. Problem unter den berühmten Hilbertschen Problemen aus dem Jahre 1900 vor. Die Formulierung von Hilbert lautet:

> „Eine Diophantische Gleichung mit irgendwelchen Unbekannten und mit ganzen rationalen Zahlenkoeffizienten sei vorgelegt. Man soll ein Verfahren angeben, nach welchem sich mittels einer endlichen Anzahl von Operationen entscheiden läßt, ob die Gleichung in ganzen rationalen Zahlen lösbar ist.“

Gefragt wird also nach einem Entscheidungskriterium für die Existenz von Gitterpunkten auf einer Hyperfläche. Hilbert präzisiert nicht genauer, was er unter einem „Verfahren“ verstanden wissen will. Er setzt offenbar voraus, daß es ein solches „Verfahren“, also einen effektiven Algorithmus in endlich vielen Schritten gibt, und verlangt, daß dieses „Verfahren“ gesucht und gefunden werden möge. Inzwischen haben

die Logiker im Rahmen der Rekursionstheorie genau definieren können, was man unter einem „Verfahren“ im Sinne von Hilbert sinnvollerweise zu verstehen hat. Im Jahre 1970 hat dann Matijacevic, aufbauend auf Arbeiten von Julia Robinson, nachweisen können, *daß das Hilbertsche 10. Problem unlösbar ist.* Mit anderen Worten: es gibt kein effektives Verfahren, das für eine beliebige Diophantische Gleichung die Lösbarkeit oder Unlösbarkeit in ganzen Zahlen zu entscheiden gestattet.

Das war für die mathematische Fachwelt sehr überraschend und wohl auch von Hilbert selbst nicht vorhergesehen.

Der Satz von Matijacevic bezieht sich ausdrücklich auf beliebige Diophantische Gleichungen mit mehreren Unbekannten. Beschränkt man sich auf den ebenen Fall, d. h. also auf Diophantische Gleichungen mit zwei Unbekannten, so ist es durchaus möglich, daß in diesem speziellen Falle doch ein Entscheidungsverfahren im Hilbertschen Sinne existiert. In der Tat zeigt das in § 4 zitierte Resultat von Baker, daß jedenfalls für kubische Kurven solch ein Entscheidungsverfahren existiert, und auch noch für eine Reihe von Kurven höheren Geschlechts. Man ist heute der Meinung, daß wenigstens im ebenen Fall das Hilbertsche Problem lösbar ist; wenn sich das als richtig erweist, so wäre das in der Tat eine bemerkenswerte Besonderheit des ebenen gegenüber dem höherdimensionalen Falle, und zwar eine prinzipielle Besonderheit, die nicht nur in dem Unterschied des Schwierigkeitsgrades der zu behandelnden Probleme begründet liegt.

Für sich allein genommen ist das Ergebnis von Matijacevic negativer Art; es zeigt uns die prinzipiellen Grenzen mathematischer Erkenntnis. Andererseits führen die Methoden und Begriffsbildungen, die dem Beweis von Julia Robinson und Matijacevic zugrundeliegen, ihrerseits zu interessanten und unvorhergesehenen Entwicklungen. Ein Bericht hierüber würde aber den Rahmen dieses Vortrages sprengen.